ASSESSING THE USE OF ELECTRONIC DATA RECOVERY IN E-PROCUREMENT FRAUD INVESTIGATION

by

ALUWANI RUFAROH THEMELI

submitted in accordance with the requirements for
the degree of

DOCTOR OF PHILOSOPHY

in the subject

CRIMINAL JUSTICE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF J.G VAN GRAAN

APRIL 2022

DECLARATION

Name:	Aluwani Rufaroh Themeli
Student number:	34165177
Degree:	Doctor of Philosophy in Criminal Justice
Title:	"Assessing the use of electronic data recovery in e-Procurement fraud investigation"

I declare that the above thesis is my own work and that all the sources that I have used or quoted have been indicated and acknowledged using complete references.

I further declare that I submitted the thesis to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

19 April 2022

Aluwani Rufaroh Themeli

Date

DEDICATION

This thesis is dedicated to:

My late father
Ntshengedzeni Themeli
20 April 1957 – February 1979

and

My late grandmother
Alilali Nthatheni Takalani Themeli
04 June 1925 – 23 October 2014

My guardian angels, I will not forget you, I will not dishonour you, I will not forsake you, I will remember and be glad that you raised me, taught me and that you loved me, always.

Ndaa

ACKNOWLEDGEMENTS

There were many people who have contributed immensely to the successful completion of this thesis. I would like to take this opportunity to convey my sincere and heartfelt gratitude to the following people:

- My Heavenly Father, Almighty God, for all the blessings and energy. His glory and gravitas will triumph over all of creation for eternity.

- My supervisor, Prof J.G van Graan for his continuous encouragement, guidance and persistent support throughout my studies.

- Mr. Dirang Modimakwane (Divisional Head: Forensic Services (FS) of the Group Audit and Risk Department (GAR) at the City of Tshwane (CoT)) for granting me approval to conduct the research with the CoT.

- All my colleagues and friends for their constant support. I had amazing friends, all unique in their own way for their pivotal roles in my expedition to complete this enormous task.

- A special “thank you” to my family, especially my wife Phathu and my children Zeldah, Jermaine and Charmaine, for their patient love, support and understanding during demanding times.

ABSTRACT

This study explores the significance of utilising electronic data recovery applications in e-Procurement fraud investigations. Data was collected by conducting in-depth interviews with forensic investigators, senior forensic investigators, senior forensic audit specialists and managers at the Group Audit and Risk (GAR) department of the City of Tshwane (CoT). The in-depth interviews provide a comprehensive understanding of participants' experiences relating to the utilisation of electronic data recovery applications in e-Procurement fraud investigations conducted by the GAR. Moreover, a review of international best practices provided an enhanced understanding of the investigation of e-Procurement fraud.

The research findings indicate shortcomings in the GAR's effectiveness in utilising electronic data recovery applications in e-Procurement fraud investigations, which limits its impact on the investigation. Based on these findings, a theoretical framework that outlines best practices of electronic data recovery in e-Procurement fraud investigations in the form of progressive stages is proposed, thus contributing to the current body of knowledge.

KEYWORDS

e-Procurement; electronic data; data recovery; computer forensics; procurement fraud; forensic toolkit; digital forensics; data acquisition; data preservation; data analysis

KAKARETŠO

Nyakišišo ye e nyakišiša bohlokwa bja go šomiša didirišwa tša tsošološo ya datha ya ilektroniki ka dinyakišišong tša bofora bja i-phorokhuwamente. Datha e kgobokeditšwe ka go swara dipoledišano tše di tseneletšego le dioditha tša forensiki, ditsebi tše kgolo tša odithi ya forensiki le balaodi ka Lefapheng la Kotsi le Odithi ya Mokgatlo (GAR) la Toropokgolo ya Tshwane (CoT). Dipoledišano tše di tseneletšego di fa kwešišo ye e feletšego ya maitemogelo a bakgathatema a go amana le tšhomišo ya didirišwa tša tsošološo ya datha ya ilektroniki ka dinyakišišong tša bofora bja i-phorokhuwamente tša go dirwa ke GAR. Gape, tshekatsheko ya mekgwa ye mekaone ya boditšhabatšhaba e fa kwešišo ye e oketšegilego ya nyakišišo ya bofora bja i-phorokhuwamente.

Dikutullo tša nyakišišo di laetša ditlhaelelo mo go šomeng gabotse ga GAR tšhomišong ya didirišwa tša tsošološo ya datha ya ilektroniki ka dinyakišišong tša bofora bja i-phorokhuwamente, tšeo di fokotšago khuetšo ya yona go nyakišišo ya bofora bja i-phorokhuwamente. Go ya ka dikutullo tše, foreimiweke ya teori yeo e hlalošago bokaone mekgwa ya tsošološo ya datha ya ilektroniki ka dinyakišišong tša bofora bja i-phorokhuwamente ka sebopego sa dikgato tša kgatelopele e a šišinywa, bjalo e ba le seabe ka gare ga sehlopha sa bjale sa tshedimošo.

MANTŠU A BOHLOKWA

i-phorokhuwamente; datha ya ilektroniki; tsošološo ya datha; diforensiki tša khomphutha; bofora bja phorokhuwamente; ditlabakelo tša forensiki; diforensiki tša ditšitale; go hwetša datha; tšhireletšo ya datha; tshekatsheko ya datha

OKUCASHUNIWE

Lolu cwaningo luhlola ukubaluleka kokusebenzisa izinhlelo zokusebenza zokuthola imininingwane yethuluzi elisetshenziswa ukwenza umsebenzi ophenyweni lokukhwabanisa lokuthengwa nokudayiswa kwezinsiza, okokusebenza, imisebenzi, nezinsizakalo ngewebhusayithi. Imininingwane iqoqwe ngokwenza izingxoxo ezijulile nabacwaningi mabhuku abahlola uphenyo, ongoti abakhulu babacwaningi mabhuku abahlola uphenyo kanye nabaphathi eMnyangweni Wokucwaninga Amabhuku Nezingozi (GAR) yeDolobha laseTshwane (CoT). Izingxoxo ezijulile zinikeza ukuqonda okuphelele kokuhlangenwe nakho kwabahlanganyeli okuhlobene nokusetshenziswa kwezicelo zokutholwa kwemininingwane yethuluzi elisetshenziswa ukwenza umsebenzi ophenyweni lokukhwabanisa lokuthengwa nokudayiswa kwezinsiza, okokusebenza, imisebenzi, nezinsizakalo ngewebhusayithi olwenziwa yi-GAR. Ngaphezu kwalokho, ukubuyekezwa kwezinqubo ezihamba phambili zamazwe ngamazwe kunikeza ukuqonda okuthuthukisiwe kophenyo lokukhwabanisa lokuthengwa nokudayiswa kwezinsiza, okokusebenza, imisebenzi, nezinsizakalo ngewebhusayithi.

Okutholwe wucwaningo kubonisa ukushiyeka ekusebenzeni kahle kwe-GAR ekusebenziseni izicelo zokutholwa ophenyweni lokukhwabanisa lokuthengwa nokudayiswa kwezinsiza, okokusebenza, imisebenzi, nezinsizakalo ngewebhusayithi, okukhawulela umthelela wayo ophenyweni lokukhwabanisa lokuthengwa nokudayiswa kwezinsiza, okokusebenza, imisebenzi, nezinsizakalo ngewebhusayithi. Ngokusekelwe kulokhu okutholiwe, kuhlongozwa uhlaka lombono oluveza izindlela ezingcono kakhulu zokuthola imininingwane yethuluzi elisetshenziswa ukwenza umsebenzi ophenyweni lokukhwabanisa lokuthengwa nokudayiswa kwezinsiza, okokusebenza, imisebenzi, nezinsizakalo ngewebhusayithi ngendlela yezigaba eziqhubekayo, ngaleyo ndlela kube nesandla endikimbeni yamanje yolwazi.

AMAGAMA ASEMQOKA

Okuthengwa nokudayiswa kwezinsiza, imininingwane yethuluzi elisetshenziswa ukwenza umsebenzi, ukutholwa kwemininingwane, ukusetshenziswa kwekhompyutha ezindleleni zesayensi ophenyweni lobugebengu, ukukhwabanisa kokuthengwa nokudayiswa kwezinsiza, iqoqo lamathuluzi asetshenziswa yizindlela

zesayensi ophenyweni lobugebengu, inqubo yokwembula nokuhumusha imininingwane yethuluzi elisetshenziswa ukwenza umsebenzi, ukuthola imininingwane, ukulondoloza imininingwane, ukuhlaziya imininingwane

LIST OF ABBREVIATIONS

ACFE	-	Association of Certified Fraud Examiners
AGSA	-	Auditor General South Africa
APC	-	Audit Performance Committee
B2B	-	Business to Business
B2C	-	Business to Customer
B2E	-	Business to Employee
BAC	-	Bid Adjudication Committee
BBBEE	-	Broad-based Black Economic Empowerment
BEC	-	Bid Evaluation Committee
BEE	-	Black Economic Empowerment
BSC	-	Bid Specification Committee
BTech	-	Baccalaureus Techonologiae
CAATs	-	Computer Assisted Audit Techniques
CoT	-	City of Tshwane
CPU	-	Central Processing Unit
EC-Council	-	International Council of Electronic Commerce Consultants
EDI	-	Electronic Data Interchange
EDR	-	Event Data Recorders
e-MRO	-	Electronic Maintenance Repair and Operation
ERP	-	Enterprise Resource Planning
e-sourcing	-	Electronic Sourcing
e-tendering	-	Electronic Tendering
EU	-	European Union
FI	-	Forensic Investigator

FS	-	Forensic Services
FTK	-	Forensic Toolkit
HPA	-	Host-Protected Area
HR	-	Human Resource
GAR	-	Group Audit and Risk Department
GUI	-	Graphical User Interface
GEPNIC	-	Government e-Procurement System of National Informatics Centre
ICEG	-	International Conference on e-Government
ICT	-	Information and Communication Technology
IMEI	-	International Mobile Station Equipment Identity Number
I/O	-	Input/output system
IRMA	-	Information Resources Management Association
ISP	-	Internet Service Provider
IT	-	Information Technology
M	-	Manager
MD5	-	Message Digest Version 5
MFMA	-	Municipal Finance Management Act, Act 56 of 2003
MPAC	-	Municipal Public Account Committee
MTech	-	Magister Technologiae
NTPASS	-	Novell NetWare Password Recovery
PDA	-	Personal Digital Assistant
PFMA	-	Public Finance Management Act, Act 1 of 1999
PO	-	Purchase Order
PPA	-	Public Procurement Authority
PPE	-	Personal Protective Equipment

PPL	-	Public Procurement Law No. 4734
PPPFA	-	Preferential Procurement Policy Framework Act
PR	-	Purchase Requisition
PRECCA	-	Prevention and Combating of Corrupt Activities Act
PRTK	-	Password Recovery Toolkit
RAM	-	Random Access Memory
RFQ	-	Request for Quotation
SAP	-	Systems Applications and Products
SAPS	-	South African Police Services
SARS	-	South African Revenue Services
SCM	-	Supply Chain Management
SEP	-	Semi-Electronic Procurement system
SFAS	-	Senior Forensic Audit Specialist
SFI	-	Senior Forensic Investigator
SHA	-	Secure Hash Algorithm
SIM	-	Subscriber Identity Module
SIU	-	Special Investigation Unit
SMS	-	Short Message Service
SSD	-	Solid State Drives
TCP/IP	-	Transmission Control Protocol/Internet Protocol
TUKS	-	University of Pretoria
TSI	-	Two-Step Injection method
UIFW	-	Unauthorised, Irregular and Fruitless & Wasteful Expenditure
UK	-	United Kingdom
UNISA	-	University of South Africa

UNIVEN	-	University of Venda
USA	-	United State of America
USB	-	Universal Serial Bus
VAN	-	Value Added Network
VMFS	-	Virtual Machines File System
VOIP	-	Voice Over Internet Protocol
VPN	-	Virtual Private Network
Web-based EDI	-	Web-based Electronic Data Interchange
Web-based ERP	-	Web-based Enterprise Resource Planning

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ANNEXURES

CHAPTER ONE
GENERAL ORIENTATION

1.1 INTRODUCTION

This research focused on City of Tshwane (CoT) as a case study. The CoT has adopted the e-Procurement system to manage its supply chain management (SCM) processes. The e-Procurement system in its entirety is automated on the CoT computer and network system. This degree of automation has opened a host of opportunities for criminal activity particularly procurement fraud and led to an increased vulnerability on these computer and network dependency e-Procurement system. This has also led to an increase in the complexity of computer systems being used to commit computer crimes such as cybercrime. Equally, the same technology (e-Procurement) provides CoT forensic investigators with more sophisticated weapons (electronic data recovery) to use in their fight against procurement fraud and computer crimes in general.

According to Pablos, Lovelle, Gayo and Tennyson (2013:240) e-Procurement is the automated system that allows for purchasing activities online. If properly implemented, e-Procurement has the potential to “connect companies and their business processes directly with suppliers while managing all interactions between them”. E-Procurement builds in an organised set of automated monitoring tools that assist with the control of costs and increased supplier performance, while improving communication throughout the process. Hattingh, Matthee, Smuts, Pappas, Dwivedi and Mäntymäki (2021:47) share the same views with Pablos et al. (2013:240) by emphasising that e-Procurement help to curb corruption and make significant economic impacts.

This study mainly focused the procurement fraud committed against the CoT’s e-Procurement system. Procurement fraud in the CoT is often committed through electronic devices. The compromised data (data that was used during the commission of procurement fraud) often mysteriously disappeared from e-Procurement systems or deliberately deleted (hidden) as most criminals do not want to leave the trail of their proscribed transactions and illicit dealings.

As indicated by Holt, Bossler and Seigfried-Spellar (2018:536), local and international studies have proved that there are modern and recent software technologies to assist forensic investigators to recover electronic data (including hidden and deleted data). For the CoT to investigate procurement fraud, the forensic investigators must be able to recover, analyse and interpret the recovered data successfully and efficiently.

1.2 PROBLEM STATEMENT

Kumar (2019:45) explains that research conducted within humanities deal with people, problems, programmes and phenomena. Dantzker, Hunter and Quinn (2016:14) state that one of the most critical steps is recognising and defining what will be studied before starting a research project. Wentz (2017:2) supports the authors' statement above and opines further that the problem statement drills down from the research topic towards a solution. The idea that you are solving a problem suggests the problem can be solved. Similarly, Hofstee (2006:85) summarises that in the problem statement the researcher needs to answer the following paramount questions with regards to the identified problem:

- What exactly is the problem or phenomenon?
- Why is this a problem?
- What are the factors involved in the problem?
- How to address the problem, and
- Why is the measures put in place not satisfactory, and if any measures are put in place?

Nowadays, most organisations, government departments and municipalities have adopted the e-Procurement system to manage their SCM processes. Similar to other organisations, the CoT has also adopted the e-Procurement system to manage its SCM affairs and processes. According to Tai, Ho and Wu (2010:30), adopting the e-Procurement system when transacting with suppliers empowers organisations to develop efficient internal procurement processes, decrease transaction costs, and increase collaboration with suppliers. Al-Sartawi, Razzaque and Kamal (2021:139) agree with Tai et al. (2010:30) by mentioning that e-Procurement is responsible for enhancing supply chain performance and is considered a vital resource.

In support of the claims made by Tai et al. (2010:30), Piotrowicz and Irani (2010:101) maintains that e-Procurement drivers can reduce product cost, improve visibility of customer demands, and reduce administration cost. Further benefits include improved inventory management and better decision-making. Altogether, this results in a procurement cycle that achieves maximum productivity and performance. Additionally, Thai (2019:447) reiterated the benefits of e-Procurement and its efficiencies. Thai mentioned that e-Procurement is the integrated database system and a Web-based network communications system which controls and manages all purchasing process of the organisation.

The challenges posed by the e-Procurement system as pointed out by Galloway (2003:16), is the security of information in the database and transactions since the e-Procurement is a web-based system and network dependency which requires internet connectivity, data is transmitted between entities and companies. These increased the vulnerability of interception. The system can be hacked, and information can land in the wrong hands. In support of Galloway’s views, Anthony (2018:44) emphasise that that a possible threat in an e-Procurement process is that it can provide the opportunity for collusion.

The challenge for the CoT is that there is a vast amount of money involved in the SCM processes. This has opened a host of opportunities for criminal activities, such as procurement fraud. This escalation in the use of e-Procurement has also led to increasingly complex electronic computer systems being used to commit procurement fraud against the CoT e-Procurement system. After the criminals and/or CoT employees committed procurement fraud (using modern advanced computer software) the electronic data or information disappeared from e-Procurement systems or deliberately deleted in order not to leave a trail of these proscribed transactions and illicit dealings. However, the same advanced electronic computer systems provide forensic investigators with sophisticated techniques (electronic data recovery) to employ in their fight against procurement fraud.

The GAR department of the CoT is responsible for the investigation of procurement fraud within the CoT. The GAR forensic investigators are unable to efficiently investigate e-Procurement fraud committed against the CoT. During 2018/2019 financial years, 29 procurement fraud cases where registered and investigated. The recovery of the electronic data involved (or suspected to have been involved) in the commission of the 29 investigated procurement fraud cases was conducted by external consultant firms.

The above is a proof that CoT forensic investigators lack the investigative capacity and advanced investigative resources (tools) to recover electronic data during the investigation of procurement fraud. This shortcoming affects CoT investigators' ability to efficiently investigate procurement fraud. As a result of the CoT's forensic investigators' lack of investigative capacity and advanced investigative resources, the CoT procured the services of external consultant firms to recover electronic data to assist the GAR to investigate procurement fraud or to conduct the entire procurement fraud investigation. This shortcoming was confirmed in the City of Tshwane Internal Audit Report (2018-2019), which illustrates that all procurement fraud investigations for this period that involved recovery of electronic data were outsourced to external consultant firms.

The preeminent solution to this problem is to build sufficient in-house investigative capacity and to acquire the necessary advanced investigative resources (tools), such as Computer Assisted Audit Techniques (CAATs) software to monitor CoT e-Procurement system and data recovery software. This would enable CoT forensic investigators to recover electronic data, eliminating external consultants, which in turn would be financially viable for the CoT as there will be no need to outsource the cases where data recovery is required to external consultant firms.

1.2.1 Experience in the investigation of procurement fraud

The researcher is a former police officer and has four years of investigation experience in the South African Police Services (SAPS) Organised Crime Unit. Furthermore, the researcher has 10 years' investigative experience in the GAR of the CoT, now he is working as a Senior Forensic Audit Specialist. He was involved in the investigation of several procurement fraud cases. His experience informs and supports his understanding of the circumstances in and procedures which CoT forensic investigators must follow to recover electronic data during the investigation of procurement fraud.

Due to the researcher's first-hand experience as a CoT forensic investigator, preliminary discussions with forensic investigators at the CoT and a preliminary literature review, he affirmed that CoT forensic investigators lack investigative capacity and resources required to recover electronic data to efficiently investigate procurement fraud. There should be serious emphasis focused on research in the field of recovery of electronic data to enhance procurement fraud investigation, together with sufficient training of CoT forensic investigators involved in the field and making available the required resources (tools) and software. This study ought to enlighten the forensic investigators with the significance of electronic data recovery to enhance the investigation of procurement fraud.

The researcher obtained a bachelor's degree in Criminal Justice from the University of Venda (Univen) in 2003, a Baccalaureus Technologiae (BTech) Degree in Forensic Investigation from the University of South Africa (UNISA) in 2012, a certificate in the Prevention and Detection of Procurement and Contract Fraud from the University of Pretoria (TUKS) in 2013, and a Magister Technologiae (MTech) Degree in Forensic Investigation from Unisa in 2017.

1.3 RESEARCH QUESTIONS

Bryman and Bell (2015:10) indicate that a research question addresses an unequivocal announcement of what the researcher needs to know. Research questions define the subjects to be investigated within the study. They will be directly investigated in search of answers, through observation, measurement, and interrogation of the facts to shed light on the topic by the researcher (Denscombe, 2014:31).

The following research questions were both relevant and vital to guiding this research as they provide key themes and clarify the topic and research problem. For the purpose of this study, the researcher identified the following primary research question:

What is the significance of utilising electronic data recovery applications in e-Procurement fraud investigation?

This study furthermore explored the following secondary research questions:

- Could the utilisation of advanced investigative resources enable CoT forensic investigators to recover electronic data to enhance e-Procurement fraud investigations?
- How could the application of advanced investigative resources empower CoT forensic investigators with knowledge to successfully investigate e-Procurement fraud?
- How could the CoT establish sufficient investigative capacity that would enable CoT forensic investigators to recover electronic data and eliminate external service providers in e-Procurement fraud investigations?
- What international best practices exist to recover electronic data in the investigation of e-Procurement fraud?

1.4 AIM AND OBJECTIVES OF THE RESEARCH

According to Mills and Birks (2014:10) research is a “declaration predicting the research outcome and that the aim of the research therefore steers the researcher to the research goal”. In support of Mills and Birks (2014:10), and as pointed out by Denscombe (2014:121) the “aim of research is to arrive at a conclusion about the state of knowledge on a topic based on a thorough overview of the research that has been undertaken”. As revealed by Joyner, Rouse and Glatthorn (2018:68), the research aim must address the following:

- An intention or yearning; what one plan to accomplish;
- Aims are statements of expectation, written in broad terms; and
- Aims set out what one hope to accomplish toward the end of the project.

The aim of this study was to assess the significance of using electronic data recovery in e-Procurement fraud investigation.

This study strives to achieve the following objectives:

- To explore, identify and pronounce the effectiveness of using electronic data recovery in procurement fraud investigation; and
- To make recommendations regarding the electronic data recovery in procurement fraud investigation based on the research findings, which could potentially be used to improve the understanding of electronic data recovery in procurement fraud by CoT forensic investigators.

1.5 KEY THEORETICAL CONCEPTS

1.5.1 E-Procurement

Thai (2019:477) defines e-Procurement as the use of internet based inter-organisational information system, which automates and integrates any part of the procurement process to improve efficiency and quality in public procurement, and to promote transparency and accountability in the wider public sector. Thai further explained that e-Procurement can be viewed as an end-to-end solution that simplifies several procurement processes throughout the organisation through integration and process streamlining.

1.5.2 Procurement Fraud

Coenen (2008:86), defines procurement fraud as “the unlawful manipulation of the process of obtaining a contract for goods or services”. Coenen goes on to explain that the aim of procurement fraud is to gain an advantage in the bidding or proposal process, and “bad acts can range from the unfair use of insider information to the use of nefarious means to influence the process”. According to the Association of Certified Fraud Examiners (ACFE, 2019:1.629) procurement fraud is when an employee influences the selection of a service provider or vendor which he/she has interest or has bribed him/her.

1.5.3 Electronic data

According to Casey (2011:7) electronic data is “any data stored or transmitted using a computer, which supports or refutes a theory of how an offence occurred or that addresses critical elements of the offence such as intent or an alibi”. In support of the views by Casey (2011:7), Reedy (2021:22) defines electronic data as any information that is stored or transmitted in binary form or any location in an increased range of devices and systems.

1.5.4 Electronic data recovery

Kruse and Heiser (2002:2) argue that electronic data recovery “involves the preservation, identification, extraction, documentation and interpretation of computer data”. Computer forensic specialists follow clear, defined methodologies and procedures, but are expected and encouraged to be flexible when encountering anomalies. Electronic data recovery as defined by Wahyudi, Riadi and Prayudi (2018:1) is a sequence of process of identifying, obtaining, analysing and presenting evidence to the court to resolve a criminal case by observing and maintaining the integrity and authenticity of the evidence.

1.5.5 Data analysis

According to Cuesta and Kumar (2016:7), “data analysis is the process in which raw data is ordered and organised to be used in methods that help to evaluate and explain the past and to predict the future.” Rather than being just about numbers, data analysis is about asking questions, developing explanations, and testing hypothesis back up by logical and analytical methods. It is a multidisciplinary field that combines computer science, statistics, artificial intelligence, machine learning and mathematics within the business domain.

1.6 VALUE OF THE RESEARCH

Neuman and Robson (2012:11) view research as being used to advance understanding of the fundamental nature of social life and knowledge, and to apply study results to solve specific, immediate problems or issues. According to Leedy and Ormrod (2015:46), it is very important for the researcher to describe the importance of the study. It is the opinion of Denscombe (2014:43) that “the research must be relevant, in terms of contributing to existing knowledge, solving practical needs and it must be of relevance to current issues.”

The results of this study strive to:

- Improve CoT investigators’ knowledge and competence with regards to the electronic data recovery in e-Procurement fraud investigation;
- Facilitate problem-solving regarding CoT forensic investigator’s inability to efficiently investigate e-Procurement fraud;
- Enhance CoT forensic investigator’s capacity through the facilitation of an improved electronic data recovery applications and modern tools;
- Contribute to the already-existing body of knowledge as an academic source for both students and prospective researchers; and
- Contribute to the broader South African community and computer forensic industry (with specific reference to those forensic investigators responsible for e-Procurement fraud) since e-Procurement fraud progressively remains to increase and have a negative impact on the South African economy.

1.7 DELIMITATION OF THE STUDY

This study was confined and limited to the forensic investigators of the GAR within the CoT who are responsible to investigate e-Procurement fraud. The GAR has 110 internal auditors employed at four sections, namely Forensic Services (FS), Performance Audit, Information Technology (IT) Audit and Risk Enterprise Management (Insurance and Business Continuity). The Forensic Investigation division of the GAR has 45 investigators. This study was limited to forensic investigators whose activities are related to e-Procurement fraud investigation and who are dependent on electronic data recovery to conduct these investigations.

1.8 RESEARCH DESIGN AND APPROACH

Bryman and Bell (2015:48) observe that the research design is a structure for the generation of evidence that is suited both to a specific order of criteria and the research question in which the researcher is interested. In support of Bryman and Bell, Yin (2003:19) suggests that the research design can be seen as a recipe that the researcher needs to follow from starting until the research study is finalised. To elaborate on the notion of Yin (2003:19), Creswell (2014:15) refers to a research design as the method that guides the researcher in the process of collecting, analysing and how to interpret observation. Liamputtong (2013: 271) supports the notion of Creswell (2014:15) in that the research design should be a logical and systematic preparation that guides a piece of research. Flick (2022:112) agrees with both Creswell (2014:15) and Liamputtong (2013:271) and confirms that research designs deal with the issue of how a study should be planned. Flick (2022:146) further maintains that a researcher's personal experience may prime a researcher in deciding to conduct research on a specific topic after a problem is discovered or defined, requiring empirical research.

Based on the writings of Yin (2003:19), Creswell (2014:15), Liamputtong (2013:271) and Flick (2022:146), the researcher conducted empirical research. Mouton (2001:149) emphasise that this type of study involves the researcher "going out into the field and obtaining the personal experience and knowledge of the participants". Maxfield and Babbie (2017:4) argue that "a combination of experience and observation are key contributors of knowledge in empirical research". Maxfield and Babbie (2017:6), furthermore, explain that empirical research can thus be seen as the creation of knowledge based on a combination of experience and observation. Empirical research allows the researcher to garner information from the research participants and has the advantage that it will allows the researcher to probe the responses from the participants in much more detail during interviews.

De Vos, Strydom, Fouché and Delport (2007:269), identify five different sets of investigative designs that can be used in qualitative research, and they are:

- Biography;
- Phenomenology;
- Grounded theory;
- Ethnography; and
- Case study.

The researcher followed the case study design. As pointed out by Flick (2022:146) a case study can be seen as an empirical investigation by a researcher concerned with a real-life phenomenon. In addition, Flick (2022:146) further suggest that case study research will be used by a researcher conducting research in social sciences as well as research pertaining to organisational studies and management studies. Yin (2003:38) distinguishes that a single case study is used to investigate whether suggestions in theory are correct and if another explanation is more relevant to the case.

Hofstee (2006:123) agrees with Yin (2003:13) by highlighting that when a single case is being researched it deals, for example, with an organisation and that the idea of case study research is to test the case which the researcher believes will be the phenomenon posed in the research problem and that the case can be understood and explained and therefore the outcome of the research can be used on other similar cases. Hofstee (2006:123) is also of the belief that the case study method is to be used by a researcher when a certain case requires research, and the researcher requires detailed knowledge to assist in the research. Hofstee further explains that the use of a case study is to explore a phenomenon in depth. Mills and Birks (2014:145) are of the opinion that most qualitative studies are case studies since qualitative research is usually used in cases where an in-depth study of a phenomenon is required.

Furthermore, Welman et al. (2005: 182-184) describe the term ‘case study’ as an in-depth study that will utilise a limited number of units of analysis, and the term case study does not refer to a specific technique that will be utilised. It is the notion of Gray (2014:8) that case studies are widely used for conducting research, and if the planning and preparation of a case study is done correctly by the researcher, the case study can “provide a powerful means of exploring situations”. According to Gray (2014:267) “the case study method is ideal when a “how” or “why” question is being asked about a contemporary set of events over which the researcher has no control”. Yin (2003:9) agrees with Gray (2014: 267) and points to the fact that “case study research has a distinct advantage when the researcher has zero or very limited control over an event of a contemporary nature”.

The case study for this research study included managers, forensic investigator, senior forensic investigators and senior forensic audit specialists who were involved with e-Procurement fraud investigations at the GAR. The researcher gathered data by using in-depth interviews as well as conducting a comprehensive literature study, which relates to a qualitative research approach. Leedy and Ormrod (2015:95) explain that a qualitative approach entails interviews must be conducted with either individuals or focus groups.

According to Creswell (2014:15) qualitative research study participants in their natural environment, going to the field, gather data, then analysing the collected data and arrive at appropriate findings as well as making relevant recommendations. The researcher therefore followed a qualitative research approach and concludes that based on the notions and opinions of the above authors a qualitative approach following a single case study design best suit this research.

1.9 POPULATION AND SAMPLING PROCEDURES

Most empirical studies involve selecting a group from which propositions will be advanced (Flick, 2022:70). Dahlberg and McCraig (2010:173) as well as Kalof, Dan and Dietz (2008:140) agree with Gray and is of the opinion that a study population relates people or organisations that the researcher would like to enquire about the research problem, and then arrive at conclusions pertaining to the identified research problem. According to Kalof et al. (2008:141) an organisation, company or people dealing with the same issues is examples of a population.

The population for this research was the forensic investigators responsible for e-Procurement fraud investigation. The researcher, however, notes that it was not practical to engage with this large of a population, therefore the researcher utilised a target population. The target population regarding this study included managers, forensic investigator, senior forensic investigators, and senior forensic audit specialists of the GAR who were involved with e-Procurement fraud investigations.

The sample of this study included 23 investigators selected from the total of 45 investigators, which comprised of five forensic investigators, 12 senior forensic investigators, three senior forensic audit specialists and three managers at GAR. The researcher made use of a non-probability sample, as this method has the least financial implications to conduct the research as well as the fact that this method uses less time. The researcher agrees with both the submissions of Mathews and Ross (2010:68) as well as Welman et al. (2005:68) stating that the major advantage of using non-probability sampling is that it is not a financial strain, and this method is less complicated to use.

For the purpose of this research, the researcher used purposive sampling as he relied on his own experience and expertise to obtain units of analyses. Gray (2014:217) explains that the qualitative researcher will generally use a small sample that is purposefully chosen. Maxfield and Babbie (2017:235) highlights the fact that using the purposive sampling method is based on a person’s “own knowledge of the population, its elements and the nature of the research aims”. Mathews and Ross (2010:167) explain that in purposive sampling, people are chosen specifically as they are well informed in their specific field thus allowing the researcher to unpack and explore the research questions. Ritchie, Nicholas and Ormston (2014:113) as well as Flick (2022:70) defines purposive sampling as units of a sample chosen for a specific purpose, namely, to achieve the research aims as well as research questions. Gray (2014:217) is of the opinion that purposive sample are used when a certain organisation or group of people since they have specific knowledge that will not be available from another sample.

1.10 DATA COLLECTION

Mouton (2001:98-105) argues that in qualitative research, data collection methods include observation, interviewing of subjects and documentary sources. Flick (2022:104) similarly shares Mouton's view by indicating that there are three primary forms of data collection: one can collect data by asking people (surveys and interviews), observing, or studying documents.

Data collection methods depend on the type and purpose of the research. Since this study followed a qualitative approach, the researcher used a literature review and in-depth interviews as data collection techniques.

1.10.1 Literature review

Mouton (2001:88) and Kumar (2019:32) as well as Welman et al. (2005:34) agree that there are various portals to identify literature that can be utilised during research. The researcher studied the relevant literature to explore best practices in both the local and international arena pertaining to the use of electronic data recovery during the investigation of e-Procurement fraud.

Denscombe (2014:86) supported by Kumar (2019:31) highlights that "the objective of the literature review is to inform the researcher about what is already known" regarding the subject to be investigated. The researcher made use of google scholar, accredited academic journals, relevant books, and newspaper articles to collect data about the use of electronic data recovery during the investigation of e-Procurement fraud.

1.10.2 In-depth interviews

According to Rubin and Rubin (2012:3) when the researcher conducts in-depth qualitative interviewing, he engages with participants who have knowledge or experience with the subject matter. “Through such interviews researchers explore in detail the experiences, motives and views of others” such as Leedy and Ormrod (2015:147-149) and learn how others perceive the subject. In-depth interview method will allow participants to speak freely from their personal experiences and knowledge, in relation to the use of electronic data recovery during the investigation of e-Procurement fraud. Based on the content of the problem statement as well as the research questions and the research aim, the researcher formulate an interview guide that was utilised to obtain data from forensic investigators at GAR.

The researcher obtained written consent from the research participants before proceeding with the interviews. The researcher used a digital voice recorder to record the interviews. The recorded interviews were transcribed for the purpose of data analysis.

The researcher followed guidelines and interview protocol provided by Leedy and Ormrod (2015:147-149), specifically:

- The researcher compiled an interview schedule containing questions specific to the research topic;
- The researcher obtained a venue that was convenient and free from disturbance;
- The interviews were conducted in an appropriate location that ensured that interviewees felt at ease;
- The researcher obtained prior written permission from the CoT municipality to conduct the interviews;

- The researcher focused on questions relating to the research and recorded interviewees answers accurately and truthfully. The researcher did not change or edit what the interviewees said nor falsify their answers; and
- For the purposes of maintaining confidentiality, the researcher anonymised to the interviewees by referring to them as participants.

The researcher also took cognisance of and adhered to UNISA's COVID-19 Position Statement on Research Ethics (UNISA, 2020) which stipulates that a responsible human participant research approach is required in the context of COVID-19. The COVID-19 Position Statement prohibited face-to-face interviews – for the duration of the lockdown period – because they posed an inherent risk to participants and/or researcher. This condition was adhered to in the interest of participants and researchers. The researcher complied with the principles prescribed by UNISA's COVID-19 Position Statement on Research Ethics, as indicated below:

- While conducting research, clear, practical risk mitigation measures were taken to protect the participants, the community, the researcher, and research support staff;
- The researcher assessed the research study's risk-benefit ratio, particularly concerning face-to-face contact and data collection in public spaces or locations where social distancing cannot be practised;
- The right to self-determination was respected and always carefully considered; and
- This approach included the participants' right to withdraw, right to decline to participate, and right to explore alternative participation methods.

1.11 DATA ANALYSIS

De Vos et al. (2007:333) define data analysis as “a process of interpreting and giving order to a large volume of data”. The researcher compared the viewpoints of all respondents; those with similar views were grouped together and those with different views were grouped together. Their responses were then analysed.

The researcher made use of the spiral data analysis, which was applicable to a wide variety of qualitative studies as described by Leedy and Ormrod (2015:161). This spiral procedure “entails using data to form the basis of research study by observing the following steps”:

- Organising raw data – the researcher broke the data into smaller pieces and organised it into a computer database;
- Perusing data – the researcher needed to know contents of the data;
- Data classification and analysis – the researcher grouped the data before conducting his analysis; and
- Synthesising the data – the researcher integrated and summarised the data to present the final report.

1.12 TRUSTWORTHINESS IN QUALITATIVE RESEARCH

According to Guba and Lincoln (as cited in Kumar, 2019:184), trustworthiness is very important in any research and in qualitative research, it is measured by credibility, transferability, dependability, and confirmability. Qualitative approach as pointed out by Gray (2014:186) strives to sustain and build trustworthiness, authenticity, credibility, transferability, dependability, and conformability.

Marshall and Rossman (2014:39), emphasised that “historically, concerns with the trustworthiness of qualitative research drew from the natural and experimental sciences for direction”. Marshall and Rossman (2014:40) furthermore suggest credibility, dependability, confirmability, and transferability as an alternative concept to explain qualitative validity and reliability.

1.12.1 Credibility

In a qualitative study, similarity can be measured by discussing the findings with the participants and if the level of similarity is high, the validity of the study is also high (Kumar, 2019:185). In support of Kumar, Dahlberg and McCraig (2010:34-35) described validity as the accuracy and/or trustworthiness of a version, description or conclusion that is reached by a researcher and that the correct application of the correct techniques pertaining to sampling will enhance research validity. The researcher compared the information obtained during the in-depth interviews with multiple sources in literature to ensure the credibility of this study.

1.12.2 Transferability

Transferability according to Liamputtong (2013:26) can be described as knowledge obtained from theory because of qualitative research that can be applied to similar groups, organisations, or situations dealt with by individuals in similar circumstances. Transferability according to Kumar (2019:185) refers to the degree that qualitative research can be transferred or generalised to other situations or frameworks.

To achieve transferability in this study, the researcher purposively selected the sample of participants and provided detailed narratives to communicate the research findings. Participants' replies to the questions posed during the interviews were illustrated by verbatim quotations. These descriptions shifted readers to the situation as experienced by the researcher during interviews, thus allowing readers to gain a sense of shared experiences. As a result, readers will be able to judge the transferability of the findings.

1.12.3 Dependability

Dependability is achieved using audit trails through the data (Gray 2014:185). Bouma and Ling (2004:84) suggest that "recorded or published materials allow other people to review the exact material" to test reliability. To ensure dependability the researcher:

- Kept digital voice recordings of all interviews as well as transcriptions of these digital voice recordings and a detailed list of references; and
- Kept and documented all records and material evidencing the manner in which data was collected and how the interviews were conducted.

1.12.4 Confirmability

Confirmability as discussed by Kumar (2019:185) refers to the way research results can be confirmed or acknowledged by other researchers, however both researchers must follow the same approach. Liamputtong (2013:26) suggests that all consulted literature utilised by researchers should be accompanied by a comprehensive list of references to corroborate the research findings as well as the researcher's interpretation thereof.

The researcher kept a detailed record of the interviews and subsequent transcripts of the interviews conducted. As a result, the findings and interpretation of those findings can be readily connected to the data provided by the participants. Any biases, motivations, interests, or perspectives of the researcher were thus eliminated, and confirmability was ensured.

1.13 ETHICAL CONSIDERATIONS

According to UNISA's Policy on Research Ethics (University of South Africa, 2016:7), "researchers should respect and protect the dignity, privacy and confidentiality of participants". The researcher will adhere to UNISA's research code of conduct. Bryman and Bell (2015:36) state that it is imperative to bear in mind that researchers bear responsibilities to the people and organisations that are the subjects of their research activities.

The researcher adhered to the following ethical guidelines to during this study:

1.13.1 Protection from harm

When one is collecting information from participants, the researcher needs to investigate carefully whether their involvement is likely to harm them in any way (Kumar 2019:245). Participant names were kept anonymous to protect them from any unnecessary physical or psychological harm. Thus, they were referred to simply as participants. The researcher obtained the necessary permission prior to conducting interviews, and further ensured that interviewees were provided with adequate information on the nature of the research.

1.13.2 Informed consent

Webster, Lewis and Brown (2014:87) view the essence of informed consent as meaning that people should be given sufficient information to enable them to make a decision about whether or not to take part in a study.

The researcher informed participants in advance, of the purpose and nature of the research. This allowed participants to make an informed decision on whether to participate in the research. The research further obtained written consent from all participants. The interviews were conducted at each interviewees convenience and at appropriate venues chosen by the researcher. The findings were reported honestly, according to the interviewees' responses.

1.13.3 Acknowledgement of sources

All sources cited in this study were duly referenced to ensure that no plagiarism is committed. The researcher appropriately cited every author quoted in this study and has included a comprehensive reference list in acknowledgement of the literature.

1.13.4 Confidentiality

Confidentiality means not revealing who has taken part and not reporting what participants said in ways that could identify them or be attributed to them (Webster et al., 2014:96). Matthews and Ross (2010:78) confirm that participants should be guaranteed that they will not be identified in the research and that their input to the research will be confidential.

In this research, confidentiality was ensured as participants names remained anonymous. Participants attended interviews from their workstations, privately and individually.

1.13.5 Right to privacy

The right to privacy of participants was respected and maintained. According to Leedy and Ormrod (2015:128), “participants should not participate in research which could cause them embarrassment.”

1.14 CHAPTER SUMMARY

This chapter introduced the research by providing a brief background to the study, followed by an exploration of the research problem. This was followed by justification of the research objectives and the research questions relevant to the study. In this chapter a summary of how data was collected and analysed was provided. Further, this chapter outlined all limitations applicable to the study, as well as all the problems encountered during the study.

All the relevant key terms were clarified, and the chapter concluded with an overview of the method chosen to ensure the trustworthiness of the study focusing on it’s credibility and dependability. Lastly, a brief overview of the ethical framework within which the research was conducted. The conceptual overview of e-Procurement follows for discussion in chapter two.

CHAPTER TWO
CONCEPTUAL OVERVIEW OF THE E-PROCUREMENT SYSTEM

2.1 INTRODUCTION

The world of technology as emphasised by Casey (2011:11) has evolved hurriedly and the rapid developments in technology, such as e-Procurement, led to the increase in several computer related crimes, for example, e-Procurement fraud. This has also created a significant demand on the side of law enforcement agencies for qualified practitioners or forensic investigator who can properly and lawfully collect, analyse, and interpret electronic data. Thai (2019:477) defines e-Procurement as an internet-based system, which automates and integrates the whole procurement process to improve efficiency, and to promote transparency and accountability in any organisation.

As alluded by Makoba, Nyamagere and Eliufoo (2017:180) e-Procurement is the use of information and communication technology in conducting procurement functions. However, according to Galloway (2003:16) e-Procurement has created a platform for criminal activities with its automated and internet reliance system of purchasing and trading. The risk associated with e-Procurement system is the security of information involved in the transactions as it is a web-based system which requires internet and network communication, data is shared between the buyers and suppliers, entities, and companies from different countries. These factors increased the vulnerability of information being intercepted and utilised for fraudulent reasons.

E-Procurement contributes to reduction of corruption within the procurement process and has the ability to create exit barriers against the buyer favouring the supplier as their relationship is terminated by its automation during the selection process, which removes human interference. Through requiring bidders to be actively involved in a real-time procurement process, it can further promote transparency. Furthermore, e-Procurement has the added benefit of reducing administration costs and the need for procurement staff, while simultaneously making communication more effective through speedier access to information (Subramani, 2004:22). In support of the views of Subramani, Makoba et al., (2017:180) indicates that the benefits of e-Procurement are to reduce costs and increase efficiency, as it enables volume purchases, wider choice of buyers and suppliers, brings better quality, improves delivery, reduces paperwork and lowers administrative costs.

This chapter provides a conceptual overview of e-Procurement, its evolution, benefits, and challenges. It also gives a clear synopsis of different models of e-Procurement and several technology applications, and system architecture (what the system needs to achieve the best intended results). Following that, the key components of e-Procurement and e-Procurement in the South African context and international benchmark on e-Procurement best practices are discussed.

The aim of this chapter is to promote an improved understanding of a conceptual overview of e-Procurement. Forensic investigators will also gain an insight into how e-Procurement technology works. It will also expand the forensic investigator’s knowledge of different elements and key components that will enhance their expertise to investigate this system in future. The evolution of e-Procurement to conceptualise how e-Procurement evolved throughout the years follow for discussion.

2.2 THE EVOLUTION OF E-PROCUREMENT

According to Dai and Kauffman (2001:2), although “private and public sector organisations have been utilising Information Technology (IT) systems” for over 40 years to streamline and automate purchasing processes, it is only recently that that e-Procurement systems have become noteworthy within the industry. This statement is supported by Vaidya, Sajeev and Callender (2006:73), when they illustrated that the implementation of the Internet in e-Procurement provided notable advantages over previous inter-organisational tools. Chan and Owusu (2022:1) share similar views with Dai and Kauffman by emphasising that since the advent of the first form of e-Procurement process, it has evolved to transform the world of commerce significantly. It has revolutionised the operations of traditional procurement and has paved the way for the development, advancement, and application of more intelligent tools for handling and executing procurement processes and activities.

Earlier tools include Electronic Data Interchange (EDI), which, since the 1960s, have provided automated purchasing transactions and records between buyers and suppliers. Following that, Enterprise Resource Planning (ERP) became widely implemented in the 1970s. It was only in the 1980s that commercial use of the Internet became common, leading the way for the 1990s, when World Wide Web's multimedia capability to became widely used and understood well enough to provide the much-needed resource to automate procurement as we know it today (Bidgoli, 2010:54). Electronic Data Interchange is the movement of information electronically between buyers and suppliers for the purpose of facilitating a business transaction to improve delivery performance (Masudin & Kamara, 2017:142).

The integration into government institutions marks the beginning of the rise of e-Procurement in the 1990s, according to Moon (2005:56). Moon (2005:56) lists examples such as "web-based proposal requests, internet bidding, and digital signatures for procurement documents, reverse auctions, electronic ordering, automated procurement systems and purchasing cards" of how e-Procurement contributed to making government processes more effective. However, it was not unprecedented, as illustrated by Bidgoli (2010:54). It is the views of Perera, Nanayakkara and Weerasuriya (2021:1) that e-Procurement can be categorised into three distinct eras. The first era, in the 1980s, used digital storage media and emails to transfer procurement-related documents. In the second era, which was web-based e-Procurement in the 1990s, suppliers communicated directly with the client's e-procurement portal. The third era involved cloud computing and system-to-system inter-communication in the 2000s.

In support of Perera et al., (2021:1) Bidgoli's (2010:54) study demonstrates that the development of EDI systems is among the first attempts to create systems that automated procurement operations, with the added benefit of improving relationships through providing easily trackable purchase transactions and records. EDI systems simply the process of exchanging standardised data or documents such as purchase orders (PO), invoices, delivery schedules contract information from one computer to another using electronic wired connections, or value-added network (VAN).

In support of Moon’s (2005:56) statements, Bidgoli (2010:55) maintains that the internet enabled e-Procurement systems to start to be actively implemented and utilised by the mid-1990s.

Furthermore, Bidgoli (2010:56) and as emphasised by Perera et al., (2021:1) sustains that after 2001/2, e-Procurement systems experienced a gradual evolution to become more efficient, sophisticated, and widely accepted within most institutions. As it settled into its status and become more affordable, e-Procurement became essential for processing, measuring, and improving companies’ procurement systems due to its extensive functionality, more efficient delivery models and better-developed catalogues and supplier networks.

Therefore, considering the views obtained through the literature review as presented above, and based on the researcher’s experience, he makes the following conclusions:

- Using EDI technology as a base, e-Procurement started to become viable in the 1980s. EDI, although a relatively basic system, laid the groundwork with a computer-to-computer information exchange that allowed an unsophisticated e-Procurement platform between companies to spring up;
- Then, in the early 1990s, when software companies started seeing potential of e-Procurement systems they invested in expanding capabilities and making e-e-Procurement more accessible to the general population. For instance, they invested in solutions like an online catalogue that offers the consumer standardised items and unit prices listed by vendors with e-Procurement references;
- By the early 2000s, the uses of the internet had grown exponentially. This was reflected by the connection of ordinary users to rapidly developing e-Procurement systems; and
- Finally, by the 2010 and into the 2020s, e-Procurement systems have ever-growing potential for growth and connectivity. For instance, remote-access cloud-based systems cut down on IT infrastructure and the need for upfront capital for many small businesses while offering 21st century solutions.

2.3 BENEFITS OF E-PROCUREMENT

Vickery, Jayaram, Droge and Calantone (2003:2) suggest that e-Procurement “allows for an increase in the free flow of relevant information that results in better decision making from both the buyer and supplier”. Vickery et al. (2003:3) further indicated that IT integration within SCM results in performance benefit. Sanders (2005:12) concurs with Vickery et al. (2003:3) when he states that the “performance benefits are a result of reduction of business costs due to the elimination of operational duplication of resources”. In other words, e-Procurement eliminates duplicate spending, while utilising volume buying to save businesses money. Another benefit is that the cost of paper-based systems is no longer a factor, such as stamps for mailing paperwork. Chan and Owusu (2022:18) illustrate that an e-Procurement system can also improve transparent governance and curb corruption if its policies can be translated into practice.

According to Sanders (2005:12) e-Procurement “can decrease coordination costs and transaction risks”. In support of Sanders (2005:12), Vickery, Droge, Seita and Sambamurthy (2010:4) stated that e-Procurement helps to coordinate and integrate activities within the organisation’s SCM system. Furthermore, it encourages collaboration between organisations and suppliers by facilitating exit barriers for the buyer, which helps the supplier retain customers (Subramani, 2004:22). According to Subramani (2004:22), e-Procurement is “capable of enhancing the buyer’s dependence on the supplier and increase the supplier’s bargaining power in the relationship”. The supplier also benefits from their business being automated, meaning faster administrative process of tasks like invoicing and payments and more efficient inventory management. Makoba et al., (2017:181) indicate that the benefits of e-Procurement are less corruption and value for money.

Dedrick, Xin Xu and Xiaoguo Zhu (2008:35) concur with Sanders (2005:12) and Vickery et al. (2010:4) when he indicated that e-Procurement “has the potential of reducing coordination costs as procurement processes are standardised and automated, thus reducing the costs of working with more suppliers”. To emphasise this matter further, Dedrick et al. (2008:35) reflected that e-Procurement allows organisations to “reduce the number of suppliers and focus on low-cost suppliers of standard goods… and consolidated their purchase to obtain discounts”. Furthermore, Abu-Elsamen, Chakraborty and Warren (2010:243) points out that all these benefits allow the organisation to utilise the e-Procurement technologies to transform the procurement process. Ibem, Aduwo, Tunji-Olayeni, Ayo-Vaughan and Uwakonye (2016:55) agree with the views of the authors above and mention that the benefits of e-Procurement include gaining access to a larger market and increased opportunities; reduction in paperwork; increased productivity; and reduction in the procurement cycle time and transaction cost.

According to Davila, Gupta and Palmer (2003:11), “by implementing e-Procurement the [organisation] could shorten the order fulfilment cycle time, lower inventory levels and price to be paid for goods and services and reduce administrative costs of procurement”. Presutti (2003:219) claims that “e-Procurement systems can bring benefits to the company, such as, reducing time to market cycles, reducing material and transaction costs, reducing stock levels”. Chaffey (2011:10) argues that “the benefits of e-Procurement include reduced purchasing cycle time and cost, enhanced budgetary control, elimination of administrative errors, increasing buyer’s productivity, lowering prices through product standardisation and consolidation of acquisitions, improving the payment process and improving information management”. Masudin and Kamara (2017:140) share similar views with Presutti (2003:219) by emphasising that e-Procurement can reduce costs of inventory, reduce stock out probability, improve customer responsiveness and finally improve competitiveness.

E-Procurement has attracted many organisations’ attention and it has the potential to increase productivity growth in Western and global South nations (Hawking & Stein, 2004:219). According to Subramani and Shaw (2002:12), this is because e-Procurement provides lower transaction costs, more accurate procurement process quality, shorter cycle time and improved inventory management, which saves governments and enterprises money. Subramani and Shaw (2002:12) also prove that e-Procurement systems improve the relationships between trading partners, controlling risks and contributing to more strategic sourcing, which all contribute to cheaper, more efficient productivity. Anthony (2018:43) illustrates that e-Procurement improve transparency and competition.

Chakravarty (2014:117) shares a similar view with Sanders (2005:12), stating that a buyer "can lower the cost of goods through comparative shopping and aggregated purchases" far more easily when shopping online and utilising an e-Procurement system. However, this is beneficial to consumers as well as suppliers, as "though enhanced matching of inventory with business volumes and stocking levels, both the buyer and supplier can lower their respective stocking levels". Thus, e-Procurement empowers buyers to find the items they want and suppliers to be able to supply those items. Bakar, Peszynski, Azizan, Sundram (2016:86) state that major e-Procurement benefits include cost savings, an increase in the return on investment, and the utilisation of just-in-time inventories. Another benefit as indicated by Bakar et al. (2016:86) is the enhancement of supply chain efficiency by providing real-time data regarding product availability, inventory levels, shipment status and production requirements.

Abramson and Morin (2003:183) summarised the benefits and prospects of e-Procurement by listing the following:

- Cheaper transaction costs;
- Speedier ordering;
- Better vendor choices;
- More efficient and standardised procurement processes;
- More control over procurement spending;
- Higher employee compliance;
- More accessible alternatives for buyers on the internet;
- Less paperwork;
- Fewer repetitive administrative procedures; and
- Reengineered procurement workflow.

Neupane, Soar, Vaidya and Yong (2012:308) identify that e-Procurement:

- Centralises data and improves audit and analysis;
- Eliminates fraud and corruption and increases internal efficiency in government departments by decreasing direct human interaction on bidding and other work and services;
- Monitors works and services systems easily and efficiently;
- Provides better status monitoring and tracking of applications
- Increases transparency in works and services by improving the quality of interaction between suppliers and vendors and citizens; and
- Employs an online bidding system that complicates involvement from cartels, decreases collusion and reduces rigging.

In support of the views of Abramson and Morin (2003:183), Chaffey (2011:10) and Dedrick (2008:35), and Neupane et al. (2012:309) can be studied to understand that by adopting e-Procurement system, organisations can improve transparency and efficiency, while reducing reduce cost. A well-implemented system also creates an environment that leads to better decision-making, more advanced monitoring of supplier performance, and a higher quality of service. E-Procurement removes the middleman in the procurement process and automate transactions with high accuracy and lower costs. It further mitigates human errors and disputes in a complex situation and ultimately save significant costs with highly efficient and effective procurement operations (Perera et al., 2021:5).

Another list of benefits to consider is by Cascarino (2013:358) who also share the same views with Bakar et al. (2016:86). According to Cascarino (2013:358), the benefits of successful e-Procurement implementation in an organisation include:

- Increased productivity coupled with decreased transaction costs;
- Continual service availability;
- Fundamental reform of the communication system between organisations and their supply chains; and,
- Increased likelihood for local business to grow and compete in the global marketplace.

Furthermore, to make application local, Anthony (2018:42) demonstrates the advantages of implementing e-Procurement in South Africa. For instance, a more efficient procurement process lowers reduced costs and supply periods, leading to better-priced goods for consumers. Another advantage is the greater transparency required by bidders, due to the active involvement in a 'real-time' procurement process, which also has implications for service delivery.

'Real time' procurement processes through e-Procurement keeps suppliers continuously informed of their competitors' bids, and, thus their own prospects of success as a supplier in relation to other suppliers – causing positive competitive price adjustments. It also contributes to reducing corruption and maladministration within the process by ensuring speedier access to information. Thus, tender documents and information in more readily always be available and can be updated with ease, reducing opportunities for corruption (Anthony, 2018:42).

Therefore, it is apparent from the literature review that it is potentially beneficial on many levels to implement e-Procurement on an organisation and government-wide basis. Chiefly, by ensuring competitive prices for goods and a more trustworthy public procurement process. By requiring that bidders are actively involved in a procurement process that takes place instantaneously, e-Procurement promotes transparency and reduces corruption. Furthermore, administration costs and costs associated with procurement staff are reduced. Greater efficiency and organisation among the suppliers can be achieved through the improved levels of communication due to much faster access to vital information such as tender documents that are constantly available to be updated accurately.

Additionally, governments and organisations can use e-Procurement systems to readily identify and publish who their regular, reputable and trustworthy suppliers are. This will incentivise transparency and quality from suppliers. Therefore, e-Procurement has been widely proven through the studies of various authors as an automated procurement process with many benefits. However, it has its own hurdles and provisos. This following discussion outlines the challenges and barriers of e-Procurement.

2.4 CHALLENGES OF E-PROCUREMENT ADOPTION AND IMPLEMENTATION

Chaffey (2011:366) indicated that there are some “barriers to adoption of e-Procurement”. He identified the following issues as challenges to e-Procurement:

- Negative perceptions about the systems from suppliers;
- Negotiated procurement benefits may be shared with other exchange users who may be competitors;
- The process of creating of catalogues can be lengthy and costly to suppliers; and
- Resistance to change by staff due to cultural profile within the company.

Additional to the statements by Chaffey (2011:366), Makoba et al. (2017:184) identify some of the challenges of e-Procurement such as computer virus and worm attacks, shortages in internet services, breach of confidentiality of information, non-compatibility issues, dishonest attacks of financial transactions and human resource risks.

However, in contrast to Chaffey (2011:366) challenges, Pomazalovà (2013:267) identified the following as the potential problems of e-Procurement in South Africa:

- Lack of computer literacy skills; and
- Limited public access to the tools needed, like Internet and other Information and Communication Technology (ICT) tools.

Pomazalovà (2013:143) further indicates that one of the major barriers to a wide adoption of e-Procurement that organisations may not have the necessary “IT infrastructure to carry out e-Procurement”. Higher costs and unaffordable prices are also resulting in organisations not being able to implement e-Procurement. The other problem relates to lack of skills of the existing workforce which may mean that they cannot operate computers and other IT systems. In support of the views of Pomazalovà (2013:143), Van Greunen, Herselman and Van Niekerk (2010:3658) illustrate that lack the necessary infrastructure and policies, capacity to pay and poor IT literacy levels are the challenges facing most organisations to adopt e-Procurement.

According to Anthony (2018:43), one of the barriers of e-Procurement is that products may be procured at a lower quality for the sake of a better price.

The above notion is supported by Information Resources Management Association (IRMA) (2020:990) which illustrates that the "impediments to the adoption of e-Procurement system are expensive investment, fast obsolescence, risk involved in applying uncertain technology to the core processes, problems integrating with existing systems, lack of common standards for e-commerce software development, and lack of supplier accessible through e-Procurement system". According to IRMA (2020:990), the need for a qualified workforce, the barriers of cultural differences and problems with security significantly obstruct or "hinder the development of e-Procurement activities. Inadequate IT infrastructure is found to be the most important barrier to the adoption of e-Procurement system[s]".

According to Galloway (2003:16), the challenges posed by e-Procurement system is the security of information in the database and transactions since the e-Procurement is a web-based system which requires internet connectivity, data is transmitted between entities and companies. These increased the vulnerability of interception and information can be garbled and lands in the wrong hands. Galloway (2003:15) further suggested that top management or employees of the organisation who do not support the change present the biggest hurdles for e-Procurement. Support from top management and employees is the footstep in the adoption and the effectiveness of the e-Procurement system. In support of Galloway (2003:16), Chan and Owusu (2022:14) listed several key technical challenges associated with e-Procurement adoption and implementation, which were primarily centered on the issues of security, authentication, standards, and integration of the system.

It is the submission of Cascarino (2013:360), who also share the same views with Chan and Owusu (2022:14) that one of the challenges of e-Procurement is the issue of security risks. For instance, proper authentication should be performed when sensitive transactions are performed. Therefore, a critical component of e-Procurement is the implementation of proper authentication. This is due to the face that once a party has been authenticated as an authorised user, "a legally binding transaction process has begun” (Cascarino, 2013:360). The risk can spread to other parties through, for example:

- The creation of fictitious suppliers (also known as masquerading). For example, a company believes it is dealing with a legitimate supplier; however, it is dealing with a hacker;
- Orders or transactions approved by unauthorised users; and
- The list of agreed suppliers can become corrupted.

In addition, Casacarino further maintains that the corruption of data is another risk of e-Procurement. He sustains that “corruption of data refers to issues of data integrity (Cascarino, 2013:360). “The commonly held view is that risks involve activities that can be performed remotely through Web resources”. Cascarino maintains that reality is that the majority of corruptions come from within the systems. Accidental or malicious corruption could result in:

- Catalogues being amended without authorisation (advertising, reporting, approval);
- An audit trail being destroyed;
- The ordering process being changed or tampered with; and
- Online tenders disrupted.

It is the view of Anthony (2018: 44) that a possible threat in an e-Procurement process is that e-Procurement, rather than removing corruption, could provide the opportunity for collusion. He maintains that a smaller number of contractors within a closed system that can provide the desired product or service could lead to a greater increased chance of collusion.

Furthermore, Anthony (2018:44) discusses the reality of the risk an IT failure during procurement process poses. He argues that this type of situation may eventually cause legal disputes regarding liability for a failed process, or a tender incorrectly awarded. According to Anthony “it has also been noted that technical expertise, knowledge, and access to IT may be limited in some companies, especially in the case of Small, Medium and Micro-Enterprises (SMMEs)”.

Thus, Anthony (2018:44) focuses on the important role that top management plays when successfully or failing to provide adequate infrastructure and support to staff regarding computer literacy and training. He shows, in turn, that the staff that transitions to the e-Procurement division should display a willingness to operate in an electronic environment. E-Procurement staff needing to do so is one of the most common challenges that hold e-Procurement successful implementation back. Nzuza and Garbharran (2015: 9) emphasise that factors like outdated technological systems, lack of financial support, and unwillingness of staff to participate in the system can negatively influence the adoption of e-Procurement.

Furthermore, Sithole (2017:3) lists the disadvantages of e-Procurement, particularly in South Africa, as follows:

- A high capital cost is required to procure the technology required;
- A lack of adequate ICT infrastructure;
- A lack of resources for e-Procurement;
- An unreliable power supply for equipment;
- The many security risks; and
- The non-compatibility of different software packages and application.

In support of the disadvantages identified by Sithole (2017:3), Kabanda, Pitso and Kapepo (2019:234) have identified similar problems:

- Government policy needed to implement e-Procurement is lacking,
- Lack of reliable ICT infrastructure;
- Installing and operating e-Procurement systems requires high costs; and
- The stigma that the adoption of e-Procurement is damaging for smaller firms.

The researcher, therefore, concludes, based on his own experience and information from reviewed literature that, the most common challenges of e-Procurement is failure of implementation of comprehensive data security which may lead to potential risks, such as:

- Private information published online;
- Transactions lost or dropped enroute;
- Networks failing due to service provider’s unreliability;

- Audit trails being lost, caused by corrupted data;
- Interception or illegal accessing of transaction in transit and amend them;
- Duplication of transactions;
- Manipulation of input by an authorised user;
- Lack of adequate IT infrastructure; and
- An unqualified e-Procurement workforce.

As illustrated by the review of the literature, while there are different models of e-Procurement, the basic principles remain the same. The chief benefit of e-Procurement is that the entity seeking to procure tenders must publish their invitation electronically, and the invitation needs to provide detailed information in the form of a description of the subject matter, clearly defined terms and conditions, as well as the criteria and procedure for evaluation of the bids, including the mathematical formula that will be applied. Lastly, the procurement invitation is required to inform bidders about crucial information such as whether or not additional aspects, other than price, such as, quality or preference, will be evaluated during the deliberation process. Different models of e-Procurement follow for discussion.

2.5 TYPES OF E-PROCUREMENT MODELS

Lysons and Farrington (2006:187), outline seven types of e-Procurement systems:

- EDI networks;
- Business-to-employees (B2E);
- Corporate procurement portals;
- First generation trading exchanges: community catalogues and storefronts;
- Second generation trading exchanges: transaction-orientated trading exchanges;
- Third generation trading exchanges: collaborative supply chains; and
- Industry consortia: buyer and supplier led.

In addition to Lysons and Farrington basic seven models, there are three business solutions identified by Jooste and Schoor (2003:14) to access suppliers' information online:

- Buy-side solution;
- Sell-side solution; and
- Neutral (independent) marketplace.

Chaffey (2011:368) concurs with Jooste and Schoor (2003:14) by sustaining that e-Procurement has three models which are buy and sell side models, and independent marketplace. Praveen and Khaliq (2018:102) agree with the statements by the authors above by emphasising that Business-to-Business (B2B) and Business-to-Customer (B2C) are two major e-Procurement models.

It is the views of Bidgoli (2019:149) that the B2B model use the technologies such as internet, extranet, virtual private networks, EDI and electronic funds transfer (EFT) extensively to help "business partners share relevant, accurate, and timely information". "The information flow with business partners is improved by creating a direct online connection in the supply chain network, which also reduces delivery time" according to (Bidgoli 2019:149).

According to the CoT e-Procurement Technology Architecture (2016:6) which was developed by Praxis to automate the entire SCM system, the CoT uses EDI solution to procure with its suppliers. This architecture was accepted and signed by the CoT on 6 April 2016 for implementation of e-Procurement. It was stated in this architecture that the CoT e-Procurement system is also known as SCM-Web. The major component of SCM-Web is called Green-Field. The CoT e-Procurement solution consists of the following main components, which together makes an integrated SCM system:

- Procurement Management - Green-Field;
- Vendor Communication - SCM-Web Vendor portal;
- Business Intelligence - Pentaho Business Analytics platform; and
- Call Logging and Tracking (Help Desk System) - JTrac.

It was confirmed through different literature studies that there are numerous e-Procurement models, however, the researcher focused only on the following models that are more relevant to this study and are discussed in detail below:

2.5.1 Electronic data integration (EDI)

According to Lysons (2000:118), EDI is “a technique based on agreed standards, which enables computers (systems) in different organisations to successfully send business or information transactions from one to the other”. The transmission of these commercial messages between organisations by EDI requires that transmitters should know what information to send and in what order. Conversely the receiving computer must know what the transaction comprises and how to process the information. Examples of messages are quotation request, quotations, orders acknowledgements, delivery notes, and invoices. EDI is also involved in the process of instructing the bank to make a payment. In support of Lyson (2000:118), Masudin and Kamara (2017:142) demonstrate that EDI represents a powerful application of computer communications technology, which reduces paperwork, eliminate data entry overheads, improve accuracy, and accelerate cash flow.

It is the view of Cascarino (2013:357) who concurs with Masudin and Kamara (2017:142), by maintain that EDI is the “computer-to-computer, application-to-application exchange of business data in a structured format”. Although the systems of electronic mail, fax, or video text all play a part in the overall network’s functioning, they are not EDI. EDI is comprised of basic conditions, namely:

- A common programming language in place between all the trading partners.
- A system for translation software in place to preform file conversions from internal application formats to a standard format and back.
- A data communications link that shuttles information between capabilities.

Lysons and Farrington (2006:189) discuss that EDI’s main purpose is to facilitate business transactions automatically between two organisations.

They also listed the following advantages of EDI solutions:

- Reduction of lead times as buyers and suppliers work together in a real-time environment;
- Replacing of the paper documents (PO and invoices for example) used by seller and buyer are conveyed between computers often without human intervention;
- Reduction of cost of inventory;
- Better customer service;
- Facilitation of invoice payment by computer-to-computer transfer of money, which eliminates the need for the preparation and posting of cheques; and
- The integration of functions, particularly marketing and purchasing.

In their study, Lysons and Farrington (2006: 189) mention that even though there are number of advantages of EDI, on the flipside, EDI is an expensive model. Organisations are required to send all EDI transactions via a Value-Added Network (VAN) that has to be set up, causing heavy overheads. High costs associated with the running of EDI infrastructure is a crucial deterrent to many small to medium enterprises. EDI is also a static and inflexible method to transmit data, therefore more applicable to straightforward business transactions and not transactions that require tighter coordination.

According to Walker and Rowlinson (2008:211), the process of EDI involves "communication and information exchange between business units within the organisation, processing transaction data between organisations, relationship marketing processes that binds parties more closely together using customer relationship management applications and inter-operability of data exchange and e-business". EDI transforms systems from substantially paper-based transactions to automated and integrated electronic forms of information exchange. This includes reports on financial transactions as well as making coordination and monitoring easier, while providing control of resources and activities. It is the submission of Chan and Owusu (2022:11), that e-Procurement is not a form, type, or method of procurement but rather the execution of forms or methods of procurement over a network system such as EDI and the Internet.

2.5.2 Business-to-business (B2B)

According to Osmonbekov, Bello and Gilliland (2002:7) “e-Procurement plays a fundamental role in B2B purchasing by streamlining the buying process and providing the information needed to make more effective purchasing decisions”. Barbieri & Zanoni (2005:11) share the same view as Osmonbekov et al. (2002:7), who suggested that B2B web-based e-Procurement systems facilitate purchasing transactions that give organisations the opportunity to save funds on transaction costs, while improving internal procurement process efficiency and increasing communication with suppliers. E-procurement could also improve a company’s procurement process by virtue of the automated procurement process. The service quality dimensions of B2B is its reliability, availability, ease of use, assurance, timelines, tangible and empathy (Eskandarian, Marthandan, Malarvizhi & Tehrani, 2016:75).

In support of the views by Barbieri and Zanoni (2005:11), Eskandarian et al. (2016:75), and Osmonbekov et al. (2002:7), Neef (2001:2) suggested that B2B “encompasses electronic buying and selling transactions” between organisations, and that e-Procurement plays a central role in the development of B2B. It is the submission of Bidgoli (2019:147) that B2B involves electronic transactions between businesses and that there are three (3) major models of B2B, based on who control the marketplace: sell-side, buy-side and third-party exchange marketplace (also known as independent marketplace). These models follow for discussion.

2.5.3 Buy-side solution

According to Abrahamson and Morin (2003:184), in the buy-side model companies invite a variety of vendors gives access to electronic catalogues. The buy-side model is made up of electronic PO, digital invoicing, the capability for electronic fund transfers (EFTs) and introduces ERP elements which increase procedural efficiency and convenience. Buy-side model of procurement refers to an organisation using electronic systems to purchase goods, such as office stationery, from contracted suppliers. These suppliers are also using e-Procurement systems for management of all processes relating to purchase (Ngabiya, 2017:9).

The notion of Abrahamson and Morin (2003:184), and Ngabiya (2017:9) was supported by Chaffey (2011:370) when he defined buy-side procurement “as a type of e-Procurement in which buyer invites bids via tendering space on its own site”. They explain that one of the advantages of a buy side e-Procurement solution is its user-friendly functions. For instance, employees have the functionality to easily to place orders or purchase goods electronically. The different types of integration needed in buy-side applications, to facilitate seamless interaction are employee connectivity, back-end systems connectivity, and supplier connectivity. This type of e-Procurement only really suits large buyers but displaces work to suppliers.

Jooste and Schoor (2003:14), in support of what was elevated by Abrahamson and Morin (2003:184) and Chaffey (2011:370), maintain that the main advantage of buy-side solution “is that buyers avoid the headache and investment of reformatting their suppliers' product data themselves”. Therefore, the vendor is required to manage content themselves. The advantage of buy-side solutions is that they streamline the corporate purchasing process by facing outwards from the consumer to the linked supply chain partners. The disadvantage is that it is difficult to control purchases or shop comparatively. Buy-side procurement as illustrated by Ngabiya (2017:9) is simply combining the corporate procurement portals and B2E applications.

2.5.4 Sell-side solutions

According to Abrahamson and Morin (2003:184), sell-side models are “a vendor-designed internet site that allows potential buyers to browse and purchase specific products from the site”. This model is designed chiefly to stimulate interest in the vendor while promoting the marketing activities of vendors. Chaffey (2011:370) also mentioned that sell-side procurement is the “type of e-Procurement in which buyer goes to supplier web site to purchase”. The supplier's “technological infrastructure, ability to integrate with different technological platforms and ability to cut costs and improve products” (Chaffey 2011:370) will determine how successful the sell side e-Procurement system is. There is more onus placed on the buyer than when using a buy side model. Furthermore, it is potentially more challenging to integrate with existing IT infrastructure than buy side models are. Ngabiya (2017:9) reiterates that the sell-side model is when one supplier sells to several buying organisations using electronic systems such as, e-Procurement systems and E-commerce technology. The sell-side procurement model is often used extensively in B2C.

It is the submission of Jooste and Schoor (2003:14) who agreed with Ngabiya (2017:9) “that managing the electronic supplier catalogue in house gives the advantage of being in control but requires a full maintenance team to perform content management”. In simple terms, the orientation of a sell-side system is that its content faces outwards from the vendor towards the purchaser, with a process that streamlines the transaction process.

2.5.5 Independent marketplace (third party exchange marketplace)

According to Bidgoli (2019:150), “third party exchange marketplace is not controlled by either seller or buyer, instead it is controlled by third party and the marketplace make revenue from fees charged for marching buyers and sellers”.

In support of the views of Bidgoli (2019:150), Jooste and Schoor (2003:14) sustain that the third-party exchange marketplace system empowers consumers by giving them access to a single portal that acts as central location for multiple vendors to display their products, services, and information. This makes it simple for similar products from different suppliers to be compared by the purchaser. Independent marketplace systems act as a hub that faces outwards to both the buyer and vendor. One of the main advantages of the independent marketplace solution is the nature of the relationships between the vendors and the consumers. As all purchases pass through a third party, there is less room for corrupt relationships to form. Another advantage identified by Jooste and Schoor (2003:14) is that independent marketplaces offer a more affordable option to vendors, as the infrastructure is already in place, and vendors need only to pay a fee to participate.

A brief overview of technology applications and system architecture follow for discussion.

2.6 TECHNOLOGY APPLICATIONS AND SYSTEM ARCHITECTURE

According to Ngabiya (2017:1) e-Procurement is supported by various applications of electronic communication and systems such as EDI, ERP, E-sourcing, and E-tendering, among others. As a web-based technology, e-Procurement needs adequate applications to support the system to be optimally effective. This system must be designed in such a way that it is able to use internet to carry out all stages of the procurement process. It must also be able to communicate with the suppliers in a secure manner. The security of information is of paramount key in the e-Procurement system as information is shared online and through internet (Chaffey, 2011:105).

2.6.1 E-Procurement technologies

Kamarulzaman and Mohamed (2013:48) postulate that e-Procurement is a set of advanced Internet technologies which gives companies the opportunity to access a simpler purchasing process that allows vendors to procure materials and other goods online. In support of the views of Kamarulzaman and Mohamed (2013:48), Ngabiya (2017:7) emphasised that internet-based e-Procurement systems need to be compatible applications to the greatest possible extent with the existing technologies, to have a reasonable chance to be widely adopted in the marketplace. “E-Procurement normally includes a system for making purchases online” (Kamarulzaman and Mohamed, 2013:48). E-Procurement brings together online and technological purchasing solutions to simplify commercial transactions inside and across organisations. Furthermore, according to Kamarulzaman and Mohamed (2013:48) “the application of e-Procurement technologies enables companies to achieve better information which can increase the efficiency of procurement processes and provide an opportunity to enhance competitiveness and profitability”. There are several types of e-Procurement technologies:

2.6.1.1 Electronic Tendering (e-tendering)

It is the submission of Perera, Ingirige, Ruikar and Obonyo (2017:172) who emphasise that Electronic Tendering (e-tendering) is the electronic conduct of tender activities from advertising through to contract placement (award), including the exchange of all relevant documentations for tender submission. The benefits of e-tendering include modernisation of working processes and improved efficiency in the way people work. E-tendering can also lead to improved commercial relationships with suppliers and reduce cost for suppliers. Jenkins, Köhler and Shackleton (2005:243) concur with Perera et al., (2017:172) in that these authors sustain that e-tendering module helps to establish a clear system for managing the placement of contracts and automatically assists staff by taking over certain SCM roles.

In support of the views of Perera et al, (2017:172), Kamarulzaman and Mohamed (2013:48) maintain that “e-tendering involves the process of sending requests for invoices and request for purchases etc. to suppliers and receiving the responses from the suppliers using web-based technology”. Therefore, E-tendering offers buyers and suppliers security while conducting tendering interactions online.

2.6.1.2 Electronic Sourcing (e-sourcing)

Kamarulzaman and Mohamed (2013:48) emphasise that “electronic sourcing (e-sourcing) refers to the process of identifying or finding new possible suppliers for a specific category of purchasing requirements using Internet technology”. Thus, the electronic sourcing makes it possible for companies to interact with a broad range of potential suppliers and make informed choices.

Bidgoli (2019:66) share the similar view with Kamarulzaman and Mohamed (2013:48) in that he points out that e-sourcing is “an e-Procurement model that is used to identify, evaluate, negotiate, and configure purchases and supplier relationships that will effectively support supply chain and other business operations”.

2.6.1.3 Electronic Maintenance Repair and Operation (e-MRO)

According to Kamarulzaman and Mohamed (2013:49) “e-MRO focuses on the process of creating and approving purchasing requisitions, placing orders and receiving goods or services ordered using system software based on Internet technology”. The system uses electronic infrastructure to send and receive digital documents for products and services. For example, PO’s, invoice, and payment notifications. In support of Kamarulzaman and Mohamed (2013:49), Mekenye (2017:13) notes that e-MRO deals with creating and approving purchasing requisitions, placing PO’s and receiving non-product related MRO supplies.

2.6.1.4 Web-based Enterprise Resource Planning (Web-based ERP)

It is the submission of Monk and Wagner (2013:19) that “an ERP system can help a company integrate its operations by serving as a company-wide computing environment that includes a shared database delivering consistent data across all business functions in real time”. In their study Kamarulzaman and Mohamed (2013:49) are of the opinion that a “web-based ERP system involves the procurement of direct goods/product related items (goods that are directly used to produce finished products) and any related transactions such as PO, invoices, payments, and other necessary documentation via online”.

According to Elango (2017:67), the advantages of online ERP is high profit, increased business capability, produce positive outcomes and enhanced streamline process in overall business operations. It is applied for various business functions especially in making integration with business management and administrative functions include accounts payable, human resources, student system, finance and purchasing.

2.6.1.5 Web-based Electronic Data Interchange (web-based EDI)

According to Kamarulzaman and Mohamed (2013:49), online “EDI systems are a cost-effective way to automate the exchange of structured documents on business arrangements between trading partners as all transactions are done electronically”.

Therefore, web based EDIs give companies the opportunity to replace expensive traditional EDI systems with web communication that provides real time information more cheaply and faster.

It is the opinion of Chaffey (2011:161), who also shares the same view as Kamarulzaman and Mohamed (2013:49) that EDI is an exchange of documents in standardised electronic format, between organisations, “in an automated manner, directly from a computer application in one organisation to an application in another”. The development of EDI is seeing new standards of integration and web-optimised capabilities that bring positive results to the orgnaisations that use them, such as lower costs and the elimination of VANs in favour of Virtual Private Network (VPNs). Srivastava, Goyal and Mathur (2021:116) concur with Chaffey (2011:161) in that the reason why the ability of EDI is created over the internet is that “the internet is a publicly accessible network, and it is largest attributes and, large scale connectivity”. It is also a seedbed for growth of a vast range of business applications.

2.6.2 System architecture

Wangui (2013:10) suggests that e-Procurement system architecture refers to the design of the system for effective performance and output. The most successful e-Procurement projects are totally embedded within the business process while remaining flexible enough to react to ongoing technological advancements. It is the submission of Nani and Ali (2020:37) that e-Procurement requires information technology that can support the process and performance. The technology such as internet connectivity, websites, applications, and systems that can maintain user security.

2.6.2.1 Internet-based system

According to Wangui (2013: 1), e-Procurement is “the purchase and sale of goods and services through the internet as well as other information and networking systems, such as EDI and ERP”. Therefore, for an e-Procurement system to be successfully implemented, it needs to have online capabilities and internet connectivity. In support of Wangui (2013:1) Makoba, Nyamagere and Eliufoo (2017:180) maintain that e-Procurement depend solely on internet and communication network technology to efficiently conducting procurement functions.

In addition, Wangui (2013:1) sustain, that, by definition, “e-Procurement refers to the use of internet-based system used to carry out individual or all stages of procurement process, including search, sourcing, negotiation, ordering, receipt, and post-purchase review”. It therefore entails that e-Procurement system require internet to function effectively and efficiently. Sharing the similar view with Wangui (2013:1), Chaffey (2011:105) put forward that intranet systems are common when supporting sell-side e-Procurement or core SCM activities. Typically, they will be deployed “as web-based services supplemented by messages and alerts delivered by e-mails or when users login to a company network”.

2.6.2.2 Communicate through website

Labelle (2012:37) suggest that organisations and companies are increasingly using new and innovative ways to be in contact with their potential suppliers. They have decided to use a single-entry website to allow suppliers to find information in a single place. These electronic portals not only provide information on procurement procedures and activities, but also support direct interaction between organisation and suppliers. In support of Labelle, Nani and Ali (2020:46) demonstrate that suppliers can access procurement information without exception from the website provided by the buyer. The procurement process can be followed by everyone, even those residing or doing business outside the local area or abroad. The buyer should strive to enhance the quality and reliability of websites by improving service convenience and minimising performance failure.

It is the submission of Wangui (2013:10) that organisations that want to adopt e-Procurement needs a reliable website to allow suppliers to access their information and to participate in the procurement activities. Websites offer the online version of a storefront and have made catalogues more accessible. E-Procurement systems must provide 24/7 information, which is accomplished through websites.

Wangui (2013:10) share similar views with Nani and Ali (2020:46), and further maintain "a good reliable and authenticated website is necessary so as to reach many customers worldwide". A website is an international calling card that both empowers customers and entrepreneurs through ready availability of "reliable, accurate and authentic information on products and services".

2.6.2.3 Security of information

It is the view of Wangui (2013:10) that "security mechanism plays a major role in adoption of e-Procurement". When considering implementing e-Procurement, companies and organisations need to bear in mind the security of the systems and see them as a vital component to the system.

It is the opinion of Thai (2019:482) who also shares similar view with Wangui (2013:10), that procurement data is usually sensitive information, such as orders and payments, which has legal implications as well as a vulnerability towards fraud. Thai (2019:482) further emphasises the importance of securely protected data. "The system must have mechanism for identifying and authenticating the user who places an order so that the suppliers know that it is safe to fulfil the order".

Imbe and Laryea (2015:374) support the view of Wangui (2013:10) who suggested there is too much security threats to information transmitted through the internet and networks, including:

- Lack of confidentiality;
- Loss of vital documents and data resulting from online scams and system crash;
- System hacking leading to violation of privacy;
- Viruses in the network can comprise the integrity of data and information.

According to Sithole (2017:30) the security risk of the e-Procurement transactions "emanates from the possibility that data may end up in the hands of the wrong recipients or can be tampered with". The other risks emanate from the unauthorised viewing, which may end in misusing of confidential and privileged data.

In the light of the above, Lysons (2000:127) highlight the mitigating steps to deal with security threats which includes:

- **Encryption technology**: encoding information to ensure that none but the holder of a secret password decrypt the message.
- **Certification authorities**: entities that certifies signatures and provides proof that a signature is valid and legitimate.

2.6.2.4 Communicate with suppliers

Imbe and Laryea (2015:369) sustain that the e-Procurement systems and tools used in facilitating effective and efficient communication, exchange of procurement information and data among participants (buyers and suppliers) are mainly through e-mail technology, websites, and portals.

According to Wangui (2013:16) “e-Procurement requires various buyers and suppliers’ systems to exchange information and electronic documents”. Wangui (2013:16) argues that notification mechanisms should be employed in e-Procurement systems Such notifications include, request for quotation (RFQs), PO, tender award, and payment among others. Furthermore, Wangui (2013:11) suggests that e-Procurement system must be able to communicate with its suppliers. Notifications and confirmations can be sent as emails. This will also help in responding quickly to market conditions and requirements.

In support of Wangui (2013:16), Chakravarty (2014:116) emphasises that “data and messaging tools enable the Internet-based exchange of transactional data between different buyers and suppliers in the e-Procurement marketplace”. This is accomplished by sending transaction ‘messages’ via the internet, which are in turn “integrated into a supplier’s or buyer’s back-office system, enabling financial postings that coincide with the receipt, payment, and invoicing processes” (Chakravarty, 2014:116). Furthermore, data messaging tools can cancel transactions. When messages fail to deliver within a predefined period or number of tries, data messaging tools can log failures. The chief advantage of messaging tools is that they ensure real-time communication between both parties involved.

2.6.2.5 Audit trail for future audit purposes

It is the views of Aduwo, Ibem, Afolabi, Oluwnmi, Tunji-Olayeni, Ayo-Vaughan, Uwakonye and Oni (2020:71) that the most important anti-corruption capability of e-Procurement identified is linked to the benefits of accountability through the provision of audit services trail in procurement transactions. Audit services trail also helps to address the issue of lack of transparency and accountability. Aduwo et al. (2020:71) further explain that audit trail reduces the level of secrecy and information asymmetry, alteration, or falsification of project information. From the above-mentioned, it is confirmed that the capability of e-Procurement can be linked to its automation feature, which is identified as a very important feature that reduces the incidence of corrupt practices in the public procurement processes.

Wangui (2013:10) alluded that the e-Procurement system “should enable audit trial mechanism to be conducted”. Audit trails have the advantage of both ensuring that a third party can inspect the supply chain activities and incentivising suppliers to participate by offering above-board audits. Wangui (2013:4) further indicated that one of the operational benefits of e-Procurement is that it improves “financial control by making it easier to match orders, improve auditing and better security by enabling staff and auditors to verify and track the movement of orders through the system.” (Wangui, 2013:4). In support of Wangui (2013:4), Erridge, Fee and Mcllroy (2001:164) are of the opinion that one of the operational benefits of e-Procurement is its potential to "reduce administrative costs of the whole procurement process by two-thirds, and the improved audit of each transaction throughout the process”.

The researcher therefore concludes based on the reviews of different authors, that for the e-Procurement system to be implemented successfully, the company’s host infrastructure must:

- Have the ability to integrate with the existing IT infrastructure;
- Be able to connect to internet and must have a reliable website;
- Have adequate security system to secure confidential and sensitive data;
- Be able to effectively communicate with its suppliers; and
- Be able to store data for future audit purposes.

2.7 KEY COMPONENTS OF THE E-PROCUREMENT SYSTEM

Chakravarty (2014:115) suggest that “e-Procurement has been able to develop its own body of language and as such regardless of its different models, each has similar components that must be properly considered and managed to ensure a successful e-Procurement system”. E-Procurement is a paramount function of present supply chains in any domain. The key components of e-Procurement include indent management, supplier management, catalogue management, e-Purchasing, and e-Contract management (Perera et al., 2021:1).

2.7.1 Catalogue management

According to Chakravarty (2014:116), “at the heart of every e-Procurement process lies an electronic catalogue”. Based on the traditional format of a mail-order catalogue, electronic catalogues are a central place with detailed information about the products or services being advertised. Content can be customised to address the specific needs of targeted buyers. With electronic catalogues, the content is imported into an electronic database and usually displayed via an e-Procurement system as web pages due to the easy international and constant access websites offer.

In his study, and in support of the views of Chakravarty (2014:116), Bidgoli (2019:60) maintains that catalogue content management involves “developing, updating, and maintaining online purchasing catalogues for the e-Procurement processes”. Populated either from the seller’s internal inventory system or from third party organisations, electronic catalogues may contain products from various sources.

2.7.2 User maintenance and management

It is the view of Chakravarty (2014:116) that user maintenance and management “serves as the foundation for managing the complex buyer-supplier relationships that will occur within the marketplace”. It defines each user’s profile, authorisation, enrolment, and access. User maintenance and management is the foundation for managing the deeply integrated buyer-supplier relationships created by the marketplace. According to Chakravarty (2014:116), e-Procurement user maintenance must address two primary tasks:

- Establish user profiles, access rules, catalogue filters, and workflow; and
- Allow for unique pricing and contractual relationships between a buyer and supplier

In addition, Chakravarty (2014:116) is of the opinion that "user maintenance requires establishing authorisation levels and associated procedures to precisely govern buyer and supplier capabilities". There are three authorisation levels to be addressed:

- Access to the electronic catalogue: accessing the catalogue, and how those users will access it;
- Creating and editing: which users are permitted to create and requisitions, or edit accounting codes; and
- Managing orders: which users have access to POs or to override shipping or billing information.

2.7.3 Billing management

Chakravarty (2014:117) maintains that "e-Procurement revenues are generally based on transaction fees". Usage charges, statements and invoices are calculated and generated by a billing management system, which also automatically distributes the documents within the network. The billing system is useful to suppliers, who may also use it to calculate ordering charges and distribute operating costs, which, which can automatically generate bills through office invoicing systems integration.

In the light of the above, Vaidya, Sajeev and Callender (2006:84) highlight that "it is also critical to link and interface the e-Procurement system to the financial management system in order to facilitate the process of online payment to suppliers". In order for purchase transactions to be recorded in financial management systems and sent to suppliers, they need to be carried out through an electronic ordering transaction support system. Payment applications can provide greater trust on transactions with automation and effective operation to mitigate payment-related issues in the procurement process (Perera et al., 2021:5).

2.7.4 Price establishment

It is the view of Chakravarty (2014:117) that e-Procurement system must be able to establish pricing. Accurately determined pricing gives buyers the opportunity to negotiate the best possible deal.

According to Chakravarty (2014:117), the following two major pricing options are used:

- **Dynamic pricing**: determined by market forces. The advantage is that buyers and sellers trade goods and services do not rely on a predetermined catalogue price list; and
- **Fixed pricing**: determined by a predetermined price list or catalogue.

2.7.5 System management

Chakravarty (2014:117) is of the opinion that “maintaining an e-Procurement system involves configuring and monitoring performance usage, average response time, transaction sources, and traffic patterns”. Thus, this information is used to analyse patterns of growth, and use this analysis as well as information about session times to fine-tune the system’s performance and maximise the benefits and strategic opportunities identified. It is critical to monitor an e-Procurement system once it is functional to analyse traffic and security. While e-Procurement systems are powerful, when they are inaccurate, they will lead to “poor marketplace performance, lack of scalability, breakdowns in security and ultimately, frustrated users” (Chakravarty, 2014:117).

2.8 E-PROCUREMENT IN THE SOUTH AFRICAN CONTEXT

South African procurement process is guided and regulated by numerous legislative frameworks. The notable one is the Constitution which outlined the pillars of the procurement system. The other legislations provide the processes and procedures that should occur when goods and services are procured in the public and private sector.

2.8.1 Core principles (pillars) of the South African procurement process

According to Van Greunen et al. (2010:3656) the South African Constitution (Act No.108 of 1996) "makes it very clear that the procurement system must be fair, equitable, transparent, competitive and cost effective" and must conform with "the five pillars of world-class procurement", namely:

- Value for money;
- Open and effective competition;
- Ethics and fair dealing;
- Accountability and reporting; and
- Equity.

In support of the views of Van Greunen et al. (2010:3656), Sithole (2017:15) emphasise that "in their endeavour to ensure compliance with the procurement objectives, the South African government introduced the five pillars of procurement". Thus, every organisation that implements e-Procurement must incorporate these core principle pillars into their procurement process. Sithole expands on the five pillars as follows:

- **Value for money**: every institution must procure goods, services or commodities that optimise the quality requirements;
- **Open and effective competition**: institutions are required to ensure that there is a reasonable chance to compete for tenders within the procurement process;
- **Ethics and fair dealing**: procurement officials must provide their service with integrity by avoiding acceptance of gifts and hospitality;
- **Accountability and reporting**: officials are required to report to the Accounting Officers and Ministers and account for any SCM process; and
- **Equity**: this relates to the commitment by government to implement measures that lead to economic growth for all parties, with a focus on the growth of small, medium and macro enterprises (SMMEs) and development of previously disadvantaged individuals.

Additional to the core pillars of procurement processes in South Africa, it is equally important to deliberate about the frameworks that guides the procurement practices. This will be discussed in detail below.

2.8.2 Legislative framework governing procurement in South Africa

Ambelm and Badenhorst-weiss (2012:248) identified numerous legislative frameworks that are guiding principles of procurement practices in South Africa as follows:

2.8.2.1 Constitution of the Republic of South Africa, Act No 108 of 1996

Section 217 of the Constitution of the Republic of South Africa requires that when an organ of the state contracts for goods and services. It must do so in accordance with the principles of "fairness, equitability, transparency, competitiveness and cost effectiveness for all public procurement in South Africa" (Selomo & Govender, 2016:1).

2.8.2.2 Public Finance Management Act No 1 of 1999 (PFMA)

Section 51(1)(a) of the PFMA 1 of 1999, emphasises the importance of "an accounting authority for, among others, a national or provincial department or public entity must ensure that the particular department or entity has and maintains an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost-effective" (Ambelm & Badenhorst-weiss, 2012:248). The National Treasury Regulations (Treasury Regulations) effectively implement the PFMA in clearly delaminated institutions, namely:

- Provincial as well as national state departments as laid out in the Public Service Act 103 of 1994;
- Listed public entities, South African government business enterprises and major public entities;
- Listed constitutional institutions; and
- Provincial legislatures.

2.8.2.3 Municipal Finance Management Act No 56 of 2003 (MFMA)

The Local Government: Municipal Systems Act 32 of 2000 and the MFMA 56 of 2003 “regulate, among others, the manner in which municipal powers and functions are exercised and performed, and the management of the financial affairs of municipalities and other institutions in the local sphere of government” (Ambelm & Badenhorst-weiss, 2012:249).

MFMA applies to the following level of government:

- Municipalities and municipal entities; and
- National and provincial arms of the state that are financing local municipalities.

2.8.2.4 Preferential Procurement Policy Framework Act No 5 of 2000 (PPPFA)

The Constitution permits departments and public entities of the state to develop previously disadvantaged persons through preferential procurement policies within certain regulations to lead to economic growth, also known as black economic empowerment (BEE). “Section 217(3) of the Constitution provides for legislation that prescribe a framework within which the policy must be implemented to be enacted” (Ambelm & Badenhorst-weiss, 2012:250). The Preferential Procurement Policy Framework Act 5 of 2000 and the regulations published under it in 2011 (PPPFA Regulations) are in alignment with section 217(3) of the Constitution. The PPPFA Regulations are applicable to the following institutions:

- National and provincial departments;
- Municipalities;
- Constitutional institutions;
- Parliament;
- Provincial legislatures; and
- Other organs of state that are included in section 239 of the Constitution and are recognised by the Minister of Finance as institutions to which the PPPFA applies.

2.8.2.5 Broad-based Black Economic Empowerment Act 53 of 2003 (BBBEE)

Section 2 of the BBBEE Act 53 of 2003 suggest that the government is to facilitate the BBBEE by:

- Encouraging the ownership and administration of enterprises by black South Africans. According to (Ambelm & Badenhorst-weiss, 2012:252), “enterprises are regarded as black-owned if 51% of the enterprise is owned by black people, and black people have substantial management control of the business”;
- Promoting meaningful participation in the economy through economic transformation;
- Realising an extensive adjustment “in the racial composition of ownership and management structures and in the skilled occupations of existing and new enterprises” (Ambelm & Badenhorst-weiss, 2012:248);
- Advancing access to financial backing and funding for black South Africans.
- Aiding rural and local communities by increasing their access to economic opportunities, land, infrastructure, land ownership and skills development;
- Increasing black human resource development via mentorships, learnerships and internships in the public sector;
- Boosting the communal ownership and ability to manage new and current enterprises of communities, workers, co-operatives, and other collective enterprises;
- Safeguarding black-owned enterprises through state-sanctioned preferential procurement policies;
- Encouraging the growth of BEE enterprises, focussing on SMMEs;
- Increasing level of black women CEOs, owners, and managers within enterprises; and
- Promoting investment programmes encourage generational growth and wider participation in the economy among black South Africans.

2.8.2.6 Prevention and Combating of Corrupt Activities Act No 12 of 2004 (PRECCA)

Purpose of PRECCA, Act no 12 of 2004 regarding corruption is to:

- Bolster existing measures that prevent and combat it;
- Provide resources for prosecuting offenders;
- Help create investigative measures;
- Act as an established register to place restrictions on offenders;
- Place an obligation on authorities to report corruption; and
- Make room for extraterritorial jurisdiction.

Section 12 of this Act (offences in respect of corrupt activities relating to contracts) states that:

- *"Any person who, directly or indirectly-*
  - *(a) Accepts or agrees or offers to accept any gratification from any other person, whether for the benefit of himself or herself or for the benefit of that other person or of another person; or*
  - *(b) Gives or agrees or offers to give to any other person any gratification, whether for the benefit of that other person or for the benefit of another person.*
    - *(i) In order to improperly influence, in any way the promotion, execution or procurement of any contract with a public body, private organisation, corporate body or any other organisation or institution; or the fixing of the price, consideration or other moneys stipulated or*
    - *(ii) As a reward for acting as contemplated in paragraph (a) above.*

This person is guilty of the offence of corrupt activities relating to contracts." (Ambelm & Badenhorst-weiss, 2012:260).

Section 13 of this Act (offences in respect of corrupt activities relating to procuring and withdrawal of tenders) states that:

- *"Any person who, directly or indirectly accepts or agrees or offers to accept any gratification from any other person whether for the benefit of himself or herself or for the benefit of another person. As-*

(a) An inducement to, personally or by influencing any other person so to act-

(i) Award a tender, in relation to a contract for performing any work, providing any service, supplying any article, material or substance or performing any other act, to a particular person: or

(ii) Upon an invitation to tender for such contract, make a tender for that contract which has as its aim to cause the tenderer to accept a particular tender; or

(iii) Withdraw a tender made by him or her for such contract: or

(b) A reward for acting as contemplated in paragraph (a)(i), (ii) or (iii).

This person is guilty of the offence of corrupt activities relating to procuring and withdrawal of tenders." (Ambelm & Badenhorst-weiss, 2012:260).

2.8.2.7 National Treasury regulations (2005), Gazette no: 27388 (15 March 2005)

Ambelm and Badenhorst-weiss (2012:445) mention that "the national treasury regulations reinforce the provisions of the PFMA and MFMA, finalise the devolution of the SCM function to the accounting officer, and formalise the integration of various functions into a single SCM function". Ambelm and Badenhorst-weiss (2012:445) further indicated that the "national treasury regulations provide the broad legislative framework for SCM by:

- *Defining the various elements of SCM such as demand management, acquisition management, logistics management, disposal management, and SCM performance;*
- *Institutionalising the creation of SCM unit in the office of the chief financial officer;*
- *Specifying the roles of the accounting officer in the management of the bidding process;*
- *Providing for processes and procedures in the case of abuse of the SCM system within a department; and requiring the national and provincial treasury and municipal finance department to establish a system to collect and report on the performance of the SCM system within their defined jurisdictions."*

According to Ambelm and Badenhorst-weiss (2012:445), the “legislation and regulations outline minimum requirements in the areas of supply chain and preferential procurement”. For instance, national, provincial, and local departments can grow “their policies, systems and structures within the ambit of the national regulatory framework” (Ambelm & Badenhorst-weiss 2012:445).

2.8.3 Public procurement in South Africa

Like any other country, South African public procurement plays a vital role economically and politically. Public procurement as a tool to drive innovation can further be categorised as either direct or general, or specific or catalytic. The procuring entity, in other words, simply uses its own demand or need to stimulate or encourage innovation. The resulting innovation is, however, often also spread to other users and can thus be beneficial for the procuring entity as well as society as a whole (Bolton, 2016:5).

In support of the views of Bolton, Mahmood (2010:103) maintains that “public procurement is increasingly recognised as a profession that plays a key role in the successful management of public resources, and a number of countries have become increasingly aware of the significance of procurement as an area vulnerable to mismanagement and corruption and have thus made an effort to integrate procurement into a more strategic view of government efforts”.

2.8.3.1 Guiding principles

There are two areas that have a significant impact on state procurement practices: Section 217 of the Constitution of the Republic of South Africa, 108 of 1996 (RSA 1996), together with the relevant parts of the PFMA, 1 of 1999 (PFMA). Most noteworthy is the shift of responsibility and ownership from the state to private individuals or enterprises. This shift requires a national framework that clearly defines the fundamentals of policy consistency that should be introduced nationwide.

According to Woods and Mantzaris (2012:112), “Section 38(1)(a)(iii) of the PFMA provides that the accounting officer for a department, trading entity or constitutional institution must ensure that the entity has and maintains an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive, and cost-effective”. This aligns with the PFMA’s efforts to democratise the decision-making process within organisations practices that enable multi-level decision making. For instance, overly centralised purchasing systems have been established in literature as a manner to deny managers opportunities to make informed calls that they are best positioned. However, the decentralisation of decision-making can also lead to more corruption and poor decisions with little consequences. Well-established guidelines can help prevent this from occurring.

It is the opinion of Ngxesha (2015:28), that “for the purpose of fairness and reasonableness, transparency and good governance, public procurement procedures must be designed to generate maximum competition (section 195(1) of the Constitution of the Republic of South Africa, Act 108 of 1996)”. This explains the importance of requiring transparency within public administration, as is also required by Section 195(1) of the Constitution of the Republic of South Africa, Act 108 of 1996. The basic values enshrined in the Constitution that should govern public administration include:

- Fairness: Services should be provided to all with partiality or bias;
- Transparency: The public should have access to accurate information in a timely fashion;
- Efficient: Resources should be used economically;
- Accountability: Public administration must be held accountable; and
- Representation: Public administration should represent all peoples and groups within South Africa.

Ngxesha (2015:5) further mentions Chapter 11 of the MFMA, Act 56 of 2003, provides for processes and procedures to be adopted by municipalities when dealing with procurement activities; to address the limitations associated with procurement legislations.

“Section 111 of the Act stipulates that each municipality and each municipal entity must have and implement SCM policy which will give effect to section 110 of the Act. According to section 112(1) of the Act, the public sector procurement management policy of a municipality must be fair, equitable, transparent, competitive, and cost-effective and comply with a prescribed regulatory framework for municipal procurement management which must cover, inter alia:

- *Open and transparent pre-qualification processes for tenders or other bids;*
- *Implement measures for combating fraud, corruption, favouritism and unfair and irregular practices in municipal procurement management and;*
- *Promote ethics of officials and other role players involved in municipal procurement management”.*

2.8.3.2 Management of public procurement in South Africa

It has been the emphasis of Ambelm and Badenhorst-weiss (2012:246) that “in South Africa, SCM is an important tool for managing public procurement”. Prudent financial management is supported by SCM because it “operates within a regulatory framework set by the national government and extended by provinces and local government bodies to specific policies, legislation and regulations”. It is the views of Ngxesha (2015:25) that SCM is the integration of key business processes across the supply chain for the purpose of adding value for customers and stakeholders.

According to Ambelm and Badenhorst-weiss (2012:246), *“The aim of SCM is to add value at each stage of the procurement process – from the demand for goods or services to their acquisition, managing the logistics process, and finally, after use, to their disposal. In so doing, SCM aims to address deficiencies in current practice relating to procurement, contract management, inventory and asset control and obsolescence planning. Adoption of an SCM policy thus ensures uniformity in bid and contract documentation, and options and bid and procedure standards, inter alia, will promote the standardisation of SCM practices.”*

Ambe (2016:279) also maintains that SCM is “a guide for accounting officers (for national departments, municipalities, and entities) which was developed to provide guidance on the adoption of the integrated SCM function and its related managerial responsibilities assigned to accounting officers in terms of sections 62 and 95 of the MFMA, and section 76 (4) of the PFMA of 1999”. Each part of the SCM cycle and the operational processes for accounting officers is explained within these guides, with the aim of giving manager a flexible framework that is both constitutionally transparent and accountable.

2.8.3.3 Categories of public procurement

Procurement as confirmed by Woods and Mantzaris (2012:113–114) “takes place at different levels in a typical public sector organisation, depending on the value of the transaction”. The authors above identify three different levels:

- Day-to-day purchases;
- Middle range purchases; and
- Higher value range purchases.

According to Woods and Mantzaris (2012:113–114), day to day purchases include “incidental stationery, cleaning materials, staff refreshments and other consumables, for which there are few specific procurement rules”. Middle range purchases, however, “are of a higher value which are subject to particular rules of competition, usually in the form of having to obtain a few competing quotations from different suppliers prior to awarding the business to a particular supplier”. Lastly, higher value range purchases are “above a predetermined amount of money” and generally will be subject to “more complex and stringent rules… known as competitive tendering”.

According to Bolton (2016:11) there are three main stages of procurement which are the planning stage, evaluation and award stage, and the contract performance stage. Van Der Waldt (2007:205), agreed with Bolton, by mentioning the following different stages of public procurement:

- **Demand management**: The first stage of the SCM process, demand management involves market and commodity analysis to determine the needs, specifications, and potential suppliers of the end buyer as well as the budget.
- **Acquisition management**: This takes place after demand management and is the process of acquiring goods and services. This stage involves:
    - The development of a plan to procure the good and services;
    - The preparation of the documents needed to bid;
    - The process of marketing the bids;
    - The development of the bid assessment criteria;
    - The selection of preferred suppliers or bidders;
    - The contract documentation preparation; and
    - The process of signing the relevant contracts.

  This stage is guided by applicable legislation, namely the PPPFA, Act 5 of 2000, the BBBEE Act 53 of 2003 and the MFMA 56 of 2003.
- **Logistics management**: This stage of SCM "involves contract and inventory management. The process includes ordering, receiving, and coding stock items, distributing stock to customers and managing the warehouse and the transport fleet" (Van der Waldt, 2007:205).
- **Disposal management**: An assessment of stock items is made to identify what is longer functional or required and must be disposed of. The process also includes the development of a disposal policy, calculating depreciation rates and maintaining a database of all redundant items. "Items must be disposed of in terms of the policy determined by the unit within the national and/or provincial department" (Van der Waldt, 2007:205).
- **Risk management**: This stage involves the management and cover of risk and residual risk (Ngcamphalala & Ambelm, 2016:1210).
- **Performance management**: "The objective of an SCM system is to ensure that goods and services are procured fairly, equitably, transparently, competitively and cost-effectively so that the goals of the national and/or provincial department are achieved. Therefore, performance management involves monitoring processes retrospectively to determine whether the objectives and goals have been achieved" (Ambelm & Badenhorst-Weiss, 2011:14).

2.8.3.4 Range of procurement process

In clause 10 of the CoT SCM Policy Amendment Report (*SCM Policy Amendment Report,* 2019), approved on 28 November 2019, goods and services procured of the value of purchase (VAT inclusive) are as highlighted in the Table 2.1, below.

Table 2.1: Value of the CoT purchase threshold

Value of purchase VAT (inclusive)	**Procurement method**	**Delegated Authority**	**Oversight Role**
R0 up to R2000	Petty cash	Group Head	City Manager CFO
R2001 up to R10 000	Written Quotations	Chief Buyer – Acquisition	Head of SCM
R10 001 up to R30 000	Three formal quotations through the e-Procurement rotation system	Chief Buyer releases the PO	Head of SCM
R30 001 up to R200 000	Formal written price quotations, in compliance with the Act: - sealed and placed in box; - advertised for seven days on noticeboards and website of the CoT; and - allocated in accordance with the points system	Director: Acquisition Management	Head of SCM and CFO
Tenders above R200 000 up to R10 million and long-term contracts	Competitive bidding process: - advertised for at least fourteen (14) days on notice boards and website of the CoT; - advertised for at least fourteen (14) days in newspapers commonly circulating locally but not limited thereto; and - allocated in accordance with the points system	Bid Adjudication Committee	City Manager
Tenders above R10 million and long term	A competitive bidding process: - advertised for at least 30 (thirty) days on notice boards and website of Council; - advertised for at least thirty (30) days in newspapers commonly circulating locally but not limited thereto; and - allocated in accordance with the points system	Bid Adjudication Committee recommends to the City Manager	Council

Panel appointment	R2 001-R10 000	Group Head	CFO
	R10 000-R30 000	Group Head	CFO
	R30 000-R200 000	Group Head	CFO
	R200 000 - R2 Million	Bid Adjudication Committee	City Manager
	R2 Million – R10 Million	Bid Adjudication Committee	City Manager
	Above R10 million open tender process	Bid Adjudication Committee recommends to the City Manager	Council

CoT SCM Policy Amendment Report (2019:37-39)

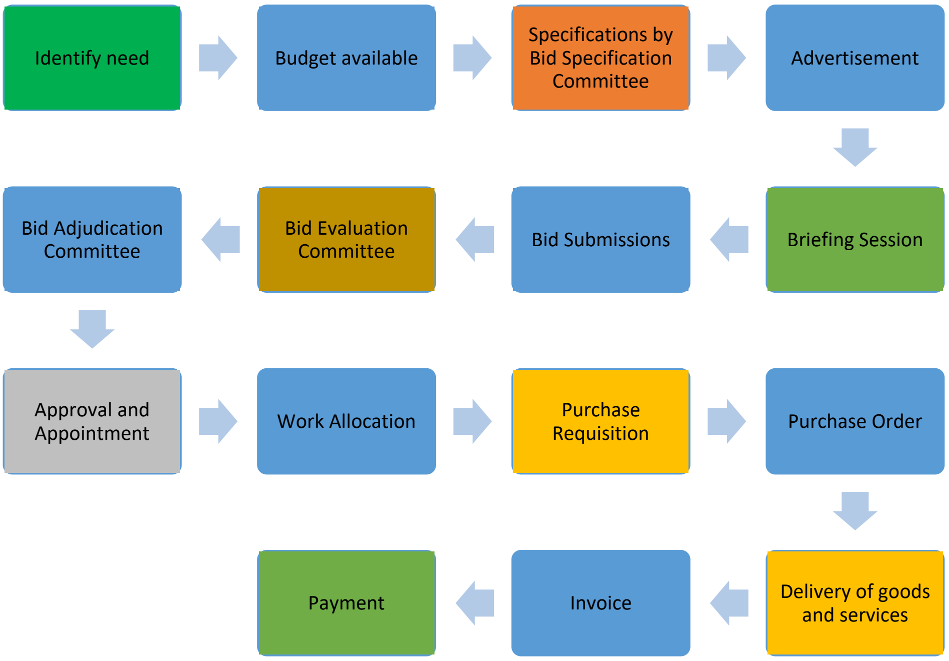
2.8.3.5 Process flow of public procurement

According to Badiru and Tacz (2016:378-379) there are 6 contract management key process areas in the public procurement:

- **Procurement Planning**: The process focusses on whether or not to, how to, what to, how much to, and when to procure based on what will meet the organisations needs the best;
- **Solicitation Planning**: Documenting program requirements, taking note of potential sources and planning and preparing which documents are needed to support the solicitation;
- **Solicitation**: Obtaining bids or proposals from prospective sellers addressing how needs can be met;
- **Source Selection**: Receiving bids and evaluating each provider based on the requirements;
- **Contract Administration**: Ensuring that contractual requirements are met; and
- **Contract Closeout**: Verifying all administrative tasks to complete a physically finished contract.

From his experience, the researcher believes that procurement process is comprised of the 15 steps as indicated in Figure 2.1 below:

Figure 2.1: **Public procurement process flow chart** (designed by the researcher)



It is worth noting that, as perceived by the researcher and illustrated in Figure 2.1, above, the procurement of any good and services will start with need identification which will be based and aligned to the available budget. Specification will be drafted and approved by the Bid Specification Committee (BSC). The tender will then be advertised. The companies and entities that are interested in the bid will attend the briefing session on how to complete their bids. After the submission of bids, Bid Evaluation Committee (BEC) will evaluate, and Bid Adjudication Committee (BAC) will adjudicate and recommend for the approval by the City Manager. Upon the approval the appointment letter will be issued and then allocation of work can begin from this stage. Before any services could be delivered, purchase requisition (PR) is created, and PO issued. Services can then be delivered, followed by the submission of the invoice and subsequent payment to the service provider. The principles of e-Procurement were further discussed in detail below.

2.8.4 The principles of e-Procurement

It is the opinion of Anthony (2018:45) who share the same views with Van Greunen et al. (2010:3656) when he highlights that Section 217 of the Constitution of the Republic of South Africa dictate that when government is contracting for goods and services, it should do so in accordance with a system which is fair, equitable, transparent, competitive, and cost-effective.

2.8.4.1 Fairness

Anthony (2018:45) indicated that “fairness in this context refers to equal access to the process and procedurally fair evaluation of bids”. Contracts are advertised electronically which leads to an accessible and equal platform for all bidders. Bids are evaluated using a mathematical formula the ensures that there can be no human interference, and that all bidders are considered fairly.

2.8.4.2 Equitable

Anthony (2018:45) sustains that “equality in the South African public procurement context refers to substantive equality”. Section 9 of the Constitution is used to evaluate contractors. To address previously disadvantaged groups, contractors’ socio-economic circumstances are taken into consideration when bids are evaluated. A 90/10 BBBEE formula is used.

In support of the views of Anthony (2018:45), IRMA (2013:1179) is of the opinion that in “light of the discrimination under the previous government in South Africa, public procurement has been used as a policy instrument for socio-economic transformation”. However, just because preference is granted to disadvantaged individuals does not meant that the right to equality and fairness (set out in section 217 of the Constitution) is violated.

2.8.4.3 Transparency

According to Anthony (2018:46), “throughout the tender process, bidders will be aware of the competing bids and the contents thereof”. However, the integrity of the process is maintained as the identity of the bidders is not revealed to prevent collusion. Thus, only the information required to participate in the process, the outcome of the process and the reasons and the evaluation of the bidders is all available to the bidders.

Sithole (2017:48) is of the opinion that “e-Procurement systems provide all records of transactions implemented within the system”. Transparency in paramount during procurement processes and e-Procurement audit trails make transparency simple. Bidders can request de-briefs about the success of their bid.

2.8.4.4 Competitiveness

It is the view of Sithole (2017:44) that e-Procurement entails that advertisement and publication must be done in the electronic platform. This means that more competitors take part in the bidding procedures, and this increases the competitive environment. Anthony (2018:46) concurs with Sithole (2017:44) by sustaining “that a minimum number of bidders should be indicated in the invitation to tender so as to ensure effective competition”.

2.8.4.5 Cost-effective

It was the suggestion of Anthony (2018:46) that e-Procurement should reduce “administrative costs, and significantly decrease the quantity of paper involved in a procurement process”. E-Procurement is faster than a traditional tender processes, leading to a more cost-effective system in compliance with section 217 of the Constitution of the Republic of South Africa.

2.9 INTERNATIONAL BEST PRACTICES OF E-PROCUREMENT

According to Bof and Previtali (2010:2) “the purchasing of goods and services in the public sector is central because it supports all functions of government; each governmental unit needs supplies and equipment to accomplish its mission”. In the public sector, e-Procurement is an umbrella term for a variety of technologies that digitise both the internal and external processes to procure goods and services. Globally, e-Procurement evolving and broadly being accepted.

In this section, the researcher presents an overview of international e-Procurement best practices, its implementations, and benefits. The international countries that are advanced in the implementation of e-Procurement are as follows and will be discussed in detail below: Turkey, Czech Republic, USA, Malaysia, China, Australia, Sweden, India, Denmark and Indonesia.

2.9.1 The E-Procurement system in Turkey and its benefit

An example of the advantage of e-Procurement can be seen in Turkey. According to Akkaynak (2004:5), in 2002, Turkey introduced a new law called Public Procurement Law No. 4734 (PPL) complying with the United Nations Standards, which was a crucial step on their electronic public procurement. “With this law, an independent central administrative authority, namely Public Procurement Authority (PPA), was established in order to regulate and audit the public procurement system” (Akkaynak, 2004:5). Through the implementation of e-Procurement, “competition, transparency, reliability, confidentiality and equal treatment and public supervision in public procurement were guaranteed” and by integrating an online platform for advertising tender notices, they allowed the administrations create and advertise tender notices with fewer mistakes that could be approved easily and expedite the process.

Akkaynak (2004:5) further indicated that the president of PPA Mr. Sener Akkaynak declared the goal of PPA to be: “*to ensure that public procurements, in all procurement methods, are completely carried out on electronic media. By this way, all proceedings* *will be carried out according to the rules on computer by putting a computer between buyer and supplier*".

As part of the benefits of e-Procurement system in Turkey, and as highlighted by Shakya (2017:135), it checks, verify, and confirm blacklisted companies before issuing a contract to prevent awarding of contract to the blacklisted companies. It will also detect fake documents submitted by the suppliers and collection of monthly procurement data.

In support of Shakya (2017:135), Pablos et al. (2013:134) sustain that e-Procurement in Turkey ensure the control by automatically organising the documents during procurement process. It also enables staff and auditors to carry out their audits easily as the system can remove risks of losing or mismatching the documents.

2.9.2 E-Procurement in the Czech Republic and its benefit

It is the opinion of Pomazalovà (2013: 215) that "the Czech Republic law on e-Procurement was based on two EU Directives-2004/18/EC of the European Parliament and the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts on one hand and 2004/17/EC of the European Parliament and the Council of 31 March 2004 on the coordinating the procurement procedures of entities operating in the water, energy, transport and postal services on the other hand".

Furthermore, Pomazalovà (2013:215) further maintains that the Czech Republic "law on e-Procurement consists of Act No. 137/2006 Coll. on Public Contracts and Act No. 139 Coll. on Concession Contracts and Concession Procedures". A strategic framework to allow for the implementation of ICT technologies into the procedure of public procurement. The main goal was to give all contractors within the private and public sector the IT support tools for complex public procurement procedures and removed all legislative, financial, and technological barriers while saving up to $50 billion.

The major benefit of the e-Procurement in Czech Republic is that it aided a statistical feature that helped strengthen the role of public as a watchdog of activities of public administration particularly public procurement. Corruption and bribery are the most frequent crimes in the public procurement and therefore requires e-Procurement to control (International Conference on e-Government (ICEG), 2010:193)

2.9.3 E-Procurement in the United States of America (USA) and its benefit

It is the views of the authors such as Pomazalovà (2013:73), who sustain that in 2006, e-Procurement fuelled USA government public procurement to become 18.42% of the world's Gross Domestic Product (GDP). The purpose of USA e-Procurement system was to promote the use of web-based systems across different industries, to promote transparency about transactions involving contractors and bureaucratic participants, bring down administrative costs and purchasing price through higher levels of efficiency and accessibility within the bidding process. According to Pomazalovà (2013:73) "it not only increased trust, accessibility and [transparency, but also] contributed to the innovation and creativity of the administration which was necessary in the design and implementation of e-Procurement system".

The benefit of e-Procurement in the USA, according to Thai (2019:486) is that it frees procurement staff from evaluation and contract management. This is to prevent staff to collude and circumvent the procurement process. It also permits the monitoring of compliance. Furthermore, information or data can be extracted for the purpose of conducting audits.

2.9.4 E-Procurement in Malaysia and its benefit

According to Pomazalovà (2013:280), to "improve service delivery, transparency, and subsequently good governance, the Malaysian government introduced the e-Procurement system; whereby the whole process of procurement is automated".

The system caused the shift by public organisations from purchasing goods using paper-based systems to electronic-based purchases. The benefits anticipated were cost savings, time efficiency as well as the more general having better access to suppliers. As long as the company is registered with the Malaysian Ministry of Finance, public organisations can purchase from them, although suppliers need to be registered within the e-Procurement system.

It is the opinion of the authors such as Pablos et al. (2013:148) that the benefits of e-Procurement in Malaysia is that it reduces errors in the procurement process. It is an intelligent data entry which eliminates data re-entry to prevent duplicates invoicing. It also prevents collusion and corruption.

2.9.5 E-Procurement in China and its benefit

According to Lin, Li, Dong and Qin (2010: 299) Chinese "government procurement has gradually become more standardised and large scale in recent year". In 2006, China issued the standards of e-Procurement, "including standards of architecture, security and selection of software components, plug-in software and the functional requirements which should be achieved" (Lin, Li, Dong & Qin, 2010: 299). Other than typical government office automation, e-Procurement is a special system designed for the transactions between government and enterprises and it has its own unique characteristics.

Salkute and Manager (2013:108) suggest that one of the major benefits of e-Procurement in China is the reduction of "unauthorised buying, more highly organised information and tighter integration of the procurement function with key back-office systems". Tighter control over the supply chain and effectiveness leads to the proactive management of key procurement data to detect any malicious intent amongst the procurement staff.

Salkute and Manager (2013:109) further indicate that another e-Procurement benefit is its logical security, database management and the ability for data recovery. Any misplaced or deleted data will be easily recovered for audit purpose.

2.9.6 E-Procurement in Australia and its benefit

There has been increasing uptake of e-Procurement with a wide of benefits to the construction sector In Australia. The e-commerce technologies applications in the construction supply chain specifically described the transition from paper-based methods to the use of electronic commerce in construction supply chain management as a typical example of IT innovation in construction (Imbe & Laryea, 2014:105).

In support of Imbe and Laryea (2014:105), Eadie, Perera, Heaney and Carlisle (2007:103) describe Australian e-Procurement as a system which brought the improvements to all aspects of the procurement process. Eadie, et al. (2007:108) further ranked the following drivers (benefits) of e-Procurement in Australia in the order of importance as:

- Price reduction in tendering;
- Negotiated unit cost reduction;
- Improved visibility of customer demand;
- Reduced administration costs;
- Improved market intelligence;
- Reduced operational and inventory costs;
- Enhanced decision making;
- Improved contract compliance;
- Shortened procurement cycle times;
- Improved visibility of SCM;
- Increased accuracy of production capacity; and
- Enhanced inventory management.

The following are the barriers to e-Procurement in Australia identified by Eadie, et al. (2007:108) and ranked in order of importance as:

- Inadequate technical infrastructure;
- Lack of skilled personnel;
- Inadequate technological infrastructure of business partners;
- Lack of integration with business partners;
- Implementation costs, company culture;

- Inadequate business processes to support e-Procurement;
- Regulatory and legal controls;
- Security;
- Co-operation of business partners;
- Inadequate e-Procurement solutions; and
- Top management support.

2.9.7 E-Procurement in Sweden and its benefit

Engström, Wallström and Salehi-Sangari (2014:315) argue that "e-Procurement within Swedish government authorities evolved significantly between 2001 and 2008" in the fields of stationery and medical supplies. The implementation of e-Procurement in Sweden, according to Engström et al. (2014:317) resulted in benefits such as both time and money saved. Better compliance with supplier contracts, and spending is more controlled. Furthermore, above the board access to information became easier through a standardised, purchasing processes. On the other hand, a few major challenges were identified, mainly ICT technical issues such as slow access to information.

It is the opinion of Parida and Parida (2005:6) that e-Procurement's benefits in Sweden "fall into two major categories: efficiency and effectiveness". Efficiency causes "lower procurement costs, faster cycle times, reduced maverick or unauthorised buying well organised reporting information, and tighter integration of the procurement functions with key back-office systems" (Parida & Parida, 2005:6). Effectiveness relates to "increased control over the supply chain, proactive management of the key data, and higher-quality purchasing decision within organisations" (Parida & Parida, 2005:6). Parida and Parida (2005:6) further argue that while "the benefits of e-Procurement are frequently discussed, it has its share of risks". Aside from technical problems, integrating new technologies with existing information systems also bring risks in.

2.9.8 E-Procurement in India and its benefit

According to Panduranga (2016:3) the “e-Procurement system is considered as one the best initiative taken by the Government of India to enhance transparency in public procurement”. The Government e-Procurement System of National Informatics Centre (GePNIC) is used to process goods, services and works. Government e-Procurement System of National Informatics Centre is generic software that enhances tender transparency and creates an environment of non-discrimination amongst bidders, as all tender documents are available free of charge.

Furthermore, Panduranga (2016:4) suggest the following as the benefit of e-Procurement in India:

- **Wide publicity**: It is mandatory that all tender documents are publicised on the e-Procurement system and vendors thus have easy access;
- **Easy to participate**: It is quite easy for the vendors to participate in the public procurement tenders as all required documents are scanned and uploaded onto the system, which also generates an acknowledgment for submission of the online tenders;
- **Large numbers of bidders**: More bids are received for online tenders due to the accessibility and ease of participation;
- **Transparency**: E-Procurement system eliminates discrimination as all bidders can view all other bids. All the bids are evaluated as per the tender specifications, and this promotes transparency; and
- **Check on corruption**: There is a possibility of corruption in traditional manual tendering. But this does not persist under e-Procurement system.

2.9.9 E-Procurement in Denmark and its benefit

As emphasised by Henriksen and Mahnke (2005:1) Denmark is amongst the forerunners in Europe to adopt the public e-Procurement system. Danish successful adoption of e-Procurement lead to potential benefits, such as reduced transaction costs, more efficient operations, and a foundation for informed decision making. In addition to the above, Henriksen and Mahnke (2005:4) argue that e-Procurement of supplies “represents the greatest potential for savings”.

It is the opinion of authors such as Neupane et al. (2012:308) that Denmark and other least developed countries uses e-Procurement systems as a key tool to reduce and control corruption by opening competition in government procurement processes to the public. Neupane et al. (2012:308) point out some of the benefits of e-Procurement system in Denmark as follows:

- E-Procurement centralise data in order to improve audit and analysis;
- E-Procurement eliminates the direct human interaction on bidding process;
- Reduces corruption significantly, and increase internal efficiency in government departments;
- Monitor all the procurement works and services more easily and efficiently;
- E-procurement system provides better status monitoring and tracking of applications;
- It ameliorates transparency and improves better interaction between supplier and vendors and citizens through online system; and
- Online bidding system automatically reduces the cartel, collusion, and riggings among the bidders.

2.9.10 E-Procurement in Indonesia and its benefit

According to Lewis-Faupel, Neggers, Olken and Pande (2014:9), “Indonesia began rolling out a “semi-electronic procurement” (SEP) system in 2004”. Under SEP, vendors can easily register interest, download detailed bidding and technical information qualification documents, submit the materials to qualify, and even post enquiries and feedback online.

Zahra, Chariri, Rohman and Karim (2017:1003) concur with Lewis-Faupel, et al. (2014:9) when they mentioned that e-Procurement in Indonesia “is a public procurement information system for the procurement committee and the public goods and service providers which creates transparency”. Furthermore, Zahra, et al. (2017:1003), maintain that “e-Procurement is a government-created control system to meet the transparency needs of the procurement process to the public and that it is also a control system designed in such a way as to control budget execution, especially in procurement of goods and services for efficiency purposes”. In support of Lewis-Faupel et al. (2014:9) and Zahra et al., (2017:1003), Wicaksono, Urumsah and Asmui (2017:1) highlight that “the Indonesian government has adopted technology for many purposes including procurement process, and that its e-Procurement is an online system that can streamline the procurement process”. Wicaksono, et al., (2017:1) further emphasise that the potential benefits of Indonesian e-Procurement are:

- Greater effectiveness and transparency;
- Improve accountability; and
- Reducing corruption risks.

Indonesian e-Procurement system, as alluded by Wicaksono, et al. (2017:4) assist to “monitor and control the quality of the procurement process”. Bidding processes can be monitored online at any time. It also “helps the government to prevent, detect, and investigate fraud in the procurement process” (Wicaksono, et al., 2017:4). In agreement with other authors such as Lewis-Faupel, et al. (2014:9), Wicaksono et al. (2017:4) and Zahra et al. (2017:1003), Candra and Gunawan (2016:1) advise that in Indonesia, “procurement of goods and services electronically increase transparency and accountability, improve market access and healthy competition, as well as improving the efficiency of the procurement process, of course it also indirectly support the process of monitoring and auditing, and meet the needs of information access in real-time”. E-Procurement causes transparent and good governance in the state procurement of goods and services.

Therefore, via inference from various literature sources relating to international best practices, the majority of the developed and developing countries’ government agenda is to “increase transparency and accountability in public procurement” through e-Procurement (Candra & Gunawan, 2016:1). The greater levels of success were found to take place in developed countries like Korea, Singapore, Denmark, Japan, and Australia. The Korean government’s successful implementation of e-Procurement led to other countries following their example, including Hong Kong, Vietnam, Pakistan, and Sri Lanka.

E-Procurement assists the state with transparent and accountable procurement processes. For instance, the Government of India a further example of how transparent government procurement activities reduces the opportunities for corruption. Another example is the republic of Bangladesh. National e-Procurement public tenders significantly reduced corruption and collusive bidding practices in Bangladesh.

From the review of various literature sources, the researcher observed and therefore concludes that besides the different approaches to e-Procurement adoption and implementation by governments around the globe, the business models and benefits are more likely the same. The following are some overarching benefits of e-Procurement reviewed in the different countries:

- Promote the principle of competition, transparency, reliability, confidentiality and equal treatment;
- Cost saving and time efficiency;
- Reduce administrative cost and purchasing price;
- E-Procurement did not only increased trust, accessibility and transparency, but also contributed to the innovation and creativity in procurement process;
- To monitor compliance with procurement regulations;
- To confirm blacklisted companies before issuing of a contract and to prevent awarding of contract to the blacklisted companies; and
- To contribute in reducing corruption and collusive practices.

2.10 CHAPTER SUMMARY

In this chapter, it has been established that the governments, companies, and entities started implementing the e-Procurement way back in 1960s. There are lots of benefits of e-Procurement for example from lowering costs, reengineering of procurement and added efficiency of workflow. Despite the benefits, there are also lots of challenges in the adoption and implementation of e-Procurement, like for instance, lack of adequate IT infrastructure and qualified workforce.

It has also been established that e-Procurement has different models such as EDI, B2B, buy-side and sell-side model, and neutral (independent) marketplace. E-Procurement has technology applications such as e-tendering, e-sourcing, e-MRO, and Web based ERP and EDI. Internet connectivity, reliable websites, adequate security mechanisms, audit trail and effective communication are factors to consider when implementing an e-Procurement system to function properly and to produce best intended results.

It has been further established that catalogue management, user maintenance, billing management, price establishment, and system management are the key components of e-Procurement. There are different models and approaches to e-Procurement adoption and implementation by different governments around the globe, however, the benefits are the same. There is widespread consensus among various authors of the benefits of an e-Procurement system.

This chapter has also recognised that the South African Constitution is the guiding principle of all procurement practices and requires that the process must be fair, equitable, transparent, competitiveness and cost effective. Different legislative frameworks were augmented in detail in this chapter. To fully conceptualise e-Procurement and to benchmark, systems and processes implemented in the international countries that are more advanced in e-Procurement such as USA, China and Indonesia were also discussed. Chapter Three includes a brief overview of electronic data recovery to unpack and theoretically contextualise this concept and follow for discussion.

CHAPTER THREE
AN OVERVIEW OF ELECTRONIC DATA RECOVERY

3.1 INTRODUCTION

According to Ngomane (2010:3) “for millions of people worldwide the use of computers has become a central part of life”. Technology is harnessed by criminals as well as state enterprises. Thus, there is a new way to gather information called ‘electronic evidence’. Ngomane (2010:3), further indicate that “the legal requirements that the collected electronic evidence must satisfy for it to be admissible in court are relevance, reliability, and authenticity”. Moussa (2021:3) concur with Ngomane by defining electronic evidence as “any electronic information that has a strength or proven value stored, transmitted, extracted, or acquired from computers, information networks, and that can be collected and analysed by using special hardware, software, or technological applications”.

In support of Ngomane (2010:3) Ndara (2013:50) is of the view that electronic evidence is quite unique, compared with other forms of documentary evidence, and it is very fragile. Ndara (2013:50) further maintain that acquisition or collection of this kind of evidence must be handled carefully, in a controlled environment, by trained professionals. When the computer crime has been committed, forensic investigator can deploy the electronic data recovery software to assist in the salvaging of crucial evidence. There are several commercial and open-source tools available to recover electronic data (Holt et al., 2018:536).

It is vital, according to Ngomane (2010:37), that “the electronic evidence must be recovered properly and legally because if not, it will be excluded as evidence in court”. Furthermore, Bryant (2008:70), states that the investigator handling electronic evidence should have established specialist knowledge and practiced using tried and tested investigative techniques and methodology to collect such evidence.

It is the opinion of Kanellis (2006:58) that electronic evidence needs to be collected correctly to ensure its integrity and value as evidence in court. Kanellis (2006:273) further mention that "securing and collecting electronic evidence with proper care is a general forensic and procedural principle that should always be applied". The source of electronic data, and the hardware that can be searched to collect evidence requires the assistance of technical experts in this field of digital forensics, are just some of the challenges that arise when handling digital evidence (Moussa, 2021:3).

This chapter provides an overview of the importance of electronic data recovery, followed by in depth discussion of techniques and types of electronic data recovery. It will also provide discussions on different data recovery tools, sources, chain of custody, the Locard principle and international best practice of electronic data recovery.

After reading this chapter, forensic investigators will have an improved understanding of a conceptual overview of electronic data recovery. They will also gain an insight of electronic data recovery. It will also expand the forensic investigator's knowledge of different electronic data recovery applications to deploy during the investigation of e-Procurement fraud.

3.2 ELECTRONIC DATA AND ITS SIGNIFICANCE

Electronic data literally refers to electronic evidence and is therefore defined by Casey (2011:7) "as any electronic information created on a computer that can link a crime and a suspect". However, other possible locations where electronic data can be stored, as explained by Lange and Nimsger (2009:72), is external hard drives, memory sticks, cloud-based internet storage, memory cards, network servers and email servers. In support of Casey (2011:1), Ngomane (2010:28) pointed out that electronic data is "information that is stored electronically on a computer and that can be used as evidence in court". Electronic evidence as confirmed by Ndara (2013:6) is "any data stored or transmitted using a computer that supports or refutes a theory of how an offence occurred or that addresses a critical element of the offence such as intent or alibi".

The importance of electronic data as advised by Casey (2011:6) is that electronic records provide evidence about when events occurred, the location of victims and suspects, records of communication, even communication about intent to commit crime. Cornick (2014:163) is of the opinion that electronic data is significant because even if the data is deleted or destroyed, it can be reconstructed or recovered. In simple terms, it means electronic data is evidence that never dies.

The significance of electronic data is also illustrated by Casey (2011:3) who pointed out that it can be used to resolve wide range of crimes such as homicides, sex offences, missing persons, child abuse, drug dealing, terrorism, and other white-collar crimes because organised criminals also use technology to communicate, recruit and to launder money. Civil cases are also depending on electronic evidence as part of their routine in resolving civil disputes.

From the researcher's experience, it has been observed that another important factor of electronic data is that everyone using an electronic device of any kind, even the most advanced criminals will always leave behind the incriminating information. This electronic audit trail "can be used to present influential legal evidence against a suspected criminal" (Cornick, 2014:163). An electronic trail can be dubbed a 'digital fingerprint' that can be used much like a physical fingerprint to as evidence. Challenges encountered during electronic data recovery follow for discussion.

3.3 CHALLENGES EXPERIENCED TO RECOVER ELECTRONIC DATA

With the development of technology, both data storage industry has been improved greatly. But, meanwhile, with data storage increasingly advanced and diverse, data recovery is meeting more and more fresh challenges (Shirley, 2017:1).

3.3.1 Virtualisation of storage devices

Virtualisation as suggested by Joysula, Orr and Page (2012:2) "is the creation of a virtual version of an operating system, computing device" (such as servers), storage device, or network devices whereby several virtual machines are connected to a single server using hypervisor technology. The advance of technology is beneficial, especially more virtualisation, however, it does make data recovery more challenging when data is deleted. This is partly because, in a virtual environment, one piece of physical hardware controls many virtual machines and if damaged, all the virtual machines are also corrupted.

As mentioned by Tipton and Nozaki (2012:407), it is important to note that there are no commercial forensic tools that provides for the recovery or analysis of the media that utilises VMware called Virtual Machines File System (VMFS). This create a serious challenge, as it is unlikely that the files deleted by a malicious third party will be able to be recovered from VMFS formatted disk.

3.3.2 Solid state drives

Hassan and Hijazi (2017:234) are of the opinion that Solid State Drives (SSD) utilises the TRIM command, which removes the deleted file data blocks instantly to create space for new files. The TRIM technique speeds up the writing process. Some SSDs execute TRIM at intervals, while others do so instantly after each deletion. Recovering data from SSD with TRIM command enabled is a considerable challenge, and at times, impossible. In support of the views of Hassan and Hijazi (2017:234), Graves (2014:435) pointed out that SSD are significantly faster than conventional magnetic drives, however the data deleted form SSD is much more difficult to recover.

3.3.3 Data encryption

According to Graves (2014:347) encryption poses a unique challenge to the forensic investigators. Most, if not all, encrypted drives and folders will be password protected and cracking password is not a simple process. The other common challenge of encryption as pointed out by Dufrasne, Fridli and Greenfield (2019:22) is that “if all copies of encryption key are lost (whether intentionally or accidentally) it is longer possible to decrypt the data”. These data will be completely lost as it is not feasible to decrypt and recover the encrypted data without the encryption key.

3.3.4 Damaged or destroyed hard drives

It is the opinion of Vacca (2009:316) that damage caused by fire, flood, earthquake, landslides, and other catastrophes often results in loss of electronic data. The handling of damaged or destroyed equipment require some degree of training and expertise. Any improper handling of damaged or destroyed computers is a leading cause lost data, as the moment a drive has been handled improperly, the chances of data recovery are low. It is the submission of Tereikovskyi, Mussiraliyeva, Kosyuk, Bolatbek and Tereikovska (2018:1559) that vibration exposure is one of the most effective methods of damaging computer systems especially the hard drive. There is no protection for the hard drive against the acoustic-vibrational effect of infra sounds. The acoustic-vibration's influence on the hard drive and the possibility of damaging it or data stored on it, is higher.

Battula, Rani, Prasad and Sudha (2009:29), share the same views with Tereikovskyi et al. (2018:1559) that the most common ways hard drives are damaged include:

- Physically damage or destruction: "If the disk is bent so that the head can no longer function there is no documented method for commercially viable recovery";
- Degaussing the drive: using a powerful magnet to destroy the drive's digital patterns; and
- Overwriting the drive's data so that it cannot be recovered.

Various CAATs and software follow for discussion.

3.4 COMPUTER ASSISTED AUDIT TECHNIQUES

Computer assisted audit techniques is defined by Al-Hiyard, Al Said and Hattab (2019:2) as robust audit tools to detect errors and fraud such as the existence of duplicate transactions, missing transactions, and anomalies. Therefore, auditors should utilise computer software applications to conduct the audit procedures in an efficient and effective manner.

In support of the views of Al-Hiyard et al. (2019:2), Champlain (2003:278) further defined CAATs as any computer programs or applications that has been designed to "enhance the efficiency and effectiveness of an audit and investigation process through automation of previously manual procedures".

Puttick, Esch and Kana (2007:492) concur with Champlain (2003:278) when they mentioned that CAATs are computer programs forensic auditors uses as part of the audit and investigation procedures to process data of audit and investigative significance contained in the companies' information systems. It is the opinion of authors such as Cascarino (2013:118) that CAATs are "information retrieval and analysis programs and procedures including programs that organise, combine, extract, and analyse information". The advantage of CAATs according to Cascarion (2012:118) is an increased "productivity, creativity, and the application of a consistent [audit and investigation] methodology".

3.4.1 Various computer assisted audit tools and software applications

According to the Association of Certified Fraud Examiners (ACFE), (2019:3.746) the most prominent CAATs software applications are as follows:

3.4.1.1 ACL

ACL is "analyst-recognised risk management, compliance, and audit platform that combines all business units into a single solution and gives an accurate view of risk and opportunities across the entire organisation" (ACFE, 2019:3.746).

3.4.1.2 IDEA

Ghani, Ismail and Saidin (2016:37) provide that "IDEA, is the software that can read the data in read-only mode, without changing the original data content". This software is useful when analysing financial and operation data and determining risk for auditors.

3.4.1.3 Excel

Excel, as pointed out by Carlberg (2018:2), “has a large array of tools that bear directly on analytics, including various mathematical and statistical functions that calculates logarithms, regression statistics, matrix multiplication and inversion, and many of other tools needed for different kinds of analytics”.

3.4.1.4 SAS

Hughes (2016:2) explain that SAS is a “software designed to automate data ingestion, cleaning, transformation, analysis, presentation, and other data-centric processes”.

3.4.1.5 Oversight

Oversight consolidates data from any source system and thus transforms auditing and risk management to analyse spend efficiently. “With a complete view, it makes better spend decisions, correct out-of-policy behaviour, eliminate cash leakage, and maximise audit efficiency enterprise-wide” (ACFE, 2019:3.746).

3.4.1.6 Arbutus

According to ACFE (2019:3.746), “arbutus provides specific data access and analysis capabilities for detecting fraud”. Arbutus assists fraud examiners and forensic investigators to “test and compare all type of organisational data, whether financial, operational or security”.

3.5 CAPACITY AND QUALITIES OF THE CYBER CRIME INVESTIGATOR IN TERMS OF ELECTRONIC DATA RECOVERY

According to Hayes (2015:10) “it is important to understand that computer forensics is a multidiscipline field that requires the skills from the field of computer science, criminal justice, law, mathematics, forensic science and linguistics”. This person must possess vast understanding of operating systems as well as the associated file systems of each operating system. Being able to locate and retrieve the evidentiary files is not sufficient. An investigator needs to have the investigative abilities to prove the connection between evidence with the suspect. Hayes (2015:10) gives the example that the “investigator must be able to prove that a suspect was in control of a computer when files were stored in that specific computer memory”.

In support of Hayes (2015:10), Shinder and Tittel (2002:137) indicated that every computer forensics investigator should have:

- “A basic understanding of computer science: knowledge of how computers work (including both hardware and software);
- An understanding of computer networking protocols: how network intrusions and attacks work;
- Knowledge of computer jargon: unique vocational jargon;
- An understanding of hacker culture: should be an expert in hacker culture; and
- Knowledge of computer and networking security issues: should be familiar with common security “holes”, security products (such as firewalls) and security policies and practices”.

Casey (2011:7) elaborates on this by saying that “when a person deals with data held in a computer, as evidence, such a person should be qualified to do the task and to testify, elaborating the importance and the involvement of their actions”. The investigator finds Casey helpful in this regard, because his own experience shoes that computer crime investigators need a wide range of computer investigative skills within different cases. Vacca (2002:4) believes that investigators thus need an adequate level of experience, and that only a trained and experienced investigator should handle computer evidence, as with an untrained investigator, the evidence will be unusable in a case.

According to Humphries, Nordvik, Manifavas, Cobley and Sorell (2021:1) forensic investigators responsible for electronic data recovery needs effective training for handling digital evidence to ensure verification, validity and accuracy which will guarantee that data was unaltered and undamaged. That is why Davis, Philip and Cowen (2005:58) argue that the most crucial part of an investigation of this nature in the immediately seizure of electronic data. Casey (2011:7) comments that doing so correctly is a challenge that requires the right skill set, thus his insistence on an experienced investigator. Fisher (2004:193) agrees and recommends that “an expert should be consulted to seize” and extract any data from a computer. Mendell (2004:242) furthermore corroborates Fisher (2004:193) and Vacca’s (2002:4) arguments, adding that “no computer investigator should arrive at the witness stand without having a clear understanding of investigation”.

This was confirmed by Maras (2015:367) that the forensic investigators will be required to provide his or her qualifications as a technical or expert and creditable witness when testifying and that they “must be prepared to answer questions relating to their work experience (position occupied and employment history), educational background, training, licenses, certificates, memberships in professional organisations, awards, publications, and previous testimony provided in other similar cases”.

Maras (2015:367) further indicates that not only must forensic investigators be experts, but they also need to be able to transfer their expertise by explaining how things about computers work in a layperson’s terms. He or she “must be able to explain complex processes in a simple and easy to understand manner”, says Maras (2015:367). This is because while recovery of electronic evidence from devices is complex, the forensic investigator must be able to testify about the data and method used to extract the data were to explain how the evidence was extracted. He or she must also be able to justify the use of a particular forensic tool to recover the evidence.

Mozayani and Noziglia (2006:84) concur with Maras (2015:367) when they highlight that the investigator must have the skills and experience to “be in a better position to present the electronic evidence to the courts considering that the judiciary has limited knowledge not only of the processes followed in the collection, preservation and analysis of electronic evidence but also in the underlying science and technology involved in this regard”. In addition, Tipton and Nozaki (2006:1884) indicated that the endeavours to win a case in a court of law require a skilled expert witness, who is able to clearly explain complex technology in a layman’s terms.

3.6 FORENSIC ELECTRONIC DATA RECOVERY STEPS

According to Cascarino (2013:399) when a computer crime is suspected to have been committed, “all subsequent steps must be specifically designed to promote the accumulation of accurate information and establish control for retrieval and handling of electronic evidence”. Gathering of electronic evidence that must be forensically acceptable will commonly involve methods to prevent contamination, such as isolating the information source. It is also important that the evidence be credible and able to withstand public and court scrutiny.

It is the view of Jahankhani, Watson, Me and Leonhardt (2010:325) that “common methods to achieve the goal of finding digital” evidence is comprised of the following steps:

- Locating the data;
- Seizing the data; and
- Recovering the data.

It is the suggestion of Maras (2015:34), that “there are four distinct steps”, rather than three, for electronic evidence recovery: “acquisition, identification, evaluation and presentation”. Holt et al. (2018:529) share a similar view with Maras (2015:34) by claiming that the procedures of forensic data recovery is complex process which involves the following steps:

- Identification of potential source;
- Collection or acquisition;
- Examination or analysis of recovered data; and
- Presentation of findings.

Solomon, Barrett and Broom (2015:2) identifies critical steps of electronic data recovery as “identifying, preserving, analysing and presenting digital evidence in a manner that is acceptable in a legal proceeding”. To avoid “accidental invalidation or destruction of evidence and to preserve evidence for later analysis”, an investigator must be experienced and competent within the field of computer hardware and software, as well as an understanding of “regional, national and international laws affecting the process of collection and retention of electronic evidence" (Solomon et al., 2015:2). According to Solomon et al. (2015:2), "this is especially true in cases involving attacks that may be waged from a widely distributed system located in many separate regions". The basic tenets of digital forensics encompass four areas as mentioned by Daniels and Daniels (2018:11) and are as follows:

- Acquisition;
- Preservation;
- Analysis; and
- Presentation.

Marcella and Greenfield (2002:18) agree with Solomon et al. (2015:2) and Daniels and Daniels (2018:11) by claiming that "computer forensics deals with the presentation, identification, extraction, and documentation of electronic evidence". Marcella and Greenfield (2002:18) further bring to light the statement that "this field is relatively new to the private sector, but it has been the mainstay of technology-related investigations and intelligence gathering in law enforcement and military agencies since the mid-1980s". Computer forensics, like other fields of forensic science, follows scientific procedures and utilises sophisticated technology tools guarantee accuracy when preserving evidence presenting results based on electronic evidence processing.

Vandermeer, Le-Khac, Kechadi and Carthy (2019:3) demonstrate that there are specific software tools aimed to support the first responder (in the crime scene) to carry out live data forensics tasks to identify and preserve electronic evidence. Newman (2007:4), and Kruse and Heiser (2002:2) express similar views in highlighting the analytical and investigative techniques of electronic data recovery and magnetic storage on the binary number system "as those activities associated with the identification and preservation of computer or electronic evidence in support of some official or legal action". Kruse and Heiser (2002:2)'s study of the methodology of electronic data recovery includes:

- Acquiring the evidence safely;
- Authenticating the recovered evidence as matching the original; and
- Analysing the data without modifying it.

Nelson, Philips and Steuart (2015:02) suggest that electronic data recovery “involves obtaining and analysing digital information for use as evidence in civil, criminal, or administrative cases”. Additionally, and as further outlined by Nelson et al. (2015:02), that this process entails “scientifically examining and analysing data from computer storage media so that the data can be used as evidence in court”.

In support of other authors above, Peterson and Shenoi (2009:39) advise that operating steps “are an important issue in the field of digital forensics”. Due to the quality validity and credibility electronic evidence being impacted by the forensic process that was taken. They further emphasise that these general procedures “should be flexible rather than being limited to a particular process or system” owing to the uniqueness of cases, changing technology and different legislations (Peterson & Shenoi, 2009:39).

The researcher focused on the four steps of electronic data recovery as outlined by Holt et al. (2018:529) and Maras (2015:34) for further discussion.

3.6.1 Identification phase

According to Holt et al. (2018:529) the identification stage is where forensic investigators “survey the physical and digital crime scene to identify potential sources of digital evidence”. Marcella and Menendez (2008:286) are of the view that the first thing the digital forensic investigators should do is to secure the scene. After securing the scene, forensic investigator should identify potential evidence visually, whether it is physical or electronic. They must then isolate and collect all suspected electronic devices. Computers and their evidence “must be handled carefully and in a manner that preserves [their] evidential value” (Marcella & Menendez, 2008:286). For instance, some electronic evidence must be collected using special packaging and transportation.

When seizing a computer, according to Marcella and Menendez (2008:290) the forensic investigator must adhere to the following rules:

- Isolate computers and other electronic devices, marking them according to their unique barcodes or identification numbers and seal in the evidence bag;
- Ensure the safety of the seized equipment;
- Do change the physical condition of the seized equipment or any devices;
- If the computer is on, look and listen for any drive activity before pulling the plug; and
- Document the process carefully to create a permanent historical record of the scene.

Casey (2011:227) concurs with Holt et al., and Marcella and Menendez when he suggested that digital crime scene “can contain many pieces of evidence” and “it is therefore necessary to apply the principles of survey, preserve and document the entire scene” (Casey, 2011:227). Thus, physical as well as digital evidence at a scene must be processed methodically and correctly. According to Mandia and Prosise (2003:199) and emphasised by Holt et al. (2018:529) computer crime scene must be documented properly, as “failure to adequately document activities when attending the scene” is both a common mistake and majorly problematic mistake.

According to Reddy, Sureka, Chakravarthy and Bhalla (2017:25) the digital forensic process starts with identification of the data also known as artifacts. The different devices and data transfer leaves different types of artifacts, which must be identified as the first part of the process. Kanellis (2006:59) points out that, to be able to identify potential electronic evidence, the investigator must have extensive knowledge of computer hardware and software, including operating systems, file systems, and cryptographic algorithms. Additionally, from the researcher’s experience, an investigator must be able to explain the origin of the evidence and the reasons why the evidence is important to the case under investigation. Given that the evidence can be interpreted from several different perspectives, it was the view of Kanellis (2006:59) that identification phase determines the context in which the evidence was found. It looks at both the physical environment and the logical context of the location of electronic evidence.

Steel (2006:18) describes the documentation of the scene as the most important action in the field of computer forensics. Steel (2006:18) believes that in documenting the scene, two individuals are recommended: one person to processes the scene while the other is responsible for documenting everything found on the scene. Ndara (2013:58) is supported by Steel (2006:18), in that investigators must work together to properly document the scene of computer crimes. As part of scene documentation, Girard (2015:21), sustain that the "chain of custody or a written chronological record of each person who had an item of evidence in his or her possession" must be always maintained.

In support of Girard (2015:21), Mandia and Prosise (2003:199), Ndara (2013:58) further highlights that the scene of computer crime "must be documented and also photographed, including taking photographs of data and electronic devices". Steel (2006:19) explains which items should be photographed:

- **Computer screens**: The screen should be captured with in high resolution and with a steadied camera (like on a tripod), to allow investigators to read the text captured;
- **Network connections**: "The connections to and from the computer must be photographed very closely, to capture the details of the connections that will also prove that the computer was connected to a specific network or phone at the time of arrival" An image-capturing camera should be used rather than a video camera to ensure quality; and
- **Peripheral connections**: "Connections to peripherals must be photographed at very close range. This will help to reassemble and prove the connection that will be needed later".

Boddington (2016:104) concurs with Steel (2006:19) by emphasising that standard procedure to be considered in the crime scene is to take photographs and record video footage of the computer monitor and any image that is displayed on the screen. To take notes of each exhibit such as its position in the crime scene, any cables connected and any removable devices, should be a routine procedure by the forensic investigators.

The researcher therefore concludes based on his own experience and information from reviewed studies that, it is best practice to take photographs or video recording of the scene of computer crime for future reference and evidence presentation during court proceedings. Once the physical and digital crime scene are investigated and potential sources of digital evidence are seized, the next is stage collection or acquisition, which follows for discussion below.

3.6.2 Collection or acquisition phase

The collection or acquisition stage involves the process of electronic data retrieval and preservation (Maras, 2015:34). One of the critical issues in electronic data recovery as explained by Johnson (2014:187) is acquisition and preservation of evidence in order to maintain the chain of custody and ensure “that it is gathered and protected through a structured processes that are acceptable to the courts” (Johnson, 2014:187).

According to Holt et al., (2018:530) retrieval and preservation of electronic data is a “process of making an exact copy (bit-by-bit) of the original drive into a new digital device”. This process is known as imaging. Holt et al., (2018:529) further contends that the “goal of evidence preservation in digital forensic is to make a copy of the original data files for examination in a way that minimises the possibility of any changes being made to the original data files”. Digital forensics has the tools to make duplicates, allowing the original source of evidence to remain intact.

In support of the views of Holt et al. (2018:529), Brown (2010:8) explains another collection technique involved the imaging of the system suspected of being compromised by “copying the entire drive at the binary level, or the data can be copied into a digital evidence bag”. Once it’s copied, it needs to be saved as ‘read-only’, which prevents it from being tampered with.

As pointed out by Holt et al. (2018:531), after the data have been imaged it must be verified. Verification establishes the integrity of the electronic evidence by demonstrating that the duplicate is the same as the original, meaning that it is a true and unaltered copy of the original data source. Digital forensic investigators as alluded by Holt et al. (2018:531) verify the duplicate copy by comparing hash algorithm values of the original source. A hash algorithm is a set of calculations that takes any amount of data (input) and create a fixed-length value (output), known as hash, which acts as a unique reference number for the original data. Nelson et al. (2015:254), sustains that is it vital that the investigator at this stage of electronic evidence recovery “make a copy of the original drive” to preserve and protect the original.

Vacca (2011:67) is of the view that “digital evidence collection process allows the investigator not only to locate key evidence, but also maintains the integrity and reliability of that evidence”. Brown (2010:8) concurs with Vacca (2011:67) by stating that “the methods used for the collection of electronic evidence can be one of the most highly scrutinised areas of the computer forensics process”. Well established and tested collection methodologies must be used. According to Brown (2010:8) the collection stage of computer forensics is when artefacts that store digital data such “as disk drives, flash memory drives, or other forms of digital media and data” are collected. However, the process can also include the collection of supporting evidence such as “corporate security policies, operating manuals, and backup procedures” (Brown, 2010:8)

As described by Brown (2010:8), there are forensic software that are available to investigators to collecting data correctly. Forensic software has the ability to enable the computer forensic investigator “to collect and digitally sign a container that electronically stores evidence” to prevent tampering and preserve it for court and corporate use.

It is vital to correctly identify and collect digital evidence while maintaining its integrity to allow it to be legally admissible in court. Thus, every step of the process needs to be documented, and as must all evidence. The investigator must therefore be familiar with which tools to use to collect, preserve and protect evidence (Kanellis, Kiountouzis, Kolokotronics & Martakos, 2006:58). According to Wahyudi et al. (2018:1) electronic data recovery deals with a sequence of identifying and collecting evidence and ensuring that the integrity and authenticity of the evidence is maintained.

According to Holt et al. (2018:530) imaging is the one of the crucial steps in the preservation process of digital evidence and must be done in the following sequence:

- Before imaging, the new digital storage device should go through the **wiping** process to clean it of electronic data that could potentially contaminate the imaging process;
- While imaging a drive, the investigator should use a **write blocker** device to ensure that their investigation is forensically sound. “To be forensically sound the tool must eliminate the possibility of making changes to the original data source” (Holt et al., 2018:530). To achieve this, forensic investigator must make use of a device called a write blocker. According to Holt et al. (2018:530) a “write blocker allows read-only access to all accessible data on a drive, as well as preventing anything from being written to the original drive, which would alter or modify the original evidence”; and
- Verification must take place through digital fingerprints called **hash values**. “Hash values are fixed in length and made up of a unique combination of hexadecimal digits (which can be numbers 0-9 or the letters a-g)” (Holt et al., 2018:531). Hash values are useful because they accurately represent changes in the original data. They are created in a process known as **hashing**. There are two common hash algorithms: Message Digest Version 5 (MD5) and Secure Hash Algorithm (SHA). The MD5 hash algorithm produces a unique string of 32 digits as a 128-bit hash value, whereas SHA is 160-bit unique value

According to Holt et al. (2018:532), the “imaging and verification process of data preservation is extremely important in order to maintain the integrity of digital evidence”. Hash values verify imaged drives’ authenticity, and will continue to be used, however, data collection, preservation and data protection relies on digital forensic tools (Holt et al., 2018:534).

From his experience and information obtained from literature review, the researcher therefore conclude that it is best practice that when imaging, use the new devices to store the data for analysis. This will ensure and validate that the data is the exact copy of the original source. Once the digital drive is imaged and verified, the next stage is the examination or analysis of data.

3.6.3 Examination or analysis phase

It is the suggestion of Maras (2015:37) that, in the examination stage, the data collected during acquisition stage “are analysed to establish their significance and relevance to the case at hand”, as well as authenticated as valid and reliable. According to Holt et al. (2018:544) the examination or analysis phase of “digital forensic investigation is concerned with the recovery of electronic data”. The data recovery process is the extraction or salvaging of digital information relevant to the case under investigation.

ACFE (2012:99) provides list of short and relevant keywords relevant to the investigation that should be established during analysis. As the case progresses, more keywords will be identified when digital evidence is analysed. Furthermore, specialised software tools and procedures using search terms can help identify patterns in the data (Solomon et al., 2015:2).

During the examination stage, as mentioned by Holt et al. (2018:559), the investigator must do what is known as data filtering, which involves “removing duplicate files, searching for keywords, or grouping data based on file types”. Filtering the dataset will increases the efficiency of the investigation. The goal of data reduction and filtering is creating the smallest dataset with the highest potential of containing relevant digital evidence.

From his experience and information obtained from literature review, the researcher therefore recommend that the analysis or examination must only be conducted on the duplicate copy not original drive as it will be required as evidence in court in line with the best evidence rule. After the examination of the data, the forensic examiner must present the findings in a form of a report to the relevant structure or organisation. The presentation of the findings will follow for discussion.

3.6.4 Presentation of findings

The presentation of a forensic examiner’s findings, filtered to be relevant, is the last step in the process of forensic analysis of electronic evidence as confirmed by Daniel and Daniel (2012:13) Holt et al. (2018:559) concur with Daniels and Daniels (2012:13) by indicating that presentation is the final stage in the digital forensic investigation and that the findings determined to be relevant, as well as well-documented and transparent, to the investigation are finalised in a report with an unbiased conclusion.

Daniels and Daniels (2012:13) further advises that presentation not only includes written findings but also the drafting of the affidavit, deposition of expert testament and providing testimony as a witness in court. There are however no set of rules or standard in reporting the results of forensic examination. Each agency or entity may have its own guidelines for reporting. However, the examination report should be written clearly, precisely, accurately and should include the following important information:

- Background and experience of the examiner;
- Collection methods used;
- Specific steps taken to protect and preserve the original evidence;
- Explaining what was examined;
- Tools used in the examination;
- Methods used to verify that data;
- Processes used to recover and extract the data;
- Statement of what was found; and
- Actual data recovered to support the statement of findings.

Casey (2011:667) is of the opinion that when the investigator dealt with number of computers during analysis, it is convenient “to create a main report describing the overall examination and several more focused reports dealing with logical groupings of computers or machines analysed”.

Holt et al. (2018:558) further recommends the deployment of an independent forensic examiner to “verify the findings of the initial examination”. The independent examiner needs to enter the process unaware of the conclusion established by the initial investigator. The final report reflects both the integrity of the evidence and the forensic examiner.

According to Purpura (2013:298) diagrams and photographs may be attached on the examination report. Vacca (2011:14) explains that the examination report should provide an opinion on the following:

- The computer system layout;
- The file structures discovered;
- Any discovered data and authorship information;
- Any attempts to hide, delete, protect and encrypt information; and
- And anything else that has been discovered and appears to be relevant to the overall computer system examination.

It is apparent from the information obtained during the literature review that a forensic examiner should use straightforward, clear language when reporting the findings. From his experience, the researcher therefore concludes when writing a comprehensive report, forensic examiner should also keep neatness and good grammar in mind when formulating a report. It must be an easy to read and simple report to present in the relevant structures and forums such as court of law or tribunals.

3.7 PROCESS OF EXAMINING ELECTRONIC DATA (END-TO-END)

According to Ashcroft, Daniels and Hart (2019:1), the examination of electronic data is the process of analysing the data after it has been imaged and preserved. The persons “conducting an examination of digital evidence should be trained for this purpose”. The examination of electronic data must only be conducted on a duplicate copy of original data because data is fragile by nature and it is easy to alter, damage or destroy evidence. Wiles and Reyes (2007:11) concur with Ashcroft et al. (2019:1) when they sustain that “analysis should be done on the duplicate copy so that the original evidence can be protected from alteration because the first rule of forensics is to preserve the original evidence”.

Ashcroft et al. (2019:7) further pointed out that before examination could begin, conduct a thorough assessment of the case, and consider the following:

- Ensure there is legal authority for forensic examination request (request for service form must be signed and approved);
- Understand the allegation and the specifications of the case;
- Request the names of potential or possible suspect from the case investigator;
- Acquire the keywords relevant to the case;
- Discuss the possibility of pursuing other investigative avenues to obtain additional digital evidence. For example, sending a preservation order to an Internet Service Provider (ISP), identifying remote storage locations, and obtaining of e-mails;
- Consider the relevance of peripheral components to the investigation. For example, in forgery or fraud cases consider non-computer equipment such as laminators, credit card blanks, check paper, scanners, and printers. In child pornography cases consider digital cameras;
- Determine the potential evidence being sought. For example, photographs, spreadsheets, documents, databases, financial records;
- Determine additional information regarding the case such as e-mail accounts, e-mail addresses, ISP used, names, network configuration and users, system logs, passwords, usernames. This information may be obtained through interviews with the system administrator, users, and employees;
- Assess the skill levels of the computer users involved. Techniques employed by skilled users to conceal or destroy evidence may be more sophisticated;
- Prioritise the order in which evidence is to be examined;
- Determine if additional personnel will be needed; and
- Determine the equipment needed.

It is the opinion of Kävrestad (2018:4) that when preparing for examination one need a proper order to collect correct data. The order in this case will include a person or devices to collect data from. It is also important as suggested by Wiles and Reyes (2007:10) to prepare should one be required to extract information from volatile data sources such as memory circuits as this kind of data needs consistent power supply for storage. Another technical consideration highlighted by Kävrestad (2018:4) is if one should expect encrypted or password-protected data.

Documentation and accurate records of every step of should be an ongoing process throughout the examination. "During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority" (Ashcroft et al., 2019:19). When this evidence is documented and identified by the case investigator, it assists in establishing an additional scope of work.

In support of the views of Ashcroft et al. (2019:19), Casey (2011:473) advises that the "primary purpose of documentation at forensic examination and analysis stage is to support a repeatable process, while allowing flexibility to accommodate unforeseen situation". A "repeatable process" allows for a high level of consistency of quality of across the board "on different cases by different digital investigators, reducing the chance of mistakes or omissions" (Casey, 2011:473).

From his experience, the researcher believes that it is equally important for the forensic examiner to take and keep the examiner's notes of the entire examination process (for example names, dates, times, and steps undertaken). This will assist the examiner to accurately report their results and findings. Examination of electronic data as highlighted by Ashcroft et al. (2019:15) entails "the extraction and the analysis of digital evidence". Extraction is the collection of data. Analysis refers to the investigation the copied data and process of creating a report from it. Different types of data extraction techniques and analysis follows for discussion.

3.7.1 Data extraction techniques

3.7.1.1 Manual extraction

According to Goodison, Davis and Jackson (2015:5), manual techniques are the most basic type of extraction, and “involve using standard inputs included with or built into the device, such as touch screens or keyboards”. It is beneficial for the operator to have a general understanding of file structure and operating systems, but few tools are required. Manual extraction is similar in structure as looking for a file on a computer using the standardised tools of a mouse and a keyboard, meaning that some functions, for instance, deleted items, are inaccessible.

3.7.1.2 Physical extraction

Holt et al. (2018:545) suggest that physical extraction identifies and recover “data across the entire physical drive regardless of the file system present on the drive”. There are three methods mentioned by Holt et al. (2018:545) are keyword search, file carving, and “extraction of the partition table and unused space on the physical drive”.

(a) Keyword search

Keyword search, according to Holt et al. (2018:545), is when “the digital forensic examiner is able to look for a word or series of words in the entire physical drive regardless of the file system”. Keyword searching, as indicated by Casey (2010:116), provides the “greatest potential to drastically reduce the volume of data to a manageable and reviewable level”. Keyword searching requires some technical skill from the operator, as a good understanding of the process is vital to deliver results that are complete and accurate.

It is the views of the authors such as Ashcroft et al. (2019:15) that “performing a keyword search across the physical drive may be useful as it allows the examiner to extract data that may not be accounted for by the operating system and file system”. In support of Ashcroft et al. (2019:15) is of the opinion that “keyword searching allows the quick identification of notable words an information, typically retrieved from the remit or the background information". The skill to be able to identify relevant keywords is vital. There are two main techniques, according to Ashcroft et al. (2019:15):

- **"Index search**: the tool used must be able to index all data, essentially recording every word present, so that it can be searched. This type of search is comprehensive as it does not care about the compression used (whether is PDF, Word or ZIP, it searches every word from all documents); and
- **Real-time search**: keyword can be created and run at any point of the investigation, this type of search takes some time to complete and is unable to search files that are compressed or in unusual formats, unless they are first uncompressed."

According to Casey (2010:126) keywords searching encompasses number of distinctive techniques, namely:

- **Advanced keywords searching concepts**: simple keywords such as "invoice" in a case of e-Procurement fraud can lead to relevant documents;
- **Keyword completion**: allows a search of a word by specifying how a keyword should start but does not specify how the word must end. For example, "gen" will find the word "general", "generation" and "generator". In other words, the search will find all the word that begin with "gen";
- **Boolean expressions**: complex keyword can be constructed to narrow the focus of the search. The Boolean expressions can include AND, OR, NOT, WHERE, WITHIN and AROUND. For example, *quo* w/4 ser*,* search will find all occurrences of the word "quotations" with four "serial" numbers, but it will not find single occurrence of either word; and
- **Keywords stemming**: the search will be able to recognise different words from a certain keyword. For example, for a word "buy", search will find words like "buys", "buying" and "bought" as variations of the word "buy".

From his experience and the review of different literatures, the researcher believes that keywords are the guideline of the relevant data to the investigation that the examiner can mainly focus on when extracting evidence.

(b) File carving

The International Council of Electronic Commerce Consultants (EC-Council), (2010:18) are of the opinion that file carving utilities “processed across the physical drive may assist in recovering and extracting useable files and data that may not be accounted for by the operating system and file system”. File carving, as highlighted by Holt et al. (2018:545), “is the process of searching for a certain file signature and attempting to extract the associated data”, regardless of a file system.

Casey (2010:36) concur with EC-Council (2010:18) and Holt et al. (2018:545) when he mentioned that “file carving tools like Foremost, Scalpel, DataLifter, and PhotoRec can search unallocated spaces for characteristics of certain file types in an effort to salvage deleted files”.

(c) Partition recovery

According to Holt et al. (2018:545), “partition recovery is the process of evaluating the partition table and the unused space on the physical drive”. Thus, “examining the partition structure will identify the file systems present and determine if the entire physical size of the hard drive is accounted for” (Ashcroft et al., 2019:15).

3.7.1.3 Logical extraction

It is the views of Ashcroft et al. (2019:15) who emphases that “logical extraction refers to the process of identifying and recovering data based on the file systems present on the computer hard drive” such as active files, deleted files, file slack, and unallocated file space. In addition, as mentioned by Holt et al. (2018:545), logical extraction may recover electronic data from hidden files, password-protected files, encrypted files, and steganography.

As pointed out by EC-Council (2010:18) logical extraction encompasses the following steps:

- “Extraction of the file system information to reveal characteristics such as directory structure, file attributes, file names, date and time stamps, file size, and file location;
- Data reduction to identify and eliminate known files through the comparison of calculated hash values to authenticated hash values;
- Extraction of files pertinent to the examination; methods to accomplish this may be based on file name and extension, file header, file content, and location on the drive;
- Recovery of deleted files;
- Extraction of password-protected, encrypted, and compressed files;
- Extraction of file slack; and
- Extraction of unallocated spaces”.

In support of the views of other authors such as EC-Council (2010:18), Ashcroft et al. (2019:15) and Holt et al. (2018:545), it is the opinion of Ndara (2013:37) that, there are three types of data that can be extracted. According to Ndara (2013:37), “these are active data, archival data and latent data, which are described as follows:

- Active data is information that can be seen by the naked eye. For example, data files, programs, and operating systems;
- Archival data is that data which has been backed up and stored. For example, floppies and hard drives; and
- Latent data is the data or information that requires special tools to deal with. For example, this may be information that has been deleted or partially overwritten”.

The researcher focused on the extraction of the following compelling evidence or data, which every examiner must consider the data of interest which are deleted, hidden, password-protected, steganography and encrypted files. The forensic question to ask is, why are these files deleted, hidden, password-protected and encrypted?

(a) Deleted file

Girard (2011:407) is of the opinion that many criminals believe that once incriminating files are deleted and the recycling bin is emptied, then the file is gone from the hard drive and cannot be used against them. However, forensic software can recover deleted files and use it as evidence unless the hard drive is overwritten by new data.

(b) Hidden files

According to Graves (2014:135), “hidden files are files that have been manipulated in such a way as to conceal the contents of the original file”. However, a cluster level search tool such as Briggs Software’s Directory Snoop, will allow one to view and extract hidden files.

(c) Password-protected files

Password-protected files, as mentioned by Beaver (2010:92), “are locked files that require a password to gain access”, preventing the files from being accessed. Beaver (2010:93) further maintains that there are “password cracking utilities that takes a set of known passwords and run them through a password-hashing algorithm”. According to Beaver (2010:93), to crack the password, the encrypted file is compared at lightning speed to the passwords extracted from the original databases. When a match is found between the newly generated data and the data in the original databases, then the password has been cracked.

From his experience and review of different literature, the researcher therefore recommends the for the investigators to use of a password modification program called Novell NetWare Password Recovery (NTPASS) which can recover any password stored locally on a windows operating system. This software “is designed to recover the password of up to 36 characters in length, regardless of the use of control character, or alpha-numerical combinations” (Beaver, 2010:92).

(d) Encryption

Holt et al. (2018:544) described encryption as a “process of transforming information (plaintext) so that it is no longer legible (ciphertext) by using a mathematical algorithm”. Most of the encryption programs require keys to access them and decrypt the file. In support of Holt et al. (2018:544), Johnson (2005:105) “is of the view that encryption is a process of scrambling information so that it is not recognisable without descrambling it". Encryption can also be employed for the converse effect, to authenticate and verify information.

Solomon et al. (2015:172) lists software utilities that can be used to “decrypt files:

- Zip Password by LastBit: password recovery utility;
- Passware Password Recovery Software: recover password from Microsoft (MS)-Office application file;
- ElcomSoft password recovery software: recover passwords from various application files”.

(e) Steganography

Holt et al. (2018:546) describe steganography as a “practice of hiding information in such a way that others are not aware that a hidden file exist”, create an environment of secrecy over privacy. Ashcroft et al. (2019:16) concur with Holt et al. (2018:546) by indicating that “steganography is the art” and process of “hiding information by embedding messages” in other, seemingly harmless messages.

3.7.1.4 Chip-off and micro read

Goodison et al. (2015:6) emphasise that chip-off and micro read are the advanced digital evidence extraction which require highly technical expertise to perform. They involve a physical removal of flash memory chips from the electronic devices. According to Goodison et al. (2015:6), “these options of extraction are similar to a microscopic examination of components or to making a physical extraction of a hard drive, though hard drives are far easier to access and generally provide data in an easy to read and interpret format".

In conclusion, Goodison et al. (2015:5) indicate, as shown in Figure 3.1 below that each extraction stage "requires a different skill set and equipment and may yield evidence not obtainable through any other stage".

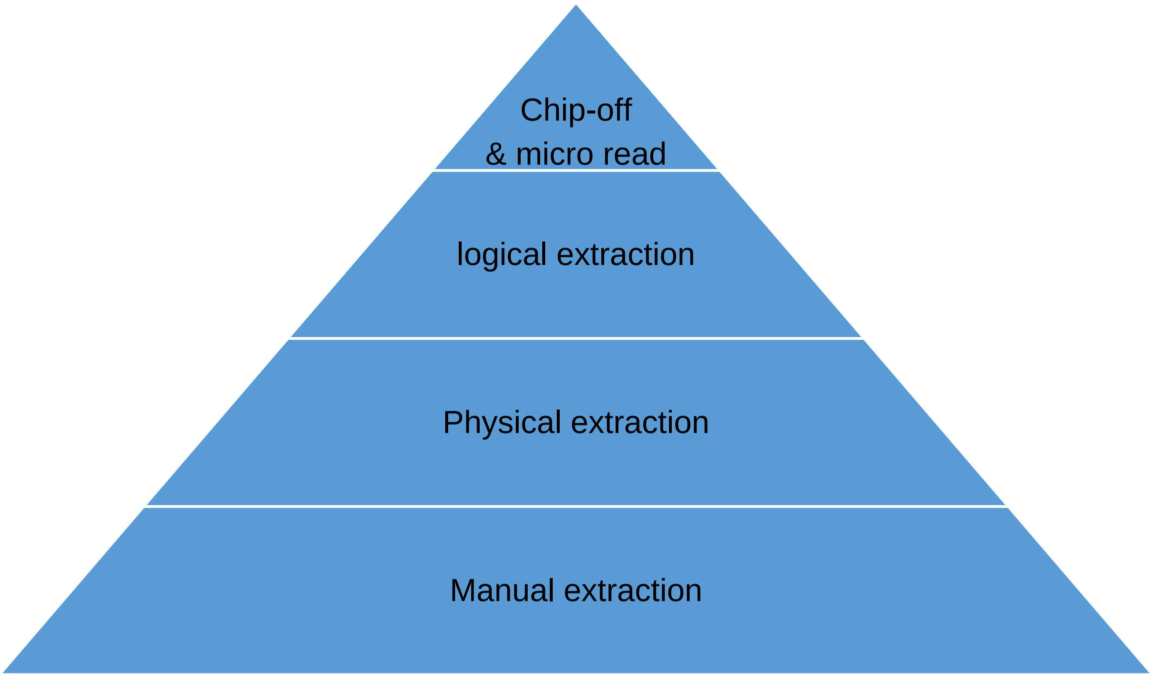


Figure. 3.1 Extraction stages (Goodison et al., 2015:5)

3.7.2 Analysis of extracted data

EC-Council (2010:18) provided that, depending on the file system on the drivers, data is extracted from:

- Active files;
- Deleted files;
- File slack; and
- Unallocated spaces

The data extracted above as highlighted by EC-Council (2010:18), is used to find the following information:

- Directory structure;
- File attributes;
- File names;
- Date and time stamps;
- File size;
- File location;

According to EC-Council (2010:18), the analysis involves examination of the extracted data to resolve the case. The characteristics of data that can be analysed are:

- Time frames;
- Data hiding;
- Application and files;
- Ownership and possession;

In support of EC-Council (2010:18), Ashcroft et al. (2019:16) emphasise that “analysis is the process of interpreting the extracted data to determine their significance to the case”. “Timeframe, data hiding, application and file, and ownership and possession” are examples of interpreting extracted data. Ashcroft et al. (2019:16) further discussed the characteristics of data analysis below:

3.7.2.1 Timeframe analysis

According to Ashcroft et al. (2019:16) “timeframe analysis can be useful in determining when events occurred on a computer system, which can be used as a part of associating usage of the computer to an individual(s) at the time the events occurred”. There are two common methods:

- Metadata review: “Reviewing the time and date stamps contained in the file system metadata (for example, last modified, last accessed, created, change of status) to link files of interest to the timeframes relevant to the investigation. An example of this analysis would be, using the last modified date and time to establish when the contents of a file were last changed" (Ashcroft et al., 2019:16); and

- System and application logs: "These may include error logs, installation logs, connection logs, security logs, etc. For example, examination of a security log may indicate when a username/password combination was used to log into a system" (Ashcroft et al., 2019:16).

3.7.2.2 Data hiding analysis

It is the views of EC-Council (2010:18) that "data can be concealed on a computer system". Using data hiding analysis, the investigator can detect and recover concealed data to prove intent, ownership, or knowledge of a crime. Even if the criminal can destroy or delete data, the investigator can still recover the data from hidden spaces of disks during analysis (Duan & Zhang, 2020:2).

EC-Council (2010:18) further explains that the "methods that can be used include:

- Correlating the file headers to the corresponding file extensions to identify any mismatches. Presence of mismatches may indicate that the user intentionally hides data;
- Gaining access to all password-protected, encrypted, and compressed files, which may indicate an attempt to conceal the data from unauthorised users. A password itself may be as relevant as the contents of the file";
- Using steganography (embedding messages and hiding information in other messages); and
- "Gaining access to a Host-Protected Area (HPA). The presence of user-created data in an HPA may indicate an attempt to conceal data" (EC-Council, 2010:18).

3.7.2.3 Application and file analysis

As pointed out by Ashcroft et al. (2019:16), "many programs and files identified may contain information relevant to the investigation and provide insight into the capability of the system and the knowledge of the user". File analysis can produce results that help the investigator discover “additional steps that need to be taken in the extraction and analysis processes” (Ashcroft et al., 2019:16). File analysis includes reviewing and examining:

- Relevance and patterns between file names;
- File content;
- The type and number of operating systems;
- The files correlated to the installed applications;
- File relationships;
- Similarities between files;
- Internet history compared to cache files;
- E-mail files correlated to e-mail attachments;
- Unknown file types;
- Default storage locations for applications;
- The file structure of the drive;
- User-configuration settings; and
- File metadata.

3.7.2.4 Ownership and possession

One important aspect in digital forensic investigation is to identify and link the perpetrator (usually a human action) to the crime committed, referred to as user attribution as emphasised by (Eze, Speakman & Onwubiko 2020:458). It is useful to the investigator to have determined the owner or potential collaborators of the data in question. In support of Eze et al. (2020:458) and as confirmed by the EC-Council (2010:18) when they highlight that, “in some instances it may be essential to identify the individual(s) who created, modified, or accessed a file”. The analysis described above as well as the following factors can place ownership or knowledge of the data to a subject:

- Proving that, at the specific date and time, the subject was at the computer;
- Demonstrating that files have been stored in unusual ways to avoid detection, or with inaccurate names, such as ‘admin’: “The file name itself may be of evidentiary value and also may indicate the contents of the file” (EC-Council, 2010:18);

- The passwords identified to access encrypted and password-protected files may identify the owner of the files; and
- Specific content or information within a file may identify the owner.

From his experience as a Senior Forensic Audit Specialist responsible for cyber forensic investigations, and from the information obtained during the literature review, the researcher therefore recommends the two most common programs to assist the examiners and forensic investigators to efficiently analyses extracted data:

- **ACL software program**: is a data analytic platform capable of importing and exporting data, joining files, and data filtering. It enables comparison between employees' details and vendor database and can assist in detecting ghost employees; and
- **CaseWare IDEA**: is a versatile data analysis tool that can import data, calculates, matching data, test for unusual transactions and missing or duplicate items. It can assist in detection of e-Procurement fraud such as duplicate payments.

Detailed description and advantages of forensic data recovery tools follows for discussion.

3.8 ELECTRONIC DATA RECOVERY TOOLS

ACFE (2019:3.841) pointed out that there are several data recovery products. These products differ in complexity, features and price, and they also employ various methodologies to extract and analyse data from computers. It is best to use a combination of different tools to gather and analyse evidence. Mohay, Anderson, Collie, de Ville and McKemmish (2003:63) agree with ACFE (2019:3841) and provide that the "growth of the data recovery and electronic evidence discovery industries has been accompanied by similar strong growth in the number of computer forensic tools available and in use". In support of the views of ACFE, Kaspersky (2006:19) emphasised that it is merely impossible to recover data without specialised tool set. Data recovery is industrious and routine work, so if you need to resuscitate a large disk, for example of more than 120 GB in size, you cannot recover data without automation. ACFE (2019:3.481) further list the frequently used products on the market.

3.8.1 EnCase Forensic Software

It is the views of Holt et al. (2018:538) that, EnCase is a computer forensic software “capable of acquiring data from variety of digital devices, including smart phone, hard drives and removable media”. This tool automatically searches the entire drive and can locate hidden and deleted files while it images “the drive, without altering its contents, and then verify that an image is an exact copy of the original drive” (Holt et al., 2018:538).

Mohay et al. (2003:67) concur with Holt et al. (2018:538) when they mention that EnCase is a computer forensic software product that “can image different forms of media, such as SCSI/IDE drives and Zip/Jaz drives as well as RAID disk sets”. EnCase software acquires the evidence and presents it “as a verifiable, proprietary bit-stream image called evidence file mount as a read-only virtual drive and reconstruct the file system structure utilising the logical data in the image”.

3.8.2 Forensic Toolkit

According to Solomon et al. (2015:176), “Forensic Toolkit (FTK) is a suite that provides an integrated user interface and is commonly known as AccessData’s Forensic Toolkit”. The advantage of FTK, aide from it being a powerful tool to examine and image electronic data, is that it runs using the widely distributed Windows operating system. It’s imaging tool also creates more than one copy, if requested to, of the primary evidence to be analysed. In support of Solomon et al. (2015:176), Holt et al. (2018:541) explain that “FTK is capable of imaging a hard drive, scanning slack space, and identifying steganography”, while also cracking passwords for protected files, and accessing encrypted files.

Holt et al. (2018:541) further maintain that "FTK 5 has new capabilities, including:

- Data visualisation tool that creates a timeline; and
- Visual depiction of the social interaction, such as e-mails of the person under investigation".

3.8.3 Password Recovery Toolkit

The Password Recovery Toolkit (PRTK) can crack passwords for a range of file types, and as pointed out by Casey (2011: 270) is the "most powerful and versatile password recovery programs currently available from AccessData". Clarke (2011:72) confirms that PRTK is a useful tool for decrypting data "that could be pertinent to an investigation". With both a "brute force" and a "multilingual" capability, PRTK can "recover passwords from over 80 applications, including Windows SAM file (the file that contain a user's login password for Windows)" (Clarke, 2011:72).

Furthermore, PRTK "is able to generate its own dictionaries based on every permutation of strings stored on the investigation system" (Clarke, 2011:72). In support of Casey (2011: 270) and Clarke (2011:72), Hayes (2015:138) is of the view that PRTK is one of the AccessData's fee-based version of FTK, which contain thousands of different hash values to crack passwords.

3.8.4 ProDiscover Forensics

Bidgoli (2019:842) suggests that ProDiscover is a Windows-based integrated forensic tool which is comprised of four products, namely:

- ProDiscover for Windows;
- ProDiscover Forensics;
- ProDiscover Investigator; and
- ProDiscover Incident Response.

According to Bidgoli (2019:842) the "most prominent difference among the four products is that the ProDiscover Investigator and ProDiscover Incident Response have the capability to conduct live analysis and imaging over transmission control protocol/internet protocol (TCP/IP) networks, whereas ProDiscover for Windows and ProDiscover Forensics are intended for workstation use only and do not include network capabilities". Bidgoli (2019:842) further mentions that imaging with "ProDiscover allows the user to perform array of common forensic tasks, such as searching for keywords, checking for file type extension mismatches, and viewing data in cluster slack space". Slack space is defined by Reddy (2021:24) as the space between the end of the file and the end of the disk cluster where it is stored. ProDiscover, as highlighted by Brown (2010:224) consists of five products. Brown's version contradicts the assertion by Bidgoli (2019:842) who affirm that ProDiscover has four products. In addition to the four mentioned by Bidgoli (2019:842), Brown (2010:224) added ProDiscover Basic Freeware as the fifth product.

Machie (2013:36) concurs with Bidgoli (2019:842) by emphasising that ProDiscover encompasses four products and describes them as follows:

- **ProDiscover for Windows** integrate Windows application for the collection of analysis, management, and reporting of computer disk evidence. It also supports all Windows-based file system, including FAT 12/16/32 and NTFS Dynamic disks;
- **ProDiscover Forensics edition** provides all the capabilities that ProDiscover for Windows does and also includes all supported file system, such as SUN Solaris UFS and Linux Ext2/3;
- **ProDiscover Investigator** takes the ProDiscover Forensics workstation and turns it into a full client/server application, allowing disk preview, imaging, and analysis over any TCP/IP network; and
- **ProDiscover Incident Response** includes all the features of ProDiscover Investigator, and it contain advanced tools for incident response and network preview, imaging, and analysis.

3.8.5 Stego Suite

Stego Suite is software bundle that, as highlighted by ACFE (2019:3.842), is ideal "for detection, analysis and recovery of digital steganography". It is composed of four products:

- **Stego Watch**: a steganography detection tool;
- **Stego Analyst**: an imaging and analysis tool;
- **Stego Break**: a password cracker; and
- **Stego Hunter**: a steganography application identifier.

According to EC-Council (2016:27), "Stego Suite is a tool that identifies the presence of steganography without prior knowledge of the steganography algorithm that might have been used against target file. This is known as blind steganography detection". EC-Council (2016:27) supported the views of ACFE (2019:3.842) by stating that steganography comprises of four tools, namely: StegoHunter, StegoWatch, StegoAnalyst and StegoBreak.

Based on his experience and the reviews of different literatures, the researcher has observed that the most prevalent forensic data recovery tools are EnCase and FTK. By creating an exact copy of the entire hard drive (bit-by-bit), these tools allow investigators to analyse the copy and protect the original evidence against being destroyed or tampered with. These digital forensic imaging tools must produce valid and reliable test result that must be repeatable and reproducible (Holt et al., 2018:535).

Holt et al. (2018:535) further describe the test of repeatability and reproducibility in detail and as follows:

- **"Repeatability** is whereby independent test results are obtained with the same method, on identical test items, in the same laboratory, by the same operator, using the same equipment within short intervals of time. In other words, the digital forensic tool replicates the same results using the exact same methodology; and
- **Reproducibility** is whereby test results are obtained with the same method, on identical test items, in different laboratories, by different operator, using different

> equipment. Thus, digital forensic tool produces the same results even in different testing environment."

In support of the views of Holt et al. (2018:535), Nelson et al. (2015:281) is of the opinion that procedures and validation of computer forensic software tools results demands accuracy "of the testing process, so results must be repeatable and reproducible". **Repeatable** results assume a consistent results from the same lab and the same machine. **Reproducible** results assume the analysis tool will bring up consistent results on a different machine in a different lab.

From the review of different literatures, the researcher therefore concludes that repeatability and reproducibility tests are necessary and important for the forensic tool's results to be admissible in the court of law. Different source of electronic evidence and their detailed description follow for discussion.

3.9 SOURCES OF ELECTRONIC EVIDENCE

Mason and Seng (2017:1) suggest that various devices can create and store data in digital form and such data is regarded as electronic evidence. They further mention the following sources of electronic evidence, amongst others: central unit processor, game consoles, networks, and smart watches. According to ACFE (2012:11), electronic evidence usually refers to evidence extracted from a computer; however, it is not limited to data from computers. It goes far beyond that. Apart from the computer hard drives, there are numerous types of electronics and storages that computer forensic investigators can search for electronic evidence. Electronic evidence, as explained by Nelson, Olson and Simek (2006:6) may resides in numerous different locations within the "technology infrastructure, so it important to ensure that all possibly relevant sources of electronic information are identified".

The views of the authors such as ACFE (2012:11) and Nelson et al. (2006:6) is supported by Biasiotti, Bonnici, Cannataci and Turci (2018:4) when they pointed out that every type of investigation potentially has a digital dimension, i.e., relevant digital information can be traced back and extracted from the electronic devices.

Yavuzcan, Bulbul and Ozel (2013:2) provided that the electronic and peripheral devices that can potentially be harvested for evidence include “computer chips, pagers, cordless landline telephones, copy machines, cellular telephones, hard drives, facsimile machines, printers, multifunction machines (such as printer, scanner, copier, and fax), wireless access points, smart cards, scanners, memory cards and personal digital assistant (PDAs)”, and must be seized by the investigator.

3.9.1 Desktops and laptops

Ferraro and Casey (2005:81) emphasise that “computers are the main source of electronic evidence”. The basic components of a computer that store information are the central processing unit (CPU), memory, input/output (I/O) systems, random access memory (RAM), internal hard drive. The valuable evidence can be recovered from a hard drive for example, it is equally important for the investigators to understand how data are stored on the hard drive. Ashcroft et al. (2019:15) explained that the “hard drive is a sealed box containing rigid platters coated with a substance capable of storing magnetic data”.

In support of the views of Ferraro and Casey (2005:81) and Ashcoft et al. (2019:15), Daniel and Daniel (2012:18) are of the opinion that “computers are often the main source of digital evidence”. Computers contain a massive amount of useful information such as user accounts, log files, time stamps, images, emails. This information can be found in the hard drive or memory (RAM).

3.9.2 Network server and mainframes

ACFE (2012:28) suggested that domain server is the central authentication server on the domain which provides access and authentication to the network. The domain server is where users are created and assigned rights, group memberships, and other security settings. The organisation server will store all the documents and e-mails of all the users. This crucial information can be recovered as most of this information is achieved on the Personal Storage (PST) file.

The views of the ACFE (2012:28) is also expanded in ACFE (2019:3.814), mentioning that most organisations are increasingly storing data and applications on the server. This implies that even if the employee deletes information on his or her computer it will still be on the server and easy for the investigator to get access to such information. As indicated by Lange and Nimsger (2009:79) computer networks are connected to a centralised server and mainframes. A network allows users to share documents, files, emails and having a group scheduling and messaging capabilities. Server and mainframe normally store all the information and transactions by users. It is therefore important for the investigator to examine the serves and mainframe when conducting any computer investigations.

3.9.3 Printers, copiers, scanners and multifunction devices

ACFE (2019:3.812) indicated that printers contain valuable electronic evidence. Many printers have internal hard drives that could contain information relevant to the investigation. Any information sent to and stored by a printer is recoverable unless the printer has overwritten the data. Thus, “when seizing a computer for forensic analysis, it is generally necessary to seize any printers connected to it”. The ACFE (2019:3.812) further alluded that copiers, scanners, and other multifunction devices are machines that provides copying, scanning and faxing functionalities in one device and might have internal storage devices that store relevant data. In fact, almost every copier built since 2002 has a hard drive that stores image of documents that machines have copied, scanned, or emailed. Some copiers store user access records and a history of copies made. It might be possible to retrieve information from a copier’s hard drive that has been deleted. It is generally necessary to seize any copiers and scanners connected to a subject computer.

Printers are useful for collecting evidence due to their memory drives or hard drives. “New printers have memory drives, which may have stored since deleted documents, and some also have hard drives which may contain relevant data” (ACFE, 2019:3.812).

According to Ashcroft et al. (2019:18) printers are connected to the computer via cable “or accessed via an infrared port”. He further stated that “some copiers maintain user access records and history of copies made”, as copiers can have functions such as scanning documents into memory to be printed later.

3.9.4 Removable and Portable Storage Devices

These are “media used to store electrical, magnetic or digital information” (Ashcroft et al., 2019:19). According to Brown (2010:190) the most common types of removable media is floppy disc, optical disc, tape backup system, external hard drives, Universal Serial Bus (USB) and flash media devices. Brown (2010:190) further indicated that understanding how to identify and process removable media can be crucial to many investigations.

According to Mason and Seng (2017:4), USB and external hard drives are secondary storage which is non-volatile and can retain its data when removed from the main device. Bey-Miller, Clarke and van Dyk (2009:369) concur with Mason and Seng (2017:4) by suggesting that external hard drive is exactly the same with internal fixed disk, except that it is not inside the computer. External hard drive can be connected to any computer that has a correct port and can present the investigator with wealth of information if found on the scene of digital crime. Similar to the external hard drive, USB as described by Bey-Miller et al. (2009:370) is a memory card on which you can save data.

3.9.5 Networks

The ACFE (2019: 3.813) insinuate that it is important to “examine the information stored on any network from which the suspect’s traffic flow”. A wealth of information that is separate from suspect’s workstation might be stored on network server. According to ACFE (2019: 3.813) “data stored on network might include documents posted to a suspect’s own home directory on the network, collaborative work saved to a shared folder or directory, email message that have been sent, received, deleted, or archived, calendars, and contact lists”.

As emphasised by Mason and Seng (2017:4), most computers are now connected, or are intermittently connected, to other computers, or a network. Given the trails left by the assortment of logs and files in computers, going online can produce electronic evidence in abundance, including the using of email, connecting to the Internet, and viewing websites, and transferring of files between computers. Other sources of electronic evidence can be obtained from server logs, the contents of devices connected to the network, and the records of traffic activity.

Cascarino (2013:404) advises that in an ongoing computer fraud investigation, “the investigator may have to monitor traffic flowing over the communication network”. This should be done by using packet sniffers to monitor traffic flow. Such activity must be done while the user or suspect is not aware. The accumulated evidence may be used to establish if the investigation should proceed or not. According to Cascarino (2013:404) “monitoring network may identify source addresses on the network as well as to intercept stolen files or downloaded hacker tools”. At its best, such monitoring can “identify the parties involved, determine the timelines of an event, and possibly even assess the skill level or numbers of individuals involved in the illicit activity”.

Cascarino (2013:405) further sustains that “in a covert investigation into the activities on a specific machine, monitoring software may be placed upon the machine to record all email sent and received, keystrokes, images on screen, mouse clicks on the screen, and Internet and intranet sites visited”. Monitoring software can run in “stealth mode” without being detected, allowing information to be gathered for subsequent retrieval. Retrieval can take place manually, or “the software can be used to automatically send the information gathered to the investigator’s machine”.

Thus, it is imperative that no matter the retrieval method, the data collected should be stored “on the target’s machine and while in transit to the investigator” to ensure that the data is not lost (Cascarino, 2013:407). To avoid detection and potentially having the data compromised, the investigator needs to have the basic knowledge to know that “many antivirus and spyware detectors can detect such monitoring and care should be taken to ensure the specific software cannot be detected on the target’s computer”

3.9.6 Personal Storage (PST) data files

ACFE (2019:1.1329) stated that PST is a file is where the e-mails are stored. It is commonly known as Microsoft Office Outlook Data File. E-mails are wealth of information for the investigators as they contain communications between two or more people. E-mail stored on the PST file which can be recovered even after deletion. However, it has its own backdrop as employees “are regularly asked to cull through their old email messages and delete those no longer needed” (ACFE, 2019:1.1329), and some organisations have an auto-delete function that removes emails from the servers at regular intervals.

It is the opinion of Bryant and Bryant (2016:180) who also concur with ACFE (2019:1.1329), when he revealed that e-mail messages can contain a wealth of information about their provenance. An examination of an e-mail’s underlying code (“header”) can provide clues to both the source and route taken by the message in its delivery. E-mail analysis can reveal the source Internet Protocol (IP) address for the particular user. The IP address function is like a telephone number, with each address being allocated to a specific ISP.

According to Mason and Seng (2017:11-12) e-mail servers only permit authorised users to obtain access to the service, usually by means of a username and password. Sources of electronic evidence from servers include logs recording when a user connects to a server, whether to grant access to the Internet or whether to download e-mails. To expand on the views of Mason and Seng, Sorell (2009:85) indicates that the examination of e-mails “is expected to reveal some contact information and certain date and times that might then be correlated with the case under investigation to develop a social calendar of events and timelines”.

3.9.7 Internet browser history

ACFE (2019:1.1331) indicate that internet is used by billions of people worldwide and is a major means of communicating and conducting business globally. It is also a tool for recreation, finding jobs and homes, making travel arrangements, and researching business and investments opportunities. It can also be vastly used to facilitate fraud as well. ACFE (2019:3.811) further suggest that internet browsers often "create temporary files that store information about websites that a user has visited". By being able to access a list of the most recently visit websites, sorted by date and time, the investigator can detect any possible or planned fraudulent activities and to solve crime already committed. For example, the subject may have visited the website about how to hack computer network shortly before the crime was committed.

It is the view of Lillard, Garrison, Schiller, Steele and Murray (2010:256) who also agree with the ACFE (2019:3.811) stating during forensic examination of a "suspect's computer, you might be able to extract firewall logs, internet history, internet browser cache, and temporary internet files". They advise performing a modified search with the dates of the incident under investigation to prepare for internet browser analysis.

From his experience and the information obtained during literature review, the researcher believes that recently most people prefer to use financial-based internet transactions (commonly known as internet banking) to conduct their financial activities. Enormous and useful information such as bank accounts, and banks statements, payment beneficiaries, business partners and associates can be recovered and create leads to the investigation and to uncover the web of deceitful activities.

3.9.8 Mobile devices

Bopape (2015:4) describes a mobile device as "a pocket-sized computing device that has a display screen with a miniature keyboard and/or a touch input". Mobile devices are useful for professional use through their ability to access emails, banking, and e-commerce, as well as personal communication and entertainment (Bopape, 2015:4). They are also a valuable source of evidence.

ACFE (2019:3.813) indicated that the proliferation of smartphones has made them extremely valuable sources of digital evidence. Smartphones "have the ability to store personal data, search the internet, check email, make video calls, download and upload content to and from the internet, take pictures, and record video". This information is crucial in resolving cases. As mentioned by ACFE (2019: 3.836), when seizing a cellular phone device, you must isolate the device and document the phone at the time of seizure. Any supporting devices and information must also be seized. This information includes:

- Removal storage media (commonly known as memory card);
- Cables for transmitting data;
- Power charger; and
- Documentation relating to the devices purchase.

It is the views of ACFE (2019: 3.836) that, the devices should be isolated from the network to prevent:

- The device user from remotely accessing the device to destroy or corrupt data;
- Cross contamination;
- New data overwriting old data; and
- New data from contaminating the existing data.

As pointed out by ACFE (2019:3.837) that, forensic investigator must set the device into flight mode to isolate the device's transceiver but allow other functions to continue running normally. The forensic investigator can only turn off the device by removing the battery instead of using the device's normal shutdown routines. The benefit of turning a phone off include:

- Preserving the call log;
- Preserving the information of the last cell tower location;
- Preventing the overwriting of deleted data; and
- Preventing communication from reaching the device and changing data.

ACFE (2019:3.838) suggest that the forensic investigator should record the device's make, model, and International Mobile Station Equipment Identity (IMEI) number. Usually, this information is found inside the device's battery compartment. After recording the device's identification information, the analysts should remove the device's subscriber identity module (SIM) card and any removable media and extract data from them using forensic tools. The important information that can be recovered from a cellular phone is contact details, SMS, emails, internet search history, bank statements and photos and videos of associates.

Bair (2018:4) categorises that the “actual artefacts that are located on mobile devices” as either **logical** or **physical**. According to Bair (2018:4), “logical data is easy to understand, it can be viewed through the graphical user interface (GUI)”. Examples of logical data include images and text messages, and no specialised tools are needed to extract logical data. However, according to Bair (2018:4), “physical data are the ingredients that make up what the user may be viewing of may have once seen, as in the case where data have been deleted”. Using “the values of the physical encoding within the binary” (Bair, 2018:4), a forensic examiner can locate deleted messages, and using “the special programs” (Bair, 2018:4) needed, the restored message can be examined for evidence.

3.10 MAINTAINING THE CHAIN OF CUSTODY OF ELECTRONIC EVIDENCE

According to Girard (2015:21), the “chain of custody refers to a written chronological record of each person who had an item of evidence in his or her possession”. A common mistake that investigators make is to fail to “maintain proper documentation throughout the recovery process” (Cascarino, 2013:404). The ACFE (2012:37) indicated that a chain of custody forms records of the possession of evidence from initial contact through the evidence lifecycle. In case of media that has been shipped by a courier, the shipping documents will suffice as records of transfer.

It is the submission of Cascarino (2013:404) that for “any forensic examination, the chain of custody must be maintained at all times”. Sammons (2012:52) highlights the journey that a computer taken as evidence goes on: “It is collected, logged in at the lab, stored, checked out for analysis and checked back in for storage”. Throughout this journey, every step of the way should be documented to maintain the integrity of the digital evidence gathered. Digital evidence must be controlled and secured properly, in order to maintain its integrity in court and not be challenged on its forensic acceptability.

Girard (2015:21) maintains that “the prosecution must account for the evidence along every step of the way, from its discovery to its collection, to its analysis, to its storage, to its transfer and throughout the entire process of court proceedings and appeals”.

Cascarino (2013:404) provides a technical example of how investigators can fail to maintain the chain of custody by “altering date and time stamps on evidence systems before recording them can inadvertently destroy the forensic nature of the evidence”. Cascarino also emphasises that the commands used to analyse evidence should be recoded, as well as be trusted and valid commands. He further maintains that “even the very act of installing the tools, if done incorrectly, can overwrite significant evidence and cast doubt on the remaining evidence”.

Barrow and Rufo (2014:145) further maintain that “all evidence collected at a crime scene should be tagged; if the item cannot be tagged, then it should be marked with the following information:

- Description of item;
- Case number;
- Date of collection;
- Location of collection;
- Collector’s name and identifier;
- Brand name; and
- Any serial number or garment information”.

It is the opinion of Barrow and Rufo (2014:145) that the chain of custody does not end after the evidence has been collected. As supported by Sammons (2012:52), Barrow and Rufo (2014:145) maintain that “it is imperative that all contacts made with the evidence after collection are recorded with the following information:

- Who had contact with the evidence?;
- The date and time the evidence was handled;
- The circumstances for the evidence being handled; and
- What changes, if any, were made to the evidence?”.

The following are current CoT processes as stipulated on FS investigation operational methodology:

- Electronic devices seizure form must be completed in full;
- Every step and everyone who came into contact with evidence must be registered on the investigation diary of the project file;
- Chain of custody must be maintained until the report is finalised and submitted, or testimony is provided in internal disciplinary proceedings or criminal court.

3.11 THE LOCARD PRINCIPLE

Sammons (2012:7), defines the Locard principle as the principle that “entails that in the physical world, when a perpetrator enters or leaves a crime scene, they will leave something behind and take something with them”, and expanded upon by Vacca (2011:317) who says that “the Locard principle implies that where there is a contact between two items, there will be an exchange and every contact will always leave a trace”. The digital equivalent of the Locard principle is that suspects, even the most careful, leave traces of their presence that can be detected and analysed with the correct technological tools. Barrow and Rufo (2014:146) indicate that digital traces are “resilient and factual physical evidence that cannot be mistaken”.

The CoT FS investigation operational methodology, explain that Locard principle refers to when two people or objects meet, there will always be evidence left behind to reconstruct the crime scene and to identify the perpetrator. Therefore, when conducting an investigation all aspects related to the irregularity must be scrutinised. The above discussion leads the researcher to conclude that documentation is the most crucial process in the recovery of electronic evidence and shall be done after each step, from the beginning of the investigation until the presentation of the evidence before a court of law.

3.12 THE BEST EVIDENCE RULE

Solomon et al. (2015:60) highlight that the best evidence rule entails that "whenever you introduce documentary evidence, you must consider introducing original document, not a copy". The purpose for this rule is to protect evidence from tampering. If an original document is required, therefore there is less opportunity for modification to occur during copying operation. According to Lange and Nimsger (2009:77), the best evidence rule requires the forensic examiner to produce the original electronic evidence when testifying. However, it does not mean that the original custodian computer, monitor and other equipment must be brought in the courtroom. It makes the provision of data stored on a computer of similar device constitute the original piece of evidence. Other electronic data stored on a computer hard drive qualify as originals under this rule.

Best evidence rule, according to ACFE (2012:89) "demands that the original of any document, photograph or recording be used as evidence at trial, rather than a copy". However, a copy is "allowed or admissible into evidence only if the original is unavailable".

As pointed out by Conrad, Misenar and Feldman (2012:411) "courts prefer the best evidence possible". This relates to using original documents and conclusive tangible objects rather than copies, or oral testimonies. The best evidence rule prefers evidence meets the five criteria for desirable evidence: relevant, authentic, accurate, complete, and convincing.

3.13 INTERNATIONAL BEST PRACTICES IN THE RECOVERY OF ELECTRONIC DATA

According to Suresh and Panigrahi (2015:395), the forensic methodology of electronic data recovery must always be repeatable and defensible. This will avoid making similar mistakes more than once.

The best practice of electronic data recovery, according to Suresh and Panigrahi (2015:395) will involve the seven progressive stages:

- Identification;
- Acquisition;
- Data recovery;
- Analysis of data;
- Data source;
- Documentation; and
- Report and presentation.

Watson and Jones (2013:5) provide that there are number of good practices and standards that have been developed for electronic data recovery to be conducted in manner that is acceptable to the relevant courts of law. In ensuring the potential evidence is handled in a manner that complies with the legal and regulatory requirements, it must align to the standard required for repeatability and consistency. For evidence to be admissible in court, it must have been legally obtained, the good practice for electronic evidence as mentioned by Watson and Jones (2013:5) is that it must be:

- Legally obtained;
- Relevant and complete;
- Reliable and authentic;
- Accurate; and
- Believable.

Holt et al. (2018:535) indicates that it is best practice for digital forensic imaging tools to produce valid and reliable test result that must be repeatable and reproducible. In support of Holt et al. (2018:535), Kruse and Heiser (2002:2) emphasise that the basic methodology for electronic data recovery comprises of the following: “acquire the evidence without altering or damaging the original, authenticate that your recovered evidence is the same as the originally seized data and analyse the data without modifying”. Solomon et al. (2015:13) confirms that electronic data recovery must be conducted by forensic examiners who are properly trained due to the complexity of computer systems and programs. It is good practice to provide training and education to your team, and it is best to constantly update their skills and knowledge of new hardware, software, and possible threats.

Hayes (2015:10) concur with Solomon et al. (2015:19) the forensic examiners must possess a one or combination of the following multidiscipline skills in the field “of computer science, criminal justice, law, mathematics, writing, forensic science and linguistics”. Even though one may possess this set of skills, the most important and best practice according to Hayes (2015:10) is the continuous learning and ability to be flexible as there is rapid change in technology. You must also adapt to changes to learn new skills and tactics.

According to Ho and Li (2015:84) “digital and multimedia forensics is a fast growing and evolving both in terms of technologies and legal requirements forensic examiners need to follow”. The lack of international standards, despite many efforts, means that each division of forensic practitioners and law enforcement agencies still follow national and local approach in dealing computer forensics.

3.13.1 Electronic data recovery in the USA

According to Baryamureeba and Tushabe (2014:2) electronic data recovery in the USA entails “the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of electronic evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal”. Baryamureeba and Tushabe (2014:3) further maintain that “the U.S. Department of Justice published a process model in the electronic data recovery which consists of the following four phases:

- Collection; which involves the evidence search, evidence recognition, evidence collection and documentation;
- Examination; this is designed to facilitate the visibility of evidence, while explaining its origin and significance. It involves revealing hidden and obscured information and the relevant documentation;

- Analysis; this looks at the product of the examination for its significance and probative value to the case;
- Reporting; this entails writing a report outlining the examination process and pertinent data recovered from the overall investigation”.

Giova (2011:2) pointed out that apart from the general electronic data recovery from computers, the USA has the modern technology and tools for electronic evidence recovery covering:

- Forensic tools for mobile cellular devices: “these are digital forensic tools used to process evidence from cell phones acquired data from specific locations in the data storage space in the phone’s SIM card. These tools are designed to ‘search’ on the phone where data can be found”;
- Data forensics in the cloud computing environment: “Internet-based or Cloud computing means accessing of applications and storing of data through the Internet, rather than on the hard drive of a local computer or server. One challenge is that if an application is accessed through the Internet, temporary files with forensic value that would traditionally have been stored on a computer hard drive will be stored within a virtual environment and will be lost when the user closes the application”;
- Forensic tools for Voice over Internet Protocol (VoIP) communications: “Forensic tools which extract data with forensic value from computers used for Internet-based telephony, such as call-log data”; and
- Forensic tools for vehicle computer systems: “Computers have become an integral component of motor vehicles, including event data recorders (EDRs), or ‘computer boxes’, which are used for accident investigation”.

The common problem for USA electronic data recovery as explained by Giova (2011:3) is the admissibility of computer evidence in court as governed by Federal Rule Evidence 901 as a general document admission. According to Giova (2011:3) “other governmental guides and norms about electronic evidence and, search and seizure” must also be considered. According to Giova (2011:3), “the other drawback is that other countries in the world have their own legislation and rules about recommended forensic measures, which naturally are related to their own law enforcement infrastructure and to a particular set of forensic tools and expertise".

3.13.2 Electronic data recovery in Australia

According to Cassim (2009:50) Australian laws, which continue to embrace technology, allow "the police to rapidly secure evidence stored on computers and to obtain real-time access to network traffic". Australia is also a member of a global treaty that is focused on defeating fraud and electronic crime. In support of Cassim (2009:50), Brown (2015:74) suggests that like many other global communities, Australia uses the increasingly more pervasive digital traces associated with cybercrime offending to help solve cases.

It is the opinion of the author such as Raghavan (2012:92) that in Australian perspective, the sequence of activities in the "multi-staged process starts with the identification of digital media from a scene as potential evidence to the stage where it is presented as evidence by an expert witness in a court of law." The sequence of these activities is illustrated at a high level in Figure. 3.2 below:

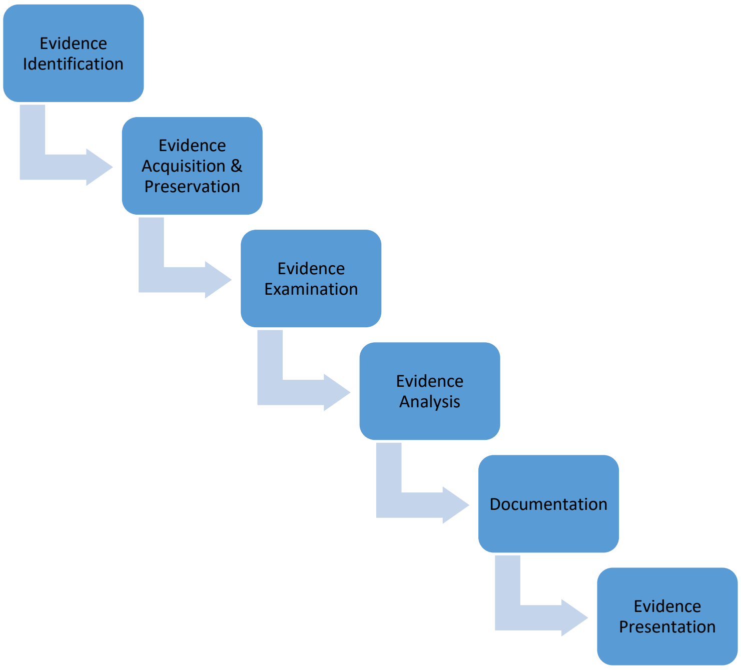


Figure. 3.2: Sequence of electronic data recovery

(Raghavan, 2012:92)

As illustrated in Figure. 3.2 above, “the very first stage of the digital forensic process is the *identification* of relevant electronic evidence” (Raghavan, 2012:92). It is followed by *acquisition*, which refers to “the process of obtaining a binary bitwise copy of the entire contents of all digital media that are identified”. This leads to the next step, which is that the evidence collected is *preserved* and “standard hash signatures like MD5 or SHA1 is used to verify integrity of the electronic evidence”. Once copies are created, the digital evidence can then be *examined* with and indexed specialised forensic tools. Following evidence examination and discovery, the stage *forensic analysis* takes place. This occurs when the recovered data is analysed. Analysis helps to sequence the series of events being investigated. Second-to-last, according to (Raghavan, 2012:92), “each individual stage is thoroughly documented and this *documentation* forms part of the evidence to be presented in a court of law”. Lastly, the evidence is *presented* in court and at times complimented with an expert witness.

Existing national legal frameworks in Australia as mentioned by Brown (2015:58) are “incapable of addressing evolving ‘modus operandi’ related to cybercrime offending”. Brown (2015:58) further provides that “it is common for cybercrime to be transnational in terms of the physical location of victims, perpetrators, and evidence”. This is due to the “interconnectivity of the global economy enables criminals to operate trans-jurisdictionally, with discrete elements of their crimes speckled widely across the globe in both time and space” (Brown, 2015:58). Brown (2015:58) further explains that “despite extra-territorial legal provisions for criminal acts perpetrated in foreign jurisdictions, the practical application of these laws is rather ineffective”. Thus, the evidence needed to investigate and indict an offender that was apprehended in one jurisdiction, may be in an entirely different country.

3.13.3 Electronic data recovery in China

Wahyudi, Riadi and Prayudi (2018:1) emphasise that in China, “the wide use of virtualisation technology is becoming a new challenge for digital forensics experts and the recovery of electronic evidence of deleted virtual machine image”. They further explain that the “virtual machine which was removed from the VirtualBox library could be recovered and analysed by using autopsy tools and FTK with analytical method, deleted files in the VMDK file could be recovered and analysed against the electronic evidence after checking the hash and metadata in accordance with the original".

Song and Kwak (2015:44) are of the opinion that considering the complications of electronic evidence China has the following technology to deal with computer crimes:

- **Electronic evidence monitoring technology**: to monitor electronic data in various system devices and storage medium and analyse whether it can be used as evidence;
- **Physical evidence collection technology**: secure acquisition of a computer system, data files, secure backup files and reconstruction of deleted files, etc;
- **Electronic evidence collection and preservation technology**: refers to saving and pre-processing of collected data according to authorised methods as well as using authorised software and hardware devices;
- **Electronic evidence processing and appraisal technology**: processing refers to pre-processing work such as filtering, pattern matching, hiding, and data mining of collected electronic evidence. Appraisal technology deals with data statistics and data mining for the processed data; and
- **Electronic evidence submitting technology**: submitting electronic evidence and the corresponding documentation to the court in acceptable form accordance to legal procedures.

The existing problems in China, according to Song and Kwak (2015:45), is that most forensic tools are replicas or Chinese version of foreign tool software which affect the legality and validity of these tools resulting in that authenticity, validity and normativity of electronic evidence cannot therefore be guaranteed. The other important challenge in China is the lack of technical skills amongst the forensic personnel and the using of traditional forensic rules and procedures.

3.13.4 Electronic data recovery in United Kingdom (UK)

According to Mason and Seng (2017:286) in the UK, "examination of electronic evidence by digital evidence professionals is a new technique known as 'digital forensic triage', which cover a range of processes, methodologies, software, and hardware that can be used to enable people to prioritise their digital forensic investigations more effectively. Mason and Seng (2017:289-302) further suggest the phase or stages of electronic evidence recovery in the UK as follows:

- Identification of electronic evidence;
- Gathering or collection of electronic evidence;
- Copying of electronic evidence: process of acquiring and handling of electronic evidence;
- Preservation includes validating electronic data, HASH collisions, the continuity of custody, transportation and storing of electronic evidence; and
- Analysis of electronic evidence to review the recovered data which includes looking for deleted files, hidden files, checking logs for activity, searching unallocated and slack space for residual data.

Like other countries discussed above, UK also has a common problem of jurisdiction when dealing cybercrime as explained by Cassim (2009:48) that there is little judicial support for the prosecution in cases where an element of the cybercrime occurred outside UK court's jurisdiction.

3.13.5 Electronic data recovery in India

The utilisation of Web has developed as most effective medium for capacity and recovery of electronic data in India (Velmurugan, 2016:13). According to Ahmed and Dharaskar (2009:180) in India, the guidelines for digital evidence recovery best practice in the forensic examination follow the following general principles:

- The general rules of evidence should be applied to all digital evidence;
- Evidence should not be tempered after seizure;
- Access to original digital evidence must be limited to suitably trained people;
- Every step must be documented;
- Electronic evidence should be preserved and available for review; and
- Chain of custody must be maintained at all times.

The basic procedures to recover electronic evidence in India as cited by Prajapati and Rai (2013:249) follow similar standards and processes as illustrated below:

- “Seize the suspected media first. Capture in all media so that no one can manipulate or divert investigation any way;
- A bit-by-bit image is created from the suspected media, duplicate number of copies for making ensure that uncorrupted and unaltered copy is used for the investigation purpose;
- Copy of one digital forensic image is now analysed for potential evidence specific to each case. Deleted files, changed files, date & time stamp of media files, internet history, Instant messaging logs, system log file, emails, etc are all searched for analysis;
- Evidence is extracted and prepared for presentation in a legal form so that court can prosecute a case in court;
- Finally, the investigator will create a customised report detailing the whole chain of events. Correlate all available events technically to each other’s for making the best decisions; and
- If it is required at any stage expert observer testimony is provided if needed in whole process to optimise the outcomes at any stage in whole process”.

Tereikovskyi et al. (2018:1559) and Battula et al. (2009:31) listed the challenges of electronic data recovery in India as follows:

- **Magnetic alteration**: Erasing files by altering the file information recorded in the directory;
- **Physically damaged drive**: Damaging the drive beyond use in a physical manner; and
- **Overwritten data**: The data that has been overwritten cannot be recovered.

3.13.6 Electronic data recovery in Indonesia

It is the opinion of authors, such as Akay (2020:291), that computer crimes in Indonesia, is usually carried out regardless of what is inside the computer. In fact, there is more evidence if the computer involved is identified. There are two methods commonly used for computer forensics in Indonesia, namely search and seizure, and discovery of information. Search and seizures are the most widely used methods, while information retrieval is to complement the evidence data.

In support of the views of Akay (2020:291), Umar, Raidi and Muthohirin (2019:1805) maintain that acquisition of electronic evidence is a collection process, identifying, labelling, recording, and retrieving evidence in the form of software, and is to be retrieved for use as digital evidence of a digital crime case. Examination of evidence as pointed out by Albanna and Raidi (2017:173) is usually associated with file recovery, which is a method for taking a logical file or recover deleted file or lost because there is no longer listed on the file system. The data is required to prove that a crime has occurred and to connect the perpetrator.

Ramadhani, Saragih, Rahim and Siahaan (2017:163) put forward and emphasise that "digital evidence is scattered in different media and contexts, so it takes more foresight than simply classifying data for forensic purposes". Ramadhani et al. (2017:163) further indicate that the "more peripherals or devices integrated into computer systems, it is more complex and involves many considerations to lift digital evidence".

Furthermore, Ramadhani et al. (2017:164) sustain that the obstacles that may occur in the field at the time of investigation to retrieve data in Indonesia, is as follows:

- Compressed file;
- Incorrect file format;
- Password-protected files;
- Hidden files; and
- Encrypted file.

3.13.7 Electronic data recovery in Italy

According to Fenu and Solinas (2013:4), the Italian "conceptual framework, the Latin maxim '*verba volant, scripta manen*' is interpreted in a digital context as: where every information (independently from the way in which the document is written) can be certainly ascribed to someone". Moreover, "information can be stored during the time through the use of accurate methods of computer security and of storage of the relevant information, with respect to the Italian legislation" (Fenu & Solinas, 2013:4). Furthermore, in relation to data recovery in Italy, Fenu and Solinas (2013:8) confirm that the data carving focuses on recovering data. The data carving, or data recovery process uses header and footer identification to recover the files.

Four-phase model of data extraction in Italy as provided by Berte, Marturana, Me and Tacconi (2012:103) entails the following:

- **Acquisition**: make a disk image in order to preserve digital evidence integrity and guarantee the analysis repeatability;
- **Extraction and normalisation**: extracting relevant data from disk images;
- **Context and priority definition**: analysis of timeline of interest; and
- **Data classification and triaging**: provide the final classification of the input data.

In concluding international best practices in electronic data recovery, based on the information obtained from local and international authors during literature review, the researcher agrees with most of the authors, particularly Syambas and El Farisi (2014:141) who suggested that to prevent "loss of digital evidence through the deletion of data by suspects", countries or entities must implement the Two-Step Injection method (TSI) to retrieve digital evidence. Syambas and El Farisi (2014:146) furthermore explain that the TSI method recovers "covert digital evidence retrieval system using a two-phase flash drive injection into the suspect's computer or laptop". This method emphasises the principle of prevention of loss of digital evidence due to the action of removing digital data by the suspect or due to an accident. The first injection is the phase of planting the Content Module to collect data without the suspect been aware. The second injection is harvesting data from the Content Module for further analysis

Additionally, Syambas and El Farisi (2014:146) is of the opinion that "the advantage of this TSI method is that the system works in secret and can be combined with other digital evidence applications that already exists, so that the accuracy and completeness of the resulting digital evidence retrieved can be improved".

They further listed the following advantages of deploying TSI:

- "Fulfils the rules of evidence (acceptable, authentic, complete, and reliable);
- Dynamic in terms of collecting data options;
- Clones folders and use this information to analyse which folder needs to be cloned further, this can save memory;
- Fulfils the chain of custody by using cloning instead of copying;
- Uses an offline (local) network capture method, so there will be no miss on logging;
- Looks for a password for file encryption effectively with predictions for passwords from online accounts, it is alternative methods for brute-force de-encryption;
- Uses an alternative for existing keyloggers that need an installation process;
- Is automated and runs in secret. The only thing that needs to be done is injecting a flash drive;
- Has a small size and is light when running; and
- Is a modular and it can collaborate with other applications directly?"

3.14 CHAPTER SUMMARY

In this chapter, it has been established that electronic data recovery involves the four distinct steps in computer forensics investigations are identification, acquisition, examination, and presentation. The process of examination comprised of extraction and analysis of data. The following are data recovery tools: EnCase, FTK, password recovery toolkit, ProDiscovery forensics and Stego.

It has also been established that desktop, and laptops, network server, printers and copiers, removable and portable devices, PST files, internet browser history and mobile devices are the sources of electronic evidence. Documentation of every step of electronic data recovery is important to maintain chain of custody. All evidence collected in the crime scene must be tagged or marked and if possible photographed.

It has been further established that preservation of original evidence and avoiding any tampering thereof, is best practice to conform to best evidence rule which require the submission of original documents before court. Training and continuous learning to enhance the forensic investigators' knowledge is cited as international best practices, as computer forensic investigations can be conducted by properly trained investigators only.

In Chapter four, an overview of the investigation of e-Procurement fraud is presented and discussed.

CHAPTER FOUR
THE INVESTIGATION OF E-PROCUREMENT FRAUD

4.1 INTRODUCTION

According to Katz (2016:1) ordinarily, SCM and procurement processes are extremely vulnerable to fraud as most of the organisation's budget is used in the purchase of goods and services. E-Procurement fraud can happen at any organisation, committed either by its internal staff or external service providers, or through internal and external collusions. For organisations to effectively deal with e-Procurement fraud, "they must have a strong fraud detection methods and processes to reduce the risk and breading space for fraud as it manifests itself through weaker SCM controls" (Katz, 2016:1). Risk management and analysis must be constantly conducted in keeping with the spirit of good governance, especially in areas where a huge amount of money has been spent on procurement. Due to the complexity and speed at which cybercrime is growing globally, organisations must develop new fraud detection strategies and investigations to reduce e-Procurement fraud and to protect their coffers against procurement fraudsters.

Katz (2016:7) further highlights that the detection and reduction of e-Procurement fraud needs collaborative efforts and a multi-disciplinary approach to resolve, as it is a multi-dimensional problem. It requires different perspectives working together towards one goal of eliminating the obvious opportunities for procurement fraud. Nigel and Samociuk (2006:1) indicate that e-Procurement fraud and corruption are two phenomenon that are not easy to manage. Even though executives and management of different organisations are trying to develop and implement extensive corporate governance and control frameworks, they are not doing enough to prevent e-Procurement fraud. Despite tougher policies and legislations, without honest and ethical law enforcement agencies to implement them, nothing will change in the world of fraud and corruption. Statistics of e-Procurement fraud and bribery scandals are on the increase, and skyrocketing now compared to twenty years ago.

In support of Nigel and Samociuk (2006:1), Ochonma (2015:11) maintains that internal controls are very important to prevent and to detect any acts of collusion and management override of the SCM processes for the purpose of personal gain. To ensure that the “personal gains by procurement officials is reduced to the lowest level; many organisations have developed and implemented stringent ethical strategies in their SCM activities (Ochonma, 2015:11).

From the researcher’s experience, he believes that not much was achieved to manage or prevent e-Procurement fraud in South Africa, despite many legislations and policies. This might have been as a result of lack of internal controls within organisation’s SCM divisions. This chapter is predominantly focused on the investigation of e-Procurement fraud. Following for discussion is the different categories of e-Procurement fraud, followed by detection and prevention of e-Procurement fraud. This chapter will also provide a detailed literature review of the extent of e-Procurement fraud and red flag indicators.

4.2 CATEGORIES OF E-PROCUREMENT FRAUD

According to Rendon (2018:593) one of the most common e-Procurement fraud is collusion. Rendo further defines collusion as “a situation where two or more employees work together to commit fraud by overcoming a well-designed internal control system”. Rendon (2018:593) concur with the views of Coenen (2008:86) that e-Procurement fraud is comprised of three main categories, namely:

- Collusion between officials and suppliers, which may result in kickbacks;
- Supplier defrauding a company by, for example, overcharging a company or fictitious invoicing; and
- Multiple suppliers colluding to defraud a company by agreeing to inflate the prices of goods and services or helping each other win certain contracts based on agreements between them.

4.3 THE COST AND EXTENT OF PROCUREMENT FRAUD

Padgett (2015:6) emphasises that the 2019 ACFE fraud survey indicates that a substantial amount of government and private organisations revenue (estimated to be five percent) is lost due to e-Procurement fraud each year. According to the 2019 ACFE report, “e-Procurement fraud is a major contributor to a loss of more than $3.5 trillion globally” (Padgett, 2015:6). According to this ACFE fraud survey, it takes more than 18 months to detect an average e-Procurement scheme. The most high-risk industries are government departments and municipalities, followed by manufacturing and construction companies. This survey further indicates that highlighted high-risk industries must improve their fraud risk management to reduce e-Procurement fraud and the future potential losses thereof (Padgett, 2015:7).

According to Corruption Watch (2013), e-Procurement fraud and corruption is costing South African government about R25 billion each year, which according to civil society activist Hennie van Vuuren, is almost twenty percent of the total government procurement budget. In 2011, Willie Hofmeyr, then head of the Special Investigation Unit (SIU), told SA Parliament that “between R25 billion and R30 billion of the government’s procurement budget was lost due to procurement fraud”.

A typical example of this is the City of Tshwane’s R4 billion fleet management tender that was recently cancelled due to procurement fraud and a corruption-riddled process. The forensic report found that there were several employees who are the directors of the companies that tendered for this contract (Moatshe, 2020).

Another example is the former Gauteng MEC of Health, Mr Bandile Masuku, who was dismissed from his position for his involvement in the irregular and fraudulently award of personal protective equipment (PPE) tender amounting to R125-million to Royal Bhaca Projects. It was later discovered that Royal Bhaca Projects is linked to his wife, Ms Thandisizwe Masuku who was also a Spokesperson for the Office of the President of the Republic (Smith, 2020).

The Auditor General (AGSA, 2020) again put the spotlight on the CoT municipality when he published a report on Local Government Audit Outcomes 2018/19, on 01 July 2020. AGSA indicated on this report that the CoT municipality has lost R2.9 billion due to procurement irregularities during 2018-2019 financial period.

4.4 TYPES OF PROCUREMENT FRAUD SCHEMES AND ITS INVESTIGATION

It was the view of Olsen (2010:112), that the following are the most common schemes of e-Procurement fraud:

4.4.1 Kickbacks

According to Olsen (2010:112), a kickback scheme is when the employee receives monetary gifts to give one bidder an unfair advantage over another during bidding process or award. In these circumstances, these improper payments between employees and suppliers are hidden and kept secret.

To investigate these types of payments, the employee bank accounts are reviewed for any suspicious activity, with specific attention being paid to the following:

- Any larger deposit made to his/her account;
- Recent trips and extravagant entertainment; and
- New high value purchase like houses and vehicles.

Padgett (2015:17) concurs with Olsen (2010:112) when stating that a ‘kickback’ might be part of an inflated purchase price as a reward for facilitating the deal, payment will normally be made at the conclusion of the deal. Wells (2011:242) is of a similar opinion to Padgett (2015:17) and Olsen (2010:112) as he explains that kickbacks money might be from the invoices for goods and services that were not delivered or were overpriced. An employee will receive some form of payment from the supplier after making sure that payment for the fictitious invoice was made.

The researcher therefore concludes that to properly investigate kickbacks, a lifestyle audit for all procurement officers must be conducted to establish whether they are not living beyond their means (i.e., known salary).

4.4.2 Vendor fraud

Varma and Khan (2017:1) alluded that vendor fraud involves a scheme in which the fraudster manipulates vendor's sensitive data or a company's accounts payable and payment systems individually or in collusion with the organisational employees for illegal personal gain. Olsen (2010:112) confirms that vendor fraud is when fraudsters submit fictitious invoices or invoices for overpriced goods. Vendors involved in fraudulent activities may need the help of the internal employee to circumvent the internal processes.

According to Olsen (2010:211), the following information will assist to effectively detect and investigate this this type of scheme:

- Duplicate addresses on the database;
- Similar addresses and names on the database; and
- Invoices with missing or duplicate PO's, duplicate date and amount.

Goldmann (2010:159) agrees with Olsen's (2010:112) statement that vendor fraud is when a vendor overcharges a company by inflating prices or delivery of substandard goods. Albrecht, Albrecht, Albrecht and Zimbelman (2019:11) share similar views as Olsen (2010:112) and Goldmann (2010:159), expressing that vendor fraud is perpetrated by a vendor who is usually acting alone or through the help of an employee.

4.4.3 Bid-rigging

According to Olsen (2010:114), bid-rigging occurs when suppliers agree in advance which bidder will win a contract. Bid-rigging defeats the principle of competitive bidding.

The following are categories of bid-rigging:

- Bid suppression: refrain from bidding to eliminate competition;
- Complementary bidding: submission of a similar but higher bid;
- Bid rotation: taking turns in winning the bids; and,
- Collusion: getting help from internal employee to win a bid.

Padgett (2015:83), who concurs with Olsen (2010:114), explains that bid-rigging is any agreement by suppliers to suppress and eliminate competition on contracts. Bid-rigging is “an agreement where two or more bidders agree to submit bids that have been prearranged amongst themselves and share the profit”. It includes “agreements to fix or inflate prices, to submit similar bids, to rotate winning bidders and to share profits”.

4.4.4 Conflict of interest

Padgett (2015:23) confirms that conflict of interest is when an employee has a competing interest between his individual self-interest and professional or public interest. Wells (2011:255), who agrees with Padgett (2015:23), suggests that a conflict of interest occurs when an employee has not declared his/her economic or personal interest in a transaction that will directly or indirectly benefit them from such a transaction. Most companies allow their employees to “declare their interest annually, if for instance, he/she is a director of a company doing business with his/her employer” (Wells, 2011:255)

In conclusion, the researcher has previous experience in the investigation of matters related to e-Procurement fraud and contends that, apart from the above-mentioned types of procurement fraud schemes, there are many other schemes such as splitting of invoices, duplicate payments and fictitious invoicing that investigator must be aware of.

4.5 DETECTION AND PREVENTION OF E-PROCUREMENT FRAUD

Olsen (2010:119) suggests a prevention approach is better than a cure approach when he mention that “a more cost-effective approach to effectively deal with e-Procurement fraud is to take proactive steps”. Olsen further indicates that organisations must strengthen their internal controls and foster compliance to enhance their fraud detection and prevention strategies. According to Olsen (2010:119), the following internal controls will assist in the detection and prevention of potential e-Procurement and related fraud:

- **Separation of powers and duties**: one person creates, another one approves;
- **Constant supervision**: supervisor to sign the final approvals;
- **Records of goods receipt**: who is receiving the invoices, and who is receiving the goods;
- **Authorisation and approval**: limit approval and authorisation to the supervisors;
- **Balancing and reconciliation**: constant reconciliation of bank statements, books and records;
- **Inventory records**: a well-defined logistical SOP to document the entire process;
- **Skills development and training**: everyone must know what they are expected to do;
- **Fraud awareness**: the employees must know the consequences of their actions;
- **Reporting protocols:** who they report to;
- **Implement policies**: prevention can be enhanced through consistent implementation of policies and procedures; and
- **Consequence management:** prosecute employees for fraud and any other misconduct.

In his study, Olsen (2010:119) claims that for investigators to detect potential e-Procurement fraud, investigators must use CATTs to:

- Monitor vendor and employee databases;

- Review any changes made to the database such as directors or banking details; and,
- Establish any relationship between employees and suppliers.

According to Varma and Khan (2017:1) proactive e-Procurement fraud detection uses technology to rapidly analyse large sets of transaction data. Varna and Khan recommend using of IT division to proactively detect any form of fraud and enable organisations to monitor and analyse large transaction database in real time.

Coenen (2008:123) concurs with Varma and Khan (2017:1) by explaining that a significant number (at least twenty-five percent) of all e-Procurement fraud is detected by accident, due to lack of fraud detection strategies. The only way to actively detect e-Procurement fraud within a company is through monitoring of its computer systems using sophisticated software to track and log computer activities. It is exceptionally important for any organisation to "track anyone who tried to log into their system, which password was used and how data was accessed (through plugin network or remote access)" (Coenen, 2008:123). As explained further by Coenen (2008:123) any unusual activities can signal e-Procurement fraud risk and need constant and continuous monitoring.

4.6 E-PROCUREMENT FRAUD RED FLAGS

According to Padgett (2015:73), red flags are sets of unusual activities that are indicative of something out of ordinary and require close monitoring or immediate investigation. Red flags do not indicate guilt or innocence, however they "provide possible warning signs of e-Procurement fraud" (Padgett, 2015:73).

The following, as listed by Padgett (2015:77) are the red flags of e-Procurement fraud:

- Continuous complaints about a specific goods or products;
- Increase in inventory but no demand of stock;
- Payments to vendors who are not registered on the supplier database;
- Overstocking from a new supplier;
- Appointments of suppliers through deviations from the normal procedures;

- Vendors with suspicious physical addresses; and
- Vendor contact details and address matching details of the employee.

In support of the views of Padgett (2015:73), Coenen (2008:58) mentions that an undetected e-Procurement fraud or fraud case not decisively dealt with by the company’s management can encourage employees to commit more fraud because they might think that evidence of fraud may be easily concealed and they can get away with it. According to Coenen (2008:58), the following documentation can signal red flags and might be useful to the investigators:

- Documents missing pages;
- Documents with multiple staple holes;
- Uncertified copies of documentation; and
- Visibly tempered-with signatures on documents.

According to the SIU Training Manual (2010:149-150), it is always important to consider the following “red flag” payments during investigation:

- More than one invoice submitted on the same day by the same supplier;
- Sequential invoices from the same supplier;
- Payment of same amount made twice;
- Same amount on the same invoice paid to a different supplier, on the same day;
- Invoices dated or submitted on weekends or public holidays;
- Invoice amount which is different to the quoted amount;
- Payments done after working hours;
- Invoices that were not paid;
- Payments made with no invoice submitted;
- Same invoice number used more than once;
- Order numbers that are in sequence;
- Sequential orders on the same day;
- Suppliers who use multiple bank accounts;
- Constantly changing of banking details;
- Payments that are just below the delegated threshold (R29 000,00 to R29 999,00) indicate possible splitting of transactions; and

- Repeated invoice paid twice.

It is worth noting as explained in the SIU Training Manual (2010:149-150) that employees living beyond their means is a clear signal of being involved in possible fraudulent activities and should be considered as a key red flag. It is therefore a conclusion of the researcher that lifestyle audits must be conducted on employees who openly live beyond their means and that sudden behavioural changes such as, for example boasting about significant new purchases and carrying unusual large sums of money are indicators of the red flags for fraud.

4.7 INVESTIGATION OF E-PROCUREMENT FRAUD

According to Wells (2011:365), it is good governance and best practice to conduct a thorough investigation after detecting any e-Procurement fraud activities. The investigation will help the organisation to identify and prosecute the fraudster, and to recover or recoup the stolen money. Investigation can also "identify weaknesses and recommend the strengthening of internal controls to boast the company's internal defences against possible e-Procurement fraud". Mamahit and Urumsa (2018:159) suggest that investigation of e-Procurement is a process that involves the application of skills, financial expertise, accounting, and investigative thinking that aim to reveal the fraudster. In the process of conducting e-Procurement fraud investigation, it is necessary for the investigator to apply intelligence, sound consideration and experience, and understanding of statutory provisions.

Golden, Skalak and Clayton (2011:433) confirm that e-Procurement fraud investigation will usually begin with the probing of the suppliers, focusing specifically on how the money was disbursed and for what purpose. All relevant disbursement information should be collected and analysed. Wells (2011:366) further emphasises that e-Procurement fraud investigation and any other investigation must follow a well-structured methodology and distinct phases or steps:

4.7.1 Planning phase

According to Albrecht et al. (2019:79), any investigation within the organisation must be approved by the management because investigation can be very sensitive and quite expensive and, should be pursued only when there is a reason to believe that e-Procurement fraud has been committed. According to Wells (2011:367), when a decision to conduct an investigation is taken, and before any activities are undertaken, the planning meeting must be convened. The purpose of this meeting is "to select an investigation team and to outline their responsibilities". Wells (2011:367) further mention that it is critical to identify team members who can legitimately contribute to the investigation and, that e-Procurement fraud investigation team must be comprised of the following types of professionals:

- **Certified fraud examiners (CFE)**: to conduct a complex fraud examination;
- **Legal Counsel**: to provide legal advice during and after investigation;
- **Internal Auditors**: to detect any irregularities that lead to e-Procurement fraud, and to identify fraud risk indicators;
- **IT and computer forensics experts**: to identify, recover, preserve and analyse any electronic evidence. They will also assist with the interpretation of electronic data during reporting phase;
- **Human resource (HR) personnel**: to safeguard the rights of employees through advising on proper implementation of laws and policies to reduce the possibility of civil action by employees;
- **Management representative**: constant progress report to the management for any necessary assistance that might be needed; and
- **Independent consultant**: to deal with cases that involve powerful or popular employees. They are not easily intimidated and are relatively immune from company politics or the threat of victimisation.

In support of Wells (2011:367), Coenen (2008:130) indicates that the first and most important step in any e-Procurement fraud investigation is the establishing of a team of qualified professionals comprised of internal officials and independent consultants. McMillan (2006:109) puts forwards that the first task of the selected investigation team is to draft and develop an investigation plan based on the available information at their disposal. The details of the investigation plan will be a “guide to the next phase of fieldwork”, but it can change, as more information becomes available.

4.7.2 Sourcing and collection of evidence

According to Wells (2011:369), the next phase of the investigation is to develop a process to collect evidence. Evidence is “any proof, such as word of mouth, recordings, documents, electronic data, or tangible objects that are legally presented at trial to prove a case” (Wells, 2011:369). Wells (2011:369) further mentions that evidence can be gathered in one or more of the following ways:

- **Subpoenas**: Order from court issued to a suspected employee or supplier to submit any relevant evidence to the case. Witnesses can be compelled through subpoena to give evidence in court;
- **Search warrants**: Having the search warrant, the investigators can search and collect any required evidence and devices suspected to have been used in the commission of e-Procurement fraud;
- **Voluntary consent**: The easiest process to obtain evidence is through voluntary consent. While consent can either be oral or written, it is recommended by Wells (2011:369) that the “consent must be acknowledged in writing”;
- **Interviewing witnesses and employees**: Interviewing witnesses is the most important part of collection of evidence as it can lead to a quick successful resolution of a case. In light of the above statement by Wells (2011:369), and as indicated by Schwartz (2010:2) that “interviewing employees can be useful in ascertaining potential e-Procurement fraud and can disclose potential inappropriate relationships between employees and suppliers which are unknown to the organisation;
- **Background checks**: According to Schwartz (2010:2), to reveal the relationships and connections between employees and suppliers, investigators must conduct a background check on the suspected individuals and entities. Relationship matrix can provide information about the integrity and reputation of an employee, and a relevant information about a vendors’ previous dealings; and,

- **Electronic discovery**: PST data file of employee can reveal any improper and questionable communication between the suspected suppliers and employees (Schwartz, 2010:2).

Golden et al. (2011:434) state that the following critical information must also be collected:

- Vendor information registered in the database;
- Awards, appointment letters, tender documents, compliance files, purchase requisitions created, POs captured, quotations, invoices, and documents used to approve payments , store inventories, and any other related documents; and,
- Background checks to qualify the vendor through public record searches.

In addition, Golden et al. (2011:434) point out that the gathering of the above-mentioned items must be done by a qualified computer forensics technician using techniques such as data mining. The investigator must ensure that all information gathered is independently corroborated and confirmed to be factually correct (Albrecht et al., 2019:81).

4.7.3 Preserving evidence

In the process of preserving evidence, the investigator must make sure that any technique used is scientifically and legally sound and fair (Albrecht et al., 2019:81). Wells (2011:371) was of the view that preservation of evidence is probably the most important phase of the investigation as a case can be lost if the investigation team contaminated the evidence and cannot be accepted by the court. Even though the “evidence was legally obtained, for such evidence to be admissible, proper process of its handling must be adhered to” (Wells, 2011:371). According to Wells (2011:372) chain of evidence must be maintained at all times, bearing in mind that only evidence that is relevant, and material to the case will be considered in court.

The following general rules for the collection and handling of documents as proposed by Wells (2011:372) should be observed:

- Acquire original documents if possible. Make couple working copies for analysis;
- Keep the original isolated. Do not conduct analysis on the original;
- Do not unnecessarily touch originals; they might later have to undergo forensic analysis; and
- Good record keeping is critical, especially when dealing with voluminous documents. Documents can be paginated sequentially for easy reference.

In support of the above, Golden et al. (2011:435) suggest that original documents should be filed separately from the rest of evidence. No one should be allowed to remove the original documents without valid reasons and granted permission.

4.7.4 Organisation and analysis of evidence

According to Mamahit and Urumsah (2018:157), evidence collected must be relevant, competent and sufficient to the case. It is said to be relevant if it can logically support or reinforce the argument. It is said to be competent, if the evidence is valid (fulfilling legal and regulatory requirements) and can be relied upon (the source and method of obtaining it is correct). It is enough if the amount of evidence collected has been used as a basis for making a decision. After collecting the evidence, analysis and evaluation are then carried out. The analysis and evaluation of evidence aim to support conclusions and findings of the investigation.

Wells (2011:373) posits that it is crucial and best practice that any evidence gathered must be properly and constantly organised early in the investigation, and as the case progresses. McMillan (2006:116) agrees with Wells (2011:373) by emphasising that it is very important to safeguard the originals and to do analysis only on the copies. Preservation of evidence also prevents tampering with originals documents or data.

Wells (2011:373) further maintains that good evidence organisation in complex fraud cases includes the following:

- **Segregation**: filing evidence in separate files, either per invoices or payments;
- **Chronologies**: a sequence of events should be prioritised at the beginning of the case in order to establish the proper chain of events until the case is finalised;
- **To-Do lists**: diaries important tasks and keep updating; and
- **Using computer software to organise documents and other data**: use of a computer database can enhance the easy saving and access to critical information gathered. There is special software that can sort, arrange, filter, chart, and graph the information in the spreadsheets and database, making it easier to scrutinise relationships and isolate inconsistencies for further analysis. The following are recommended case management and reporting software programs as listed by (ACFE, 2019:3.746):
    - IBM's i2 Analysis;
    - Regulatory DataCorp;
    - Safe Banking System;
    - Infoglide Software; and
    - World-Check.

Coenen (2008:134), who shares a similar view with Wells (2011:373), explains that an investigation with volume of documents must have good document management system or processes. Coenen (2008:134) recommends computer database or spreadsheet to chronologically organise documents, and if possible, to separate them by payments or invoices.

4.7.5 Report writing

Wells (2011:374) confirms that at the end of the investigation, the investigator must draft a well-structured investigation report with findings and results. This report will usually be "presented in the internal disciplinary hearings but may also be used to report to other law enforcement agencies" such as SAPS and SIU or claims to insurance companies. Investigators must report all facts fairly and objectively in the final investigation report (Albrecht et al., 2019:81).

The purpose of the investigation report, as mentioned by Wells (2011:374), is to:

- Interpret evidence: what were the findings and results of the investigation;
- Add credibility: to prove the allegations and to validate details reported earlier; and,
- Accomplish objectives of case: being compelled to issue a written report forces the investigator will be objective throughout the investigation.

In this respect, McMillan (2006:110) explains that when the investigation is completed, a written report summarising the findings, supported by evidence gathered during fieldwork must be prepared. Coenen (2008:139) agrees with McMillan (2006:110) and Wells (2011:374) by pointing out that a written report will conclude the investigation where the details of the findings are captured.

From his work experience at the CoT, the researcher outlines how the forensic investigation report is structured. The forensic report is structured as follows:

- Introduction: introduce the allegation under investigation and the mandate of the GAR;
- Background: in detail, how the allegations was reported, by who and what was reported;
- Scope: what will the investigation cover?;
- Investigation purpose: why are we conducting this investigation and what is the objective and what are we aiming to achieve;
- Investigation methodology and approach: methods deployed to conduct this investigation;
- Regulatory framework: guiding principles, relevant legislations, and policies;
- Detailed findings: after the analysis of evidence acquired, findings should be reported;
- Conclusions: based on the findings, the investigator must conclude on the allegations; and

- Recommendations: recommend what is to be done and by who, for instance, the recommendations can be one or more of the following:
    - The improvement of internal controls and procedures;
    - Disciplinary action against an employee;
    - Civil litigation;
    - Insurance claim;
    - Where criminal elements are uncovered: registering of a criminal case with SAPS;
    - If the outcomes point to unauthorised, irregular, and fruitless and wasteful expenditure (UIFW), the expenditure should be disclosed, and the irregular expenditure register updated in terms of section 32 of the MFMA;
    - Reporting to oversight committees like Municipal Public Account Committee (MPAC) and Audit Performance Committee (APC);
    - In case of any tax violation, referral to the South African Revenue Services (SARS) in terms of section 43 of the Tax Administration Act, Act no: 28 of 2011; and,
    - Any applicable alternative dispute resolution.

4.8 CHAPTER SUMMARY

This chapter established that e-Procurement fraud is a global phenomenon, which requires the multi-dimensional approach to deal with. It requires the implementation of effective internal controls, strong detection methods and fraud prevention strategies. It has been further established that to ensure that organisations reduce the risk of e-Procurement fraud, they must have effective internal auditors and risk practitioners to identify high-risk areas and fraud risk indicators for early detection and prevention of e-Procurement fraud.

In this chapter, it has also been established that to effectively investigate e-Procurement fraud, the most important aspects is setting up a strong investigation team. Proper gathering and preservation of evidence cannot be overemphasised. The evidence must be appropriately organised using case management and reporting software programs.

The investigation report will conclude the e-Procurement fraud investigation which will be presented to the management and any other relevant structures. Chapter five provides a presentation, discussion, and interpretation of research findings of this study.

CHAPTER FIVE
PRESENTATION, DISCUSSION AND INTERPRETATION OF FINDINGS

5.1 INTRODUCTION

This chapter presents, discusses, and interprets the findings of the study and illustrates participants' viewpoints regarding the use of electronic data recovery in e-procurement fraud investigation. The transcripts from the in-depth interviews conducted with the CoT GAR participants are presented in this chapter. Each of the themes in this chapter has a holistic approach and the patterns within each are illustrated. It is within each theme that the objectives of the study will be addressed, as mentioned in Section 1.4 of Chapter One.

The questions posed to participants helped structure this chapter as well as how the dialogue continues and eventually forms the various themes. This approach pinpoints the views of the participants.

The participants' experiences and perceptions served as catalyst for the presentation of the research findings regarding the use of electronic data recovery in e-Procurement fraud investigations at the CoT. Consequently, it was thus vital to explore participant experiences and the daily reality of CoT forensic investigators. Participants' experiences as illustrated in this chapter therefore promotes enhanced insight of the use of electronic data recovery in e-procurement fraud investigations at the CoT.

5.2 OUTCOMES OF INDIVIDUAL INTERVIEWS AND INTERPRETATION OF FINDINGS

With the permission of the CoT GAR management, the 23 candidates were chosen for this study based on purposive sampling. The candidate were sampled based on their work responsibilities as follows, 5 Forensic investigators, 12 Senior Forensic investigators, 3 Senior Forensic Audit Specialists and 3 Managers Their rank, experience, and knowledge in the investigation of e-Procurement were also the deciding factors for inclusion in this study.

The following section includes the verbatim responses from participants; the interpretation of the responses; how those responses inspired the topic; consideration of the literature to the topics; and lastly an interpretation of each topic. The participants' view of the benefits of e-Procurement in terms of fraud risk management at the CoT is the first topic. Table 5.1 below contains the list of themes and sub-themes as they appear.

Table 5.1: Clusters of common themes and sub-themes that emerged from findings

Theme 1	**THE BENEFITS OF E-PROCUREMENT IN TERMS OF FRAUD RISK MANAGEMENT AT THE CoT**
Sub-themes	1.1 It is easier to access data during investigation 1.2 e-Procurement provides an electronic chain of evidence 1.3 e-Procurement provides an opportunity to reduce fraud
Theme 2	**THE CHALLENGES OF E-PROCUREMENT IN TERMS OF FRAUD RISK MANAGEMENT AT THE CoT**
Sub-themes	2.1 e-Procurement presents opportunities for fraudulent Activities
Theme 3	**FI'S LACK KNOWLEDGE OF THE DIFFERENT TYPES OF E-PROCUREMENT MODELS/SOLUTIONS AT THE CoT**
Sub-themes	3.1 FI's lack knowledge of e-Procurement system in general 3.2 FI's lack knowledge of the procurement models/ solutions at the CoT
Theme 4	**FI'S KNOWLEDGE OF THE LEGISLATIVE FRAMEWORKS THAT GOVERN E-PROCUREMENT PRACTICES IN SA**
Sub-themes	4.1 FI's knowledge of the legislative frameworks that govern procurement in SA 4.2 FI's knowledge of legislative frameworks that govern e-Procurement
Theme 5	**FI'S OPINION WITH REGARDS TO THE EFFECTIVENESS OF ELECTRONIC DATA RECOVERY IN THE INVESTIGATION OF E-PROCUREMENT FRAUD AT THE CoT**
Sub-themes	5.1 FI's are of the opinion that electronic data recovery in the investigation of e-Procurement fraud has capacity to be effective 5.2 FI's are of the opinion that electronic data recovery in the investigation of e-Procurement in the CoT is currently not effective
Theme 6	**FI'S EXPERIENCE CHALLENGES WITH REGARDS TO RECOVERING ELECTRONIC DATA DURING THE INVESTIGATION OF E-PROCUREMENT FRAUD AT THE CoT**
	6.1 FI's experience challenges with regards to a lack of training on e-Procurement 6.2 FI's experience challenges to access the information in the CoT system

Sub-themes	6.3 FI's are not familiar with the most prominent CAATs software applications 6.4 FI's are not familiar with the most critical steps and phases of electronic data recovery 6.5 FI's are not familiar with the process of examining electronic data 6.6 FI's lack advanced resources to electronic recover data 6.7 FI's lack support from CoT Management 6.8 Current budget is spent on outsourcing rather than capacitating internal forensic investigators
Theme 7	**UNIQUE THEME: FI'S ACKNOWLEDGE THE SIGNIFICANCE OF USING ELECTRONIC DATA RECOVERY IN E-PROCUREMENT FRAUD IN CoT**
Sub-themes	Theme 7 is unique and therefore has no sub-themes
Theme 8	**SUGGESTIONS TO IMPROVE THE CAPACITY OF FI'S TO INVESTIGATE E-PROCUREMENT FRAUD USING ELECTRONIC DATA RECOVERY AT THE CoT**
Sub-themes	8.1 Teamwork 8.2 Access to the systems 8.3 Acquisition of advanced resources to recover electronic data 8.4 Training of investigators

Source: Designed by researcher

5.3 THEME 1: THE BENEFITS OF E-PROCUREMENT IN TERMS OF FRAUD RISK MANAGEMENT AT THE CoT

The first theme presents the participants' perceptions of the benefits of e-Procurement in terms of fraud risk management at the CoT. This was sought to understand whether the participants know the benefits of e-Procurement.

The answers to the following question gave rise to this theme and its sub-themes:

- *"According to you, what are the benefits of e-Procurement in terms of fraud risk management at the CoT?"*

It is necessary for the participants to know the benefits of e-Procurement in order to be able to curb e-Procurement fraud within the CoT.

Three sub-themes emerged from this theme.

5.3.1 Sub-theme 1.1: It is easier to access data during investigations

Neupane, Soar, Vaidya and Yong (2012:308) identified the following benefits of using e-Procurement as noted in Section 2.3:

- Every single activity can be easily overseen;
- Different applications can be tracked;
- The sheer volume of information creates better internal and external communication; and
- Online bidding system decreases corruption.

From the in-depth interviews conducted participants identified access to data during the investigation as one of the benefits of e-Procurement. Four Senior Forensic Investigators (SFI) responded similarly by saying access to the data during investigation is one of the main benefits of e-Procurement. Notably, one participant a SFI talked about efficiency during investigation as a benefit of e-Procurement. The following are extracts of the storyline by SFIs to substantiate this sub-theme:

SFI 1: *"The benefit will be you can get access to the data, unlike when we do the manual one. The manual one it's whereby you do everything manually. The benefit is when you do your investigation, it will help you get documents more easily and it is more accessible like when you do manual you have to go ask from whoever. So, you just go to the system, and you click whatsoever. So, whatever that you need will be there. I think that's the benefit."*

SFI 2: *"It is easier to get access. If you want to do something, you don't have to go in. You can do it online. You can access all your stuff there and submit and so on, probably saving you time."*

SFI 3: *"If I want to go in there to see what's going on, I can go in there. Then I said, because if you talk to me over the phone and say go and check, check, check, I can see, then you don't have to be with me. So, I can go in and check it there. You can access it from anywhere."*

SFI 4: *"Electronic is better. For us as investigators, you can track a trail of document of…it helps with the investigation and then you must do a tracking of invoices. It's easier. Previously, you needed to go and draw all the documentation, go through the documentations. and make copies. You must know. If you've got access to the system, it's easier."*

SFI 5: *"The benefit would be time-save, no loss of documents, I think those two are the main things."*

The above sentiments were echoed by the two Senior Forensic Audit Specialist (SFAS) who emphasised the efficiency and access to the information as a benefit of e-Procurement.

SFAS 6: *"It is assisting us in order to get information very quickly because already information is within the system itself and if you need them, it's very easy to retrieve it. You can approach your client, suspect, whoever, via your electronic means and then it can be supplied very much easier, and you could be specific what you want in terms of the evidence. And in terms of securing it, once you've got it you can save it on various formats. You can do it in the cloud, you can do it on the memory stick, you can even create folder with passwords on your computer, saving it there, so it's not public knowledge. Yes, you put it in one memory stick, you put the memory stick in your pocket. I can retrieve the e-mails, I've got a [sic] external hard-drive with me– As a backup. All I need now to do is just get the hardware again. So, if it was the manual documents, they should have been gone forever."*

SFAS 7: *"It is obviously quicker. It's quicker to do it electronically. That's why you have to see that you always update your computer and be sure that you use the right security measures in blocking the hackers."*

Similar to what was mentioned during the interviews by SFASs above, two Forensic Investigators (FI) concurred that the investigation is much quicker and more efficient when information can be accessed electronically.

FI 8: *"From the top of my head, I would say that one of the benefits would be the costs of the transactions being much less or reduced from what the costs would normally be, and obviously since it's electronic it would be much less paperwork that needs to be performed or used. I think that since it's a [sic] online process, those employees or people that are using such methods, it will assist them to have a greater productivity should they understand how to use the system. Should they not have any challenges with using the system, it would obviously help them to work faster and work better. And I would think that it would assist investigations to run effectively and more efficiently on a system…"*

FI 9: *"I think you can be more precise, you can get your information much quicker, and everything that is there is supposed to be there, approved, signed, not signed in a normal signature at that moment but if it's approved the person is authorised to do that and you know that the evidence that you collect there, electronically, is there what you need it. So, the case can be closed or finalised much quicker."*

It appears from the participants' responses that easier access to the data during the investigation and the efficiency to conclude investigation is a highlight to e-Procurement. The majority of participants share a similar view about this highlight but notably, one participant (FI:8) further explained the advantages of e-Procurement that the costs of the transactions are much less or reduced and that since it is electronic it would be much less paperwork that needs to be used.

5.3.2 Sub-theme 1.2: e-Procurement provides an electronic chain of evidence

As stated in Section 2.3, Anthony (2018:42) indicate that live bidding becomes an honest process because of e-Procurement. Neupane et al. (2012:309) reveal in Section 2.3 that organisations perform better after installing the e-Procurement system. Generally, organisations will budget better and deliver quality and ethical service. "E-Procurement can centralise data in order to improve audit and analysis" as mentioned by (Neupane, Soar, Vaidya & Yong 2012:308) and noted in Section 2.3. Below is the extract from the participant's transcriptions to illustrate this sub-theme:

From the in-depth interviews conducted participants emphasised that e-Procurement can provide the electronic chain of evidence. Two SFIs put forward the following response during the interviews:

SFI 10: *"You can create and develop a proper audit trail, you can have event logs, change logs, so you'll see who's accessed what, when did they access it, has something been changed. You can also take a look at duplicated or altered or tampered-with data. You can also set up preventative protocols. That would involve things like automatic flagging, automatic notification, automatic, what do you call it, transaction termination or halt, very similar to how the banks use their HCH rules with financial transactions. It can be done exactly the same. I think it's extremely powerful. And looking at the direction the world is moving in terms of 4IR, I think that that is the proper adequate direction to actually take procurement. That's not withstanding additional systems that can provide support just for synergy and simplicity, things like apps or different devices to make everything quicker, easier, bring more accountability and transparency, especially in terms of bid submissions and specification drafting."*

SFI 11: *"With the electronic evidence, it can lead to identified risks and then mitigating it as well. Where, in terms of this, to build up a proper case against somebody, it's obvious that we require the evidence. The thing is the accessibility now to that electronic evidence and validation thereof. So, obviously it will…if you have received proper training, you know your legislation around electronic evidence, because it's something that's new to us, we normally deal with hardcore evidence, and then once it's accessed from Systems, Applications and Products (SAP) or whatever the case is, we are not experts on the system. So, obviously then you need to still get a statement from somebody else to confirm that the information retrieved* *from the system is in actual fact factual information and it's a true reflection of the course of events. You need a chain of evidence as well."*

The Managers of Forensic Investigators believe that e-Procurement system will always leave an electronic trail of events that can be used during an investigation or general audit. The three Mangers agreed with the sentiments of the above SFIs and commented that:

M12: *"I think the benefit is that it's on a hard drive, there's less paper. I think you will not have paper trail, but you will have electronic trail. It's actually the same as a paper trail. And the main thing is your software must be updated, your licenses must be updated, and your antiviruses must be updated. I think that's the most benefits, I think it is less time-consuming to do it electronic. It's readily available."*

M13: *"And if you finish your part, you go to the next part. The next person must access it for the next part. So, I think the in between is being cancelled out. [the footprint] will always be on a backup system."*

M14: *"I think being an electronic process it will be beneficial in terms of tracing the process where it starts from the requisitioner to the cost-centre owner to supply-chain management and then to the vendor. I think because the application process will be electronic, I think it's easier to determine if there is a risk involved."*

The above-quoted statements are complemented by one FI who stated that:

FI 15: "*To us as investigators and also, I think, to auditors it's easy for us to get evidence. So, there is that thing. History or…there's this other word. Footprint. So, it's easy for us to get that when you are investigating such things."*

From the response from the interviews, there was a unanimous and overwhelming agreement amongst the participants that e-Procurement can provide electronic chain of evidence and electronic trail of events.

5.3.3 Sub-theme 1.3: e-Procurement provides an opportunity to reduce fraud

It is the submission of authors such as Subramani (2004:22) and Makoba et al., (2017:180) that e-Procurement contributes to the reduction of corruption within the procurement process and increase fairness by automating the selection process and removing human interference. Using e-Procurement results in better communication, an increase in moral standards in a form of accountability and reduced costs in all departments. (See Section 2.1).

As mentioned in Section 2.3, and according to Anthony (2018:42) the advantages of implementing e-Procurement in South Africa are high. For one, the transparency of competitors' bids and tender information means that prices can be adjusted. This will also make service provides better as they will aim to beat the competition. There will be less corruption, organisations will be able to reduce costs and improve messaging. As noted in Section 2.3, Neupane, Soar, Vaidya and Yong (2012:308) maintain that favouritism, corruption and miscommunication are sorted by the exclusion of the human error in e-Procurement.

The sentiments shared by participants was that e-Procurement can reduce fraud and corruption as five SFIs commented that:

SFI 16: *"I think it's money, so revenue. If you don't have e-Procurement, a lot of fraud can happen. So, it prevents fraud and to manage your finances."*

SFI 17: *"E-procurement, reduces a lot of fraud within the City, which is beneficial in terms of the operations of the City with regard to procurement processes."*

SFI 18: *"As you know that the benefit of moving from manual to automated system, it actually eliminates lots of fraud risk, particularly when it comes to* *fraudulent document, fraudulent signatures. So, this will come as a great benefit in terms of fraud risk management. And then it's not necessarily easy to manipulate the. It is all automated. So, the benefit, it basically talks to what I've mentioned about the elimination of tempering of document, fraudulent signatures. Because you'll just have to look on the system and process the transaction without one going into the actual document as a way of doing conservative processing of documentation."*

SFI 19: *"I think the benefits is to minimise corruption, it reduces fraud, and minimum errors as the process is transparent. You are able to trace the whole procuring process from when the user creates a requisition and also to the…to procure certain goods and services until the end when the invoice is paid. So, you can trace who interacted with the purchase and who created the requisition, who sourced the supplier, the pricing also is there, when and who authorised, and then also when was the invoice submitted and when it was paid. You will have that audit trail that is available that can't be deleted or tampered with. In this case, it will be easier to catch if there's any fraudulent activities involved. It is also timesaving, and also buying is standardised. There is automated and Purchase Order generation and all that. And e-Procurement also it promotes competitiveness and it ensure higher level of supplier participation in the tender process. And there is less paperwork. Also, there is no administration or transactional cost. It is also easy to manage the vendors."*

SFI 20: *"I think it is best at the end of the day because you can put someone's information on electronic devices, and I think you can have a broader view. I think it's positive. I think it's more effective. Also, environmental matters it's also good. Yes, I think it's better control, it's effective to eliminate fraud. Also, with preventing fraud, to identify, to highlight risk, red flags. So, I can see it definitely positive."*

The above-mentioned statement was supported by one Manager who indicated that e-Procurement can detect any fraudulent activities:

M21: *"The system is supposed to pick up duplications, people that are linked to Council, government, provincial organisations, and the system is supposed to block them and flag them and inform the people of supply chain when they detect any such anomalies. The system is also supposed…or I know that it is blocking people when the information is not correct. They need to go through a registration process at the National Treasury where most of the vetting is done or supposed to be done. So, in theory, the system should work, and it should detect…because there's more people or more processes the application goes through, to detect any possible fraud or corruption at an early stage. In theory that's the idea. Unfortunately, it's not working perfectly."*

Two FIs agreed and concurred with the above-mentioned sentiments by summing up the benefits of e-Procurement as follows:

FI 22: *"I think the e-Procurement, the establishment of e-Procurement, is time-consumption, that is one of the advantages, and then as well as I think it will also minimise fraud and corruption in the sense that it can be traceable if there is any maladministration or any mischievous being committed by an employee. So, it would be easy to trace it because it keeps record. And then the effectiveness of it is that it will show you the time, the date, the employee who processed each and every thing. That is the advantage of it."*

FI 23: *"I think e-Procurement is going to minimise corruption because the data from…or the information from the service providers is going to be put into the system, so that will eliminate this thing of people trying to corrupt the system."*

From the above, it seems all participants know the benefits of e-Procurement. The participants have a common view that it is easier to access data during an investigation, and that e-Procurement provides an electronic chain of evidence, and it can reduce fraud and corruption. There was a clear understanding of the advantages of e-Procurement by all participants based on their affirmative response.

5.4 THEME 2: THE CHALLENGES OF E-PROCUREMENT IN TERMS OF FRAUD RISK MANAGEMENT AT THE CoT

This theme discusses the participants' understanding of the challenges of e-Procurement in terms of fraud risk management at the CoT. This theme explored the experiences of participants about the challenges of e-Procurement.

The answers to the following question gave rise to this theme and its sub-themes:

- *"In your opinion, what are the challenges of e-Procurement in terms of fraud risk management at the CoT?"*

The question helped gauge the experiences of participants with reference to the challenges of e-Procurement in terms of fraud risk management at the CoT. It is necessary for the participants as Forensic Investigators to know the challenges of e-Procurement for them to effectively use e-Procurement fraud within the CoT.

The sub-theme that emerged provided an understanding of the challenges of e-Procurement by participants.

5.4.1 Sub-theme 2.1: e-Procurement presents opportunities for fraudulent activities

As noted in Section 1.2, the challenges posed by e-Procurement system as pointed out by Galloway (2003:16), is the security of information in the database and transactions since the e-Procurement is a web-based system and network dependency which requires internet connectivity, data is transmitted between entities and companies. These increased the vulnerability of interception. The system can be hacked, and information can land in the wrong hands.

According to Cascarino (2013:360) and as mentioned in Section 2.4, some of the challenges of e-Procurement is individuals not correctly confirming their identity when using the system. This missing validation means that the individual or party cannot be legally liable for their action. Another issue is the risk of data integrity, where data can be remotely altered. Whether intentional or accidental, corruption results in:

- Amending catalogues without authorisation (advertising, reporting, approval);
- Destruction of audit trail;
- Tampering with the ordering process;
- Interrupting the recording of transactions; and
- Disrupting online tendering.

Anthony (2018:44), as presented in Section 2.4, suggest that collusion among the small group of suppliers is something to be noted in an e-Procurement process.

The managers at GAR contend that a major risk or threat to e-Procurement is that it presents the opportunity for fraudulent activities due to its internet and Web dependency. The three Managers mentioned during the interviews that e-Procurement is vulnerable to fraud. They put forth the following responses:

M1: *"When it was done manually, the vendor was every time required to complete certain supply-chain management documents which needed to be accompanied to the quotations, a declaration of interest document. So, when it was manual, you will find that the particular vendor would not necessarily remember…if he's got more than one company registered individually or separately as different vendors, he will not necessarily remember for Company A which address or telephone number he used. So, sometimes in the manual version we were able to pick up that it's two different vendors, two different owners, but using the same contact number or addresses. Then you know there's something happening there. But with the e-Procurement, the system will guide the vendor and say but you can't use this address because it's already used before. So, then he will realise* *his mistake, he will fix it then, and then the quotation will be accepted. So, I think the e-Procurement will sometimes guide the vendors of mistakes that could have been picked up by the investigators."*

M2: *"The challenges of e-Procurement. From an investigation point of view, I actually…when I did supply-chain investigations, it was better when companies or directors completed the forms by hand because they made a lot of errors on the form, especially when they try to register more than one company. So, that was easier to pick up a link with companies, people, directors, and so on. But, unfortunately with e-Procurement, the system blocks them to make such mistakes. So, sometimes you want people to make the mistakes, you must leave them to make the mistakes, then it's easier to detect, but the system will block them if they use more than one number, more than one e-mail, more than one ID number. So, the system is actually helping them not to make the mistakes."*

M3: *"Everybody must know the system, our security system, our software updates, our antiviruses must be top notch to detect hacking. Hackers can use your company. A good hacker can infiltrate e-Procurement system."*

The views by the Managers above were also complemented by the statements made by four FIs during the interviews that e-Procurement can be hacked and manipulated. The following quotes support this:

FI 4: *"The challenges are just that because there are some instances of electronic systems are concerned, they can manipulate it. But chances are slim. Only on condition if somebody knows or if somebody can steal your passwords in order to get through it, that is the disadvantage of it."*

FI 5: *"I think the challenges is people have to be trained, people have to make a mind-shift of going to the electronic side. I think there's a challenge as well that it can be hacked, it can be manipulated, but only if people that…it is normal hackers that can do it. They can do it while sitting at home, they're* *doing it in the KwaZulu-Natal ports, they do it in the banks, so they can manipulate it."*

FI 6: *"In terms of investigations, specifically to the City, I think our challenge is us not being trained on how to get or achieve the footprint. And remember, a person who works straight with whatever, the e-Procurement or something, they can manipulate the system somehow. And remember, we also rely on them, on IT, for us to get that footprint. So, the challenge is that it can be manipulated."*

FI 7: *"There will be some challenges every day…because nowadays we use the computers, we do experience some challenges. I think even in the e-Procurement, we are experiencing some challenges here and there. Because you'll find that some of the information is missing, it's not in the system."*

In corroborating the sentiments by FIs above, eleven SFIs are of the view that e-Procurement system can be tampered with, manipulated and is susceptible to fraud through hacking. They also emphasise that suppliers can inflate the prices which is another form of corruption. The following verbatim quotations of SFIs illustrate this sub-theme:

SFI 8: *"The challenges will be whereby if someone is not scanning the right documents, or they duplicate the document on the system. Because when you do on your system, the problem is someone can just collect document from other people and then do them electronically, unlike the people…I don't know, I gather that is when the digital investigation come in. But then tampering it will be based on the approval and the scanning and all those things. I think that's when the tampering will come in because it's the person at the end of the day who's doing the capturing on the system. But deleting, that's when the digital will come in, in that way they don't see what has been deleted on your system."*

SFI 9: *“The challenges are probably they can defraud stuff, they can get stuff…if they have to submit, they can change it and then send it through and pretending it’s theirs. That is also the other stuff that they can make fraud with it, all the online stuff that you can do, all the documentation that you can get. Maybe getting somebody else’s documentation, changing a couple of things, and then submitting it as yours.”*

SFI 10: *“It doesn’t red flag us about the officials. It’s only the official that’s dealing with it at that level that knows, and they don’t disclose. We have to rely on them to get the information. The inflated prices are one issue. So, it’s not market-related prices that we are receiving. So, whatever comes through the e-Procurement system, the City then just accepts whichever one. Even if it’s the lowest but it’s not market related. That’s one of the problems that They [departments] just take the lowest. So, it’s not necessarily market related. That’s what we need to look at, to zoom in.”*

SFI 11: *“The risk is that the rotation of the suppliers contacted, from what I’ve been told, is the issue where some of them interact…from what I’ve found is that some of the people they consistently use the same suppliers. Number two, they also use suppliers that are family-friend orientated and so on. And then with our direct interaction with them, even with presentations, we found that that was brought forward to us. So, then they wanted to know what they do in the instance where they have relationships now or family orientated, whatever, friends, whatever, with specific companies, and some of them have not been declared. So, then they just process it, and they go ahead.”*

SFI 12: *“Based on some of my interactions with the colleagues at SCM, we found that the prices that we obtain as well as the suppliers that are contacted through this e-Procurement system, number one, they do not necessarily respond to it timeously, number two, we’re receiving quotes with inflated prices.”*

SFI 13: *“The one is the officials did not declare. So, the systems that we have in place is basically…let us put it this way, it’s not sufficient to deal with this type of thing. With the tender processes, there’s declaration, then you can physically verify but with the e-Procurement system you cannot verify the relationship between the supplier and the employee. But ten to one, they might have the same surname or a different surname. It might be, for example, a female working there with the sister’s stuff, but the sister carries a different surname. So, that is basically the deficiency that we pick up with.”*

SFI 14: *“Not capturing the information in time or somebody misplace the documents purposely or along the line fraudulently or certain delay or changing the information to his own benefit probably.”*

SFI 15: *“I think the amount of people that must authorise transactions. Sometimes they are not available, or the system can still be manipulated to help a certain vendor get the work. It might be manipulated.”*

SFI 16: *“If it is electronic, people can hack the system…”*

SFI 17: *“The other thing is you’ve got issues such as malware, spyware, that kind of stuff that has got malicious intent to monitor the system. Then you’ve got hardware issues to actually run the specific software or the code. Then it will also open the City up or make the City more susceptible to cybercrime such as ransomware, phishing, hacking, that kind of stuff which makes City of Tshwane data more valuable. The City of Tshwane have to be stricter in adherence to data privacy laws, whether national or international, especially in terms of the new POPI Act. The GDPR is also going to play a significant role. Vetting and screening in terms of vendors is going to be a little bit more complicated, especially if they also have to form subject to GDPR as well as certain specific POPI requirements, which means that will become an additional vendor requirement before they are even allowed to be a vendor.”*

SFI 18: *"The challenges may come as a result of lots of…it may come as a result of the system itself for those who don't have adequate training to procure to use the system, and particularly with other risk such as…the other challenges such as hacking of a system without abuse of the system, one can be able to access some official's credentials and process a fraudulent transaction. So, these are the things that I think it might be some challenge. And then moving from manual to automated system, it might be a mammoth task if it's not done well because some of the things can be lost in transition."*

Notably two SFASs reiterated during the interviews that the main challenges of e-Procurement system are that it can be infiltrated and manipulated. The following quotations illustrate their views:

SFAS 19: *"The challenges already you're going to get them because normally you've got some of the officials that they wanted maybe to infiltrate the system and those red flags definitely show. You are going to encounter them. People can manipulate the system easily. The challenges. Persons who are knowledgeable about the electronic environment are people who can easily manipulate that information as well. People who know how to hack computers can hack your computer. There are pros and cons, but I prefer to see more the pro than the cons. Your handling of the evidence, in other words if it's…you don't have to carry around a lot of documentation, especially if it's documents."*

SFAS 20: *"The first thing, the City does not have a fraud risk register. That is the key issue. So, we have not assessed e-Procurement system But in terms of our strategy and all that, we're supposed to have a fraud risk register in place already. And, unfortunately, we're still in developmental stage to attain that. But from virtue of the type of work that we do, obviously electronic quotations are sourced through the e-Procurement system, which is an advantage to the City."*

It is clear the 20 participants know the challenges of e-Procurement. These participants share a similar view that e-Procurement system presents opportunities for fraud. The common views of these participants are that e-Procurement is susceptible to fraud, it can be hacked and manipulated. Notably and important to mention is that one participant (FI:7) confirm during the interviews that in one of his investigations of e-Procurement fraud, some of the information was missing in the system (either deleted or altered). This was clear proof that e-Procurement can be tampered with. It also emerged during the interviews that three participants seem not to be aware of the challenges of e-Procurement as they did not respond affirmatively. They provided the following responses:

SFAS 21:	*"I don't know of any challenges of e-Procurement."*
SFI 22:	*"I am not familiar with e-Procurement, and I can't really talk much about it."*
FI 23:	*"I don't want to lie to you, I'm not familiar with any challenges."*

The findings revealed that the investigators must acquaint themselves with the challenges of e-Procurement to be able to effectively investigate it and to mitigate any risk and shortcomings associated with it. It is necessary for the investigators to know the whole e-Procurement system and its operations precisely so that they will be able to pick up any anomaly during probity reviews and preliminary enquiries.

5.5 THEME 3: FI'S LACK KNOWLEDGE OF THE DIFFERENT TYPES OF E-PROCUREMENT MODELS/SOLUTIONS AT THE CoT

This theme presents the participants' familiarity with different types of e-Procurement models or solutions as it is essential knowledge for GAR investigators to know the models or solutions that they are investigating.

This is the main question in line with the theme:

- *"Are you familiar with the different types of e-Procurement models/solutions? If yes, which model/solution does the CoT use?"*

The GAR investigator’s comprehensions and acquaintance were questioned to see how familiar they are with different types of e-Procurement models or solutions. This research also sought to establish which e-Procurement model is the CoT are currently using. This is how the sub-themes unfold:

5.5.1 Sub-theme 3.1: FI’s lack knowledge of e-Procurement system in general

As noted in Section 1.5.1, “e-Procurement is the use of internet-based inter-organisational information system, which automates and integrates any part of the procurement process in order to improve efficiency and quality in public procurement and to promote transparency and accountability in the wider public sector” (Thai (2019:477). Thai (2019:477) goes on to say that the e-Procurement is a comprehensive and holistic solution to other acquisitions in the organisation.

The participants lack knowledge of e-Procurement in general, as illustrated in their responses below. The verbatim responses clarify this sub-theme:

The sentiments of the two managers are that they are not familiar with the e-Procurement system. The following quote supports their view:

M1: *“I cannot really talk about e-Procurement. My experience is only in general procurement.”*

M2: *“I don’t know much about e-Procurement system.”*

The statement above was complemented by what was pointed out by 6 SFIs that they are not familiar with e-Procurement system. The following responses were put forth:

SFI 3: *“I’m not familiar with this kind of procurement. I have never worked with e-Procurement.”*

SFI 4: *“I haven’t done e-Procurement so far. I have done general procurement sorry.”*

SFI 5: “*I haven’t done any procurement since I came here. I can only talk about general procurement.”*

SFI 6: “*I am not familiar with e-Procurement.”*

SFI 7: “*I haven’t done e-Procurement.”*

SFI 8: “*We just know of the e-Procurement system. That is basically it, with the interlink with the SAP system and that’s it. We are not given full insight into it.”*

It is clear, based on the responses from the majority of participants that they are not aware of the e-Procurement system. It is necessary for the investigators to be familiar with the system that they are required to use during e-Procurement investigations. The lack of knowledge of the e-Procurement system makes it practically impossible to efficiently investigate e-Procurement. GAR investigators must acquaint themselves with the entire e-Procurement system. They should know how it operates.

5.5.2 Sub-theme 3.2: FI’s lack knowledge of the e-Procurement models/solutions at the CoT

According to Bidgoli (2019:149), the B2B model uses technologies such as the internet, extranet, virtual private networks, EDI and EFT extensively to help everyone involved to communicate effectively. Lysons and Farrington (2006:187) agreed with Bidgoli (2019:149), as noted in Section 2.5, e-Procurement solutions can be broken into seven sections:

- EDI networks;
- B2B;
- B2E;
- Corporate procurement portals;
- First generation trading exchanges: community catalogues and storefronts;
- Second generation trading exchanges: transaction orientated trading exchanges;

- Third generation trading exchanges: collaborative supply chains; and
- Industry consortia: buyer and supplier led.

As presented in Section 2.5, Chaffey (2011:368) agrees with Jooste and Schoor (2003:14) indicating that e-Procurement has three models which are buy and sell side models, and independent marketplace. According to the CoT e-Procurement Technology Architecture (2016:6), the CoT uses EDI solution to procure with its suppliers (See Section 2.5).

There was an overwhelming lack of knowledge about e-Procurement models or solutions amongst the participants. It appears from interviews with participants that there is an enormous lack of knowledge of the model or solution that the CoT is currently using, which is a serious predicament to investigations. In essence, the investigators are utilising a system even though they are not familiar with the model.

The sentiment of five FIs, with the exception of one FI, is that they are not conversant with e-Procurement models or solutions. Only one participant was able to allude to the e-Procurement models affirmatively. 22 participants are not acquainted with the model or solution the CoT is currently using. The following excerpts illustrate the participants' sentiments:

FI 9: *"I've come across one or two solutions. I'm not very well-knowledgeable about it. I've heard about the business-to-business, I've heard about electronic data integration, but that's just through maybe conversation or one article. But I have very limited knowledge about that. That I am not sure if the City is using any of these solutions."*

FI 10: *"At this stage, I don't want to lie to you, I'm not so much familiar about them."*

FI 11: *"No, I am not familiar with them"*

FI 12: *"No, I'm not familiar with that. Because I've just read a bit about e-Procurement, so I didn't get into deeper details to see how it really works.*

But I think in future maybe the City will do something to sensitise us so that we are more familiar with"

FI 13: *"It's just like now, presently, I came across the e-system and e-Procurement is one and the same thing. The advantage part of it as I'm busy conducting investigation indigent…the POP, …[Poorest of the Poor], those are the indigent people. I came across the Department of Social Health and Social Development that they are implementing the e-system whereby they are no longer going to use the manual system, and then they've just taken me through that processes of the e-system, how it works. It's the only which I think now…that one it looks very much excellent."*

The above-quoted sentiments by FIs are echoed by the view of a manager who was even confused about the e-Procurement models and stated that:

M14: *"I think we are supposed to know the system/the e-Procurement model that the City is currently using, but I've got no idea. I did not even know there's more than one e-Procurement model. Is there more than one e-Procurement model?"*

In support of the above-mentioned statement, three SFASs remarked that they are not familiar with e-Procurement models, and which model the CoT is currently using. The following quotes illustrate their views:

SFAS 15: *"No… I don't know the whole process."*

SFAS 16: *"No, I am not familiar with the solution that the City is currently using."*

SFAS 17: *"No, I don't know."*

The six SFIs summed it up with the following quotes to support their views:
SFI 18: *"I don't want to. I don't know what they [the City] are using."*

SFI 19: *"I don't know which one the City is using"*

SFI 20: *"Not really. I can't…I'm not that clued up with that."*

SFI 21: *"No, I'm not familiar with those ones."*

SFI 22: *"I don't know the different types of E-procurement and solutions"*

SFI 23: *"I don't know what the City is using"*

From the responses of the participants, it evidently appears there is a massive gap in what e-Procurement systems and models are. Notably, only one participant who is a junior FI managed to respond affirmatively about e-Procurement models. 22 participants are not familiar with the e-Procurement model the CoT is currently using, which is EDI. The fourth theme presents the participant's knowledge of the legislative framework that governs e-Procurement practices in SA and will be discussed next.

5.6 THEME 4: FI'S KNOWLEDGE OF THE LEGISLATIVE FRAMEWORKS THAT GOVERN E-PROCUREMENT PRACTICES IN SA

The participants' knowledge and experiences were pursued to establish their familiarity with legislative frameworks that govern e-Procurement and procurement in general. Legislative frameworks are guiding principles that outline the methodologies to be followed when procuring any goods and services in SA. Equally important, the investigators are required to follow these prescripts when conducting an investigation.

The answers to this question motived this theme:

- *"Are you familiar with the legislative framework that governs procurement practices in South Africa?"*

This question was explored to measure the participants' comprehension of the legislative framework governing procurement practices in SA. The below sub-themes support the argument.

5.6.1 Sub-theme 4.1: FI's knowledge of the legislative frameworks that govern procurement in SA

As noted in Section 2.8.2, Ambelm and Badenhorst-weiss (2012:248) identified numerous legislative frameworks that are guiding principles of procurement practices in South Africa as follows:

- Constitution of the Republic of South Africa, Act no:108 of 1996;
- PFMA;
- MFMA;
- PPPFA;
- BBBEE;
- PRECCA; and
- National treasury Regulations (2005).

The sentiments of the majority of participants were that MFMA is the guiding principle for the Municipalities. Three Managers commented MFMA, PFMA, BBBEE and National Treasury Regulations as the main regulatory framework that governs procurement practices in SA. The following are quotes to illustrates participants' views:

M1: *"National Treasury Regulations. I'm familiar with those. Not out of hand do I know that [legislative frameworks]."*

M2: *"The Municipal Financial Management Act is one. That will give local government, not necessary only the City of Tshwane but local government in whole, and even the BBBEE will also be part of that. But it will give guidance to all municipalities. But even government has got a similar act PFMA, but we are focusing on local government."*

M3: *"I do because I'm working with MFMA. No, I can't think now"*

The sentiments by Managers above are supported by the views of three SFIs who also remarked that MFMA is a guiding principle that governs procurement in SA:

SFI 4: *"The Municipal Finance Management Act. I will not be able to give it to you. I've got it on my PC"*

SFI 5: *"The Systems Act and MFMA."*

SFI 6: *"We actually don't to that many procurement cases, I can only think of MFMA."*

Contrary to the above statements by Managers and some SFIs, 1 FI was not able to list any regulatory frameworks citing that he is not familiar with:

FI 7: *"No. On that part, I'm not familiar. But one day when I was going through some information on the computer, I did see that framework, but I didn't have time to read about it. But I know that there is something like that."*

It is clear the majority of the participants were able to allude to the regulatory framework and the common understanding was that MFMA is the guiding principle for the Municipalities.

5.6.2 Sub-theme 4.2: FI's knowledge of legislative frameworks that govern e-Procurement

Ambelm and Badenhorst-weiss (2012:445) point out that the national treasury regulations push the agenda of the PFMA and MFMA, while combining the different responsibilities of the SCM function into a singular function performed by not only the accounting officer. In addition, Ambelm and Badenhorst-weiss (2012:445) mention that all departments, from national to local, are to work within the confinement of the supply chain and procurement regulations (See Section 2.8.2.7).

From the responses during the interviews, there was an unequivocal common view that participants are familiar with a regulatory framework that govern e-Procurement in SA. The essence raised by the majority of the participants is that frameworks that govern general procurement and e-Procurement are the same. The researcher shares the same sentiments with the participants' opinions.

In addition to National Treasury Regulations, MFMA and PFMA, which are widely cited as the main guiding principles of procurement, the three SFASs hinted at other frameworks that govern procurement in the CoT, which are the SCM policy, CoT Systems Act, CoT Structures Act, SCM SOPs and Code of Conduct for SCM officials. The following quotations illustrate their views:

SFAS 8: *"We have got Procurement Policy, meaning that is a Supply Chain Management Policy, which are in line with the MFMA. Because we must not deviate, create our own legislations.*

SFAS 9: *"Procurement, yes. Treasury has got proper prescriptions, the National Treasury regulations, and Public Finance Management Act prescribes, as well as the Municipal Finance Management Act prescribes, as well as our policies, procedures, and Structures Act, Systems Act. …the Supply Chain Management policy. Even Code of Conduct for SCM officials."*

SFAS 10: *"Yes, I am. It depends on what case you're busy with in the investigation. MFMA is an umbrella"*

The common view was also shared by four FIs who also corroborate the statements by SFASs above, however, the FIs notably included the additional regulatory frameworks namely: Electronic Communication and Transactions Act (ECTA) and Protection of Personal Information Act (POPI Act). The following responses was put forth:

FI 11: *"I would think, from the top of my head, I would say that the Electronic Communication and Transactions Act would give some guidance as to the procurement practices. Maybe the PFMA or the MFMA may have some guidance on it as well."*

FI 12: *"I can say partially I am, just because now we are dealing with Procurement. Supply chain management policy, that is one which we are dealing deeply with it, and then when dealing with them we have to consider what says the South African legislation as far as procurement is concerned because the one from the City and the one from the National is nearly the same as they have been drafted from top to the lowest level of government, which is the municipality. Municipal Finance Management Act and public Finance Management Act."*

FI 13: *"Not in the Council but POPI Act and those I know. Treasury Regulations and so on. It is there but I don't think about it now, but it is there. All of them are there."*

FI 14: *"There's that Treasury Regulation, if I'm correct. MFMA or what. But I think usually the e-Procurement thing it should be under Treasury Regulations."*

Nine SFIs also supported the sentiments of all other participants. However, they also included other frameworks not stated by other participants namely: Whistleblowing Policy, PRECCA, Protected Disclosures Act, Companies Act, Value Added Tax (VAT) Act, SARS legislations, and Cooperatives Act. Notably, they also mention the Constitution of SA as one of the guiding principles that governs procurement. SFIs summed it up with their quotes as follows:

SFI 15: *"I think MFMA. Treasury Regulations… –What is this? Procurement regulations and all that. …I think it has to be PFMA, what's this one? I gather they must have BBBEE, then they must also have…what is this? Can I just name all those?"*

SFI 16: *"Whistleblowing and Prevention and Combating of Corrupt Activities Act, a whole lot of legislation that goes with."*

SFI 17: *"In the main, they start from the constitution, that is where procurement is first regulated. Plus, you have the supply-chain management regulations, you have the supply-chain management policy that also covers these types of things. National Treasury regulations. Regulations and directives issued by them as well."*

SFI 18: *"Companies Act. There's various legislation that…because it's endless actually, that goes into play. Apart from that, it's the Protected Disclosures Act 26 of 2000 read in conjunction with the Whistleblowing Policy adopted by the City in 2012. When you get whistleblowing is another challenge. It needs to be tested to see if they're acquainted with this type of thing, and how do they handle the confidential information that's being sourced through whistle-blowers?"*

SFI 19: *"Yes. In terms of local government, you have Supply Chain Management policies and principles and protocols. You also have the MFMA, Municipal Finance Management Act. In terms of provincial and national, it converts to the PFMA."*

SFI 20: *"PFMA and PPPFA. And then you've also got your other legislation that factors in, such as you've got the Value Added Tax (VAT) Act, you've got SARS legislation, you've got Companies Act. It's extremely broad field, Cooperatives Act as well."*

SFI 21: *"The constitution. The MFMA, the Supply Chain Management policy, and Preferential Procurement Policy Framework Act. The Electronic Communication and Transactional Act. I'm thinking of those."*

SFI 22: *"I'm familiar [with legislative frameworks]. For the City, you've got the MFMA and those stuff."*

SFI 23: *“Yes. Preferential Procurement Act, Supply Chain Management Act. Those are the two that…and, again, you will have to get the guidelines from National Treasury, which they normally issue the practice notes with regard to procurement. When we investigate procurement, the major act that one will have to consult, is MFMA which the MFMA and Supply Chain Management Act.”*

Based on the feedback from the interviews and literature review, there were enormous common sentiments shared by the majority of participants that the main regulatory frameworks that govern procurement are the Constitution of SA, PFMA, MFMA, PPPFA, BBBEE, PRECCA and National Treasury Regulations. Some participants mention Whistleblowing Policy, Protected Disclosures Act, Companies Act, VAT Act, SARS legislations, and Cooperatives Act as other frameworks that govern procurement. Other participants listed the framework that governs procurement in the CoT as follows: SCM policy, CoT Systems Act, CoT Structures Act, SCM SOPs and Code of Conduct for SCM officials. ECTA and POPI Act are also equally important as mentioned by other participants.

All these frameworks will be guided by the Constitution of SA which conform to the five pillars of world-class procurement, such as transparency and fairness (See Section 2.8.1). The fifth theme presents the participant’s perspective and experience of the effectiveness of electronic data recovery in the investigation of e-Procurement fraud and will follow for discussion.

5.7 THEME 5: FI’S OPINION WITH REGARDS TO THE EFFECTIVENESS OF ELECTRONIC DATA RECOVERY IN THE INVESTIGATION OF E-PROCUREMENT FRAUD

This theme presents the participant’s perspectives and experiences about the effectiveness of electronic data recovery in the investigation of e-Procurement fraud. GAR investigators are required to apply the electronic data recovery to enhance their investigation of e-Procurement fraud. This theme is centred around the issue of capacity of the GAR investigators to recover electronic data in the investigation of e-Procurement fraud.

The next set of questions are linked to the sub-themes:

- *"In your opinion, do you regard the application of electronic data recovery in the investigation of e-Procurement fraud effective or not?"*
- *From your experience, does the CoT forensic investigators have sufficient capacity to recover electronic data during the investigation of e-Procurement fraud?*
  If yes, please elaborate your answer?
  If no, how does the CoT deals with electronic data recovery?

The GAR investigators' opinions were sought to understand their viewpoints on the effectiveness of electronic data recovery in e-Procurement fraud investigation, and also how the CoT forensic investigators perform in this regard. This research also sought to establish if the CoT forensic investigator did have sufficient capacity to recover electronic data. The participants' responses were unanimously negative, indicating that they do not have the capacity to recover electronic data. The participants' perspectives on how the CoT currently deal with electronic data recovery was also sought. The overwhelming view was that the CoT is outsourcing electronic data recovery to the panel of service providers. Notably and equally important is the unequivocal common sentiments shared by all the participants that electronic data recovery in the investigation of e-Procurement fraud has the capacity to be effective if done correctly and properly.

5.7.1 Sub-theme 5.1: FI's are of the opinion that electronic data recovery in the investigation of e-Procurement fraud has the capacity be effective

As noted in Section 3.2, the importance of electronic data as advised by Casey (2011:6) is that they reveal the who, what, when and why in an investigation. Cornick (2014:163) is of the opinion that electronic data is significant because even if the data is deleted or destroyed, it can be reconstructed or recovered. In simple terms, it means electronic data is evidence that never cease to exist.

Even though all participants lack capabilities to recover electronic data, they are aware of the basics, which is that this system is to find, copy and present digital data, which will enhance the investigation of any e-Procurement fraud investigation. Electronic data recovery is the most important stage of an e-Procurement fraud investigation because a substantial amount of evidence, if not all, are stored electronically in the e-Procurement system and need to be recovered and analysed.

The views of the three Managers emanated from the interviews are that electronic data recovery has the capacity to be effective in the investigation of e-Procurement fraud as an investigator can retrieve any evidence from the e-Procurement system. It is much safer, better, and less time-consuming. The following are verbatim prescription quotes to illustrates participants' views:

M1: *"It will be effective if you do it the right way."*

M2: *"I think it's effective. Because it's fool-proof. You can't manipulate it like you can manipulate a paper trail. I think it's much safer and better and less time-consuming."*

M3: *"Yes. It's effective. It can be recovered but, again, the investigators need access, you need to understand what the document is offering you, where to get the document, what does it mean. If I steal your computer, it's still on the server. You can retrieve everything back into the system…I think it should help a lot."*

The sentiments of Managers above are supported by an SFAS who indicated that electronic data recovery in the investigation of e-Procurement can be effective and can improve investigation success by 70 percent to 80 percent. The following response was put forth:

SFAS 4: *"In my opinion, it is effective. The reason why, because already when we do projects, especially on e-Procurement, there is a success at the end of the day regarding that, maybe seventy to eighty percent that we can detect them."*

The above-mentioned statement was corroborated by five FIs who commented that electronic data recovery in the investigation of e-Procurement can be effective and it can assist one's investigation to be conducted smoother and more efficient. The following quotations illustrate participants' views:

FI 5: *"I would definitely think that it would be effective. If anything is helping your investigation to move smoother and better, it will obviously be effective in conducting your duties and your tasks."*

FI 6: *"Because of if you are given a task to execute, it's going to be easy if you know electronically just because you can investigate while sitting down on the table because more of the information you are going to get from the system. Just for example, I can give you one thing now, the one I'm dealing with. I'm sitting here in my office and then doing investigation of the indigent people."*

FI 7: *"Yes, I do. I think most of your information is there. It will be on-hands. I think you can prove it in a much better way."*

FI 8: *"I think it's going to be effective because I don't think they will implement something which is not effective. Remember, we are moving to improve things. What I'm trying to say is that, as we go on, we move from the old practices which were not effective to more things which are more effective and try to shorten the time. Yes, I think it will be effective."*

FI 9: *"It's effective because, remember, you get it raw anyway. So, I'm going back to the first ones that you're not relying on anyone. So, you get it raw as it is, you get all the history as it is, so there's no need for you to* *manipulate it or something. So, that's why it's effective. So, it's somehow true. You know you can rely on it, that relying on someone. We can recover it."*

There was a common view by seven SFIs and also supported the above-mentioned statements by FIs that electronic data recovery in the investigation of e-Procurement fraud can be effective because any electronic transaction that was performed on e-Procurement system does leave a footprint that can be recovered. The following quotes were put forth:

SFI 10: *"I think the electronic data recovery have got the capacity to acquire…retrieve and presenting data that has been processed electronically and stored on a computer, which will be compellable to investigate, if there's any fraud in the e-Procurement."*

SFI 11: *"It can be effective at the end of the day, if they put everything there. Remember, to retrieve something is actually that you can get everything back. As long as it's a computer, it's a matter of extracting and you can go and dig further."*

SFI 12: *"It is effective. Because in that way you can discover what you have missed out when you were doing the manual investigation."*

SFI 13: *"It is definitely effective. It is effective because when you do recovery of this electronic equipment, you go when the suspect is not informed that on that day you are coming. Most of the information will be still intact. Therefore, you'll find them and it's still able to recover."*

SFI 14: *"It is effective. I think any electronic transaction that you do does leave a footprint, so it must be effective, if you, again, know the system. So, if I know how to do the investigation and know more about electronic recovery, you can trace it back to an individual or an individual's PC. So, it is very effective if you know it. The information [footprint] will be there. Even after it was* *deleted, you can be able to recover it. Even if you try to break the hard drive, it must leave something on the frame as well."*

SFI 15: *"It is effective, particularly when it's being done well, in a sense that you only rely on what has been done. In most cases, the electronic evidence, it will forever remain there, meaning that you can't delete. You can either recover it even though someone has just made an input into that particular PC. It will always leave the footprint forever. Unlike a manual, if I can burn the papers, then there's no way that you can retrieve. You just shred then it disappeared."*

SFI 16: *"If it is applied correctly, it will be extremely effective. You're going to have a much higher level of integrity in your evidence. The investigation process is also going to be a lot more simplified with much better quality of evidence. You will be able to obtain more real evidence instead of just circumstantial evidence. Moving away from documents and affidavits to what is the find in terms of the ECT Act as computer-generated evidence, which is viewed as either documentary or real evidence, depending on the circumstances of the case. I know that in South African legislation they've moved quite far forward in terms of the law of evidence, and computer-generated evidence is no longer deemed hearsay evidence. In terms of section 3 of ECT Act requires that courts provide for computer-generated evidence and must give weight to it. So, on a case-by-case basis, that will then be assessed. So, whatever evidence is obtained through a computerised system or computerised intervention is by default in terms of the ECT Act and obviously now in terms of the new Act, already deemed as evidence. It will then just have to go through an assessment or vetting phase to be given a specific weight and to validate it.*

Electronic data recovery is a very crucial component of the investigation of e-Procurement fraud, as can be deducted from the responses of participants. It has the capacity to be effective if conducted correctly and properly. The majority of participants expressed that electronic data recovery can improve the success rate of e-Procurement fraud investigations.

5.7.2 Sub-theme 5.2: FI’s are of the opinion that electronic data recovery in the investigation of e-Procurement fraud in the CoT is currently not effective

As noted in Section 3.5, Casey (2011:7) makes it clear that there should be a separate investigator who works with electronic data recovery and presents it to the court. According to Humphries et al. (2021:1) forensic investigators responsible for electronic data recovery needs effective training for handling digital evidence to ensure verification, validity and accuracy which will guarantee that data was unaltered and undamaged. The case will move faster and smoother when the investigator is able to immediately deal with technical incidents.

As indicated by Hayes (2015:10), and Shinder and Tittel (2002:137) in Section 3.5, the computer forensics investigator must have basic skills, namely:

- Computer science foundation and the jargon;
- Know computer network protocols such as dealing with a breach and other security issues; and
- Expert in hacker culture.

There was a unanimous view by the participants that even though electronic data recovery has the capacity to be effective, GAR Forensic Investigators lack the skills and capabilities to recover electronic data. Participants commented that it is the sole reason why electronic data recovery during the investigation of e-Procurement fraud is currently not effective in the CoT. The common expression by the participants is that they are not applying electronic data recovery during the investigation of e-Procurement fraud. The sentiments shared by the participants are that the CoT is dealing with this predicament by outsourcing the recovery of electronic data to external service providers.

It is clear from the responses of the two SFASs that GAR investigators do not have capacity to recover electronic data in the investigation of e-Procurement fraud due to lack of skills and training. CoT uses external service providers to recover electronic data. The following participant responses were put forth:

SFAS 17: *"I don't think its effective in the CoT. I think we should be sent to some training ourselves [sic], because there are some investigations whereby, we will hear that, no, this one we'll outsource it. So, I don't think we have enough capacity. They deal with it by outsourcing."*

SFAS 18: *"No. We are outsourcing it. We don't have the capacity. I'm not aware of any professional in our department that have the skills. We haven't got the capability, we are not trained to do that, we're not open on a system to do that."*

The above-mentioned statements are supported by five SFIs who revealed during the interviews that GAR investigators have no capacity, no skills and training to recover electronic data which makes it practically impossible for them to optimally investigate e-Procurement fraud. Instead, the CoT is outsourcing this crucial part of e-Procurement investigation. The following quotations illustrate participants' views:

SFI 19: *"We don't have the capacity in the CoT. They outsource."*

SFI 20: *"No. We haven't got the knowledge and the people to do that. Maybe small little stuff that you want but, like I said, you have to use the consultants. We haven't got the ability to do that. If you want few things but if you really go into depth, I don't think we've has the capacity. We haven't got the people or the expertise to do that."*

SFI 21: *"No. We don't. That's a simple answer. No, we don't have the capacity."*

SFI 22: *"I don't think we have sufficient capacity."*

SFI 23: *"We don't have the skill in that one. No, the internal capacity doesn't have the skill."*

The unequivocal sentiments by the participants are that the electronic data recovery has the ability to be effective. However, it is currently ineffective in the CoT due to lack of capacity amongst GAR investigators. They also lack skills and training in electronic data recovery as confirmed by the participants. Some participants commented that electronic data recovery can only be done by qualified and skilled forensic investigators and should be done correctly and properly to have presentable evidence or other consequence management forums.

5.8 THEME 6: FI'S EXPERIENCE CHALLENGES WITH REGARDS TO RECOVERING ELECTRONIC DATA DURING THE INVESTIGATION OF E-PROCUREMENT FRAUD AT THE CoT

The participants experienced challenges regarding the recovery of electronic data during e-Procurement fraud investigations due to several challenges that this research unpacks.

The themes and sub-themes come from the following questions:

- *"In your opinion, do CoT investigators experience challenges to recover electronic data during the investigation of e-Procurement fraud at the CoT?"*
- *"Have you received any formal training in electronic data recovery to investigate e-Procurement fraud at the CoT?"*
- *"Are you familiar with the most prominent Computer Assisted Audit Techniques (CAATs) software applications?"*
- *"Are you familiar with the most critical steps or phases of electronic data recovery?"*
- *"Are you familiar with the process of examining recovered electronic data?"*
- *"How does the CoT deal with electronic data recovery in the investigation of e-Procurement fraud"*

The GAR investigator's experiences and opinions were sought to understand their challenges to recover electronic data recovery in the investigation of e-Procurement fraud. During the in-depth interviews, the participants' familiarity with the most prominent CAATs software applications were sought. This research also pursue to ascertain if the CoT forensic investigator received any formal training in electronic data recovery to investigate e-Procurement fraud. The participants' familiarity with the most critical steps of electronic data recovery and the process of examining recovered electronic data were pursued. The participants' common responses were that they all experience different challenges. Responses to the different questions posed to participants, as mentioned above, are presented separately in the sub-themes below.

5.8.1 Sub-theme 6.1: FI's experience challenges with regards to a lack of training on electronic data recovery

As noted in Section 3.5, and according to Hayes (2015:10) "it is important to understand that computer forensics and electronic data recovery in particular, is a multidiscipline field that requires the skills and training in the field of computer science, criminal justice, law, mathematics, forensic science, IT and linguistics".

There was a common view by the majority of the participants that one of the biggest challenges for them to recover electronic data in the investigation of e-Procurement fraud is lack of training. The three Managers cited that they did not receive any formal training in electronic data recovery, however one participant commented that he trained himself by using the system on a regular basis. The following are their quotes that were put forth:

M1: *"Formal training? No. Mostly in-house and teaching yourself through using the system on a regular basis."*

M2: *"No [formal training], not yet, but I will like to."*

M3: *"No [formal studies], but I need it."*

The above-mentioned sentiments are supported by the three SFASs who echoed that they did not receive any formal training in electronic data recovery. Notably one participant said that he learned data recovery at the ACFE which was not in depth but basic. The following quotations illustrate their views:

SFAS 4: *"Knowledge of what and how to do it. I think we have to do courses on how to do it."*

SFAS 5: *"No "I haven't received any training."*

SFAS 6: *"No training from City of Tshwane, but I learned basics of data recovery at ACFE."*

The common perspectives of the five FIs are that they lack training to recover electronic data and to effectively investigate e-Procurement fraud. Their views corroborated with the statement by the viewpoints of SFAS shared above. The following are quotes to support participants' views:

FI 7: *"It was just informal training, a discussion. Because I'm not familiar with most of the things as well, you find that most of the time I rely on my colleagues to help me. I haven't received any training"*

FI 8: *"I haven't received any training"*

FI 9: *"I personally haven't had any training."*

FI 10: *"I would say lack of training would be a factor. I would say that, as much as I would also say…the main thing for me is the training. I feel it would be so important to get training on this because once you have that training it gives you a whole different perspective of how to handle e-Procurement investigation. So, I think that I would recommend to my supervisors to get this training done."*

FI 11: *“The problem is that we are not trained in these things, and they are complex to investigate”*

The above-mentioned sentiments are supported by the 12 SFIs who also share a common view that GAR investigators lack formal training in electronic data recover in the investigation of e-Procurement fraud. The following quotes illustrate participants’ sentiments:

SFI 12: *“No, formal training in terms of electronic evidence recovery. Nothing. You basically have to deal with it on your own.”*

SFI 13: *“No formal training. Informal training, yes. Sitting here and listening how to do…in meetings and stuff, yes.”*

SFI 14: *“It is a struggle. We need training”*

SFI 15: *“No training from the City”*

SFI 16: *“Accessibility is the first thing. Training is automatic, that goes together with that. And then if we were to retrieve information from the SAP system, we must have the necessary competency to retrieve information from that system. So, I think those are the lacking areas, we don’t have training.”*

SFI 17: *“I think the bottom line is actually training, the one that actually stand out. You can’t investigate e-Procurement if you don’t have at least a basic skill. What you can do is just to maybe do a search in terms of the normal way of doing investigation, in terms of criminal procedure. But it also had an element of risk, particularly when you go and seize a laptop but not knowing that you might compromise a lot of the evidence by only touching the laptop because you are not even aware of how do we handle a laptop after you have seized that particular laptop. The evidence is very sensitive. Just the touch of a button, it might crash. Then it became compromised and then you come at a later stage, then you won’t be able to use that particular* *evidence. It's also volatile, when you're busy with it, somebody remotely can delete, an ex-staff and then everything is wiped out."*

SFI 18: *"I do have all the access for e-Procurement-related systems, but I need training."*

SFI 19: *"You will also need access because you can be trained but with no access or you can have access but without training is useless. Access with no training, that's a big problem. If you give me access to SAP now, it's fantastic but I wouldn't know what to do because of lack of training. It goes back to training."*

SFI 20: *"It is a challenge to conduct that kind of thing because we don't have training or whatsoever, nothing"*

SFI 21: *"I haven't received any training. Since I joined the department"*

SFI 22: *"No training, we don't have that training or whatsoever"*

SFI 23: *"No, so far, I've never received training. Nothing."*

The transcription shows that lack of formal training is a major drawback for GAR investigators to be able to recover electronic evidence, which enhances the effectiveness of investigating e-Procurement fraud. There was a common view by the majority of participants that they need formal training in electronic data recovery.

Notably, one participant mention that he received basic training at the ACFE and another participant who claimed to have trained himself by working on e-Procurement system on regular basis. It is necessary for the investigator to acquire formal training in electronic date recovery to be able to carry out their investigative mandate and to improve their investigative skills. Currently, it is practically impossible for them to effectively investigate e-Procurement fraud without having knowledge and expertise of electronic data recovery which can only be acquired through formal training.

5.8.2 Sub-theme 6.2: FI’s experience challenges to access the information on the CoT system

From the literature presented in Section 3.6, Solomon et al. (2015:2) identify first critical step of electronic data recovery as identification and preservation. Newman (2007:4), and Kruse and Heiser (2002:2) share the same opinions about electronic data recovery being the practice of finding and storing computer evidence.

The discussion and interpretation of this sub-theme, namely FI’s experience challenges to access the information on the CoT system will follow below:

The GAR investigators’ comprehensions and impressions were sought to understand what the contributors to their challenges are to recover electronic data in the investigation of e-Procurement fraud. It is the views of the majority of participants that they do not have access to the CoT system, such as e-Procurement, SAP and HR system. That is one of the setbacks that hamper their process in investigating e-Procurement fraud. The first important step to recover electronic data is identification and preservation and if the GAR investigators do not have access, it is not possible for them to identify and preserve the data. Some of the participants mentioned that they are often frustrated when conducting investigations because of not having access to the system to get the required evidence and preserve it.

All three Managers have acknowledged that not having access to the systems is a major drawback in the process of recovering electronic data during e-Procurement fraud investigation. These participants echoed they even cannot preserve electronic evidence as they do not have access to such evidence in the first place. Participants, however, agreed that some investigators do have access to some systems but not full access to all the systems as expected. This section of the interview inspired the sub-theme:

M1: *“We are limited to the access to systems. Some people have access to SAP. Not everybody has access to e-Procurement. I would think one of the crucial factors will be access. I don’t think there’s any investigators having* *access to e-Procurement to see and to red-flag certain transactions that might be out of the ordinary. So, access is a major aspect."*

M2: *"The majority of the time, we were working with documentation and then suddenly, immediately, we went to digital systems and unfortunately, we do not have access. I cannot talk about other organisations or other municipalities, but as forensic investigators at the City of Tshwane, we are lacking behind with technology.*

M3: *"We had to battle to get access to systems, we are blocked, we are denied, and if we want to get it right, we must give full access to systems. So, you had to go back to get advice how to get information, where to get information, how to interpret specific pages. Now that we are using digital, we need to learn about the digital footprint. Because each document that you complete through a system leaves a digital footprint and if you don't know where to get it and how to understand it you will not be able to use it in your investigations to prove some of your evidence."*

The above-mentioned statement is supported by the views of the three SFASs who revealed that one of the major challenges to recovering electronic data is the lack of access to the systems. Interestingly, one SFAS participant remarked that blocking of investigators' access is caused by political interference by politicians who don't want to be exposed. The following are quotes to illustrate these participants' views:

SFAS 4: *"Lack of access, because of political interference, and we must be honest about that. There's always political interference, doesn't matter what political party. As soon as you are busy investigating…and they will be trying to influence our view of what we found.*

SFAS 5: *"Access and training go hand in hand. You can be trained but without access, useless. Access without training, useless. You can't perform. Because, normally, investigations are about profiling. You do profiling. You* *don't have tools to do that. You don't have it. The City's not…it's reluctant, it's not even willing to purchase licences–*

SFAS 6: *"And on the access into a system? …we need more access on more systems, like on the SAP"*

The above-mentioned sentiments by SFASs are supported by the views of the five FIs by specifying that investigators are very limited as far as access to the systems is concerned and it is a serious challenge for them to recover electronic data and to optimally investigate e-Procurement fraud. The following quotations support their views:

FI 7: *"We are very limited to what we may have, and in trying to recover this information we then have to go and seek possibly assistance from, let's say, other CoT officials because we don't have the access to that information, or we're not allowed to access that information. So, then we have to go out and ask them please can you assist me, I'm investigating, I need so-and-so information."*

FI 8: *"Yes, of course. As I said before, one of the main challenges is that we don't have the access to recover this information ourselves. We have to go out, we have to outsource, we have to basically ask and request people to assist us."*

FI 9: *"It's frustrating, especially as an investigator, when you need particular information, and you are unable to access that information and you have to go through so many different channels to just get a particular piece of information that is required. That's a serious challenge. It's only open for certain employees.*

FI 10: *"You're depending on other people, and it shouldn't be like that when you're investigating. If we don't have access to SAP, we don't have access to e-Procurement itself*

FI 11: *"The CoT forensic investigators experience some challenges. Because as I've already mentioned it before that lack of access makes it difficult to go deeper into the e-Procurement system. So, for us, if we can be granted access it's going to be an advantage to the organisation".*

The above-mentioned statements are corroborated by the 12 SFIs commenting that lack of access is indeed a serious problem for them to be able to recover electronic data in the investigation of e-Procurement fraud. There were overwhelming common sentiments by the participants that it is difficult to investigate without full access to the relevant systems. The quotes below illustrate their views:

SFI 12: *"It will be unfair for me to say that we are able to investigate e-Procurement because we don't even have access. …not even viewing rights."*

SFI 13: *"The lack of access is a struggle…"*

SFI 14: *"We don't have access to all those systems?"*

SFI 15: *"Most of us are not linked on certain systems. We are not part of systems. We are not one of the users on systems. As soon as the systems are available for us, we can access, and we can function and we can do our work. But at this stage, that is our limitation. We don't have access."*

SFI 16: *"I don't have enough search engines to work on. I haven't got access to search engines. Like I said, I must rely on other people to get information."*

SFI 17: *"Having access will be better."*

SFI 18: *"No access. If you've got the access like you saying, you can go in and see what it must be, what it must actually be. I suppose communication with the people that must assist access is needed."*

SFI 19: *"I think you know that we do not have access to the systems. So, we are expected to investigate and when we need to get information, we must ask the client department for the information. So, sometimes your information you received can also be manipulated. I'm not too sure if you have but we do not have access to e-Procurement or SAP. It's a big risk. So, when you ask something from the department that you investigate, they are the ones sending you that information from SAP or from e-Procurement but you're not sure if it's the correct information. It means they will give you what they want."*

SFI 20: *"The limitation obviously is in terms of accessibility to all the investigators in the City. And then the other issue that goes with that is if you give information or give access to investigators in terms of information there, it's also…what comes into play is confidentiality, number one, and then did these investigating officers get clearance in terms of security clearance from the State or the local authority…? And that's one of the issues – Access. The risk is also abuse of that information. The thing is that the investigator, if they have access to HR, then they can zoom into anyone's salary and obviously it's confidential. There have to be restrictions. Having three/four/five investigators who have got security clearance and who signed the confidentiality clauses and everything, who can have access to those."*

SFI 21: *"Accessibility is our number one challenge. To validate the information, to retrieve the information, then you don't get the cooperation that you need from supply-chain management with that, and sometimes, to be honest, we think there's a link between them and our management structure here in terms of colluding. To obtain the information, it should be a very easy process but they're so bureaucratic and – it is a simple email. They're so bureaucratic and controlling over the investigating officers, it raises red flags as to why they actually want this. And from all of this, it goes to consequence management in the City and that's where we're totally lacking. So, you can investigate, you can finalise your report, and then you* *don't know what happens to the report. You don't see the final version as the investigating officer, until a department queries it, then you have to refer it. But as an investigating officer, you don't see the final report. …you don't know what is the final outcome. You are not informed."*

SFI 22: *"That's true. I agree with you. We don't have access to any system, maybe other do have access but as for me, no."*

SFI 23: *"Again, it's accessibility. We don't have that accessibility to that. Like I said, if we have centralised systems and a sophisticated environment where we can work with electronics and you give the investigating officers that access as well, then you automatically see what's going on, …red flag a transaction/see what is going on instantly"*

According to the replies of the participants, the obvious lack of access to the e-Procurement system is a serious contributor to the investigators' misery of not being able to recover electronic data. Notably was the issue of political interference as a reason for denying investigators access. Without access to the relevant systems, it is impossible to recover electronic data to facilitate efficient e-Procurement investigations. As supported by the reviewed literature and responses from the interviews, the first and foremost important step in electronic data recovery is identification and preservation, thus one needs access to the system he/she is investigating to be able to identify and preserve the data. The common view by the participants is that it is paramount for the CoT management to grant their investigators access to all the systems during investigations and to prevent undue political interference into investigations.

5.8.3 Sub-theme 6.3: FI's are not familiar with the most prominent CAATS software applications

As presented in Section 3.4, CAATs is defined by Al-Hiyard et al. (2019:2) as "robust audit tools to detect errors and fraud such as the existence of duplicate transactions, missing transactions and anomalies". It is the opinion of authors, such as Cascarino

(2013:118) that CAATs retrieve and study information. According to ACFE (2019:3.746) the most prominent CAATs are ACL, IDEA, Excel, SAS, Oversight and Arbutus (See Section 3.4.1).

Successful recovery of electronic data depends largely on the programs and software applications, and it is important for investigators to be familiar with the application of this software. Based on the responses from the interviews, it appears that the majority of GAR investigators are not familiar with CAATs software applications. This software can assist the investigator to detect any anomaly on the system, retrieve the affected data, organise and analyse it. Surprisingly, even the Managers are not familiar with CAATs software applications. The following are quotes to illustrate participants' views:

M1: *"I'm not familiar with that [CAATS], we don't work with them"*

M2: *"I am not familiar with software applications [CAATS], we don't apply them"*

M3: *"I didn't know that we got [CAATS], I have never seen them in our department".*

The sentiments shared by the three Managers are supported by the statements by the three SFASs commenting that they are not familiar with CAATs software applications. These participants reiterated that they do not apply CAATs during the investigation of e-Procurement fraud where they are required to recover electronic data. Their response are as follows:

SFAS 4: *"But I'm not familiar – I trained myself on Excel. I never went for training"*

SFAS 5: *"The most prominent computer-assisted audit technique]. No, we don't apply them. We don't have them. I have to be honest."*

SFAS 6: *"No, I don't know CAATs. Not even trained to use them".*

Contrary to the views of the Managers and SFASs above, four FIs responded positively and remarked that they are familiar with CAATs. They correctly mentioned software such as ACL, TeamMate, IDEA and Excel, however, one of four participants indicated that the CoT TeamMate license has expired and therefore not being used. One FI commented that he was not familiar with the CAATs software application. The following participant verbatim quotes support this sub-theme:

FI 7: *"I am familiar with it. Name-wise, on the top of my head I would say the most prominent ones, it's not really in my mind at the moment but I would say it's something that…I know of. CAATS that I would say that I use predominantly or most often would be firstly…and I could be wrong here, it could be…it's the ACL that we use to analyse the information."*

FI 8: *"My understanding of the CAAT, something that I frequently use would be the Excel application, which helps me to filter a lot of information, it helps me to summarise, it's a very useful tool that I use. Also, the graphs help me to identify information as well."*

FI 9: *"I am familiar with some software. TeamMate is not working properly. I am not applying it due to expired license. We are also using Excel."*

FI 10: *"CAATs? That one, I don't know. But I'm having one which I can just punch ID number and it gives me the information about our EPWP employees, it's called IDEA program."*

FI 11: *"I am not familiar with those. I don't apply them"*

To substantiate the sentiments by the four FIs above, five out of the 12 SFIs consistently agreed that they are familiar with CAATs software application and proceeded by listing ACL, TeamMate and Excel as the most prominent software. Below are their views illustrating this sub-theme:

SFI 12: *"I know you can use Exel for any other investigation"*

SFI 13: *“I’m not familiar with the softwares. I don’t apply them”*

SFI 14: *“No. I’m not familiar with those. I don’t apply it”*

SFI 15: *“I’m …not familiar, actually heard of, I’ve never used them, tools, which is…what do they call it? ACL and IDEA. These are the only tools that I’m actually aware of. I think it’s the ACL that is being used, and what else? I’m not sure of any other.”*

SFI 16: *“No, I do not know. Because I’m not on the SAP systems and I am not on any system. We ask to be on systems but I’m not. I’m battling. Like I said, I can’t go on SAP, I can’t go on CPB, all that stuff because I’m not registered to be there. We are asking. It’s now more than a year… Either there’s no money or there’s no time. I don’t actually know what is the top management’s problem. Because we need search engines to do our job properly. Without software, it is practically impossible to conduct proper investigation”*

SFI 17: *“We don’t apply those things. Remember, we’re sitting here, SAP is somewhere. They will give you just the minimum and no training…”*

SFI 18: *“No, I’m not familiar with all of them. Let’s just say then we need more training on certain things.”*

SFI 19: *“At the moment I am only using Excel for data analytics, but this is exactly one of the problems when it comes to the support of the investigators. I am waiting roughly for about eight months for the systems that I’m supposed to be using and to date nothing.”*

SFI 20: *“Excel, it’s a simple basic one, but even that one, all of us didn’t even have training on Excel. We train ourselves as we go. We learn from each other and…”*

SFI 21: *"Excel. That's the main the one we use. Definitely. So, I am able to help myself with that. I do use it in all my investigations."*

SFI 22: *"I know we have CAATs but I think the problem is that we don't have license. We must pay for it."*

SFI 23: *"Yes. ACL, TeamMate. Those are the two that we have. No, I didn't use them. The license is not renewed, so we are not using any, none of those."*

The participant responses illustrates that many of them do not recognise the full potential of the CAAT's in recovering electronic data in an e-Procurement investigation.

Only nine participants were able to correctly name some software applications, 14 participants remarked that they are not familiar with CAATs. It is extremely important for the GAR investigators to familiarise themselves with CAATs software applications as they are the only tools that enable the recovery and analysis of electronic data. Without this software applications, there will be no recovery of electronic data done and ultimately no e-Procurement fraud investigation can be completed in the CoT. The unanimous view by the participants is that they need formal training to be able to operate the software applications.

5.8.4 Sub-theme: 6.4: FI's are not familiar with the most critical steps and phases of electronic data recovery

As noted in Section 3.6 and as suggested by Maras (2015:34), electronic evidence recovery has four factors: "acquisition, identification, evaluation and presentation". Holt et al. (2018:529) share a similar view with Maras (2015:34) by stating that the procedures of forensic data recovery is complex process which involves the following steps:

- Identification of potential source;
- Collection or acquisition;
- Examination or analysis of recovered data; and

- Presentation of findings.

Solomon et al. (2015:2), and Marcella and Greenfield (2002:18) agree that the investigators need advanced computer skills to work with the electronic data recovery to successfully defend the case. Recovery of electronic data requires a well-documented methodology on how to go about it; it is therefore important for forensic investigators to be educated with regard to the steps and phases of electronic data recovery to be able to apply it properly. The interviews revealed that GAR investigators are predominately not familiar with these steps and phases.

The common sentiments by the three Managers are that they are not familiar with the most critical steps and phases of electronic data recovery. They failed to mention these steps and below are their responses to support their views:

M1: *“No, I am not familiar”*

M2: “*I am not sure. It is tricky. We are not trained. I think it will go back to if you have been trained on that particular thing, then you’ll be able to know what to do.”*

M3: “*I’m not aware of that.”*

The above-mentioned statements are corroborated by views of the three SFAS who stated that they are not trained and are therefore not familiar with the critical steps and phases of electronic data recovery. The following participant responses illustrate their views:

SFAS 4: *“No. We have to do undergo training and attend courses on that”*

SFAS 5: *“Critical steps and phases? No. I am not an expert on that.”*

SFAS 6: *“I don’t know these steps. We haven’t been trained”*

It was the views of the five FIs that they are not familiar with the critical steps to recover electronic data apart from one participant (FI: 7) who correctly mentioned preservation as one of the steps to recovering electronic data. The following are the responses put forth:

FI 7: *"I would say that, with data recovery, I would think one of the most important factors would be preserving the data or the evidence, ensuring that its integrity is upheld. And I would also talk about identifying which information would be necessary. You need to be able to identify at the beginning of an investigation what you need from this investigation, each particular fact. And then, also, when you're analysing the information, you need to be able to filter what is necessary or relevant to this particular investigation."*

FI 8: *"To recover the information, first of all you have to know the name of the person you're dealing or you're investigating, or you are digging information because you can't just go widely not knowing whom are you looking for. First one is the name. After knowing the name, then you check if that person maybe is the South African citizen, whatever, or a foreign national, and then from there you'll be looking…if it's a foreign national, you'll be looking at required documents to be in a foreign country, if that person does qualify to be in the country if it's a foreign national, or if it's a South African you see if he got the right ID. And then from there, after gathering that information, the next step is to consider exactly what you are looking at, what you are trying to establish as far as investigation is concerned. From there, you have to draft your report of what you have got [sic]. And then what you have detected or what you find during your investigations, then you come to your… findings, and then come with the conclusions, you go to your recommendations."*

FI 9: *"Let's say the laptop is not by the person somehow or locking the system. Then you go to the deleted items, you check there. If already they have deleted it on that one, you go to your backups on the cloud. I think you'll find something there. I learned it myself. Self-trained"*

FI 10: *“No I don’t know them”*

FI 11: *“No. I haven’t done it before”*

The above-mentioned statements are supported by the views of the 12 SFIs indicating that they are not familiar with the most critical steps of electronic data recovery because of lack of training about recovery. Following are the responses put forth:

SFI 12: *“We haven’t been too much involved in these things.”*

SFI 13: *“One program that was for three-day, there was a presentation on it but, no, I’m not familiar with it.”*

SFI 14: *“I don’t know because I don’t know what to look out for. If you need more information, I don’t know where to go to retrieve it. Because they gave us a quick thing on Teams, just more or less, but you have to work with it daily and if you don’t know you must ask the people. But, yes, there is stuff, no, I don’t know where to go.”*

SFI 15: *“No. we are not familiar with it. In my experience, obviously to retrieve information or electronic evidence, you need the specialist to then retrieve the data and then the specialist…either in the form of an affidavit or statement to validate the information that was retrieved by a person who has, number one, the authority and access to that system, number two, that person must be trained and then…which validates the information retrieval from that system and then obviously give you a statement to validate what was retrieve, and then obviously the investigating officer then uses that as part of his or her final report.”*

SFI 16: *“Let me answer you honestly. The experience, I’ve got my training from how to do investigations. There’s basic steps that you follow on investigations. My basic steps in investigations I know how to do a statement, I know how* *to get information, and…but electronically, for myself, I'm not equipped to get electronic information."*

SFI 17: *"No, not all of them. Little bit I'm familiar but not all of them I'm familiar with. Because it's more sensitive and you had to apply it without loss of any information or interference of the evidence and all those stuff. yes, I do remember the steps. Immediately you arrive, you secure the scene and everything you must capture it safely, lock it. And you label each and every document the way you found it in the scene."*

SFI 18: *"I've got a document to do it step by step, but I know you must first come and take pictures and mustn't touch anything and…there is a process. I'm familiar there is a process. Yes. I can't remember all the steps. I will work from that. So, don't log in, don't take the device without a person as a witness. I can't remember the steps. I'm working on a document if we need to do that"*

SFI 19: *"So, the first step would be then to ensure that no one has access to the device needs to be investigated and then, from that device, while the device is live, before any data is changed or timestamps or hash values have been modified, there needs to be an image of the original, which needs to be kept in a safe place. If ever the integrity or the accuracy of the information or evidence gets questioned, there is a [sic] original copy. Then there needs to be…obviously from that copy there needs to be a working copy for the investigators to use and analyse as well as a secondary copy for future use to make copies from. The idea of the secondary copy is so that the original copy remains untouched until a court orders that we need to verify, where's the original? And that there will be a comparative value, after which I know that there needs to be…because of the volatility of the data, there needs to be a hard shutdown. That basically means that the power to the computer is terminated immediately without the computer having to change any data points or any metadata or hash values or anything like that. …or something might come in and change the format or size. Or during the shutdown* *process, it might change a date stamp or some part of the data, or it might autosave, leading to altering of the data. All the components of the PC, the power, everything around needs to be off."*

SFI 20: *"I don't know the critical steps and phases of electronic data recovery"*

SFI 21: *"During one of the seminars, they actually touched more into how to recover data, what are the steps that one has to do. I'll just touch them without going into chronology. They told us when the computer is actually plugged to the network, you don't have to switch it off to that particular network because some of the data might be lying on the network. So, if you can take it off the plug, the network point, then it will…the data won't be able to be recovered. And then they've also touched on how you should do the hash count. Hash count, you basically…you'll just need to do some sort of validation of data, that the data that we have actually stored in the PC is exactly the same size with what we retrieved in that hard drive. But you can't be able to do this without that particular software, because the software itself will tell you that from this hard-drive, there's so much data, meaning that there is one gig or one-megabyte data and then what you have copied, if it is less than that, it basically means that the data lose credibility."*

SFI 22: *"I don't know much about electronics I also need to learn about how to retrieve. It has been long since I've done this. And ever since I've attended that particular training, I never had an opportunity to work with the…to gain experience into that particular field."*

SFI 23: *"No, I am not familiar with these steps. Never done them before."*

It evidently came to the fore from participants' responses that most of the participants are not clear on all the steps and phases needed to recover electronic data. The fact that they are required to recover electronic data during the investigation of e-Procurement fraud places them in a difficult situation if they are not aware of the steps needed to recover electronic data. This implies that they won't be able to investigate e-Procurement fraud investigation because most of the critical information about e-Procurement is embedded in the e-Procurement system and to access such information it must first be recovered. The common sentiment by participants is that they are not trained on the recovery of electronic data and therefore formal training is required.

5.8.5 Sub-theme 6.5: FI’s are not familiar with the process of examining recovered electronic data

From the literature presented in Section 3.7 and according to Ashcroft et al. (2019:1), a trained examiner will go through the process of analysing the data after it has been imaged and preserved. The examination of electronic data must only be conducted on a duplicate copy of original data because data can be manipulated. The discussion and interpretation of this sub-theme follows for detailed illustration below.

The participant’s familiarity with the process of examining recovered electronic data was sought. GAR investigators are not familiar with the process of examining the recovered electronic data, as revealed from the interviews. The reason put forth during the interviews was that they did not receive any training concerning examination of recovered electronic data.

M1: *“No. Because of the lack of training. I am not aware of the process to examine electronic data.”*

The sentiments of the Manager are corroborated by the views of 1 SFAS who revealed that:

SFAS 2: *“I don’t think we’ve ever received training on that. So, I am not familiar.”*

There was an overwhelming common perspective about the lack of knowledge to examine recovered electronic data. The replies of four FIs, from the interviews, are that they are not familiar with the process of examining recovered electronic data. However, one participant (FI: 3) responded positively and stated that data can only be examined on a copy instead of the original to avoid damaging or destroying data which might compromise its integrity. The following responses were put forth:

FI 3: *"When you are examining or analysing the data, it needs to be examined in such a way or handled in such a way that you must not damage or destroy or alter the information in any way. You need to be, I would say, protective of the data. And, also, if you are examining or analysing the information, it is best that you don't use original information. It's best that you make copies of the information or duplicates so that you can work on those duplicates. So, that would be important for me when analysing or examining the data."*

FI 4: *"To analyse the evidence you have gathered? Yes, there's the evidence on the table….the first thing we have to do, you have to know what you are looking at, what you need to establish. Does the information on my table or in my presence link with what I'm looking for? Does it make sense that what I'm looking for should I deduce it from there? It's the first thing you have to look at. And then immediately you have established that, yes, indeed, this is what I'm looking for, then it is whereby you'll be starting to do with your report because you have found everything what you are in need of. That is the way forward. According to my little knowledge."*

FI 5: *"Now at the moment? There's challenges. There's no dedicated people inside the office that have got the expertise to do that."*

FI 6: *"Not fully, but I think partially I can examine. It will be difficult if it's all about IT language or – I don't apply it. I've never been there"*

Similar to the responses provided above by the FIs, most of the SFIs responded with just a simple "no" or "they don't know" which implies that they are not aware of the process of examining recovered electronic data. The responses from 10 SFIs are as follows:

SFI 7*:* *"No, I don't know"*

SFI 8: "*No"*

SFI 9: "*No, I don't know anything about that."*

SFI 10: "*I don't know. I don't know where to start."*

SFI 11: "*I don't know the process."*

SFI 12: "*I'm not familiar with the analysis because I'm not on computer stuff that. I think that is more in details to specialised people on that level."*

SFI 13: "*No, I don't know how to do it, but I know it can be done. That will also be outsourced. We don't have that"*

SFI 14: "*No, I don't use it. I've never been part of that. I don't know."*

SFI 15: "*That one I don't know. I don't have an idea [of how to apply the examination process]. But what I can tell you is the basic stuff that have…it's like you want the name of the laptop and that kind of stuff, then there's a template that we use for affidavit to take all those kind of basic stuff. But on getting to examine and making sure that…what do they call it? I think there's a term that they use. Indexing the evidence, digital evidence. I don't know how –If you don't have a software, you never had an exposure to it, then forget it."*

SFI 16: "*I must be honest; I've never done electronic analysis before but I would imagine that the principles of laws of evidence would remain the same. Chain of custody needs to be maintained, so that would mean then obviously the day you decide to access you have to keep a detailed log of accessing and what you're accessing. I would prefer that the activity be recorded. Because it's electronic, you will need to do that. You can record how you access and analyse and all of that."*

The participants made it clear that they are not familiar with the process of examining recovered electronic data. There was a nearly unanimous suggestion that there is lack of training about the steps to examine recovered electronic data apart from one participant (FI: 3) who cited that *“examination of electronic data can only be conducted on a copy instead of original to avoid damaging or destroying data which might compromise its integrity”.* The mutual view of the majority of the participants is that they never performed these steps before. Lack of training is contributing largely to this challenge facing GAR investigators.

5.8.6 Sub-theme 6.6: FI’s lack advanced resources to recover electronic data

As noted in section 3.8, ACFE (2019:3.841) pointed out that there are several data recovery products. These products differ in complexity, features and price, and they employ various methodologies to extract and analyse data from computers. It is best to use a combination of different tools to gather and analyse evidence.

It is very crucial for the participants to have tools and resources to recover electronic data. Without these resources and tools, it is impossible to recover electronic data. It appeared that GAR investigators lack advanced resources to recover data. Based on the responses of the Managers, it seems as if the GAR have no resources to recover data. Following are the verbatim quotation of the two Managers to support their views:

M17: *“Resources. I think we are limited with resources, definitely resources. I think that’s my main problem that I have now. And also, We don’t have competent staff members. According to my knowledge, we don’t have any qualified person to deal with electronics. We don’t have the human resources to deal with such”*

M18: *“No software. We don’t have software. That’s why it’s being outsourced to specialists. We don’t have sufficient electronic devices to do such recovery”*

The above-mentioned sentiments by Managers were supported by common views of two SFASs who explained lack of resources as follows:

SFAS 19: *"We haven't got any equipment and resources to do our work"*

SFAS 20: *"The main drawback here is we haven't got a cyber-forensic section. The cyber forensic section should have been established ten years ago already."*

The participants in the study consistently agreed that GAR has no advanced tools and resources to recover electronic data for e-Procurement fraud investigations. This was also confirmed by the common views shared by three SFIs who indicated that:

SFI 21: *"Resources, obviously there's…we have that issue of incapacity. We need to look at capacitating or reviewing the structure and make budget allocations for it. We must tell the Council, that we want to capacitate our internal investigators, we want to put in electronic system, we want to give them the IT technology to deal with these types of things, and so on."*

SFI 22: *"We require a proper computer lab. The live monitoring studio is very proactive. I think it will be extremely effective. If we can digitise that process and semi or fully automate it, then such an approach would virtually make the City of Tshwane's procurement process impenetrable from the outside and would most likely then…any fraud or corruption that would happen in such a system would then most likely in the majority of instances come from internal sources, which then a lab like that would then be able to instantly identify, flag, and successfully prevent fraud."*

SFI 23: *"Yes, a lot, daily. There's always issues because we don't have adequate resources and I think the perpetrators knows that as well. So, it's very easy for the people to steal money from council again. It's a grey area."*

The interview feedback proves that CoT does not have the required tools and resources to recover electronic data. Participants shared the opinion that they are unable to effectively investigate e-Procurement fraud due to lack of resources to recover electronic data. Participants also agree that CoT should invest in modern technology to keep up with cybercriminals' latest tactics. Consequently, the CoT needs advanced resources like CAATs to be able to deal with e-Procurement fraud, obviously enhanced by the recovery of electronic data.

5.8.7 Sub-theme 6.7: FI's lack support from CoT Management

As presented in Section 4.7.1, Wells (2011:367) remarks that management of the organisation as a key role player of the team. The rest of the team must keep the manager up to date and in turn the manager should be readily available as far as recovery of electronic data is concerned. Albrecht et al. (2019:79) mentioned that the management must approve any investigation, because investigation can be very sensitive and quite expensive and, should be pursued only when there is a reason to believe that e-Procurement fraud has been committed.

It appears that CoT management is not fully supporting the Forensic Investigators to be able to recover electronic data and to effectively investigate e-Procurement fraud. Two SFASs shared a common view that there is no management support for them to recover electronic data. The following verbatim quotations illustrate participants views:

SFAS 1: *"Lack of training, lack of knowledge, lack of equipment, lack of assistance from management and lack of management support. Lack of will to empower forensic investigators."*

SFAS 2: *"We don't recover electronic data. We don't apply it. We don't have it in the City. Remember, there is a management that's supposed to identify the gaps that each individual investigator has. Management don't support us during investigations. We are on our own."*

The same sentiments as those identified above was shared by two FIs who also attempted to explain lack of management support. The following quotes illustrate this:

FI 3: *"I don't have support from management. The problem, which I see personally, is that we don't have a person who is permanently employed. In our management, you find that people are given five years' contract. After five years, there will be another person coming with different experience and management style."*

FI 4: *"I don't have access. I don't have any access. My supervisor since said he will arrange access to SAP and I'm still waiting. Our supervisors don't support us. No support from Top Management whatsoever."*

The above-mentioned statements are corroborated by six SFIs citing that there is no management support and political will to empower investigators. In addition, it appears from participant responses there is no administrative willpower to acquire modern tools and resources to capacitate investigations and recovery of electronic data.

Following are the verbatim quotes to illustrate participants' perspectives:

SFI 5: *"I am very well-versed in the concept of the tone at the top, which is basically the management's approach and support towards this kind of a problem or this concept, and unfortunately, currently as we stand now, the tone at the top is outsource everything and there is too little attention or no attention given to the needs of the investigators at the CoT, and especially with regards to ICT-related requests."*

SFI 6: *"When I interview people from IT, they will tell you of super, super solutions and models to recover electronic data but when they go to the management and politicians for approval, there is no support."*

SFI 7: *"They don't want us recover data. We once proposed a live system that can pick up any anomaly in the e-Procurement system proactively. But for them* *it's a no-go area. So, the political will is not there. Also, from the administration at the top, from City Manager and the Group Heads and EDs, it's not there. Because those are the people actually committing the serious SCM irregularities and so on, and even Directors, right down to the middle management. The willpower is definitely not there."*

SFI 8: *"To get the structure approved, we first need to get buy-in from the political Head (Mayor) and obviously the City Manager and the political structure in the council. Then they have to approve and support this type of investigations and so on. So, that still remains a challenge and for us to get through that, we need management support."*

SFI 9: *"The City management does not want it. That is the problem. Because if we invest money to empower our internal investigator, it will be better. If they invest the money into electronics systems, data recovery tools, the investigations will improve."*

SFI 10: *"The political will and administrative will that we talk about has to come from the top. From the department level, we're not seeing that, they're not seeing it as a priority. Our investigating officers just become frustrated by the workload and by the lack of support from even our managers to deal with these types of things."*

The greater part of the participants identified lack of support from management as one of the challenges for them in recovering electronic data. Participants specifically referred to the lack of political and administrative will to empower them by purchasing the ICT advanced tools and resources for them to recover electronic data and ultimately be able to efficiently investigate e-Procurement fraud. The reciprocal perception of the participants was that there is no support from management to motivate them and this resulted in most of them being demoralised and affect their ability to investigate e-Procurement investigations. Notably, one participant (SFAS: 1) said that:

"The problem is that there is lack of training, lack of knowledge, lack of equipment, lack of assistance and support from management."

5.8.8 Sub-theme 6.8: Current budget is spent on outsourcing rather than capacitating internal FI's

As noted in Section 4.7.1, Wells (2011:367) emphasises that an investigation can be outsourced to external consultants if the offence is internal. Power and influence could negatively affect the success of the investigation, and therefore outsourcing is important. In many cases external consultants will be experts.

From the information gathered from the literature review and interviews conducted, it appears that the CoT is outsourcing most, if not all, e-Procurement fraud investigations where recovery of electronic data is required. As remarked by the majority of the participants, the CoT spends most of its budget outsourcing these investigations instead of investing in appropriate training for investigators and acquiring the advanced tools necessary to recover electronic data to enhance e-Procurement investigations.

To further illustrate this sub-theme briefly, the three Managers comments that the CoT is outsourcing every e-Procurement fraud investigation and recovery of electronic data. Following are the responses to support participants' views:

M11: *"We don't do e-Procurement; we don't recover electronic data because the City is outsourcing to private companies"*

M12: *"I know from my experience I've done one investigation that was with computers, and it backfired completely. …and then we had to send it out and outsource. So, currently we are outsourcing"*

M13: *"Currently City of Tshwane is using external services, external consultants, to recover the electronic data, to investigate procurement fraud or to conduct the entire procurement fraud investigation. They are outsourcing."*

The above sentiments by Managers are supported by the statement of one SFAS who indicated that the CoT is spending a great deal of money in outsourcing electronic data recovery. This participant also remarked that there are no tools, no training and no skills transfer by external consultants. The following response was put forth:

SFAS 14: *"I think if when we do outsourcing, we must also do what we call co-source. There must be a skills transfer. Secondly, training is very important. Thirdly, the issue of tools, we don't have tools to detect e-Procurement fraud because we have never been trained to do that, or regarding that. Fourthly, the City is spending a lot of money on outsourcing"*

Similar to the views that were cited by SFAS above, another three FIs emphasised that the CoT is outsourcing electronic data recovery and e-Procurement investigations. The following verbatim participant responses illustrate this sub-theme:

FI 15: *"They are actually outsourcing. They're actually outsourcing those function to the service providers"*

FI 16: *"This is a type of investigation they normally outsource to service providers in our panel"*

FI 17: *"It's being outsourced to the service providers? It is cost the City a lot of money."*

There was an overwhelming commonality in the views shared by six SFIs that the CoT is spending most of its budget in outsourcing e-Procurement investigations and subsequent recovery of electronic data instead of capacitating CoT investigators with appropriate training and resources. Their responses were as follows:

SFI 18: *"Currently, the way I understand it is the City outsources it, which is a financial burden on the City, especially during this time. I don't know why the city is not training us. …and they are still paying us salary, irrespective."*

SFI 19: *“They just spend the budget on outsourcing. They are not training us to recover the data. I don’t see any will, administration will, to empower us with the skill to recover those electronic evidence. We don’t even have a chance to do it.”*

SFI 20: *“I know a lot of investigations with regard to this has been outsourced and the reason cited for that is incapacity, lack of knowledge and training, and all of that. So, hence, I think the majority of these cases are actually outsourced, but with outsourcing goes another challenge because the skills transfer is not in place, and it is costing the city a huge sum. It goes into Millions of Rands.”*

SFI 21: *“And the other thing is our leadership, they’re lacking direction when it comes to IT. If you look at the data solutions that you get throughout other companies and private companies and so on. The vision is not there in terms of that. Because you might have certain officials inside our system that are very competent when it comes to IT, but we are not capacitating them to deal with these investigations, so we’re not proactive. We’re just outsourcing everything to the service providers instead of having the in-house resources to deal with this type of things.”*

SFI 22: *“In the City we prefer to spend money on external companies rather than capacitating our unit or the forensic division inside the City. Also, with the e-Procurement, from where our investigating officers sit, we cannot proactively red-flag issues that are going on, and that’s one of the challenges.”*

SFI 23: *“If feels for me like the outsource companies got more privilege than us working here. That’s how it feels for me.”*

It was the participants' view that the CoT is spending most of its budget in outsourcing the recovery of electronic data and investigations of e-Procurement fraud instead of empowering or capacitating its own internal investigators. There was a concern raised by participants that there is no skill transfer to CoT investigators by outsourced external consultants, no training, and resources to recover electronic data. This negatively affect their skills development and inadvertently resulted in most of them being frustrated by not being able to efficiently perform their job as investigators. The mutual view of participants is that as investigators they must be formally trained in electronic data recovery to be able to be conversant with the ever-growing cyber world and to align themselves with international standards of effectively investigating e-Procurement fraud and electronic data recovery. This will also eliminate the outsourcing of electronic data recovery and e-Procurement investigations to external consultants in future and will save the CoT money as investigations will be done internally.

5.9 UNIQUE THEME 7: FI'S ACKNOWLEDGE THE SIGNIFICANCE OF USING ELECTRONIC DATA RECOVERY IN E-PROCUREMENT FRAUD IN CoT

This theme discusses and interprets the participants' perspectives of the significance of using electronic data recovery in e-Procurement fraud investigations. GAR investigators' knowledge about the importance of electronic data recovery was pursued. This theme is primarily focused on the GAR investigators' opinion of whether there is any significance of utilising electronic data recovery application in e-Procurement fraud investigations.

The answers to the following questions gave rise to this theme:

- *"According to you, is there any significance of utilising electronic data recovery applications in e-Procurement fraud investigation within the CoT?"*

This question was asked to measure the importance of utilising electronic data recovery in e-Procurement fraud investigations within the CoT. This is a unique theme and therefore there is no sub-themes. The insight of GAR investigators' viewpoints about the significance of electronic data recovery in the investigation of e-Procurement fraud are deliberated below.

As presented in the literature in section 3.2, the significance of electronic data recovery is illustrated by Casey (2011:3) who pointed out that apart from e-Procurement investigations, it can be used to resolve wide range of crimes such as “homicides, sex offences, drug dealing, terrorism and other white-collar crimes.” Organised criminals also use digital technology to conduct their crimes.

It was the view of all participants that electronic data recovery is very important as it makes investigations easier to complete and improve success rate. The below transcripts from the interviews support this claim:

M1: *“Absolutely, most importance is to have electronic evidence, to have a trail, start from the beginning. I think it is significance. I think it’s actually the real evidence. And that evidence can be presented in court now these days also.”*

M2: *“Yes, electronic evidence. You can use it in court. So, it is significant, definitely.”*

M3: *“The importance? Oh, for sure. Maybe if we’re not just talking about e-Procurement, if we look at other systems, digitally, where we recover digital information like from SAP, it makes the investigation easier. It definitely reduces the investigation time; it cancels out setting up meetings where it gets cancelled because people are not available. So, if you know the systems and you’ve got access to the systems, you can sit in your office and you can recover any information you want.”*

SFAS 4: *“It is very significant. As soon as you’ve got documentation in front of you, which you’ve obtained through whatever means, and there’s an allegation of fraud or corruption or whatever, it can either be backed up through your electronic evidence or it can refute what is in front of you.”*

SFAS 5: *“It’s very important. If we can do that, if we can take our investigators to training, we need to acquire those knowledge, therefore we can implement* *it. It's going to be a very successful in that environment, these skills can enhance everything we do."*

SFAS 6: *"Yes. I think it's very important. Because of its evidentiary value. It leaves a footprint."*

FI 7: *"I would say definitely it is significance. Firstly, how could I say it, by using this, and especially if the investigators are privy or access to these applications, we then cut off the middleman, meaning we don't have to outsource to consultants and assist us with recovering this information. It will allow us to perform our investigations faster and effectively."*

FI 8: *"From my point of view, the importance of it is that if we got those skills it will be very much advantageous because any complaint or any fraudulent activity which has been executed within the City is going to be very much easy for us to can detect and penetrate deeply into the system and come up with the results of what exactly been committed or whatever we are looking for. It is very much important. It is needed. It is necessary. It's a necessity for the City to run effectively. It needs this to be put in place."*

FI 9: *"Yes. I think it's just a better way of keeping control, record, all of that."*

FI 10: *"Yes. As I've already said, actually it improves things."*

FI 11: *"Yes, it is important. It will make our jobs easier and also for validation of the evidence.*

SFI 12: *"It is important because sometimes…when you [recover evidence manually], manual is easily manipulated and then electronically it's whereby you can see what was there before it was deleted."*

SFI 13: *"Yes, because everything is there. You can…click on a button you can get all the information that you need. it will be good to have."*

SFI 14: *“Definitely [significant]. This type of things will assist, number one, in terms of investigations, identifying risks that we have in the City, proactively dealing with it. So, the idea is that when we’re dealing with these systems and recovery of the information, all of that, they should create a balance between red flagging, between irregularities, and compliance. So, that will actually…if you have the systems, you have everything in place, then it’s easier to control things proactively”*

SFI 15: *“Definitely because that is the baseline, that is your worksheet, that’s what you use for your entire investigation. You rely on that information, so it has to be accurate. Without that information, you can’t produce anything. It is the heart of the investigation.”*

SFI 16: *“It is important to have it. Like I said, going back to the same answer every time. If the evidence is here and we can see everything, then it makes it easier.”*

SFI 17: *“Definitely. I could say yes, it’s very important. As long all the procedures and measures are followed properly.”*

SFI 18: *“It is significant because it’s about the evidence. So, you can find who was the criminal, who was the person causing the trouble in the system.”*

SFI 19: *“Digital is the way to go. Utilising electronic evidence recovery is very important to apply in the City.”*

SFI 20: *“Yes. Highly important. It’s extremely important. The reason for this is because data, computer evidence is extremely volatile. So, you need a properly trained person with a properly-trained system that can give an accurate recollection of events or give an accurate description of the data at the time of discovery or at the time of capture.”*

SFI 21: *“Yes, it is important, particularly when it comes to the investigation. It is important in such a way that you can’t do the investigation without touching a laptop, particularly when we deal with sophisticated investigation. So, some of the investigations are actually implant in our electronic device. So, for you to do a comprehensive investigation, you need to touch this. We needed to go electronically as well as investigators”*

SFI 22: *“Yes, it’s very important. Times are changing, you’re gonna get more and more and more investigations like that, and then you need to keep up with it to be able to do your job in future.”*

SFI 23: *“It is very important. Without data, we won’t be able to investigate. Where would we get that information to carry out investigation? I don’t know if I’m making any sense.”*

All participants unequivocally agreed that it is important to use electronic data recovery in e-Procurement fraud investigations. The common view shared by the participants is that electronic data recovery is needed and is a necessity for the investigation of e-Procurement fraud investigations at the CoT due to its evidentiary value. According to the participants, electronic data recovery allows them to be able to conduct e-Procurement fraud investigations faster and effectively.

The participants further indicated that the application of electronic data recovery facilitates the detection of e-Procurement fraud and to identify risks proactively. It evidently came to the fore that without electronic data recovery, CoT investigators will not be able to effectively investigate e-Procurement fraud. It is further vividly clear that electronic data recovery is significant and necessary to conduct e-Procurement investigations within the CoT, however it should be coupled with formal training of the investigators, access to the systems granted for effective investigation of e-Procurement fraud, and access to the necessary internal resources.

5.10 THEME 8: SUGGESTIONS TO IMPROVE THE CAPACITY OF FI’S TO INVESTIGATE E-PROCUREMENT FRAUD USING ELECTRONIC DATA RECOVERY AT THE CoT

The feedback from participants helped form ideas around the kind of support the CoT management needs to make e-Procurement investigations yield improved results. In some instances, participants remarked their experience and frustrations about the lack of understanding of what the GAR was doing. The answers to the following questions gave rise to this theme and its sub-themes:

- *“How could your ability as an investigator be improved to investigate e-Procurement fraud by using electronic data recovery?*

The GAR investigators’ background added valuable information on investigating e-Procurement fraud using electronic data recovery. Suggestions were made on how the capacity of CoT forensic investigators could be improved. Participants’ suggestions for improvements towards the capacity of CoT investigators arose from the matters illustrated and discussed in themes 2 and 6. The central theme of the suggestions revolves around training and access to the systems. Some of the interviewees explicitly mentioned the need to acquire advanced resources to recover electronic data internally within the CoT. The following sub-themes emerged, that are substantiated by relevant excerpts from the transcripts.

5.10.1 Sub-theme 8.1: Teamwork

As presented in the literature in Section 4.7.1, Wells (2011:367) stated that it is crucial to know those who will be essential to the work and those who are merely curious. Albrecht et al. (2019:79) indicates that any investigation within the organisation must be approved by the management. Wells goes on to list the team members needed in a single e-Procurement investigation:

- **CFE**: CFE comprises a team of specialised members dealing with unique challenges encounter in fraud inquiry. They grasp issues from financial transactions to classic methods used in investigations;

- **Legal Counsel**: A legal counsel will help the team answer inevitable legal enquires; and
- **Internal Auditors**: Auditors are the first to notice discrepancies and report the fraud. They are necessary for future uncovering and finding the culprit.

Some participants were of the opinion that to improve their capacity, they need to work as a team. Two SFIs cited that working as a team will let them learn from each other especially working with experienced investigators. The following responses support their views:

SFI 1: *"I think at the end of the day there's many ways in which we can improve. Myself, there's many ways I can improve. I think we learn as a team together. Everybody's got a different strength and weaknesses. So, currently, my first is I can learn from somebody else's strengths, and they can learn from my strengths, so that's how we can developed ourselves."*

SFI 2: *"Get yourself familiar. The more you do the investigations, the more you get to know how certain kind of investigation are approached. You run with somebody who knows what's going on."*

It is clear from the responses of the participants that teamwork is one of the approaches that the CoT can implement to improve the investigative capacity of forensic investigators. The next sub-theme, namely: access to the systems follow for discussion.

5.10.2 Sub-theme 8.2: Access to the systems

As noted in Section 4.7.4, Wells (2011:373) highlighted the importance of digital technology during investigations, as they are record keepers and save investigators time on research.

In support of the views by SFIs, all five FIs interviewed suggested that they should be given full access to the systems to be able to investigate e-Procurement fraud effectively. The following responses were put forth by these participants:

FI 3: *"Give me access to certain systems. So, access to all, not few. Your investigators should have everything. There mustn't be a grey area at all, otherwise there's no purpose of investigating."*

FI 4: *"Access can be granted with priorities in terms of your profile. You can't have access and not be trained or be trained and no access, it's useless. The priorities in terms of what you need to do, what you are entitled to retrieve, what you are entitled to do on the systems."*

FI 5: *"You need access, you need training. And then you can complete the investigation much quicker. Much, much quicker."*

FI 6: *"I've been an investigator for thirty-five years. The problem is I've got counter-investigators in ABSA who are my friends, they finish an investigation within three days. Not us. We don't have access; we don't have the resources. We finish it in two years. We do it in two years."*

FI 7: *"If I have the correct training. If I've got access to all the systems. If I've got assistance from our management. So, that's very important. Now because things are going around and turning around in the Council, maybe we will have access to the systems."*

The common suggestion among participants is that if investigators could be given full access to the system, they will improve in terms of conducting investigations more efficiently. Some participants recommended that access to the appropriate systems should be combined with relevant training. The following sub-theme deals with the acquisition of resources to enhance the investigation of e-Procurement using electronic data recovery.

5.10.3 Sub-theme 8.2: Acquisition of advanced resources to recover electronic data

According to Solomon et al. (2015:176) and as noted in Section 3.8.2, FTK is also known as AccessData and is created by AccessData to run on Microsoft Windows operating system. FTK is an accessible and powerful program that will read, sort, locate and store relevant information from the hard drive. The program uses imaging tools to make copies of pertinent information that the investigators can then review. Solomon et al. (2015:176) as well as Holt et al. (2018:541) explain that "FTK is capable of imaging a hard drive, scanning slack space, and identifying steganography. It is also capable of cracking password and decrypting files."

It is the views of the three Managers that GAR lack advanced resources and there is a need for the acquisition of those resources to be able to effectively investigate e-Procurement fraud using electronic data recovery. They mentioned that licenses for software utilised has expired which renders them unusable. The three Managers suggested the following:

M8: *"We need advanced hardware and software."*

M9: *"Resources in terms of the software and the advanced tools recover data."*

M10: *"Always update the license, City must pay for expired license. Otherwise, it is useless to have resources without licenses."*

The common recommendation by the participants is that CoT must acquire advanced forensic tools to recover electronic data to effectively investigate e-Procurement fraud and to pay for licenses to keep them operational. The overwhelming suggestion by the majority of the participants was the provision of formal training which is illustrated in detail below:

5.10.4 Sub-theme 8.4: Training of investigators

From the literature in Section 3.5, and as confirmed by Maras (2015:367) that the forensic investigators will be required to provide his or her qualifications as a technical or expert and creditable witness when testifying and that they "must be prepared to answer questions relating to their work experience (position occupied and employment history), educational background, training, licenses, certificates, memberships in professional organisations, awards, publications, and previous testimony provided in other similar cases". Also refer to Section 3.5 in this regard.

There were similar sentiments shared by three SFASs who unequivocally suggested that to improve the capacity of CoT investigators formal training must be provided. Participants also mentioned that training should specifically focus on electronic data recovery and the investigation of e-Procurement fraud. The responses from the three SFAS clearly illustrate their need for the provision of formal training regarding electronic data recovery:

SFAS 11: *"From my personal view, I don't think the City's at this stage can become successful as far as the electronic investigations. We still need a thorough training on electronic data recovery. So, there's still more which needs to be done. The City still needs more to equip its employees. It needs skills development."*

SFAS 12: *"Training. Obviously, e-Procurement investigation training as well. Remember, you can go to training, and they will give you the training, but you must practice it."*

SFAS 13: *"Training is needed. I remember, we once attended a digital evidence and recovery at Pretoria University but, honestly speaking, we never even apply that in practice, we never even apply it practically when we came back. So, I will say we still need training on that one."*

The statements below by 10 SFIs represent the main opinions voiced:

SFI 14: *"We need [ongoing] training. Everything is changing. The technology is evolving. Every day it's upgrading. Technology is moving fast. So, you must be on par with technology. Like, for instance, cybercrime, I'm taking that for an example, at this stage, I don't have any experience in cybercrime because I don't have access and I don't have a proper training into it. That's my main thing. But, like I said, the technology changes every day. If they can keep us updated the whole time, it will be nice."*

SFI 15: *"Proper training into cybercrime. I don't have. I can investigate but cybercrime I never actually touched on cybercrime for myself. If they can send us all of us to training, then it will be better. If they invest in us so that we are trained properly, yes, we need training and skills development."*

SFI 16: *"From where I'm actually sitting…in fact, based on my collective experience, it basically means that one has to be enrolled in the programme that will be almost like a live training programme, meaning that it has to go in line with the changes that are actually happening in the market, particularly when it has to deal with IT-related aspects. So, in this environment, one will appreciate of some tactics or whatever that is actually happening in that particular space."*

SFI 17: *"We need formal training to be on practical basis so that we can be abreast with any development that are happening in the market because technology is evolving. We need to catch up with the new development."*

SFI 18: *"And the main thing is that we will need the systems and the programs to do the investigations. And we need continuous training. Cybercrime is changing and moving fast."*

SFI 19: *"I think you should provide me with proper training so that I can have skills The department …yes, there is a need to provide me with proper training so that I can be more knowledgeable about the electronic evidence recovery and be able to carry out my tasks."*

SFI 20: *"Training, there can definitely be development. We can look into that because…for sure. It will be best for us to develop our skills, to improve our investigations at the end of the day, to highlight the red spots and to see where corruption and fraud is, and to conduct where we are not actually doing that much of investigation.*

SFI 21: *"It goes back to training, and constant training, I think. If you get trained in a system or a process, it will change over years. So, you must constantly have an update or more training or just a refresher course. And that should also be linked to access within the City. Because new systems get implemented without people being trained."*

SFI 22: *"The way to improve us is to obtain the necessary training equal into the job we are doing for e-Procurement and other investigations."*

SFI 23: *"Obviously with any training it will increase your efficiency and effectiveness in conducting that investigation. If you have that particular knowledge, then your investigation moves faster. It will help you to move faster in your investigation."*

The participants are of the view that through constant training they will improve their investigative skills, particularly in electronic data recovery and e-Procurement. Some participants suggested that training will increase their efficiency and effectiveness of conducting investigations. The mutual view of the participants is that technology and cybercrime are evolving fast, and to deal with their own predicament of not being able to recover electronic data during the investigation of e-Procurement fraud, continuous training and refresher courses are needed to enhance their skills. Lack of training in electronic data recovery inadvertently resulted in GAR investigators being demoralised and some end leaving the CoT either by taking early retirement or looking for greener pasture somewhere else.

5.11 CHAPTER SUMMARY

In this chapter, the content from the transcribed interviews was illustrated, explained and justified. The responses from the interviews proved that the GAR investigators are not able to recover electronic data for e-Procurement fraud investigations. Training is urgently and desperately needed to improve the investigative capacity of the investigators. Full access to the relevant CoT electronic systems must also be granted to the investigators. The CoT must also acquire advanced resources to recover electronic data internally. Participants unanimously agreed that electronic data has the capacity to be effective however, this is not the case at the CoT due to the challenges they raised under theme 2 and 6. Teamwork and access to the system are some of the suggestions mentioned by the participants to improve their capacity to investigate e-Procurement fraud using electronic data recovery.

The testimony in this chapter is from well experienced participants in their field. Their experience offered insight into different scenarios and the working of the electronic data recovery at GAR. The information from the participants was further interpreted and simplified to create meaning. The interviews were recorded using a recording device and then transcribed. The participants echoed similar challenges in recovering electronic data and effectively investigating e-Procurement fraud.

In the following chapter, a set of recommendations are made, along with a summary of the data and a conclusion. The literature study presented in Chapters 2, 3 and 4 of this study will be compared and paired with the themes identified in this chapter.

CHAPTER SIX
SUMMARY, RECOMMENDATIONS AND CONCLUSION

6.1 INTRODUCTION

This chapter begins with a synopsis of chapters one to five, after which the interpretations of the study findings are deliberated and presented. Subsequently, recommendations will be put forward based on the key findings from the themes and sub-themes explored in chapter five to contribute to the body of knowledge regarding the use of electronic evidence in the investigation of e-Procurement investigations.

Recommendations made in this chapter can promote the use of electronic evidence in the investigation of e-Procurement fraud investigations. This study is important since it explores the use of electronic evidence in the investigation of e-Procurement fraud investigations at the CoT and offers practical recommendations to improve the use of electronic evidence in the investigation of e-Procurement fraud investigations.

Consequently, a theoretical framework that practically outlines best practices of electronic data recovery in e-Procurement fraud investigation in the form of progressive stages is proposed. This framework presents practical solutions to address the use of electronic evidence in the investigation of e-Procurement fraud investigations at the CoT and thus promotes the existing knowledge on the use of electronic evidence in the investigation of e-Procurement fraud investigations.

6.2 SUMMARY

Chapter one set the scene of the study by detailing the methodological boundaries. The research problem set the parameters for the ensuing research aim. The research objectives of the study derived from the identified problem statement and research aim then followed.

The aim of this study was achieved; namely, to assess the significance of using electronic data recovery in e-Procurement fraud investigations, with the purpose of:

- Exploring, identifying, and pronouncing the effectiveness of using electronic data recovery in e-Procurement fraud investigations; and
- Making recommendations regarding the electronic data recovery in e-procurement fraud investigations based on the research findings, which could potentially be used to improve an understanding of electronic data recovery in e-Procurement fraud by CoT forensic investigators.

The following primary research question was explored and answered in this study:
What is the significance of utilising electronic data recovery applications in e-Procurement fraud investigations?

The below secondary research questions originated from the primary research question and were subsequently answered:

- Could the utilisation of advanced investigative resources enable CoT forensic investigators to recover electronic data to enhance e-Procurement fraud investigations?
- How could the application of advanced investigative resources empower CoT forensic investigators with knowledge to successfully investigate e-Procurement fraud?
- How could the CoT establish sufficient investigative capacity that would enable CoT forensic investigators to recover electronic data and eliminate external service providers in e-Procurement fraud investigations?
- What international best practices exist to recover electronic data in the investigation of e-Procurement fraud?

The viewpoints of forensic investigators, senior forensic investigators, senior forensic audit specialists and managers at GAR was explored. Extensive interviews were carried out with these participants. This chapter also illuminated the key theoretical terms central to this study. The research methodology applied in this study was outlined and included an explanation of the research approach and design, data collection and analysis methods, ethical considerations, and the processes followed to ensure trustworthiness.

Chapter two presented a thorough conceptual overview of the e-Procurement system. The chapter then highlighted the evolution of e-Procurement, benefits of e-Procurement challenges of e-Procurement adoption and implementation, types of e-Procurement models, technology applications and system architecture, key components of the e-Procurement system, e-Procurement in the South African context. A discussion of international best practices of e-Procurement concluded this chapter.

Chapter three provides an overview of electronic data recovery. This chapter started with a presentation of electronic data and its significance. Consequently, the challenges experienced to recover electronic data, computer assisted audit techniques, capacity and qualities of the cyber-crime investigator in terms of electronic data recovery, forensic electronic data recovery steps, process of examining electronic data (end-to-end), electronic data recovery tools, sources of electronic evidence, maintaining the chain of custody of electronic evidence, the Locard principle, and the best evidence rule. This chapter concluded with an overview of international best practices in the recovery of electronic data.

Chapter four reviewed the investigation of e-Procurement fraud. This chapter commenced with the categories of e-procurement fraud, where after light was shed on the cost and extent of e-Procurement fraud. The reader was furthermore enlightened on the types of procurement fraud schemes and the investigation, as well as the detection and prevention of e-Procurement fraud. This chapter ended with a discussion on e-Procurement red flags.

Chapter five articulated the participants' experiences and viewpoints, which allowed the reader to obtain thorough acumen into the data collected that derived from the interviews. Participant experiences and viewpoints were classified by means of themes and sub-themes that arose from the interviews. Verbatim excerpts were presented to express the interviewees’ replies to the themes and sub-themes. Each theme was presented and supported with the appropriate literature from chapters one to four to assess the significance of using electronic data recovery in e-Procurement fraud investigations.

6.3 RECOMMENDATIONS EMANATING FROM THE FINDINGS

E-Procurement fraud has resulted in great financial losses for the CoT. The analysis and interpretation of the research results disclosed that CoT GAR forensic investigators experience various shortcomings and challenges that impacts these investigators’ capability to use electronic data recovery in the investigation of e-procurement fraud.

The researcher recommends a theoretical framework that outlines best practices of electronic data recovery in e-procurement fraud investigations in the form of progressive stages. These recommendations are based on the in-depth interviews conducted with participants as well as on national and international literature reviewed in the study. Moreover, best practices of electronic data recovery as applied in the USA, UK, Italy, China, Australia, India, and Indonesia were explored and may serve as best practices for the CoT.

6.3.1 Recommendation regarding the lack of knowledge of different types of e-Procurement models or solutions at the CoT

Lack of knowledge of different types of e-Procurement models is one major contributor to the GAR investigators' inability to investigate e-Procurement fraud cases successfully. For one to be able to investigate e-Procurement fraud, one needs to be acquainted with the model or solution the CoT is using currently. Without the knowledge of the e-Procurement model that the CoT is using, it becomes practically impossible for the investigators to successfully investigate it. The formal training of investigators on e-Procurement, in general, is highly recommended. It will improve their knowledge and skills and the level of productivity will be enhanced.

In addition to formal training, it is further recommended that CoT provides constant workshops to the investigators to be able to grasp the basic knowledge of e-Procurement models to allow them to investigate. In the interim, while waiting for formal training, the investigator can be stationed at e-Procurement offices to get the orientation of what the e-Procurement model entails. They will therefore be able to conduct the investigation with the assistance of the e-Procurement officials and by so doing they will be learning the processes of the e-Procurement model.

Because e-Procurement is a Web dependency and electronic system, the following are recommended training courses for the GAR investigators. These courses are mostly IT-related since all if not most, of the evidence of e-Procurement fraud investigation will be in electronic form:

- Introduction to IT audit;
- Basic IT Training (Software and Hardware);
- From Cradle to the Grave;
- General e-Procurement;
- E-Procurement fraud investigation; and
- Investigation of contract fraud.

Lastly, it is recommended that the GAR investigator must be given full viewing access to the e-Procurement system to be able to proactively identify the anomalies and to easily access the evidence needed for investigations.

6.3.2 Recommendation regarding the ineffectiveness of electronic data recovery in the investigation of e-Procurement fraud at the CoT

One of the mandates of the GAR investigators is to effectively investigate any acts of fraud. This includes e-Procurement fraud which is problematic to the CoT as most of the budget is utilised on goods and services. A whole lot of evidence of e-Procurement fraud investigation are in the e-Procurement system. For the investigators to get hold of this electronic evidence, they must be able to recover this electronic evidence. The management of the CoT must capacitate the internal investigator to be able to recover electronic data because without recovery, it will be impossible to successfully investigate e-Procurement fraud.

Capacitating GAR investigators will save the CoT money as they will now investigate e-Procurement fraud cases internally instead of outsourcing to the external consultant as it is happening currently. It is therefore recommended that formal training in the recovery of electronic data should be provided. The following are recommended training courses in electronic data recovery:

- Advance Digital Forensics;
- ACFE South Africa and International Chapters;
- The Electronic Evidence and Discovery;
- Advanced Forensic Crime Intelligence.

For the recovery of electronic data to be effective in the CoT, it is further recommended that coupled to training, the management of the CoT must give the investigators full access to systems such as e-Procurement and SAP. The CoT management must also procure the modern and appropriate IT resources like software and hardware's to be able to recover electronic data while investigating e-Procurement fraud.

6.3.3 Recommendation on the challenges with regards to recovering electronic data during the investigation of e-Procurement fraud at the CoT

For the successful investigations of e-Procurement fraud in the CoT, GAR investigators are required to be well versed with adequate skills and knowledge of electronic data recovery. Due to a skills deficit amongst GAR investigators, the CoT is currently outsourcing most of the e-Procurement fraud investigation to resolve the predicament of having these cases investigated. It is recommended that when the CoT outsources e-Procurement fraud investigations, the external consultant must work with the internal investigator to transfer skills. Alternatively, the CoT must co-source these investigations, this will allow external consultants and internal investigators to work together on the same case. This will ultimately result in skills transfer.

Capacitating the GAR organisational structure by recruiting qualified IT personnel to deal with the recovery of electronic data and seasoned Managers to supervise the investigators. This will improve the success rate of investigating e-Procurement fraud. A sufficient budget focused on training must be provided. The electronic evidence that is required to investigate e-Procurement cases is found in the electronics and systems such as computers, servers, SAP and e-Procurement. The CoT management must provide full viewing access to these systems in order to access electronic data for the purpose of investigations.

The fight against e-Procurement fraud in the CoT cannot be left to the GAR investigators alone, it should start from the top Management of the CoT. It is recommended that there should be a political will to capacitate GAR investigators with required training and adequate resources to recover electronic data in the investigation of e-Procurement fraud. The investigators must be given full support by the management in what they are expected to deliver as far as investigation is concerned.

The management support must not only be limited to administrative, but it must also be extended to shield the investigators from political interference. It is therefore further recommended that investigators must be protected from any form of intimidation and threat by the suspects being investigated. The management must also set aside a budget to procure the most prominent software to recover and analyse electronic data. The recommended tools and software applications to analyse recovered data are as follows:

- ACL software program;
- Caseware IDEA;
- SAS; and
- Arbutus.

For all these tools and software (mentioned above) to be useful and beneficial, licenses must be paid and renewed in time. The CoT must also have a compatible IT system for the investigators to operate these software applications.

6.3.4 Suggestions to improve the FI’s capacity to investigate e-Procurement fraud using electronic data recovery at the CoT

The long-term solution for the GAR Investigator to be able to investigate e-Procurement fraud using electronic data recovery is the provision of formal training. The investigators must be enrolled at a recognised University or college which provide training relating to e-Procurement fraud and recovery of electronic data. It is therefore recommended that Managers and SFASs must be enrolled first and any other SFIs and FIs can then be registered. This training will improve the capacity of FIs to investigate e-Procurement fraud effectively.

The acquisition of advanced resources to recover electronic data will enhance the ability of the FIs to recover electronic data which in turn will improve the investigation of e-Procurement fraud. To improve the capacity of GAR investigators, they must be conversant with the latest tools and software in the market. The following advanced resources are recommended:

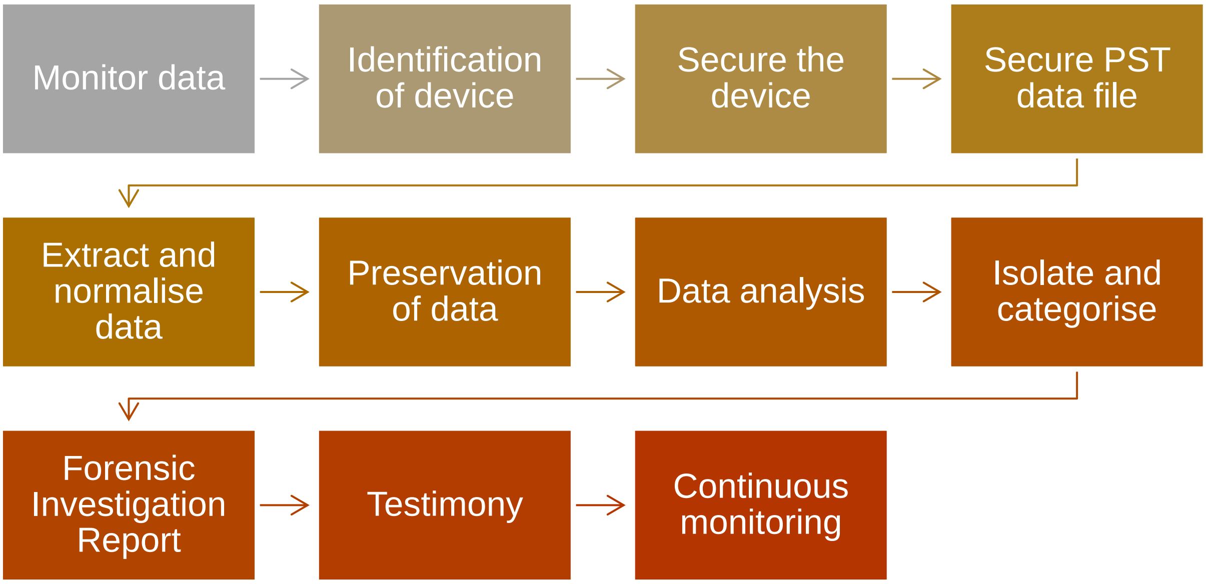
- AccessData Forensic Toolkit;
- EnCase Forensic Software;
- ProDiscover Forensics;
- Password Recovery Toolkit;
- Stego Suite;
- Access Data’s Password Recovery Program; and
- Novell NetWare Password Recovery.

Additionally, and equally importantly, the CoT must create a Live Computer Lab to monitor the activities, especially where there is a high risk of committing e-Procurement fraud and corruption. This will allow them to proactively identify the problematic area and red flags. It is further recommended that CoT management must acquire hardware such as high-tech computers and cameras to process the crime scenes. There is a need for voluminous external hard drives or servers to store recovered electronic data for preservation. It will be advantageous for the CoT to have Cloud storage to preserve the data before it is deleted or tampered with, and FIs must be given full access to that Cloud server. This will enhance their capacity to investigate e-Procurement fraud using electronic data recovery.

It is further recommended that after providing the formal training to the FIs, the management of the CoT must give full viewing access to the e-Procurement system and SAP for the investigators to be able to recover any relevant electronic data during the investigation of e-Procurement fraud. Again, to close a gap of skills and experience CoT management must allow the investigators of different skill sets and experience to work together to transfer on the job knowledge between themselves. The qualified CFEs, Internal Auditors, Risk Practitioners and IT auditors must work closely with FIs to share different knowledge about e-Procurement fraud. Risk Practitioners will help with identifying high-risk areas for the FIs to focus on and Internal Auditors will assist with identifying fraud indicators and by detecting any anomalies in the e-Procurement system.

A procedural framework for an electronic data recovery strategy to investigate e-Procurement fraud at the CoT is proposed (see Figure 6.1 below). By implementing this procedural framework, the occurrence of e-Procurement fraud could be effectively addressed by identifying fraudsters and consequently ensuring arrests and convictions. It is further proposed that the CoT adopt, implement, and maintain the proposed procedural framework for an electronic data recovery strategy in the investigation of e-Procurement fraud at the CoT to address e-Procurement fraud.

Figure 6.1: A procedural framework for an electronic data recovery strategy in the investigation of e-Procurement fraud at the CoT (designed by researcher).



To address the identified problem at the CoT, a practical procedural framework (figure 6.1 above) is recommended for implementation by the CoT management. This framework prescribes the process to be followed by the CoT investigators to recover electronic data in the investigation of e-Procurement fraud. As designed and illustrated by the researcher in the above figure 6.1, the following is a step-by-step process to recover electronic data:

1. Monitor the data:
   - The investigator must monitor the data in the CoT network, storage server, SAP and e-Procurement system;
   - Monitor for any unusual activities to proactively detect possible e-Procurement fraud;
   - Active and ongoing review of data; and
   - If any anomalies are detected, then follow the second step.
2. Identification of the device used:
   - Use the IP address to locate the device affected; and
   - Check the network point the device was connected to.

3. Secure the device:
    - Document the scene properly by taking pictures and video recordings of all the activities in the scene;
    - Label all the devices to be seized;
    - Write the brand name of the device, serial number and the CoT barcode on the seizure form; and
    - When seizing the device, use the suitable container for storage and transportation of electronic devices.
4. Secure PST data file:
    - Immediately contact IT division to secure e-mail cache (outlook data) for the suspect user;
    - PST data file will be mounted on the outlook of the investigator for further analysis; and
    - Request IT personnel to disable the user account from the network.
5. Extract and normalise data:
    - Bit by bit image using FTK or EnCase software to recover data;
    - Make a number of copies for future analysis; and
    - To normalise data, the investigator must cleanse and convert data to a format suitable for analysis before executing any data analysis tests.
6. Preservation of data:
    - Secure the data in the storage suitable for that purpose;
    - Not to be tempered with in any way; and
    - Chain of custody to be maintained all the time.
7. Data analysis:
    - Analysis of timelines of interest;
    - Analysis to be done on the copies only;
    - No analysis on the original data; and
    - Secure original for court purposes.
8. Isolate and categorise:
    - Identified data of interest must be isolated from other irrelevant data and categorised as evidence in the investigation; and
    - These crucial findings will be used to compile a forensic report.

9. Forensic investigation report:
    - The investigator must create a customised forensic investigation report detailing the whole chain of events based on the correlation of the identified timelines;
    - The report must outline the examination process and pertinent data recovered during investigation; and
    - Each individual step/stage of electronic data recovery must be thoroughly documented.
10. Testimony:
    - The investigator must be able to interpret each step undertaken during investigation;
    - Explain the collection methods used;
    - Processes used to extract and recover data;
    - How and where the data was preserved;
    - Tools used in examination of data; and,
    - How the tests were done and the results that lead to the findings.
11. Continuous monitoring:
    - Constant monitoring on a periodic or continuous basis; and
    - In a highlighted high risk areas for e-Procurement fraud, continuous monitoring will provide increased assurance of early detection and can serve as a deterrent.

The steps outlined above must follow each other and must be implemented in a sequence as recommended above. The effectiveness of this procedural framework is dependent on the correct implementation by the CoT investigators.

6.4 CONCLUSION

This chapter summarised Chapter 1 to Chapter 5, after which recommendations were made on how the CoT could improve e-Procurement investigations through the application of electronic data recovery. Based on the literature review and the in-depth interviews, the research findings draw attention to limitations restricting GAR forensic investigators’ efficiency and its impact on the investigation of e-Procurement fraud using electronic data recovery.

The research findings also indicate shortcomings in the GAR's effectiveness in utilising electronic data recovery applications in e-Procurement fraud investigations, which limits its impact on the investigation of e-Procurement fraud. Based on these findings, a theoretical framework that outlines best practices of electronic data recovery in e-Procurement fraud investigations in the form of progressive stages is proposed, thus contributing to the current body of knowledge.

Additional to the proposed theoretical framework, it is recommended that the CoT consider the limitations and challenges experienced by the GAR in the use of electronic data recovery to improve its impact on e-Procurement fraud. Formal training to improve the capacity of the GAR investigators and the acquisition of advance resources such as modern technological tools and software are highly recommended for implementation by the CoT.

LIST OF REFERENCES

Abramson, M.A. & Morin, T.L. 2003. *E-government 2003*. New York: Rowman & Littlefield.

Abu-Elsamen, A., Chakraborty, G. & Warren, D. 2010. A process-based analysis of e-Procurement adoption. *Journal of Internet Commerce*, 9(3):243-259.

Aduwo, E. B., Ibem, E. O., Afolabi, A. O., Oluwnmi, A. O., Tunji-Olayeni, P. F., Ayo-Vaughan, E. A., Uwakonye, U. O. & Oni, A. A. 2020. Exploring anti-corruption capabilities of e-procurement in construction project delivery in Nigeria. *Construction Economics and Building*, 20(1), 56-76.

Ahmed, R. & Dharaskar, R.V. 2009. *Mobile Forensics: An Introduction from Indian Law Enforcement Perspective*. Paper presented to International Conference on Information Systems, Technology and Management. 10-12 March.

Akay, Y.V. 2020. Computer Forensics and Cyber Crime Handling*. Jurnal Teknik Informatika,* 15(4):291-296.

Akkaynak, O.S. 2004. The Benefits and Barriers of Electronic Public Procurement System: A Case Study on Public Hospitals in Turkey. *E-Procurement Management for Successful Electronic Government Systems*. Ankara: Sinus.

Albanna, F. & Raidi, I. 2017. Forensic Analysis of Frozen Hard Drive Using Static Forensics Method. *International Journal of Computer Science and Information Security*, 15(1):1947-5500.

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C. & Zimbelman, M. F. 2019. *Fraud examination*. (5th edition). Boston (MA): Cengage Learning.

Al-Hiyard, A., Al Said, N. & Hattab, E. 2019. Factors that influence the use of computer assisted audit techniques (CAATS) by internal auditors in Jordan. *Academy of Accounting and Financial Studies Journal*. 23(3), 1-15.

Al-Sartawi, M. A., Razzaque, A. & Kamal, M. M. 2021. *Artificial intelligence system and the internet of things in the digital era*. Proceedings of EAMMIS 2021. Switzerland: Springer.

Ambe, I.M. 2016. Public procurement trends and developments in South Africa. *Research Journal of Business and Management*. 3(4): 277-290.

Ambelm, I.M. & Badenhorst-weiss, J.A. 2012. Procurement challenges in the South African public sector. *Journal of Transport and Supply Chain Management.* 46(3):1100–15.

Anthony, A. 2018. The use of e-Procurement in South African public procurement law: challenges and prospects. *Law, Democracy and Development*. 22(1): 39 – 47.

Ashcroft, J., Daniels, D.J. & Hart, S.V. 2019. *Forensic examination of digital evidence: A guide for law enforcement.* Washington, DC. National Institute of Justice.

Association of Certified Fraud Examiners. 2012. *Introduction to digital forensics: gathering and preserving electronic evidence*. Available at: https://www.acfe.com/content.aspx?id=2247 (accessed 10 November 2020).

Association of Certified Fraud Examiners. 2019. *Fraud prevention and deterrence*. Available at: https://www.acfe.com › 2019INTFEMTOC (accessed 10 November 2020).

Auditor General South Africa. 2020. Report on Local Government Audit Outcomes 2018/19. Pretoria: SA Government.

Auditor General Victoria. 2003. *Electronic Procurement in the Victorian Government.* Melbourne: Government of Victoria.

Badiru, A. B. & Tacz, L. 2016. *Handbook of measurements: Benchmarks for system accuracy and precision*. Boca Raton: CRC Press.

Bair, J. 2018. *Seeking the truth from mobile evidence: basic fundamentals, intermediate and advanced overview of current mobile forensic investigations*. Amsterdam: Elsevier.

Bakar, N. A., Peszynski, K., Azizan, N. & Sundram, V. P. K. 2016. Abridgment of traditional procurement and e-Procurement: Definitions, tools and benefits. *Journal of Emerging Economies and Islamic Research*, 4,(1), 76-91.

Barbieri, P. and Zanoni, A. 2005. The e-Procurement experience in Italian universities*.* *Journal of Public Procurement*, 5 (3), 323–343.

Baryamureeba, V. & Tushabe, F. 2004. *The enhanced digital investigation process model*. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.492&rep=rep1&type=pdf (accessed 28 May 2020).

Barrow, L.M. & Rufo, R.A. 2014. *Police and profiling in the United States*. Boca Raton (FL): Taylor & Francis.

Battula, B.P., Rani, B.K., Prasad, R.S. & Sudha, T. 2009. Techniques in Computer Forensics: A Recovery Perspective. *International Journal of Security,* 3(2):27-35.

Beaver, K. 2010. *Hacking for dummies*. (3rd edition). Indianapolis: Wiley & Sons.

Berte, R., Marturana, F., Me, G. & Tacconi, S. 2012. *Data Mining based Crime-Dependent Triage in Digital Forensics Analysis.* Paper presented at the International Conference on Affective Computing and Intelligent Interaction, Taipei, Taiwan, 27-28 Feb.

Bey-Miller, R., Clarke, R. & van Dyk, V. 2009. *Introduction to information systems*. Cape Town: Pearson.

Biasiotti, M. A., Bonnici, J.P.M., Cannataci. J. & Turci, F. 2018. *Handling and exchanging electronic evidence across Europe*. New York (NY): Springer.

Bidgoli, H. 2010. *The handbook of technology management: supply chain management, marketing and advertising, and global management*. Hoboken (NJ): John Wiley & Sons.

Bidgoli, H. 2019. *Management information system*. (9th edition). Richmond: John Wiley & Sons.

Brown, C. L. T. 2010. *Computer evidence: collection and preservation*. (2nd edition). USA: Cengage Learning.

Brown, C. S. D. 2015. Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*. International Journal of Cyber Criminology* (9)1:55 - 119.

Bryant, R. 2008. *Investigating digital crime*. London: John Wiley & Sons.

Bryant, R. & Bryant, S. 2016. *Policing digital crime*. Milton Park: Routledge.

Bryman, A & Bell, E. 2015. *Business research methods*. Oxford: Oxford University Press.

Boddington, R. 2016. *Practical digital forensics*. Birmingham: Packt.

Bof, F. & Previtali, P. 2010. National models of public (e)-procurement in Europe. *Journal of e-Government Studies and Best Practices.* 2(1): 1 – 14.

Bolton, P. 2016. Public Procurement as a Tool to Drive Innovation in South Africa. *PER / PELJ*, (19), 5.

Bopape, R. K. 2015. *Towards a unified fraud management and digital forensic framework for mobile applications*. Pretoria: Unisa.

Bouma, S. D. & Ling, L. 2004. *The research process*. (5th edition). New York: Oxford University Press.

Candra, S. & Gunawan, F. E. 2016. *The impact of e-Procurement practice in Indonesia government: A Preliminary Study (The case of Electronic Procurement Service at Bekasi District)*. Journal of Physics: Conference Series 801:1-6.

Carlberg, C. 2018. *Predictive analytics*: *Microsoft Excel*. (2nd edition). London. Pearson education.

Cascarino, R. E. 2013. *Corporate fraud and internal control*: *A framework for prevention*. Hoboken (NJ): John Wiley & Sons.

Casey, E. 2010. *Digital forensics and investigation*. Amsterdam: Elsevier.

Casey, E. 2011. *Digital evidence and computer crime: forensic science, computers and internet*. (3rd edition). Orlando (FL): Academic Press.

Cassim, F. 2009. Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study. *Potchefstroom electronic Law Journal*, 12(4): 36 – 81.

Chaffey, D. 2011*. E-business & e-commerce management: strategy, implementation and practice.* (5th edition) London: Pearson.

Chakravarty, A. K. 2014. *Supply chain transformation: evolving with emerging business paradigms*. New York (NY): Springer.

Champlain, J. J. 2003. *Auditing information systems*. (2nd edition). Hoboken (NJ): John Wiley & Sons.

Chan, A. P. C. & Owusu, E. K. 2022. Evolution of electronic procurement: Contemporary review of adoption and implementation strategies. *Buildings*. Available at: https:// doi.org/10.3390/buildings12020198 (accessed 28 May 2020).

City of Tshwane Supply Chain Management Policy. 2019. *Amendment Policy Report*. Pretoria: City of Tshwane Metropolitan Municipality.

City of Tshwane Forensic Investigations. 2020. *Internal audit report (2018 to 2019).* Pretoria: City of Tshwane Metropolitan Municipality.

City of Tshwane e-Procurement Technology Architecture. 2016. *Automation of SCM project*. Praxis Computing: Johannesburg.

Clarke, N. 2011. *Transparent user authentication: biometrics, RFID and behavioural profiling*. New York: Springer.

Coenen, T. L. 2008. *Essentials of corporate fraud*. Hoboken (NJ): John Wiley & Sons.

Conrad, E., Misenar, S. & Feldman, J. 2012. *CISSP study guide*. (2nd edition). Amsterdam: Elsevier.

Cornick, M.S. 2014. *Using computers in the law office*. (7th edition). Boston (MA): Cengage Learning.

Corruption Watch. 2013. *Dodgy procurement*. Available at: http://www.moneyweb.co.za/archive/r25bn-lost-every-year-to-dodgy-procurement/ (accessed 21 March 2021).

Creswell, J. W. 2014. *Qualitative inquiry and research design: choosing among five approaches*. (3rd edition). Thousand Oaks (CA): Sage.

Cuesta, H. & Kumar, S. 2016. *Practical data analysis*. (2nd edition). Birmingham: Packt.

Dai, Q. & Kauffman, R.J. 2001. *Business Models for Internet-Based E-Procurement Systems and B2B Electronic Markets: An Exploratory Assessment.* Paper presented to the Thirty-Fourth Annual Hawaii International Conference on Systems Sciences. January 3-6.

Davila, A., Gupta, M. & Palmer, R. 2003. Moving procurement systems to the Internet. The adoption and use of e-procurement technology models. *European Management Journal*, 21(1):11-23.

Davis, C., Philip, A. & Cowen, D. 2005. *Hacking exposed computer forensics*. New York (NY): McGraw-Hill.

Dahlberg, L. & McCraig, C. 2010. *Practical research and evaluation. A start-to-finish guide for practitioners*. Los Angeles: Sage.

Daniels, L.E., & Daniels, L. E. 2012. *Digital forensic for legal professionals: understanding digital evidence from the warrant to the courtroom*. Amsterdam: Elsevier.

Dantzker, M. L., Hunter, R. D., & Quinn, S. T. (2016). R*esearch Methodology for Criminology and Criminal Justice*. (4th edition). England: Jones & Bartlett Publishers.

Dedrick, J., Xin Xu, S., & Xiaoguo Zhu, K. 2008. How does information technology shape supply-chain structure? Evidence on the number of suppliers. *Journal of Management Information Systems*, 25(2): 41-72.

Denscombe, M. 2014. *Ground rules for social research: Guidelines for good practice*. New York: Open University Press.

De Vos, A. S., Strydom, H., Fouché, C.B. & Delport, C. S. L. 2007. *Research at grassroots for the social sciences and human services professions*. (3rd edition). Pretoria: Van Schaik.

Duan, R. & Zhang, X. 2020. Research on Computer Forensics Technology Based on Data Recovery. *Journal of Physics: Conference Series*,1648: 1-4

Dufrasne, B., Fridli, R. & Greenfield, A. 2019. *Data-at-rest encryption for the IBM spectrum accelerate family*. Available at: https://www.redbooks.ibm.com/redpapers/pdfs/redp5402.pdf (accessed 28 November 2020).

Eadie, R., Perera, S., Heaney. & Carlisle, J. 2007. *Drivers and barriers to public sector e-procurement within Northern Ireland's construction industry*. Available at: https://itcon.org/papers/2007_6.content.07965.pdf (accessed 21 March 2021).

EC-Council. 2010. *Computer forensics: evidence collection & preservation*. Clifton Park (NY): Cengage.

Elango, D. 2017. The Web- Based ERP Systems vs Offline ERP Systems of SMEs: A Review. *Research Journal of Social Science & Management*, 7(7), 67-77.

Engström, A., Wallström, A. & Salehi-Sangari, E. 2014. *Implementation of Public e-Procurement in Swedish Government Entities*. Paper presented to the International Multiconference on Computer Science and Information Technology (IMCSIT). Mrągowo, Poland, 12-14 October.

Erridge, A., Fee, R. & Mcllroy, J. 2001. *Best practice procurement: public and private sector perspectives.* Hampshire: Gower Publishing.

Eskandarian, M., Marthandan, G., Malarvizhi, C. A. & Tehrani, S. Z. 2016. Quality in e-Procurement success. *International Journal of Management & Information Systems,* 20 (3), 73-86.

Eze, T., Speakman, L. & Onwubiko, C. 2020. *Proceedings of the 19th European conference on cyber warfare and security*. University of Chester. UK: ACPI

Fenu, G. & Solinas, F. 2013. Computer forensics between the Italian legislation and pragmatic questions. *International Journal of Cyber-Security and Digital Forensics*, 2(1): 9-24.

Ferraro, M. M. & Casey, E. 2005. *Investigating child exploitation and pornography: the internet, the law and forensic science*. Amsterdam: Elsevier Academic Press.

Fisher, A. J. B. 2004. *Techniques of crime scene investigation*. (7th edition). Boca Raton, FL: CRS Press.

Flick, U. 2022. *An Introduction to qualitative research.* (7th edition). Thousand Oaks (CA): Sage.

Galloway, J. 2003. *An investigation of E-procurement Risks*. Paper presented at the 14th Australasian Conference on Information Systems. Perth, Australia, 26-28 November.

Ghani, R., Ismail, N. A. & Saidin, S. Z. 2016. *Adoption of Computer-Assisted Audit Tools and Techniques (CAATTs): An Exploratory Study in Audit Firms*. Paper Presented to the International Conference on Accounting Studies (ICAS). Langkawi, Kedah, Malaysia, 15-18.

Giova, G. 2011. Improving chain of custody in forensic investigation of electronic digital systems. *International Journal of Computer Science and Network Security*, 11 (1): 2-3.

Girard, J. E. 2011. *Criminalistics: forensic science, crime, and terrorism*. (2nd edition). Burlington (MA): Jones & Bartlett Learning.

Girard, J. E. 2015. *Criminalistics: Forensic science, crime, and terrorism*. (3rd edition). Burlington (MA): Jones & Bartlett Learning.

Gray, D. E. 2014. *Doing research in the real world*. (3rd edition). Thousand Oaks (CA): Sage.

Graves, M.W. 2014. *Digital archaeology: the art of science of digital forensics*. New York (NY): Pearson Education.

Golden, T. W., Skalak, S. L. & Clayton, M. M. 2011. *A guide to forensic accounting investigation*. Hoboken (NJ): John Wiley & Sons.

Goldmann, P. D. 2010. *Financial services: Anti-fraud risk and control*. Hoboken (NJ): John Wiley & Sons.

Goodison, S. E., Davis, R. C. & Jackson, B. A. 2015. *Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence*. Santa Monica (CA): Rand Corporation.

Hassan, N. A. & Hijazi, R. 2017. *Data hiding techniques in windows OS: A practical approach to investigation and defence*. Amsterdam: Elsevier.

Hattingh, M., Matthee, M., Smuts, H., Pappas, I., Dwivedi, Y. K. & Mäntymäki, M. 2021. *Responsible design, implementation and use of information and communication technology*. 19th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society. Skukuza: South Africa. April 6-8. 2020 Proceedings.

Hawking, L. B. & Stein. 2004. Supply management and e-procurement creating value added in the supply chain. *Industrial Marketing Management*, 32 (3): 219-226.

Hayes, D.R. 2015. *A practical guide to computer forensics investigations*. New York (NY): Pearson Education.

Henriksen, H. Z. & Mahnke, V. 2005. E-Procurement Adoption in the Danish Public Sector: The Influence of Economic and Political Rationality. *Scandinavian Journal of Information Systems*, 17(2): 85–106.

Ho, A.T.S. & Li, S. 2015. *Handbook of digital forensics of multimedia data and devices*. Hoboken (NJ): John Wiley & Sons.

Hofstee, E. 2006. *Constructing a good dissertation: A practical guide to finishing a master's, MBA or PhD on schedule*. Sandton: EPE.

Holt, T.J., Bossler, A.D. & Seigfried-Spellar, K.C. 2018. *Cybercrime and digital forensics: An introduction*. (2nd edition). New York (NY): Routledge.

Hughes, T. M. 2016. *SAS data analytic development*: *Dimensions of software quality*. Hoboken (NJ): John Wiley & Sons.

Humphries, G., Hordvik, R., Manifavas, H., Cobley, P. & Sorell, M. 2021. Law enforcement educational challenges for mobile forensics. *Forensic science international: Digital investigation,* 38, 1-11.

Ibem, E. O., Aduwo, E. B., Tunji-Olayeni, P., Ayo-Vaughan, E. A. & Uwakonye, U. O. 2016. Factors influencing e-Procurement adoption in the Nigerian building industry. *Construction Economics and Building*, 16(4), 54-67.

Ibem, E. O. & Laryea, S. 2014. Patterns of technological innovation in the use of e-Procurement in construction. *Journal of Information Technology in Construction (ITcon),* 19, 104-125.

Ibem, E. O. & Laryea, S. 2015. E-Procurement use in the South African construction industry. *Journal of Information Technology in Construction,* 20, 364-384.

Information Resources Management Association (IRMA). 2013. *Small and medium enterprise: concept, methodologies, tools and applications*. Hershey (PA): IGI Global Publisher.

Information Resources Management Association (IRMA). 2020. *Open government: concepts, methodologies, tools, and applications*. Hershey (PA): IGI Global.

International Conference on e-Government (ICEG). 2010. *Proceedings of the 6th international conference on e-Government.* Cape Peninsula University. Cape Town. South Africa.

Jahankhani, H., Watson, D. L., Me, G. & Leonhardt, F. 2010. *Handbook of electronic security and digital forensics*. Singapore: World Scientific Publishing.

Jenkins, T., Köhler, W. & Shackleton, J. 2005. *Turning content into competitive advantage: enterprise content management methods*. Canada: CM methods.

Johnson, L. R. 2014. *Computer incident response and forensics team management: conducting a successful incident response*. Amsterdam: Elsevier.

Johnson, T. A. 2005. *Forensic Computer Crime Investigation*. Boca Raton (FL): Taylor & Francis.

Jooste, M. V. & de W. van Schoor, C. 2003. A framework for the implementation of e-Procurement. *SA Journal of Industrial Engineering*, 14(2): 1-22.

Joyner, RL, Rouse, WA & Glatthorn, AA. 2018. *Writing the winning thesis or dissertation: A step-by-step guide*. California: Corwin Press.

Joysula, V., Orr, M. & Page, G. 2012. *Cloud computing: Automating the virtualised data center*. Indianapolis: Cisco Press.

Kabanda, S., Pitso, N. & Kapepo, M. 2019. The role of institutional pressures in the adoption of e-Procurement in public institutions in developing countries: The case of Lesotho. *The African Journal of Information Systems*, 11(3): 5.

Kalof, L., Dan, A., & Dietz, T. 2008. *Essentials of social research*. Berkshire: Open University Press.

Kamarulzaman, N.H. & Mohamed, Z. 2013. Application of e-Procurement technologies for selecting suppliers of agro-based SMEs in Malaysia*. International Journal of Economics and Management,* 7(1): 45-60.

Kanellis, P. 2006. *Digital crime and forensic science in cyberspace*. London: Idea Group.

Kanellis, P., Kiountouzis, E., Kolokotronics, N. & Martakos, D. 2006. *Digital Crime and Forensic Science in Cyberspace.* London: Idea Group.

Kaspersky, K. 2006. *Data recovery tips & solutions: windows, linux, and BSD*. Wayne County: alist publishing.

Katz, N. A. 2016. *Detection and Reduction of Supply Chain Fraud*. London: Gower.

Kävrestad, J. 2018. *Fundamentals of digital forensics: Theory, methods, and real-life applications*. Switzerland: Springer.

Kruse, W. G & Heiser, J. G. 2002. *Computer forensic: Incident response essentials*. Indianapolis (IN): Pearson Education.

Kumar, R. 2019. *Research methodology: A step-by-step guide for beginners. (*3rd edition). Thousand Oaks (CA): Sage.

Labelle, H. 2012. *A new role for citizens in public procurement*. Distrito Federal: Transparencia Mexicana.

Lange, M. C. S. & Nimsger, K. M. 2009. *Electronic evidence and discovery: What every lawyer should know*. (2nd edition). Chicago (IL): ABA Publishing.

Leedy, P. D. & Ormrod, J.E. 2015. *Practical research: Planning and design.* (9th edition). Hoboken (NJ): Merrill Prentice Hall.

Lewis-Faupel, S., Neggers, Y., Olken, B. A. & Pande, R. 2014. Can electronic procurement improve infrastructure provision? Evidence from public works in India and Indonesia. *National Bureau of Economic Research,* 20344: 2-35.

Liamputtong, P. 2013. *Qualitative research methods*. (4th edition). Melbourne: Oxford University Press.

Lillard, T. V., Garrison, C. P., Schiller, C. A., Steele, J. & Murray, J. 2010. *Digital forensics for network, internet, and cloud computing: a forensic evidence guide for moving targets and data*. Amsterdam: Elsevier.

Lin, N., Li, D., Dong, T. & Qin, Z. 2010. A new framework for designing E-government procurement in China based on ontology and business component. *Journal of Service science & management*, 3:298-308.

Lysons, K. & Farrington, B. 2006. *Purchasing and supply chain management*. (7th edition). London: Pearson Education.

Machie, E. K. 2013. *Network security traceback attack and react in the United States Department of Defence Network*. Bloomingdale (IN): Trafford Publishing.

Makoba, N., Nyamagere, G. & Eliufoo, H. 2017. E-Procurement risks and mitigation: The case for Tanzania construction companies. *International Journal of Construction Engineering and Management*, 6(4): 180-186.

Mamahit, A. I. & Urumsah, D. 2018. The Comprehensive Model of Whistle-Blowing, Forensic Audit, Audit Investigation, and Fraud Detection. *Journal of Accounting and Strategic Finance,* 1(2), 153-162.

Mandia, K. & Prosise, C. 2003. *Incident response & computer forensics*. (2nd edition). Emeryville (CA): McGraw-Hill.

Maras, M.H. 2015. *Computer forensics: Cybercriminals, laws and evidence*. (2nd edition). Burlington (MA): Jones & Bartlett Learning.

Marshall, C. & Rossman, G. B. 2014. *Designing qualitative research.* (6th edition). Thousand Oaks (CA): Sage.

Mason, S. & Seng, D. 2017. *Electronic evidence*. (4th edition). London: Huminites Digital Library.

Masudin, I. & Kamara, M. S. 2017. Electronic Data Exchange and Demand Forecasting implications on Supply Chain Management collaboration: A customer service perspective. *Journal Teknik Industri*, 18(02): 138-148.

Mathews, B. & Ross, L. 2010. *Research methods: A practical guide for the social sciences*. Essex: Pearson Education.

Maxfield, M. G. & Babbie, E. 2014. *Research methods for criminal justice and criminology*. (7th edition). Oxford: Cengage.

McMillan, E. J. 2006. *Policies and procedures to prevent fraud and embezzlement*. Hoboken (NJ): John Wiley & Sons.

Mekenye, B. A. 2017. *An assessment of the roles of electronic procurement strategies on procurement performance in business in tea manufacturing companies in Kenya: A case study of Nyankoba Tea factory in Keroka*. Kisii Town, Kissi University.

Mendell, R. L. 2004. *Investigating computer crime in the 21st century*. (2nd edition). Springfield: Charles C. Thomas.

Mills, J. & Birks, M. 2014. *Qualitative methodology: A practical guide.* Thousand Oaks (CA): Sage.

Moatshe, R. 2020. *R4 billion Tshwane fleet management tender riddled with corruption*. Available at: https://www.iol.co.za/pretoria-news/news/r4-billion-tshwane-fleet-management-tender-riddled-with-corruption (accessed 21 March 2021)

Mohay, G., Anderson, A., Collie, B. & McKemmish, R. 2003. *Computer and intrusion forensics*. London: Artech house.

Moon, M. J. 2005. E-Procurement management in state governments: diffusion of e-Procurement practices and its determinants. *Journal of public procurement*, 5(1): 54-72.

Moussa, A. F. 2021. Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, 11(20), 1-10.

Mouton, J. 2001. *How to succeed in your master's and doctoral studies: A South African guide and resource book.* Pretoria: Van Schaik.

Mozayani, A. & Noziglia, C. 2006. *The forensic laboratory handbook: Procedures and practice*. Totowa (NJ): Humana Press.

Nani, D. A. & Ali, S. 2020. Determinants of Effective E-Procurement System: Empirical Evidence from Indonesian Local Governments. *Journal Dinamika Akuntansi dan Bisnis*, 7(1), 33-50

Ndara, V. 2013. *Computer seizure as technique in forensic investigation*. Pretoria: University of South Africa.

Neef, D. 2001. *E-Procurement: From strategy to implementation*. New Jersey: Prentice-Hall.

Nelson, B., Philips, A. & Steuart, C. 2015. *Guide to computer forensics and investigation*. (5th edition). Boston (MA): Cengage Learning.

Nelson, S. D., Olson, B. A & Simek, J. W. 2006. *The electronic evidence and discovery handbook: forms, checklist, and guidelines.* Chicago (IL): ABA Publishing.

Neuman, L.W. & Robson, K. 2012. *Basics of research: Qualitative and qualitative approaches*. Toronto: Pearson.

Neupane, A., Soar, J., Vaidya, K., & Yong, J. 2012. *Role of public e-Procurement technology to reduce corruption in government procurement: international public procurement conference*. Paper presented at 5th International Public Procurement conference. Seattle, Washington, August 17-19.

Newman, R.C. 2007. *Computer Forensics: Evidence Collection and Management*. Boca Raton (FL): Taylor & Francis.

Ngabiya, S. W. 2017. *An assessment of the effects of e-Procurement adoption on procurement management: A case of Tuskys supermarket, Kisii town*. Kisii University

Ngcamphalala, T. K. T., & AmbeIm, I. M. 2016. Policies and regulations guiding procurement practices in the commuter bus sector. *Journal of Contemporary Management*, 13:1204-1224.

Ngomane, A. R. 2010. *The use of electronic evidence in forensic investigation*. Pretoria: University of South Africa.

Nigel, L. & Samociuk, M. 2006. *Fraud and corruption: Prevention and detection*. London: Gower.

Nzuza, Z. W. & Garbharran, H.L. 2015. Enhancing municipal e-Procurement using inventory stock control: South African design approach. *Journal on Public and Municipal Finance*, 4 (2): 9-10.

Ochonma, E. 2015. *Procurement and Supply Chain Management: Emerging Concepts, Strategies and Challenges*. Bloomington (IN): Author House.

Olsen, W. P. 2010. *The Anti-Corruption Handbook: How to protect your business in the global marketplace.* New Jersey: John Wiley & Sons.

Pablos, P. O., Lovelle, J.M.C., Gayo, J.E.L., & Tennyson, R.D. 2013. *E-Procurement Management for successful electronic government system*. Hershey (PA): IGI Global Publisher.

Padgett, S. 2015. *Profiling the fraudster*. Hoboken (NJ): John Wiley & Sons.

Panduranga, V. 2016. Transparency in public procurement through e-procurement in India. *Journal of Internet Banking and Commerce*, 21(3): 3-4.

Parida, U. & Parida, V. 2005. *E-procurement: An Indian and Swedish perspective*. Unpublished MA Dissertation. Luleå: Luleå University of Technology.

Peterson, D. & Shenoi, S. 2009. *Advances in digital forensics V*. New York (NY): Springer.

Perera, S., Ingirige, B., Ruikar, K. & Obonyo, E. 2017. *Advances in construction ICT and E-business*. New York (NY): Taylor & Francis.

Perera, S., Nanayakkara, S. & Weerasuriya, T. 2021. *Blockchain: The next stage of digital procurement in construction.* Academia letters. Academia Inc.

Piotrowicz, W., & Irani, Z. 2010. Analysing B2B electronic procurement benefits: information system perspective. Journal of Enterprise Information Management, 23(4): 559-579.

Pomazalova, N. 2013. *Public sector transformation process and internet public procurement: Decision support system*. Hershey (PA): IGI Global Publisher.

Praveen, N. & Khaliq, M. 2018. A General Study for Role of the Quality in the E-Procurement Process. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3(1), 102-106.

Presutti, W.D. 2003. *Supply management and e-procurement: creating value added in the supply chain*. Industrial Marketing Management, 32 (3), 219–226.

Purpura, P.P. 2013. *Security and loss prevention: An introduction*. (6th edition). Amsterdam: Elsevier.

Puttick, G., Esch, S. & Kana, S. 2007. *The principles and practice of auditing*. (9th edition). Cape Town: Juta.

Raga, K. 2008. Public sector procurement: South African ethics and legislative aspects. *African Journal of Public Affairs*, 2(1): 114-115.

Raghavan, S. 2012. Digital forensic research: Current state of the art. *CSI Transactions on ICT*. 1(1):91–114

Ramadhani, S., Saragih, Y.M., Rahim, R. & Siahaan, A.P.U. 2017. Post-genesis digital forensics investigation. *International Journal of Scientific Research in Science and Technology*, 3(6): 164-166.

Reedy, P. 2021. *Strategic leadership in digital evidence*. Washington: Elsevier Inc.

Reddy, K. P., Sureka, A., Chakravarthy, S. & Bhalla, S. 2017. *Big data analytics*. 5th international conference, BDA 2017. Hyderabad, India: Springer.

Rendon, J. M. 2018. Auditability in Procurement: An Analysis of DoD Contracting Professionals' Procurement Fraud Knowledge. *Acquisition Research: Creating Synergy for Informed Change*, (1), 588-605.

Republic of South Africa. 1996. Constitution of the Republic of South Africa Act, 108 of 1996. Pretoria: Government Printer.

Ritchie, J., Lewis, J., Nichols, C. M & Ormston, R. 2014. *Qualitative research practice*. (2nd edition). Thousand Oaks (CA): Sage.

Rubin, H. J. & Rubin, I. S. 2012. *Qualitative Interviewing: The art of hearing data*. Thousand Oaks (CA): Sage

Salkute, V. R. & Manager, Z. 2013. Exploratory Study of E-Procurement Adoption in Indian and Chinese Companies: Case Study with Innovation Approach. *American Journal of Economics and Business Administration*, 5(3): 107-115.

Sammons, J. 2012. *The basics of digital forensics: The prime for getting started in digital forensics.* Amsterdam: Elsevier.

Sanders, N.R. 2005. IT Alignment in Supply Chain Relationships: A Study of Supplier Benefit. *The Journal of Supply Chain Management*, 41(2): 4-13.

Schwartz, R. 2010. *Procurement fraud: Investigative techniques to help mitigate risk*. Swiss: Deloitte Development.

Selomo, M. R. & Govender, K. K. 2016. Procurement and Supply Chain Management in Government Institutions: A Case Study of Select Departments in the Limpopo Province, South Africa. *Dutch Journal of Finance and Management*, 1(1), 37.

Shakya, R. K. 2017. *Digital governance and e-government principles applied to public procurement*. Hershey (PA): IGI Global Publisher.

Shinder, D.L. & Tittel, E. 2002. *Scene of the cybercrime: computer forensic handbook*. Oxford: Syngress.

Shirley, Z. 2017. *Biggest challenges in data recovery today.* Available at: https://www.datanumen.com/blogs/6-biggest-challenges-data-recovery-today/ (accessed 21 March 2021).

Sithole, R. A. 2017. *Implementation of e-Procurement by the Gauteng Department of Infrastructure Development and its impact on the development of small and medium construction firms*. Johannesburg: University of Witwatersrand.

Smith, S. 2020. *Special Investigating Unit probes Covid-19 tenderpreneurs*. Available at: https://mg.co.za/coronavirus-essentials/2020-08-08-special-investigating-unit-probes-covid-19-tenderpreneurs/ (accessed 21 March 2021).

Solomon, M. G., Barrett, D. & Broom, N. 2015. *Computer forensics JumpStart*. Hoboken (NJ): John Wiley & Sons.

Song, Y. M & Kwak, K. S. 2015. *Electronics, information technology and intellectualization.* Paper presented to the International Conference of Extractive Industries Transparency Initiative. Shenzhen, China, 16-17 August.

Sorell, M. 2009. Forensic in telecommunications information and multimedia. (Pp. 19-21). In M. Sorell. (Eds). *Second International Conference, e-Forensic*. Adelaide: Springer.

Special Investigating Unit. 2010. *Training manual on procurement fraud*. East London: SIU.

Spollen, A. L. 1997. *Corporate Fraud: The danger from within*. Dublin: Oak Tree Press.

Srivastava, S., Goyal, M. & Mathur, N. 2021. *Essential of E-commerce*. SBPD publications.

Steel, C. 2006. *Windows forensics*. Indianapolis (IN): Wiley.

Subramani, M. 2004. How do suppliers benefit from information technology use in supply chain relationships? *MIS Quarterly*, 28(1), 45-73.

Subramani, M. & Shaw, L. 2004. The effects of process characteristics on the value of B2B E-procurement. *Information Technology and Management* 5(1):161-180.

Suresh, L. P. & Panigrahi, B.K. 2015. *Proceedings of the international conference on soft computing systems.* Volume 2. India: Springer.

Syambas, N. R. & El Farisi, N. 2014. Two-Step Injection method for collecting digital evidence in digital forensics. *Journal of ICT Research and Application,* 8(2): 141-156.

Tai, Y., Ho, C., & Wu, W. 2010. The performance of implementing Web-based e-Procurement systems. *International Journal of Production Research*, 48(18): 5397-5414.

Tereikovskyi, I., Mussiraliyeva, S., Kosyuk, Y., Bolatbek, M. & Tereikovska, L. 2018. An Experimental Investigation of Infrasound Influence Hard Drives of a Computer System. *International Journal of Civil Engineering and Technology*, 9(6), 1558–1566

Thai, K. V. 2019. *International handbook of public procurement*. Boca Raton (FL): CRC Press.

Tipton, H. F. & Nozaki, M. K. 2006. *Information security management handbook*. (5th edition). Boca Raton (FL): CRC Press.

Tipton, H. F. & Nozaki, M.K. 2012. *Information security management handbook*. (Volume 6). Boca Raton (FL): CRC Press.

Umar, R., Raidi, I. & Muthohirin, B.F. 2019. Live forensics of tools on android devices for email forensics. *TELKOMNIKA*, 17(4): 1803-1809.

University of South Africa. 2016. *Policy on Research Ethics*. Florida: University of South Africa.

University of South Africa. 2020. UNISA COVID-19 position statement on research ethics. Available at: https://www.unisa.ac.za/static/corporate_web/Content/Colleges/CAES/Research/docs/UNISA_COVID-19_POSITION_STATEMENT_ON_RESEARCH_ETHICS.pdf (accessed 14 July 2022).

Vacca, J. R. 2009. *Computer and information security handbook*. Burlington (MA): Elservier.

Vacca, J. R. 2002. *Computer forensics: Computer crime scene investigation*. Hingham (MA): Charles River Media.

Vacca, J. R. 2011. *Computer forensics: computer crime scene investigation*. Boston (MA): Charles River Media.

Vaidya, K., Sajeev A. S. M. & Callender, G. 2006. Critical factors that influence e-Procurement implementation success in the public sector. *Journal of public procurement*, 6(1), 70-99.

Vandermeer, Y., Le-Khac, N., Kechadi, T. & Carthy, J. 2019. *Electronic Evidence Discovery, Identification and Preservation: Role of the First Responder and related capacity building challenges. Available at: https://researchrepository.ucd.ie/bitstream/10197/11697/1/insight_publication.pdf* (accessed 21 March 2021).

Van der Waldt, G. 2007. *Municipal management: Serving the people*. Cape Town: Juta.

Van Greunen, D., Herselman, M. E., & Van Niekerk, J. 2010. Implementation of regulation-based e-Procurement in the Eastern Cape provincial administration. *African Journal of Business Management*, 4(17): 3655-3665.

Van Rooyen, H. J. N. 2004. *The A-Z of investigation: A practical guide for private and corporate investigators*. Pretoria: Crime Solve.

Varma, T. N. & Khan, D. A. 2017. SAP System as Vendor Fraud Detector. *Journal of Supply Chain Management Systems*, 6(2), 1.

Velmurugan, V. S. 2016. A study of use of e-resources by the students of engineering colleges in virudhunagar district, Tamilnadu, India. *Journal of Political Affairs and Public Administration,* 1(4), 1-14.

Vickery, S. K., Jayaram, J., Droge, C., & Calantone, R. 2003. The effects of an integrative supply chain strategy on customer services and financial performance: an analysis of direct versus indirect relationships*. Journal of operations management*, 21(2), 523-539.

Vickery, S. K., Droge, C., Seita, P., & Sambamurthy, V. 2010. Supply chain information technologies and organisational initiatives: complementary versus independent effects on agility and firm performance. *International Journal of Production Research*, 48(23), 7025-7042.

Wahyudi, E., Riadi, I. & Prayudi, Y. 2018. Virtual Machine Forensic Analysis and Recovery Method for Recovery and Analysis Digital Evidence*. International Journal of Computer Science and Information Security*, 16(2): 1-2.

Walker, D. H. T., & Rowlinson, S. 2008. *Procurement system: A cross-industry project management perspective*. New York: Taylor & Francis.

Wangui, K. M. 2013. *The effect of e-Procurement on supply chain management at teachers' service commission*. Nairobi: University of Nairobi School of Business.

Watson, D. & Jones, A. 2013. *Digital forensic processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements.* Amsterdam: Elsevier.

Webster, S., Lewis, J. & Brown, A. 2014. *Ethical considerations in qualitative research*. In Ritchie, J., Lewis, J., Nichols, C.M. & Ormston, R. (eds.) 2014. *Qualitative research practice: A guide for social science students & researchers*. 2nd edition. Thousand Oaks, Califonia: Sage.

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

Wells, V. D. 2011. *Principles of fraud examination*. New Jersey: John Wiley & Sons.

Wentz, E. (2017). How to design and present a successful dissertation proposal. California: SAGE.

Wicaksono, A. P., Urumsah, D. & Asmui, F. 2017. *The implementation of e-Procurement system: Indonesia evidence*. *SHS Web of Conferences*, 34: 3 – 9.

Wiles, J. & Reyes, A. 2007. *The best damn cybercrime and digital forensics*. Burlington (MA): Syngress Publishing.

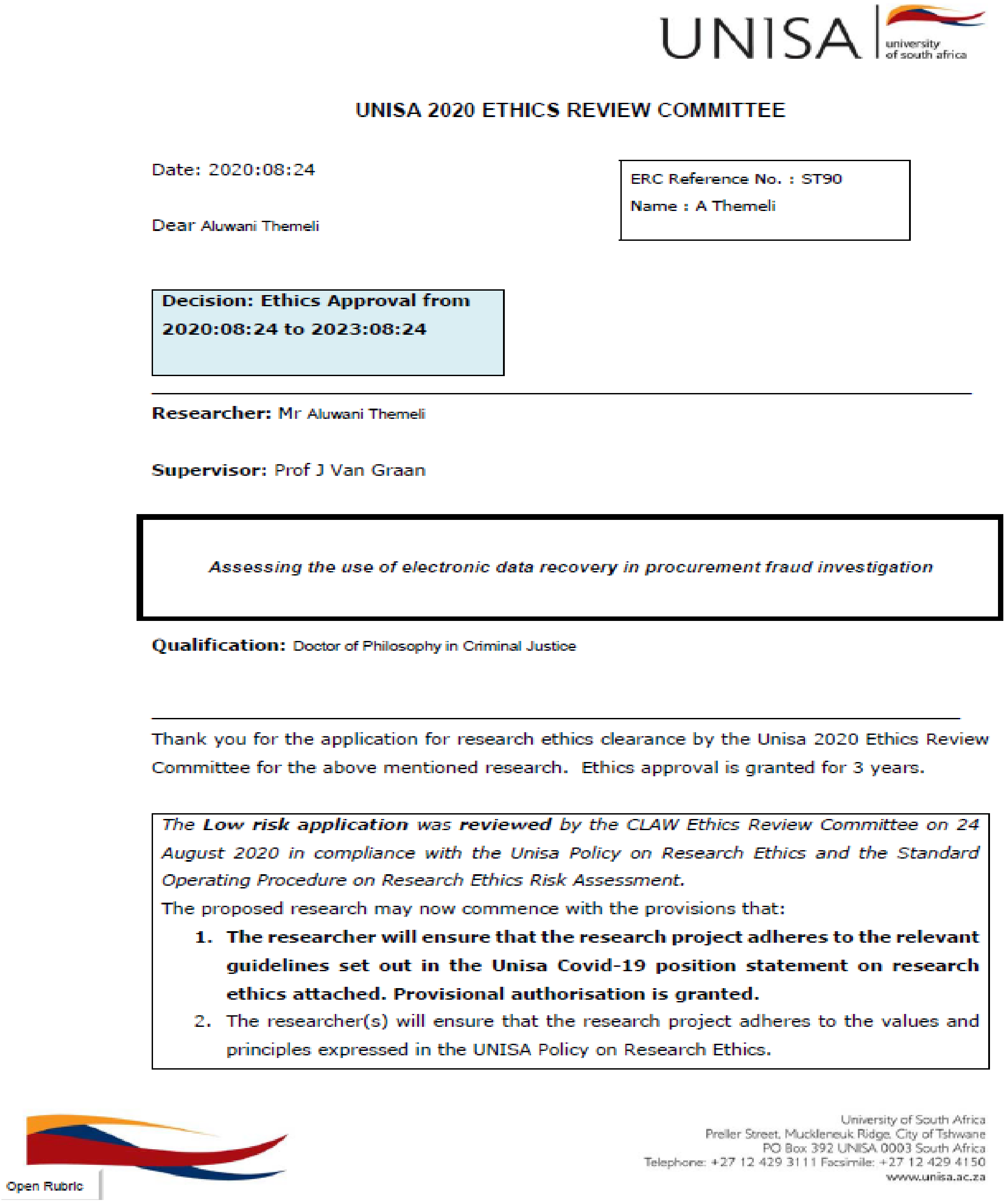
Woods, G. & Mantzaris, E. 2012. *Anti-Corruption Reader*. Stellenbosch: Anti-Corruption Centre for Education and Research of the University of Stellenbosch, School of Public Leadership, University of Stellenbosch.

Yavuzcan, H. G., Bulbul, H. I. & Ozel, M. 2013. *Crime Scene Digital Evidence Management Workflow Model.* 1st International Symposium on Digital Forensics and Security (ISDFS'13). Elazığ: Turkey, 20 – 21 May.

Yin, R. K. 2003. *Case study research: Designs and methods. Applied Social Method Series.* (2nd edition). Thousand Oaks (CA): Sage.

Zahra, F., Chariri, A., Rohman, A. & Karim, F. 2017. Does e-Procurement solve Indonesia local government budgetary slack through IT adaptive culture? *International Journal of Civil Engineering and Technology*, 8(8): 1001–1010.

ANNEXURE A: ETHICS APPROVAL FROM THE COLLEGE OF LAW, UNISA RESEARCH ETHICS REVIEW COMMITTEE



UNISA university of south africa

UNISA 2020 ETHICS REVIEW COMMITTEE

Date: 2020:08:24

Dear Aluwani Themeli

ERC Reference No. : ST90
Name : A Themeli

Decision: Ethics Approval from 2020:08:24 to 2023:08:24

Researcher: Mr Aluwani Themeli

Supervisor: Prof J Van Graan

Assessing the use of electronic data recovery in procurement fraud investigation

Qualification: Doctor of Philosophy in Criminal Justice

Thank you for the application for research ethics clearance by the Unisa 2020 Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

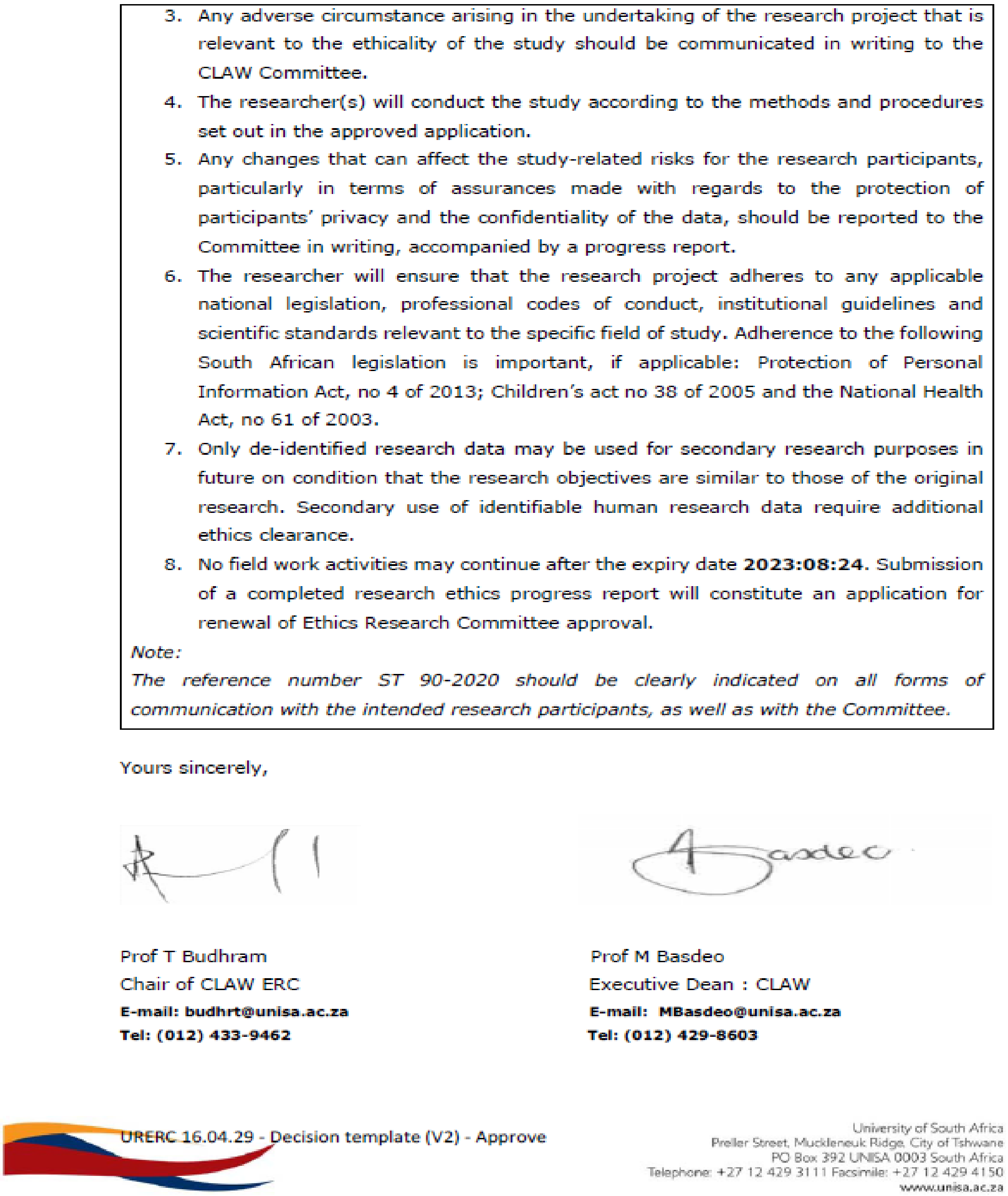
*The **Low risk application** was **reviewed** by the CLAW Ethics Review Committee on 24 August 2020 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.*

The proposed research may now commence with the provisions that:

1. **The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa Covid-19 position statement on research ethics attached. Provisional authorisation is granted.**
2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.

Open Rubric

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za



3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CLAW Committee.
4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data require additional ethics clearance.
8. No field work activities may continue after the expiry date **2023:08:24**. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

The reference number ST 90-2020 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely,

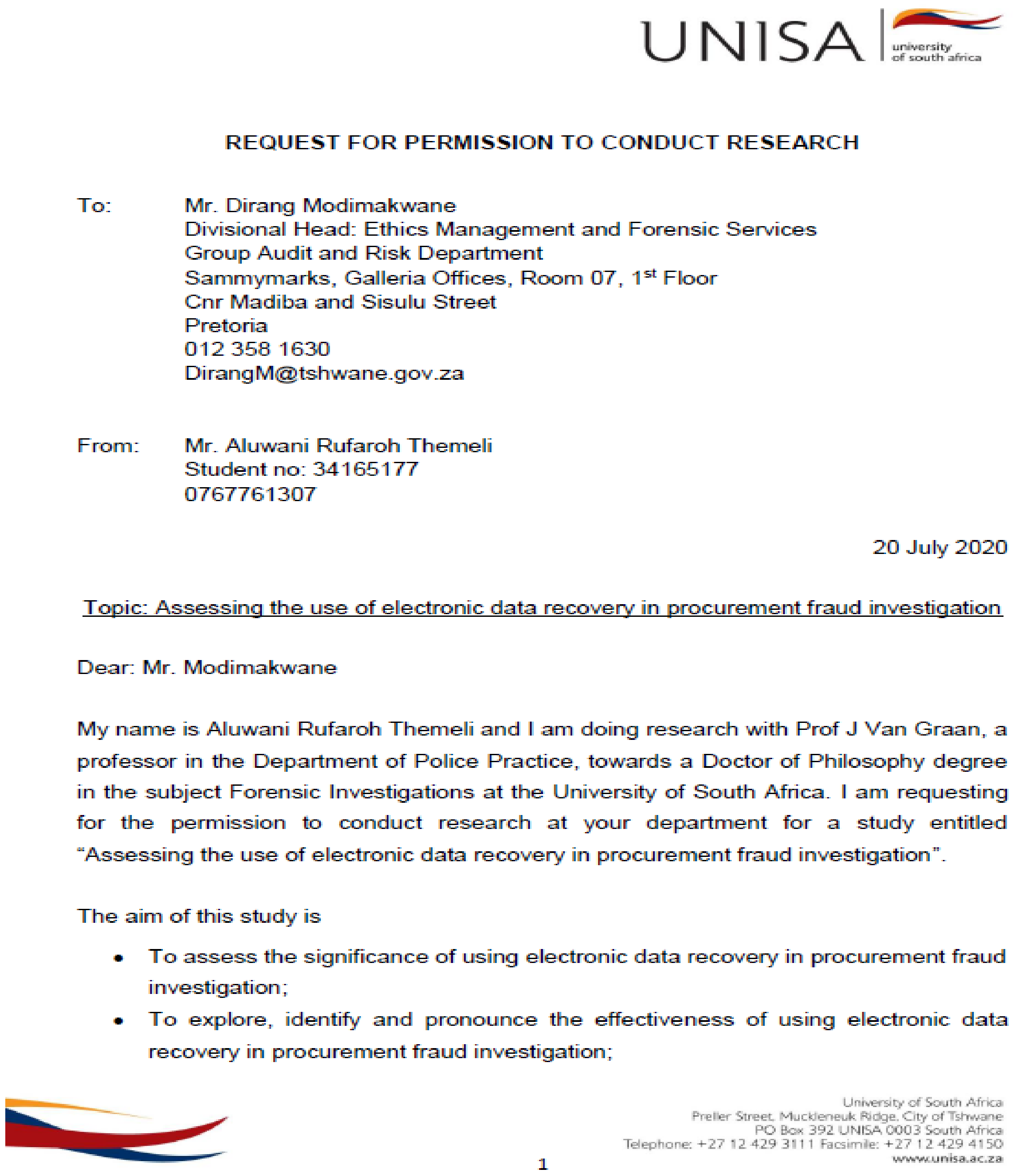
Prof T Budhram
Chair of CLAW ERC
E-mail: budhrt@unisa.ac.za
Tel: (012) 433-9462

Prof M Basdeo
Executive Dean : CLAW
E-mail: MBasdeo@unisa.ac.za
Tel: (012) 429-8603

URERC 16.04.29 - Decision template (V2) - Approve

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE B: APPLICATION TO CONDUCT RESEARCH IN THE CITY OF TSHWANE



UNISA university of south africa

REQUEST FOR PERMISSION TO CONDUCT RESEARCH

To:
Mr. Dirang Modimakwane
Divisional Head: Ethics Management and Forensic Services
Group Audit and Risk Department
Sammymarks, Galleria Offices, Room 07, 1st Floor
Cnr Madiba and Sisulu Street
Pretoria
012 358 1630
DirangM@tshwane.gov.za

From:
Mr. Aluwani Rufaroh Themeli
Student no: 34165177
0767761307

20 July 2020

<u>Topic: Assessing the use of electronic data recovery in procurement fraud investigation</u>

Dear: Mr. Modimakwane

My name is Aluwani Rufaroh Themeli and I am doing research with Prof J Van Graan, a professor in the Department of Police Practice, towards a Doctor of Philosophy degree in the subject Forensic Investigations at the University of South Africa. I am requesting for the permission to conduct research at your department for a study entitled "Assessing the use of electronic data recovery in procurement fraud investigation".

The aim of this study is

- To assess the significance of using electronic data recovery in procurement fraud investigation;
- To explore, identify and pronounce the effectiveness of using electronic data recovery in procurement fraud investigation;

- To highlight the appropriate processes of identification, acquisition, examination, and handling of electronic data;
- To examine and explore the best international practice regarding the electronic data recovery in procurement fraud investigation that the CoT Forensic Services can adopt to improve their investigative capacity;
- To make recommendations regarding the electronic data recovery in procurement fraud investigation based on the findings of this research, which could be used to enhance the understanding of electronic data recovery in procurement fraud by CoT Forensic Auditors.

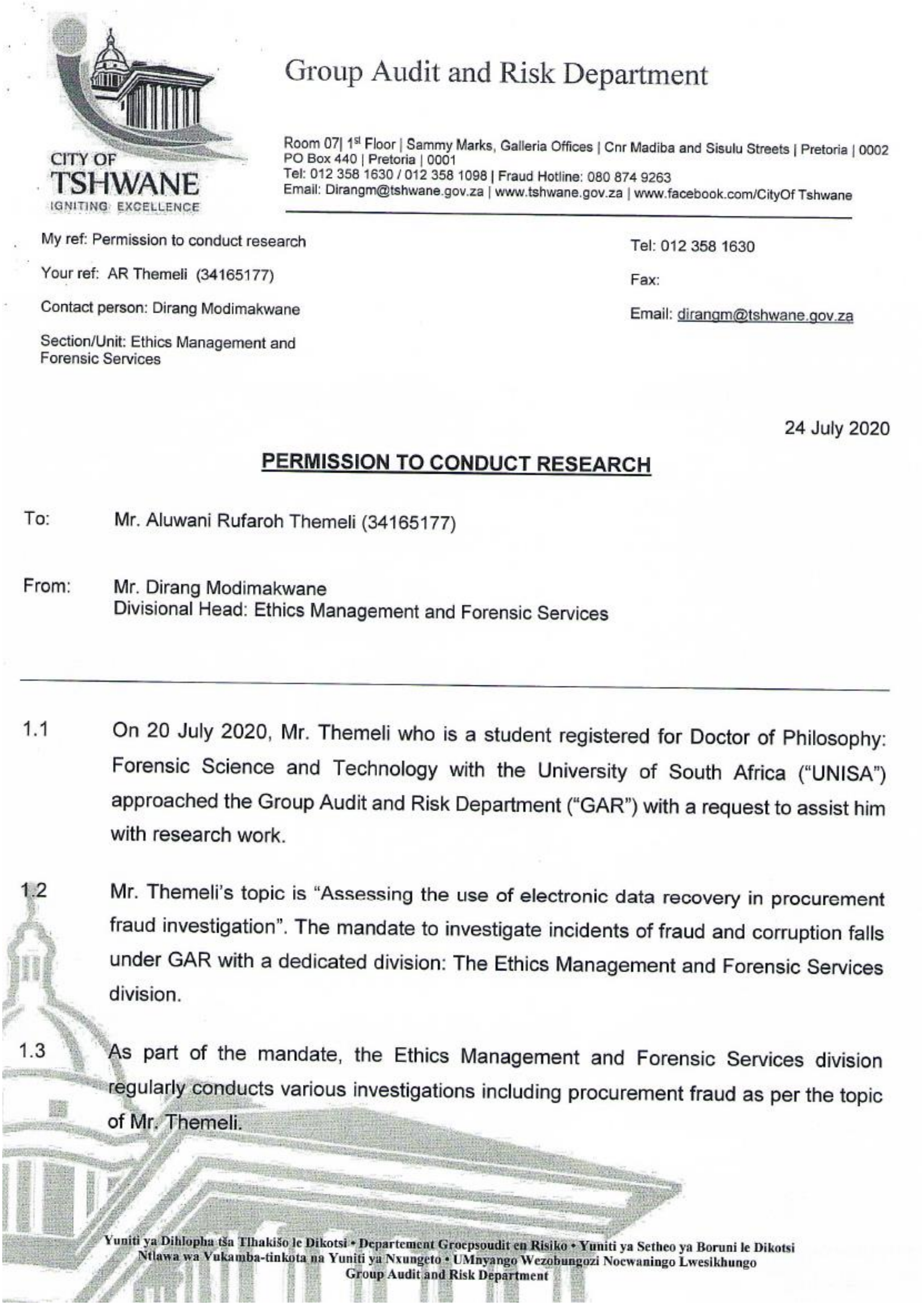
Your department has been selected because of the relevance in its to investigate procurement fraud and the understanding that CoT Forensic Auditors are required to handle electronic data during investigation which is the main focus of the study.

I will conduct one on one interviews with the Forensic Auditors who are volunteering and willing to participate. Their names will not be recorded anywhere and that no one, apart from the researcher and identified members of the research team, will know about their involvement in this research. Their answers may be reviewed by people responsible for making sure that research is done properly, including the transcriber, external coder, and members of the UNISA Research Ethics Review Committee. These anonymous data may be used for other purposes, such as a research report, journal articles and/or conference proceedings. However, the privacy of the participants will be protected in any publication of the information.

The benefits of this study is to:

- Improve CoT investigators' knowledge and competence regarding the electronic data recovery in procurement fraud investigation;
- Enhance CoT forensic investigator's capacity through the facilitation of an improved electronic data recovery applications and modern tools;
- Contribute to the existing body of knowledge as an academic source for students and prospective researchers;
- Contribute to the broader South African community and computer forensic industry (with specific reference to those forensic investigators responsible for

ANNEXURE C: PERMISSION GRANTED TO CONDUCT RESEARCH



CITY OF
TSHWANE
IGNITING EXCELLENCE

Group Audit and Risk Department

Room 07| 1st Floor | Sammy Marks, Galleria Offices | Cnr Madiba and Sisulu Streets | Pretoria | 0002
PO Box 440 | Pretoria | 0001
Tel: 012 358 1630 / 012 358 1098 | Fraud Hotline: 080 874 9263
Email: Dirangm@tshwane.gov.za | www.tshwane.gov.za | www.facebook.com/CityOf Tshwane

My ref: Permission to conduct research

Your ref: AR Themeli (34165177)

Contact person: Dirang Modimakwane

Section/Unit: Ethics Management and Forensic Services

Tel: 012 358 1630

Fax:

Email: dirangm@tshwane.gov.za

24 July 2020

PERMISSION TO CONDUCT RESEARCH

To: Mr. Aluwani Rufaroh Themeli (34165177)

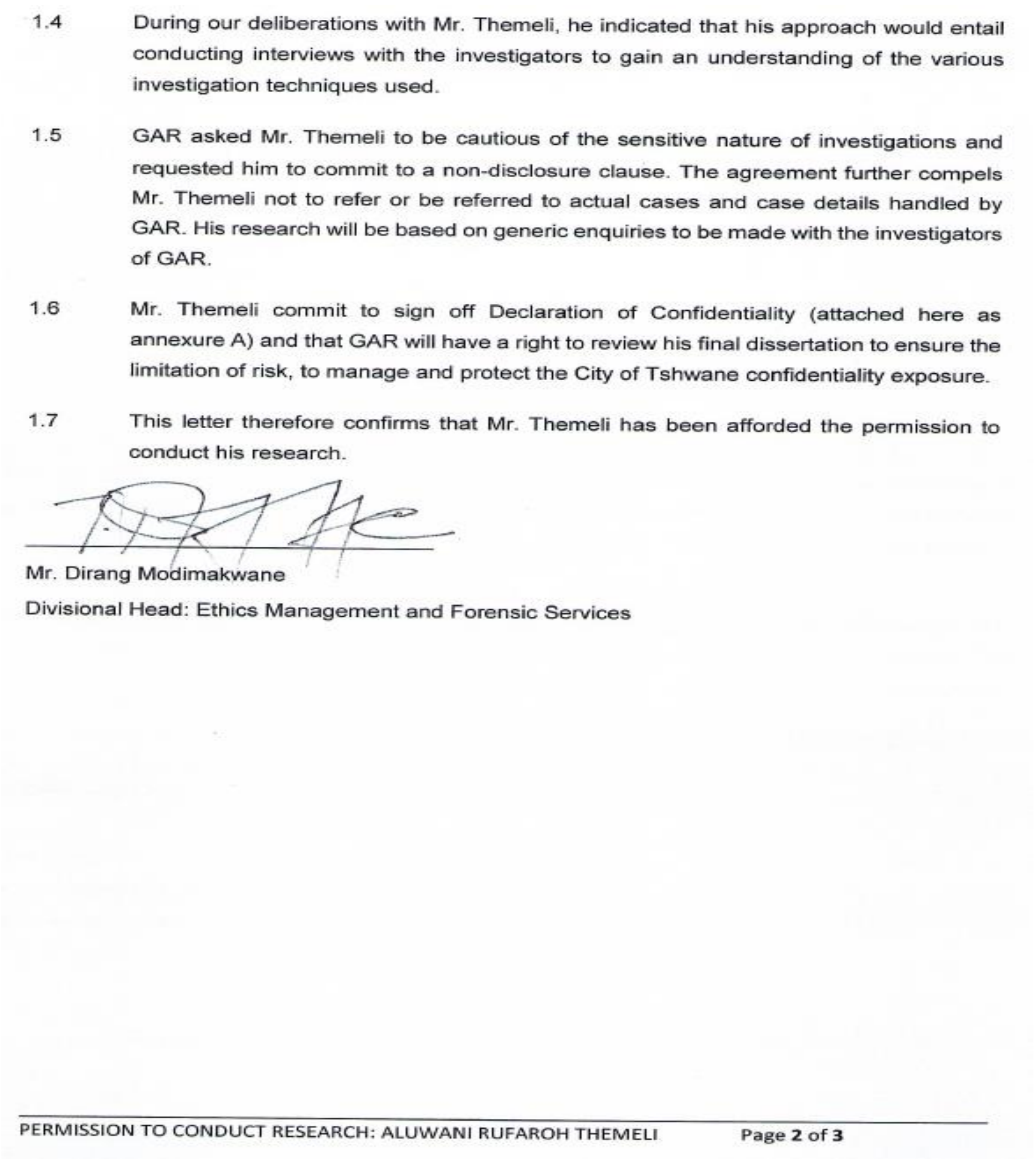
From: Mr. Dirang Modimakwane
Divisional Head: Ethics Management and Forensic Services

1.1 On 20 July 2020, Mr. Themeli who is a student registered for Doctor of Philosophy: Forensic Science and Technology with the University of South Africa ("UNISA") approached the Group Audit and Risk Department ("GAR") with a request to assist him with research work.

1.2 Mr. Themeli's topic is "Assessing the use of electronic data recovery in procurement fraud investigation". The mandate to investigate incidents of fraud and corruption falls under GAR with a dedicated division: The Ethics Management and Forensic Services division.

1.3 As part of the mandate, the Ethics Management and Forensic Services division regularly conducts various investigations including procurement fraud as per the topic of Mr. Themeli.

Yuniti ya Dihlopha tša Tlhakišo le Dikotsi • Departement Groepsoudit en Risiko • Yuniti ya Setheo ya Boruni le Dikotsi
Ntlawa wa Vukamba-tinkota na Yuniti ya Nxungeto • UMnyango Wezobungozi Nocwaningo Lwesikhungo
Group Audit and Risk Department



1.4 During our deliberations with Mr. Themeli, he indicated that his approach would entail conducting interviews with the investigators to gain an understanding of the various investigation techniques used.

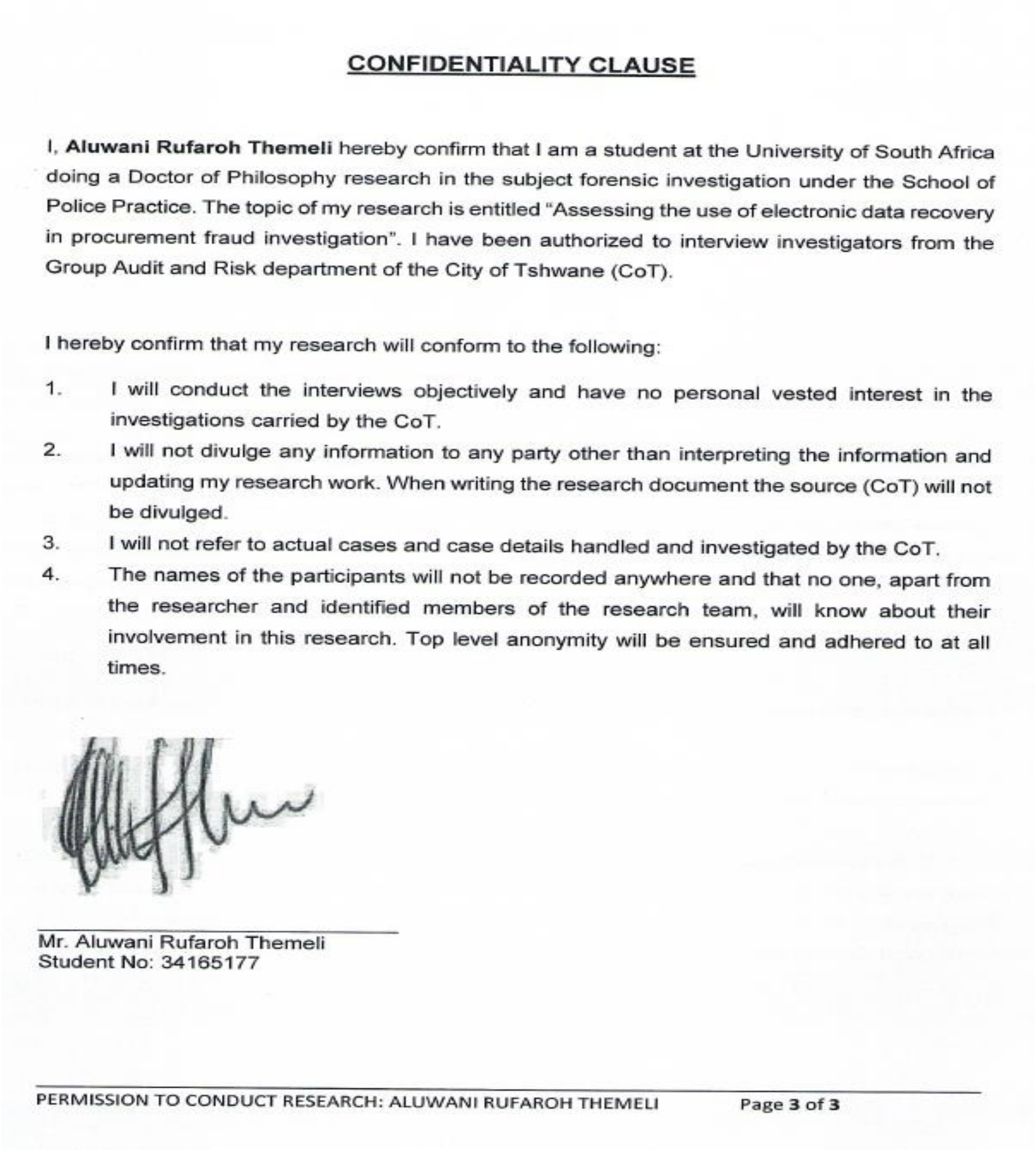
1.5 GAR asked Mr. Themeli to be cautious of the sensitive nature of investigations and requested him to commit to a non-disclosure clause. The agreement further compels Mr. Themeli not to refer or be referred to actual cases and case details handled by GAR. His research will be based on generic enquiries to be made with the investigators of GAR.

1.6 Mr. Themeli commit to sign off Declaration of Confidentiality (attached here as annexure A) and that GAR will have a right to review his final dissertation to ensure the limitation of risk, to manage and protect the City of Tshwane confidentiality exposure.

1.7 This letter therefore confirms that Mr. Themeli has been afforded the permission to conduct his research.

Mr. Dirang Modimakwane

Divisional Head: Ethics Management and Forensic Services



CONFIDENTIALITY CLAUSE

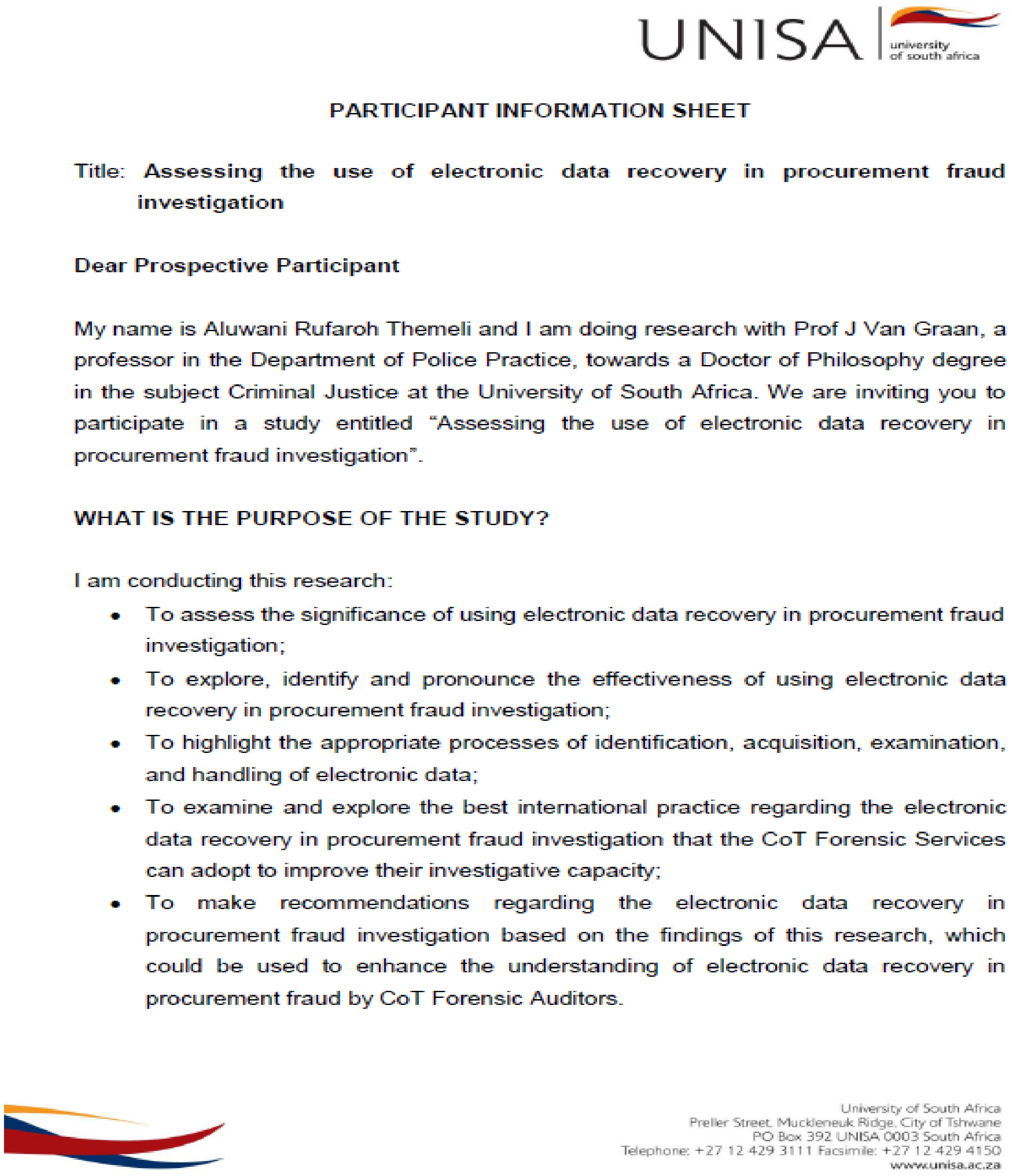
I, **Aluwani Rufaroh Themeli** hereby confirm that I am a student at the University of South Africa doing a Doctor of Philosophy research in the subject forensic investigation under the School of Police Practice. The topic of my research is entitled "Assessing the use of electronic data recovery in procurement fraud investigation". I have been authorized to interview investigators from the Group Audit and Risk department of the City of Tshwane (CoT).

I hereby confirm that my research will conform to the following:

1. I will conduct the interviews objectively and have no personal vested interest in the investigations carried by the CoT.
2. I will not divulge any information to any party other than interpreting the information and updating my research work. When writing the research document the source (CoT) will not be divulged.
3. I will not refer to actual cases and case details handled and investigated by the CoT.
4. The names of the participants will not be recorded anywhere and that no one, apart from the researcher and identified members of the research team, will know about their involvement in this research. Top level anonymity will be ensured and adhered to at all times.

Mr. Aluwani Rufaroh Themeli
Student No: 34165177

ANNEXURE D: INFORMED CONSENT FORM



UNISA university of south africa

PARTICIPANT INFORMATION SHEET

Title: **Assessing the use of electronic data recovery in procurement fraud investigation**

Dear Prospective Participant

My name is Aluwani Rufaroh Themeli and I am doing research with Prof J Van Graan, a professor in the Department of Police Practice, towards a Doctor of Philosophy degree in the subject Criminal Justice at the University of South Africa. We are inviting you to participate in a study entitled "Assessing the use of electronic data recovery in procurement fraud investigation".

WHAT IS THE PURPOSE OF THE STUDY?

I am conducting this research:

- To assess the significance of using electronic data recovery in procurement fraud investigation;
- To explore, identify and pronounce the effectiveness of using electronic data recovery in procurement fraud investigation;
- To highlight the appropriate processes of identification, acquisition, examination, and handling of electronic data;
- To examine and explore the best international practice regarding the electronic data recovery in procurement fraud investigation that the CoT Forensic Services can adopt to improve their investigative capacity;
- To make recommendations regarding the electronic data recovery in procurement fraud investigation based on the findings of this research, which could be used to enhance the understanding of electronic data recovery in procurement fraud by CoT Forensic Auditors.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

WHY AM I BEING INVITED TO PARTICIPATE?

You were referred to me by your Divisional Head and you were chosen to participate in this study since you have the necessary knowledge and experience of the investigation of procurement fraud and could thus provide insightful information. Approximately 40 participants will participate in this study.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves in-depth interviews. You will be expected to answer questions pertaining to recovery of electronic data during procurement fraud investigation. The expected duration of the interview will be more or less 45 minutes.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Your participation is voluntary and there is no penalty or loss of benefit for non-participation. Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

This study could have the following possible benefits:

- It will improve CoT investigators' knowledge and competence regarding the electronic data recovery in procurement fraud investigation;
- Enhance CoT forensic investigator's capacity through the facilitation of an improved electronic data recovery applications and modern tools;
- To contribute to the existing body of knowledge as an academic source for students and prospective researchers;
- To contribute to the broader South African community and computer forensic industry (with specific reference to those forensic investigators responsible for

procurement fraud) since procurement fraud progressively remains to increase and negatively impact the South African economy.

- The attained knowledge will be made available to students and faculty of the University of South Africa and the greater academic community, for use in curriculum development. It will also be available as a research source for students and researchers.
- The broader South African society will also benefit if procurement fraud can be undertaken professionally and timeously, thereby creating a higher conviction rate. The reduction of procurement fraud and the increased conviction of perpetrators will benefit the country's economy.

ARE THEIR ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

I do not foresee any potential level of inconvenience and/or discomfort to you as participant. Your anonymity will be ensured, thus, there will be no risk that others will identify your participation in this research. There are no risk of injury or harm attributable to participating in the study.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

Your name will not be recorded anywhere and that no one, apart from the researcher and identified members of the research team, will know about your involvement in this research. No one will be able to connect you to the answers you give. Your answers will be given a code number or a pseudonym and you will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings.

Your answers may be reviewed by people responsible for making sure that research is done properly, including the transcriber, external coder, and members of the Research Ethics Review Committee. Otherwise, records that identify you will be available only to people working on the study, unless you give permission for other people to see the

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the researcher for a period of five years in a locked cupboard/filing cabinet at the researcher's office for future research or academic purposes; electronic information will be stored on a password protected computer. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. Electronic copies will be permanently deleted from the hard drive of the computer through the use of a relevant software programme.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

You will receive no payment or any incentives for participating in this study.

HAS THE STUDY RECEIVED ETHICS APPROVAL

This study has received written approval from the Research Ethics Review Committee of the College of Law, Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

If you would like to be informed of the final research findings or require any further information or want to contact the researcher about any aspect of this study, please contact Mr Aluwani Rufaroh Themeli on 0767761307 or email at ataluwanit5@gmail.com.

Should you have concerns about the way in which the research has been conducted, you may contact Prof J Van Graan at vgraajg@unisa.ac.za or contact the research ethics chairperson of the College of Law Research Ethics Sub-Committee, Prof T Budhram at budhrt@unisa.ac.za if you have any ethical concerns.

Thank you for taking time to read this information sheet and for participating in this study.

Thank you.
Mr Aluwani Rufaroh Themeli

ANNEXURE E: IN-DEPTH INTERVIEW SCHEDULE

ASSESSING THE USE OF ELECTRONIC DATA RECOVERY IN PROCUREMENT FRAUD INVESTIGATION

1. According to you, what are the benefits of e-Procurement in terms of fraud risk management at the CoT?

2. In your opinion, what are the challenges of e-Procurement in terms of fraud risk management at the CoT?

3. Are you familiar with the different types of e-Procurement models/solutions?

   - If affirmative, briefly name these models/solutions.
   - If not, please motivate your answer?
   - Does the CoT use one or more of these models/solutions? Which module/s or solution/s does the CoT use?

4. Are you familiar with the legislative frameworks that governs procurement practices in South Africa?

   - If affirmative, briefly name these legislative frameworks?
   - If not, please motivate your answer?

AN OVERVIEW OF ELECTRONIC DATA RECOVERY

5. Have you received any formal training in electronic data recovery to investigate e-Procurement fraud at the CoT?
   - If affirmative, mention the name(s) of the training intervention(s)?
   - Was the training intervention/s efficient?
   - If not, how could your ability as an investigator be improved to investigate e-Procurement fraud by using electronic data recovery?

6. In your opinion, do you regard the application of electronic data recovery in the investigation of e-Procurement fraud effective or not?

   - Please motivate your answer?

7. From your experience, does the CoT forensic investigators have sufficient capacity to recover electronic data during the investigation of e-Procurement fraud?

   - If yes, please elaborate your answer?
   - If no, how does the CoT deals with electronic data recovery?

8. According to you, is there any significance of utilising electronic data recovery applications in e-Procurement fraud investigation within the CoT?

   - Please motivate your answer.

9. In your opinion, do CoT investigators experience challenges to recover electronic data during the investigation of e-Procurement fraud at the CoT?

   - Please motivate your answer?

10. Are you familiar with the most prominent Computer Assisted Audit Techniques (CAATs) software applications?

    - Briefly name these CATTs applications?
    - Do you apply these CAATs during e-Procurement fraud investigations at the CoT?

11. Are you familiar with the most critical steps or phases of electronic data recovery?

- Please elaborate your answer?

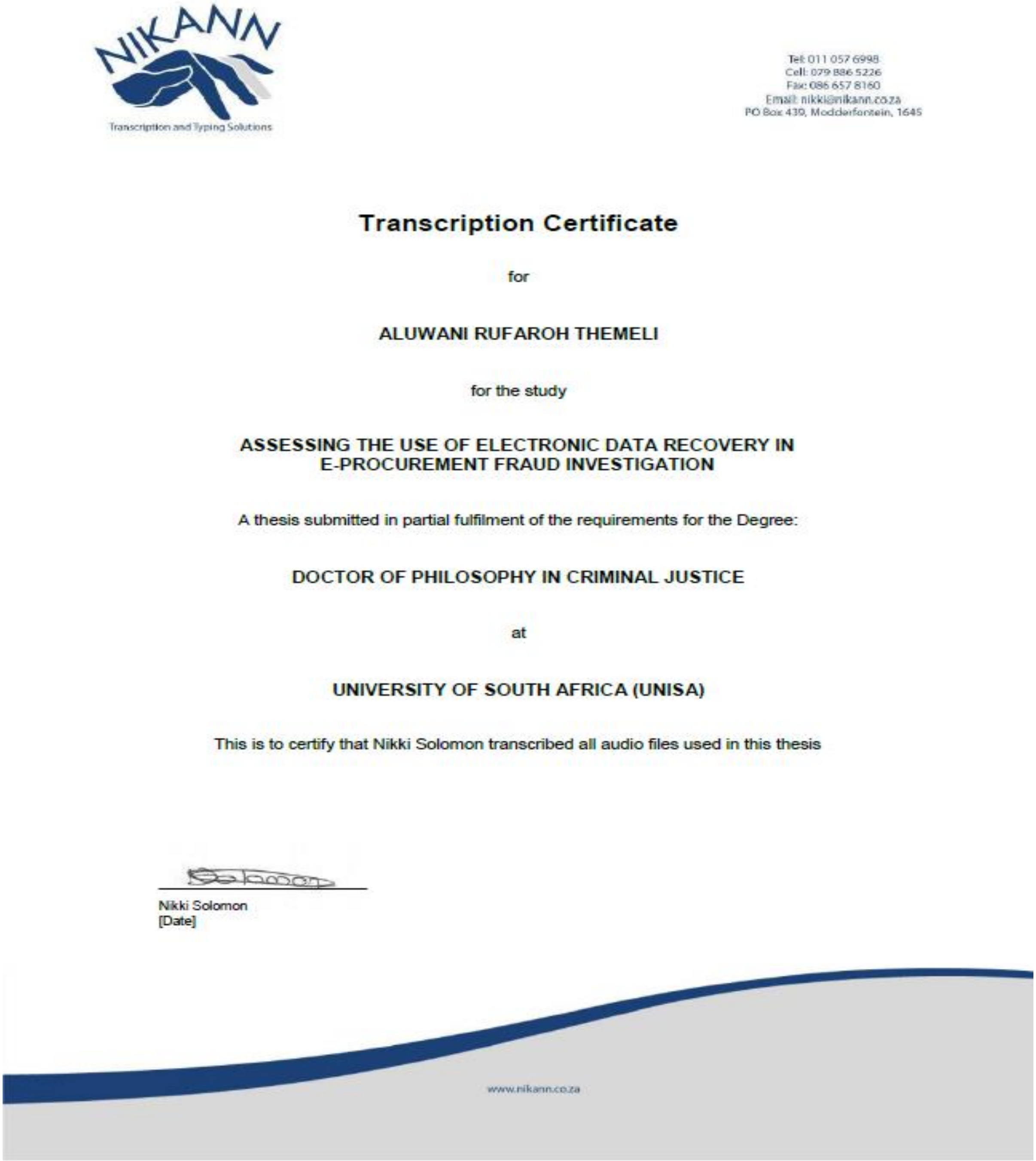
12. Are you familiar with the process of examining recovered electronic data?

    - Briefly explain the examination of recovered electronic data?
    - Do you apply this examination process during e-Procurement fraud investigations at the CoT?
    - Please elaborate your answer?

13. Do you experience any inhibiting factors that affect your ability to investigate e-Procurement fraud optimally at the CoT?

    - Please motivate your answer?

ANNEXURE F: TRANSCRIBER'S CERTIFICATE



NIKANN
Transcription and Typing Solutions

Tel: 011 057 6998
Cell: 079 886 5226
Fax: 086 657 8160
Email: nikki@nikann.co.za
PO Box 439, Modderfontein, 1645

Transcription Certificate

for

ALUWANI RUFAROH THEMELI

for the study

ASSESSING THE USE OF ELECTRONIC DATA RECOVERY IN E-PROCUREMENT FRAUD INVESTIGATION

A thesis submitted in partial fulfilment of the requirements for the Degree:

DOCTOR OF PHILOSOPHY IN CRIMINAL JUSTICE

at

UNIVERSITY OF SOUTH AFRICA (UNISA)

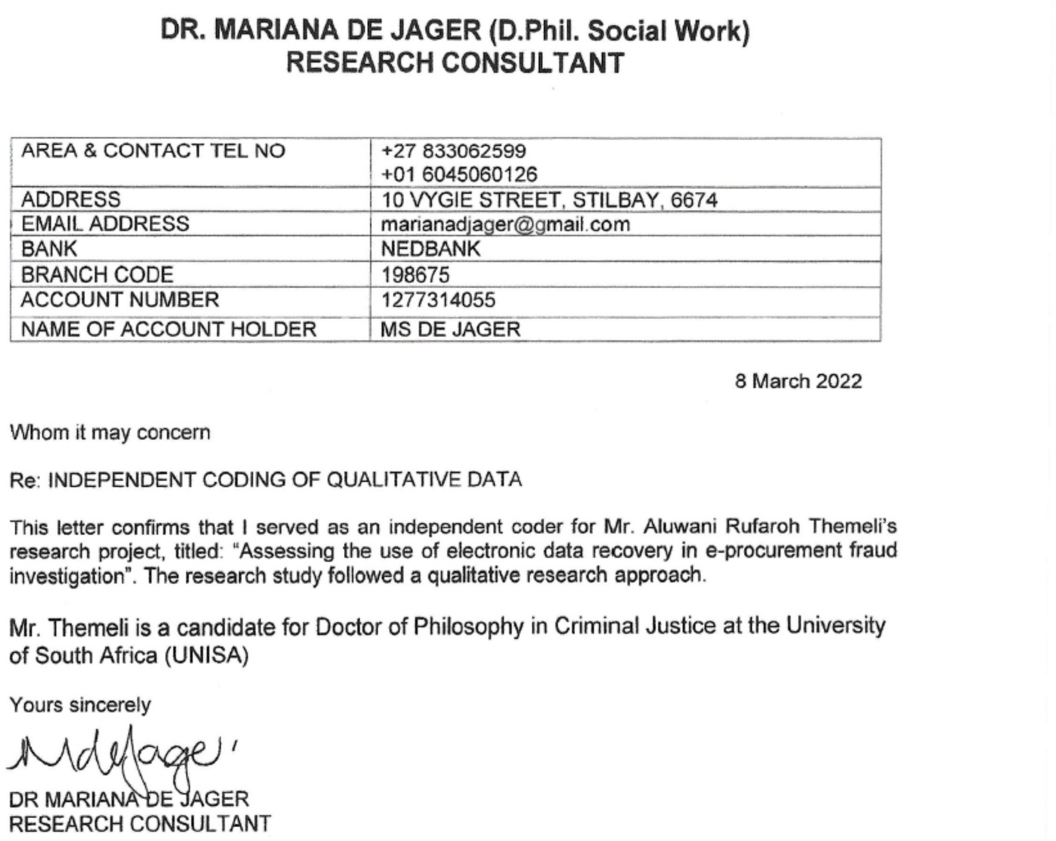
This is to certify that Nikki Solomon transcribed all audio files used in this thesis

Solomon

Nikki Solomon
[Date]

www.nikann.co.za

ANNEXURE G: INDEPENDENT CO-CODER CERTIFICATE FOR DATA ANALYSIS



DR. MARIANA DE JAGER (D.Phil. Social Work)
RESEARCH CONSULTANT

AREA & CONTACT TEL NO	+27 833062599 +01 6045060126
ADDRESS	10 VYGIE STREET, STILBAY, 6674
EMAIL ADDRESS	marianadjager@gmail.com
BANK	NEDBANK
BRANCH CODE	198675
ACCOUNT NUMBER	1277314055
NAME OF ACCOUNT HOLDER	MS DE JAGER

8 March 2022

Whom it may concern

Re: INDEPENDENT CODING OF QUALITATIVE DATA

This letter confirms that I served as an independent coder for Mr. Aluwani Rufaroh Themeli's research project, titled: "Assessing the use of electronic data recovery in e-procurement fraud investigation". The research study followed a qualitative research approach.

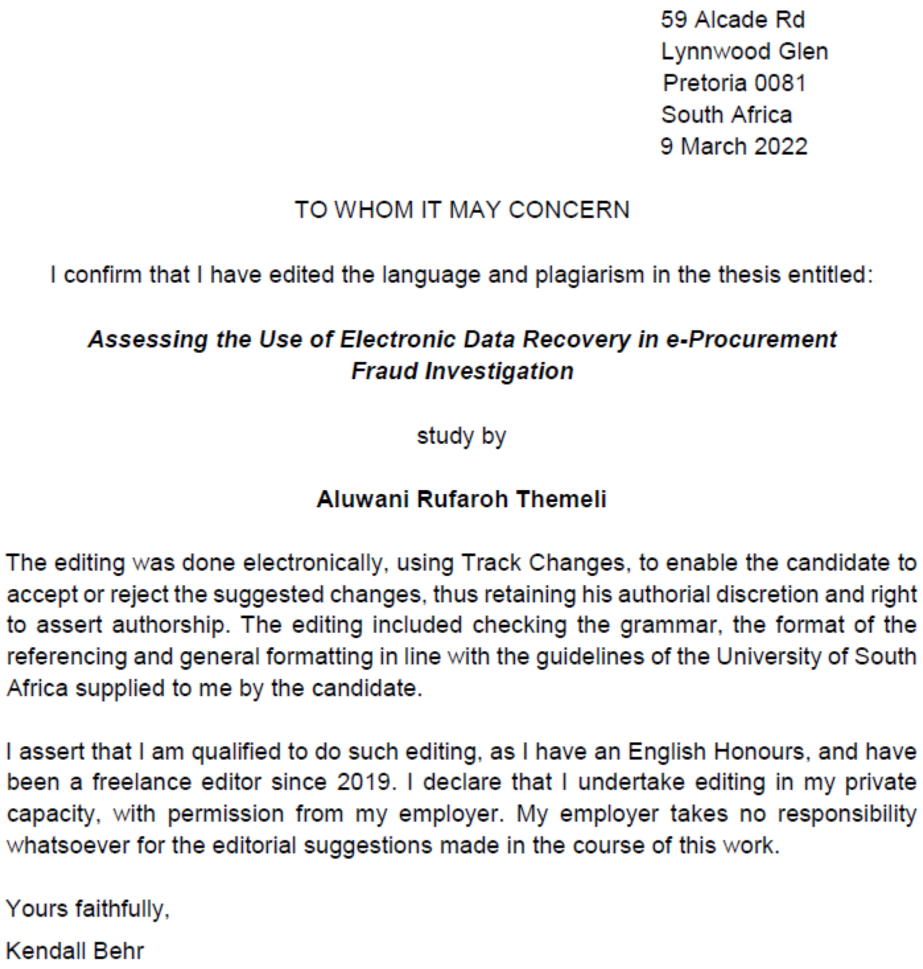
Mr. Themeli is a candidate for Doctor of Philosophy in Criminal Justice at the University of South Africa (UNISA)

Yours sincerely

Mdejager

DR MARIANA DE JAGER
RESEARCH CONSULTANT

ANNEXURE H: EDITOR'S STATEMENT



59 Alcade Rd
Lynnwood Glen
Pretoria 0081
South Africa
9 March 2022

TO WHOM IT MAY CONCERN

I confirm that I have edited the language and plagiarism in the thesis entitled:

Assessing the Use of Electronic Data Recovery in e-Procurement Fraud Investigation

study by

Aluwani Rufaroh Themeli

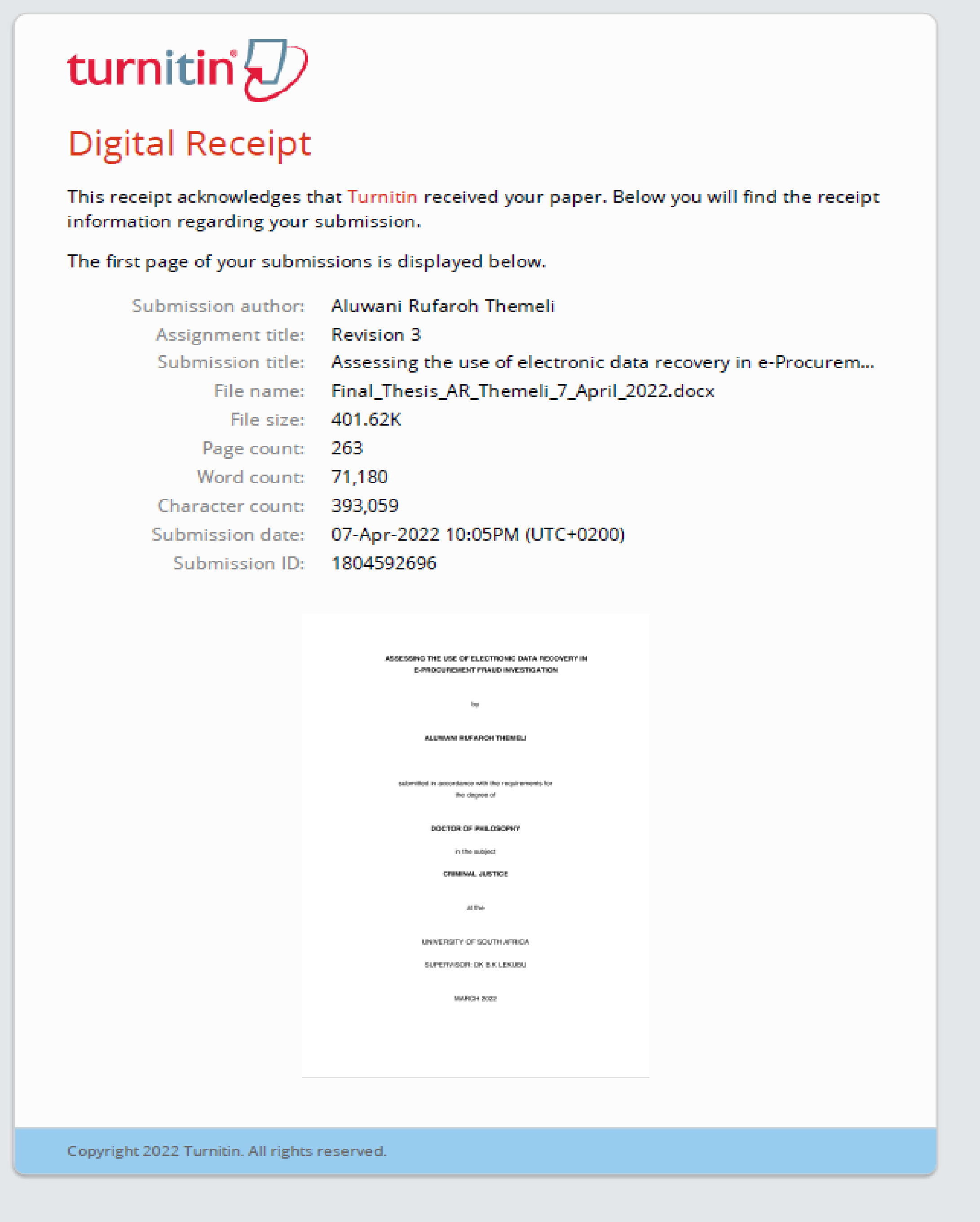
The editing was done electronically, using Track Changes, to enable the candidate to accept or reject the suggested changes, thus retaining his authorial discretion and right to assert authorship. The editing included checking the grammar, the format of the referencing and general formatting in line with the guidelines of the University of South Africa supplied to me by the candidate.

I assert that I am qualified to do such editing, as I have an English Honours, and have been a freelance editor since 2019. I declare that I undertake editing in my private capacity, with permission from my employer. My employer takes no responsibility whatsoever for the editorial suggestions made in the course of this work.

Yours faithfully,

Kendall Behr

ANNEXURE I: TURNITIN DIGITAL RECEIPT



Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Aluwani Rufaroh Themeli
Assignment title:	Revision 3
Submission title:	Assessing the use of electronic data recovery in e-Procurem...
File name:	Final_Thesis_AR_Themeli_7_April_2022.docx
File size:	401.62K
Page count:	263
Word count:	71,180
Character count:	393,059
Submission date:	07-Apr-2022 10:05PM (UTC+0200)
Submission ID:	1804592696

ASSESSING THE USE OF ELECTRONIC DATA RECOVERY IN
E-PROCUREMENT FRAUD INVESTIGATION

by

ALUWANI RUFAROH THEMELI

submitted in accordance with the requirements for
the degree of

DOCTOR OF PHILOSOPHY

in the subject

CRIMINAL JUSTICE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: DR B.K LEKUBU

MARCH 2022