



**UNIVERSITY OF NAIROBI**

**SCHOOL OF COMPUTING AND INFORMATICS**

**ICS 699: SYSTEMS PROJECT**

**Thomas kizito**

**P56/61643/2013**

*AN E-CORRUPTION CONTROL FRAMEWORK FOR THE KENYA PUBLIC SECTOR.*

**June 2015**

**SUPERVISOR**

**DR. CHRISTOPHER CHEPKEN**

## **DECLARATION**

This thesis is a presentation of my original research work. Wherever contributions of others are involved, every effort is made to indicate this clearly, with due reference to the literature, and acknowledgement of collaborative research and discussions. The work was done under the guidance of Dr Christopher Chepken, at the University of Nairobi, Kenya.

**Thomas Kizito Oduor**

In my capacity as supervisor of the candidate's thesis, I certify that the above statements are true to the best of my knowledge.

Date:

## Acknowledgements

I would like to thank my supervisor, Dr. Christopher Chepken, for the patient guidance, encouragement and advice he has provided throughout my time as his student. I have been extremely lucky to have a supervisor who cared so much about my work, and who responded to my questions and queries so promptly. I would also like to thank the panel chair, Dr. Omwansa and Prof. Okelo Odongo for their valued corrections and suggestions made in reference to chapter 5 of this work. I would also like to thank my family for the support they provided me during the entire period.

## TABLE OF CONTENTS

DECLARATION .....	ii
TABLE OF CONTENTS .....	iv
List of Figures.....	viii
List of Tables .....	viii
List of Abbreviations .....	ix
Abstract .....	x
CHAPTER ONE: INTRODUCTION.....	1
1.1 BACKGROUND .....	1
1.2 The Research Problem .....	1
1.3 Objectives of the Study .....	2
1.3.1 Overall objective .....	2
1.3.2 Specific objectives.....	2
1.4 The Research Questions .....	2
CHAPTER TWO: LITERATURE REVIEW .....	3
2.1 Introduction .....	3
2.2 Emerging Technologies in the Public Sector .....	4
2.2.1 E-Governance – A Way to Modernize Governance.....	4
2.2.2 E-procurement.....	4
2.2.4 Bring your own Device (BYOD) Technology .....	5
2.2.5 Telecommunication (PBX/VoIP).....	6
2.2.6 Social Media.....	6
2.3 Review of Existing Control Frameworks .....	8
2.3.1 A CONCEPTUAL FRAMEWORK OF E-FRAUD CONTROL IN AN INTEGRATED SUPPLY CHAIN. ....	8
2.3.2 A CONCEPTUAL FRAMEWORK FOR E-FRAUD PREVENTION FOR GOVERNMENT AGENCIES-MALAYSIA.....	11
2.5.3 COBIT 5 FOR INFORMATION SECURITY FRAMEWORK .....	13
2.5.4 ISO/IEC 27002:2013.....	16
Structure of ISO/IEC 27002:2013 framework .....	16
2.5.5 Regulations Related To Information Security.....	17
2.5.6 Information Security Management Framework for the Government of South Australia- ISMF.....	19

2.6 Summary of Literature Review .....	23
<b>CHAPTER THREE: CONCEPTUAL FRAMEWORK.....</b>	<b>24</b>
3.1 Conceptual Framework for E-Corruption Control in Public Institutions .....	24
3.1.1 Purpose of the Control Framework .....	24
3.1.2 Scope .....	24
3.1.3 Framework Details .....	24
3.1.4 Technical Components .....	25
Physical security perimeters.....	26
Physical Access Controls .....	26
Securing Offices, cubicles .....	27
Access Control.....	27
Access control policy .....	27
User Access Management .....	27
User registration .....	27
User password Management .....	28
Password use .....	28
Network access control .....	29
Dedicated Connection Paths.....	30
Prevention Of Information Leakage.....	31
External Organizations/Contractors .....	31
BYOD Controls.....	31
3.1.5 Social components.....	32
Policies .....	32
Policy Ownership And Review .....	33
Compliance with legal requirements.....	33
Intellectual property rights and licensing.....	33
Protection of Government Records.....	34
Pre-employment .....	35
During Employment.....	35
Information Security Awareness and Education .....	36
Disciplinary Process.....	36
Cessation or Change of Employment.....	37

Return of Assets .....	37
Removal of Access Entitlements.....	38
Protection from Malicious Software and Scripts .....	38
Information Backup, Archival and Retrieval .....	39
Protection and Disposal of media.....	39
Information Handling Procedures .....	40
Social Media and Messaging Risk Management .....	40
Electronic Commerce Controls .....	41
Acceptable Use Policies .....	42
Intellectual property rights and licensing.....	42
CHAPTER FOUR: METHODOLOGY .....	43
4.1 Introduction .....	43
4.2 Sampling.....	43
4.3 Instrumentation.....	43
4.3.1 Reliability of Data Collected .....	44
4.4 Instructional material.....	45
4.5 Research Design .....	46
4.6 Procedures .....	47
4.7 Data analysis.....	48
4.8 Summary.....	48
CHAPTER FIVE: RESULTS .....	49
5.1 Introduction .....	49
5.2 Demographics and General information.....	50
5.3 Security Information.....	51
5.4 Applications information-IFMIS.....	53
5.5 BYOD and Email.....	56
5.6 Literacy, Training and Awareness.....	58
5.7 Fraud Deterrence and Prevention .....	59
5.8 Physical Protection .....	63
5.9 Ethics .....	64
5.10 Methods used to Perpetuate E-corruption .....	67
CHAPTER SIX. VALIDATED E CORRUPTION CONTROL FRAMEWORK.....	71

6.1 The structure of the validated framework.....	71
<b>CHAPTER SEVEN: SUMMARY OF RESEARCH, OUTCOMES AND RECCOMENDATIONS</b> .....	96
7.1 General Information/Demographics .....	96
7.2 Security Information.....	96
7.3 BYOD and Email.....	98
7.4 Regulatory Responses.....	98
7.5 Conclusion.....	100
7.6 Implications for Future Research .....	101
<b>REFERENCES .....</b>	<b>102</b>
<b>APPENDIX A- List of Survey Questions.....</b>	<b>105</b>
<b>APPENDIX B-Letter of Authorisation.....</b>	<b>114</b>

## List of Figures

<b>Figures</b>	<b>Page Number</b>
Fig 2-1 Conceptual Framework fraud Control	10
Fig 2-2 Components of E-fraud prevention	11
Fig 2-3 COBIT Product Family	13
Fig 2-4 COBIT 5 Enterprise Enablers	14
Fig 2-5 Structure of ISMF of South Australia	20
Fig 3-1 E-Corruption Control Framework	24
Fig 4-1 Work plan Methodology	46
Fig 5-1 Age Group Respondents	50
Fig 5-2 Level of Education Respondents	51

## List of Tables

<b>Tables</b>	<b>Page Number</b>
Table 5-1 Respondents view on security status	52
Table 5-2 Applications Information	53
Table 5-3 Application Information	55
Table 5-4 Email Respondents	56
Table 5-5 Corporate Email use	56
Table 5-6 WIFI Enterprise system	57
Table 5-7 Literacy, Training and Awareness	58
Table 5-8 Application Training	59
Table 5-9 Fraud Detection, Deterrence responses	60
Table 5-10 Fraud Detection, Deterrence responses	62
Table 5-11 Physical Protection of Resources	63
Table 5-12 Access Control Types	63

Table 5-13 Disposal of Media	64
Table 5-14 Ethics Responses	64
Table 5-15 Ethics	66
Table 5-16 Personnel involved in Fraud	66

**List of Abbreviations**

<b>Acronym</b>	<b>Expanded version</b>
BYOD	BRING YOUR OWN DEVICE
COBIT	COMMON OBJECTIVES FOR INFORMATION TECHNOLOGY
COSO	COMMITTEE FOR SPONSORING ORGANISATIONS
COGIT	COMMON OBJECTIVES FOR GOVERNMENT INFORMATION TECHNOLOGY
IFMIS	INTEGRATED FINANCIAL MANAGEMENT INFORMATION SYSTEM
ICT	INFORMATION COMMUNICATION AND TECHNOLOGY
ISO/IEC	INTERNATIONAL STANDARDS ORGANISATION/INTERNET ENGINEERING COUNCIL
RFID	RADIO FREQUENCY IDENTIFICATION TAGS
SOX	SARBANES-OXLEY ACT
SSL	SECURE SOCKET LAYER
D1	DOMAIN ONE
D1	DOMAIN TWO
SD1	SUB DOMAIN ONE
SD2	SUBDOMAIN TWO

## Abstract

Information security is subjective and contextual therefore, every organizations approach to a security strategy should be different and customized accordingly, because each organization has its own threats risks and business drivers.

Threats to organizational Information and Information Systems are increasing in occurrence and in complexity and this emphasizes the need to have control frameworks in place to prevent e-corruption and to better protect information.

To improve governance of IT and comply with regulatory standards, institutions are using best practice control frameworks. One of these frameworks is COBIT (Control Objectives for information and related Technology).

COBIT provides guidance on what is to be done within a Technology reliant institution in terms of control, activities, measures and documentation. This framework is however generic and requires specific knowledge.

The ISO/IEC 27001 –an information security management framework – was also a studied, but it too like its counterpart, the COBIT, fell short as it was also generic.

A COGIT (Common Objectives for Government and Information Technology) framework developed by David Gisora, 2012 which was a derivative of the COBIT model proposed security measures based on eight processes and thirty activities. It covers broad areas of IT governance which are included in the four domains as per the COBIT framework. This framework was specific to government initiatives but it lacked an essential component: internal benchmarks as a process.

The research methodology that was adopted was an exploratory study. The population of interest was parastatals in the following ministries: Ministry of Health, Education, Finance, Justice and constitutional affairs, information and communication.

Purposive sampling was used with targeted interviews to ICT officers who are custodians of information systems in the different ministries. Data was analyzed by use of descriptive statistics such as percentages, bar charts, frequency distribution tables.

The research established that the ministries faced a number of challenges in relation to implementing information security for controlling e-corruption. There seems to be no coordination between ministry staff and IT staff on the role and importance of information.

The Key recommendations included the need for management to fully understand that e-corruption control needs to be prioritized and that benchmarks, policies and regulations need to be aligned with the associated risks involved. An implementation e-corruption control framework was developed and was recommended for use to the government.

# **CHAPTER ONE: INTRODUCTION**

## **1.1 BACKGROUND**

The Australian National Commission of Audit, 2012 notes that Governments the world over are increasingly delivering services electronically as this has been found to be cost effective and efficient. However, electronic delivery of services is a double-edged sword. On one hand, electronic delivery of services brings benefits; yet on the other, the same electronic medium creates enormous opportunities for economic offenders.

Initiatives to combat corruption propose that e-Governance will help. The Kenya ICT act of 2009 outlines how new and emerging information technology is one of the pillars of the government's plans for reforming the public services, administration and obligations. Inter-ministry functions, use of internet/intranet, e-commerce, and e-procurement are examples of initiatives involving emerging technology. However, effective implementation of e-Governance initiatives demands sound ICT (Information and Communications Technology) infrastructure and sustained strategic commitment.

## **1.2 The Research Problem**

Center for Applied Philosophy and Ethics, 2001 defines e-corruption as that species of corruption that arises out of the existence or use of IT. The rapid introduction of e-government has brought with it significant new opportunities for corruption. Ethics and Anti-corruption Commission, 2009 notes that the public sector, especially managers lacks awareness of the threat of e-corruption, and specifically of the need for computer security. In the public sector, a manager's unauthorized disclosure of information and fraud are regarded as the greatest risks. Safeguards against e-corruption in the public sector agencies are not adequate e.g. policies are not well defined, technical safeguards are not regularly tested for adequate security posture, and audit trails are not followed, Moen, V, 2003. This necessitates the study that follows.

### **1.3 Objectives of the Study**

#### **1.3.1 Overall objective**

To develop a control framework for e-corruption in the public sector.

#### **1.3.2 Specific objectives**

- i. To identify the loopholes used to perpetuate e-corruption in the public sector.
- ii. To develop an E-corruption control framework for the public sector.
- iii. To Test and validate the Framework.

### **1.4 The Research Questions**

The research seeks to answer the following questions:

- i. What are the methods used in carrying out corrupt activities as a result of technology use in the Kenyan public sector?
- ii. What control mechanisms are can be adopted to address the e-corruption risks for the public sector?
- iii. What method will be used to test the framework?

## **CHAPTER TWO: LITERATURE REVIEW**

### **2.1 Introduction**

Technology adoption is driving businesses innovation and growth in Kenya, at the same time it is exposing the country to new and emerging threats. Cyber terrorists, spies, hackers and fraudsters are increasingly motivated to target our ICT infrastructure due to the increasing value of information that is held within it- driven by our dependence on them – and the perceived lower risk of detection and capture in conducting corrupt activities. The growth in the use of systems and networks to connect various organizations (e-governance) has made it relatively easy to obtain information, to communicate and to control these systems across great distances. Kigen et al, 2014

As a result of the gains made by the use of these technologies, they have been incorporated into a vast number of applications and into virtually every sector of the country's critical infrastructure (government, IT, energy, water, food and financial services). The revolution in connectivity has increased the potential for those who want to cause harm thus making it possible for a malicious agent (internal/external) to penetrate millions of computers in the country in a matter of minutes.

## **2.2 Emerging Technologies in the Public Sector**

### **2.2.1 E-Governance – A Way to Modernize Governance**

As governments the world over increasingly deliver services electronically they have to face the risk of possible fraud. The US 2002 E-Government Act, defines e-government as: the use by the Government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to

a) Enhance the access to and delivery of Government information and services to the public, other agencies, and other Government entities or

b) Bring about improvements in Government operations that may include effectiveness, efficiency, service quality, or transformation, U.S. Congress, 2002.

However with the implementation of e-governance, corrupt tendencies arise especially when trust issues are not addressed. There has to be a balance between ensuring that a system prevents fraudulent transactions and the burden that extensive checks can take place on people who are honest.

### **2.2.2 E-procurement**

There is a strong consensus among researchers and practitioners regarding the strategic importance of developing efficient purchasing to reduce costs. N.A Panayitou et.al (2004) says that an increasing number of government authorities are adopting e-procurement solutions to reap the benefits that companies in the private sector have already achieved.

K Mitchell, 2000 defines E-procurement as the process of purchasing goods and services electronically and can be defined as “the use of integrated (commonly web-based) communication systems for the conduct of part or all of the purchasing process; a process that may incorporate stages from the initial need identification by users, through search, sourcing, negotiation, ordering, receipt and post-purchase review.

E-procurement is vulnerable to process risks. These risks relate to the security and control of the e-procurement itself. Such issues can be related to, for example data security and fraud prevention e.g. fake suppliers, fake bids. An example of an e-procurement system is described:

## **INTEGRATED FINANCIAL MANAGEMENT SYSTEMS (IFMIS)**

Emerging information and communication technology (ICT) can play an important role in fighting corruption in public finance systems by promoting greater comprehensiveness and transparency of information across government institutions. As a result, the introduction of Integrated Financial Management Systems (IFMIS) has been promoted as a core component of public financial reforms in many developing countries. Chêne, 2009.

IFMIS provide an integrated computerized financial package to enhance the effectiveness and transparency of public resource management by computerizing the budget management and accounting system for a government. It consists of several core sub-systems which plan, process and report on the use of public resources. The scope and functionality of IFMIS can vary across countries, but sub-systems normally include accounting, budgeting, cash management, debt management and related core treasury systems. In addition to these core subsystems, some countries have chosen to expand their IFMIS with non-core sub-systems such as tax administration, procurement management, asset management, human resource and pay roll systems, pension and social security systems and other possible areas seen as supporting the core modules.

A well designed IFMIS can provide a number of features that may help detect excessive payments, fraud and theft. These include, for example, automated identification of exceptions to normal operations, patterns of suspicious activities, and automated cross-referencing of personal identification numbers for fraud, cross-reference of asset inventories with equipment purchase to detect theft, automated cash disbursement rules, identification of ghost workers.

### **2.2.4 Bring your own Device (BYOD) Technology**

Computerweekly.com, 2014 defines BYOD (Bring your own device) as the use of employee-owned mobile devices such as tablets and smart phones to access business enterprise content or networks.

An effective BYOD strategy can lead to a number of benefits for businesses, including improved employee job satisfaction, increased job efficiency and flexibility. BYOD can also provide cost savings from initial device purchase to on-going usage and IT helpdesk support as employees

invest in their own devices. But allowing employees to use their own devices to access company information gives rise to a number of issues that a business must answer in order to comply with its data protection obligations.

The use of personal devices in the workplace continues to rise, as do the potential legal and data protection risks, increasing the chances of data abuse and so businesses need to think carefully about BYOD and put in place appropriate policies and processes to tackle these issues and thereby minimize the risks with BYOD.

### **2.2.5 Telecommunication (PBX/VoIP)**

The telecommunications arena has not been left behind in the pursuit of efficiency, productivity. The migration from circuit switched communications technology to packet switched is based on a number of factors, most importantly cost savings, management and administration benefits and the availability of new features and applications that boost staff efficiency and productivity.

Kigen et.al, 2014 in their cyber security report outline how VoIP fraud is carried out and the immediate implications for businesses attempting to roll out VoIP. Criminals infiltrate vulnerable PBX systems to make international and long distance calls, listen to voice mail or monitor conversations. Victims of compromised PBX systems unknowingly allow the hackers to “sell” the use of their telephone system to others or provide the hackers with an opportunity to maliciously reprogram the system leaving the business who owns the PBX phone system liable for all the bills. The types of fraud are numerous: toll fraud, including “clip-on” and “shoulder surfing” methods, call-sell operations established by organized crime groups who engage “phreaks” to hack into phone line, subscription fraud, which frequently also involves identity theft, PBX fraud, which also involves call-sell operations, calling card fraud, remote call forwarding, and computer terrorism/sabotage. The use of help lines to make prank calls simply because they are toll free constitutes crime.

### **2.2.6 Social Media**

There is no debating the significance of social media to the online world as we know it today. Twitter, Facebook and the numerous other social media platforms have transformed everything from marketing and brand reputation to communicating official government information. They are popular platform that many Kenyan organizations use to build new relationships and contacts.

Government officers need to understand the intended business use of social media and evaluate and clearly convey the associated security and privacy risks. But they also must provide leadership and guidance, keeping other decision-makers properly informed to ensure any intended adoption of social media is both controlled and secure.

However, social media can be used corruptly by individuals in different agencies of the government. For instance it is easy to either intentionally or unintentionally expose sensitive data to unauthorized entities. Information officers must understand and communicate with other organizational leadership regarding the potential disclosure of proprietary or sensitive organization data via social media.

Although acceptable risk-tolerance levels will vary from one organization to another, access to external social media and networking sites from government systems should be limited to only individuals with an official business need. Personal use can be limited to personal devices (i.e., smart phones) not connected to government systems or networks, and personal devices should not be used to access official government accounts. Shared social media accounts used for corporate purposes and information dissemination need to transition from a single username and password to a more secure authentication approach, such as two-factor authentication. Information Week, 2014.

## **2.3 Review of Existing Control Frameworks**

### **2.3.1 A CONCEPTUAL FRAMEWORK OF E-FRAUD CONTROL IN AN INTEGRATED SUPPLY CHAIN.**

Lucian, V. (n.d.) describes a conceptual framework of e-fraud control in an integrated supply chain that needs a control function to take into account the cultural issues that exist across an integrated supply chain. Computer information systems do not become vulnerable just because adequate technical controls have not been correctly selected and/or implemented. As Dhillon (1997) argues, the domain of information systems security presents a rich source of behavioral issues, not always fully understood. To solve the information systems security problem, the behavioral/cultural issues need to be taken into account and adequately addressed. If managers do not take a systemic, holistic view of organizations, technology driven information systems invariably fail, as Ambaye and Hayman (1995) observe—this is even more the case in an integrated supply chain.

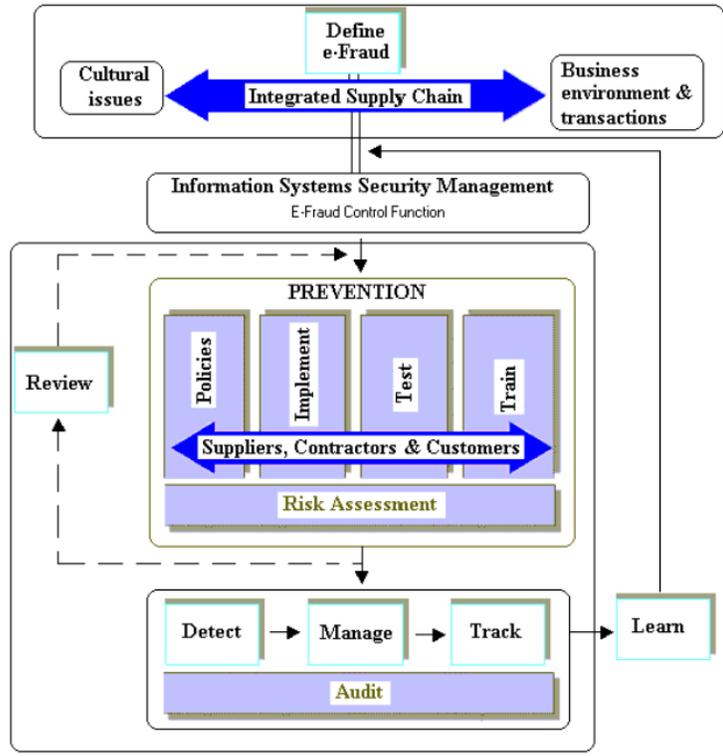
Those in charge of e-corruption control should work with the information systems users in order to understand who and how the systems will be used, to understand the business environment, and the transactions involved. Prevention should be paramount in any e-fraud control approach—the risk of loss is higher with reactive/detection strategies because either the crime is ongoing or has occurred; hence, the ability to stop or recover the loss is often very limited.

E-corruption prevention, which aims, in the first place, to reduce opportunities for corrupt activities from taking place, must be based on a risk assessment process that considers organization's vulnerability to fraudulent activities within the integrated supply chain (horizontal approach). Next, the processes, controls, and other procedures that are needed to mitigate the identified risks should be identified.

The policies and the implementation of prevention mechanisms—the hardest part, particularly when considering suppliers, contractors, and customers, their use of the information systems, and the functional requirements—should be in response to the threats/vulnerabilities identified. While some risks are inherent, most can be addressed with an appropriate system of controls. The security mechanisms should be tested to accurately assess system's security position, and training should be provided to users. Testing should be conducted more frequently for the components constantly

and highly exposed to attacks (e.g. firewalls or web servers). Training should be specific to employees' level within the organization and to the assigned responsibilities. Team feedback and dialog should be used to induce employees to be better equipped for work and change. The policies, their implementation, the testing, and the training are at organization level (vertical level). However, all suppliers, contractors, and customers will need to be considered, as a chain is only as strong as its weakest link (Arce 2003). Any policy modifications will require re-testing of systems' secure posture. Further, as computerized information systems are constantly targeted by creative perpetrators that patiently and diligently search for ways to get around implemented controls, a periodic process of continuing improvement is necessary. Testing, design review, and implementation review can contribute significantly to reducing the risk of e-fraud.

Since a fraud-proof system does not exist—even the best engineering solution would leave residual risks—, and because resources that can be or are allocated to the prevention function will always be limited (Grupe et al. 1998), organizations must have a detection function. In the detection function, if e-fraud occurs, it should be rapidly detected, managed to recover or minimize the losses, then effectively investigated to identify the perpetrator(s), and to gather digital evidence for prosecution. Adequate audit strategies across the integrated supply chain can be an essential success factor in a posteriori fraud detection. After an e-fraud incident, the lessons learned from the detection, management, and investigation must be incorporated in the e-fraud control function so that knowledge increases and better prevention strategies can be devised and implemented. The e-fraud control coordination should not end after the initial rollout. As the e-fraud risk changes and poses new challenges, those in charge should remain as the coordination organ for any future issues and improvements. Fig 2-1 presents a conceptual framework of e-fraud control in an integrated supply chain.

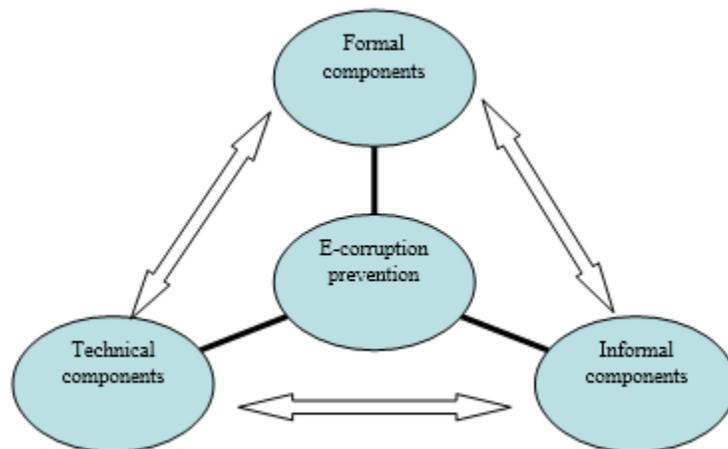


**Fig 2-1: Conceptual Framework fraud Control**

### 2.3.2 A CONCEPTUAL FRAMEWORK FOR E-FRAUD PREVENTION FOR GOVERNMENT AGENCIES-MALAYSIA.

The taxonomy of computer fraud by Vasiu & Vasuiu, 2004 defines perpetration platforms as With or Without Authorization. The first class of perpetration platform is With Authorization. This defines a legitimate user that exceeds the authorized access. The crimes are always committed by internal threats, especially senior employees because they may have greater access to assets in the organizations for their own benefits.

Centeno C, 2002, discusses how the three components of formal, technical and informal could address the E-corruption issues in the government agencies, see Fig 2-2. First is prevention through formal component, second is prevention through technological component and third is prevention through informal component. The non-technological solutions such as formal and informal components are considered as soft measures and technological are considered as hard measures.



**Figure 2-2 Components of E-Fraud Prevention**

#### ***Formal components.***

Not much IS security researchers focus on formal components such as IS security vision, the alignment between business and IS security, IS security standards, IS security policies, procedures and laws/regulation. The IS security research is primarily dominated by the technological and computational solutions .For instance, Siponen, et.al 2007 highlighted many security researchers

using mathematical approaches to prevent any type of IS risks.

***Informal components***

Informal components are referred to employee values, culture and norms of the organization. The strongest factor in information security is not technology but the people, Kumar, 2007. Human value is a non-technology based factor, which needs special attention because human maybe the weakest link in securing information systems and they have an access to system and very sensitive information. Security incidents that involve internal user such as employees, particularly at management level happen more frequently than attacks from people outside the organization. This is because of opportunities are presented through improper security. Even though the Policies and Codes of Ethics are in place, but it is not enough to manage E-corruption alone as these policies or codes have its limitations.

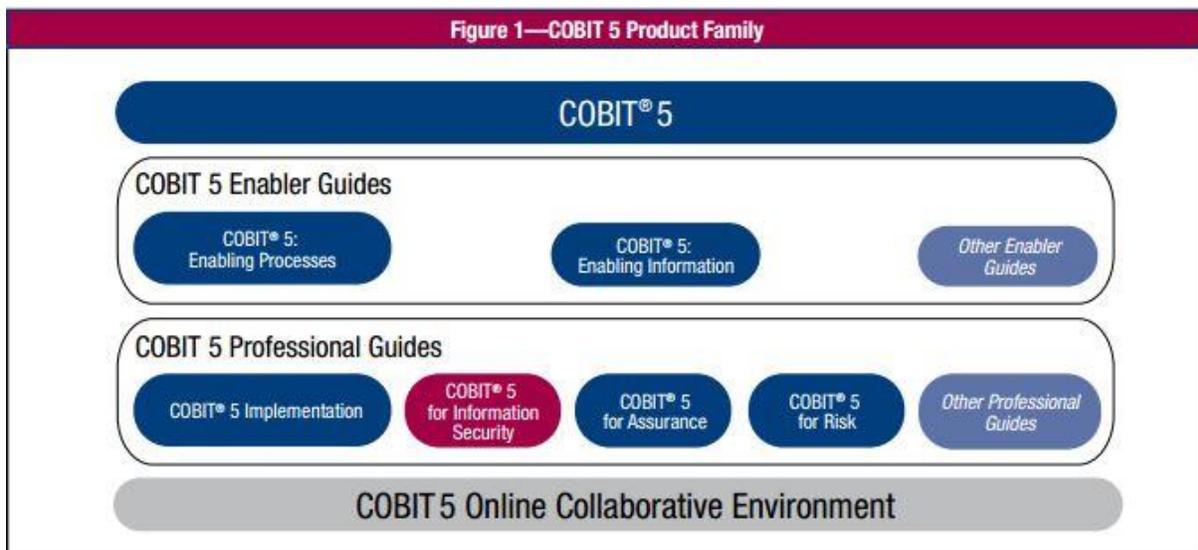
***Technical components***

The Technical component may vary ranging from hardware, network to software approaches. There are many security controls and countermeasures can be employed by government agency to minimize risk relating to IS/IT especially E-Fraud activities. For example, Secure Socket Layer (SSL) can be used to protect sensitive information, firewalls can be used to protect internal networks and data storages, virus scanning software can be used to protect against viruses, security patches should be used to update used software.

### 2.5.3 COBIT 5 FOR INFORMATION SECURITY FRAMEWORK

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from information technology (IT) by maintaining a balance between realizing benefits and optimizing risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking into account the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

COBIT 5 for Information Security, highlighted in Figure 2-3, builds on the COBIT 5 framework in that it focuses on information security and provides more detailed and more practical guidance for information security professionals and other interested parties at all levels of the enterprise.



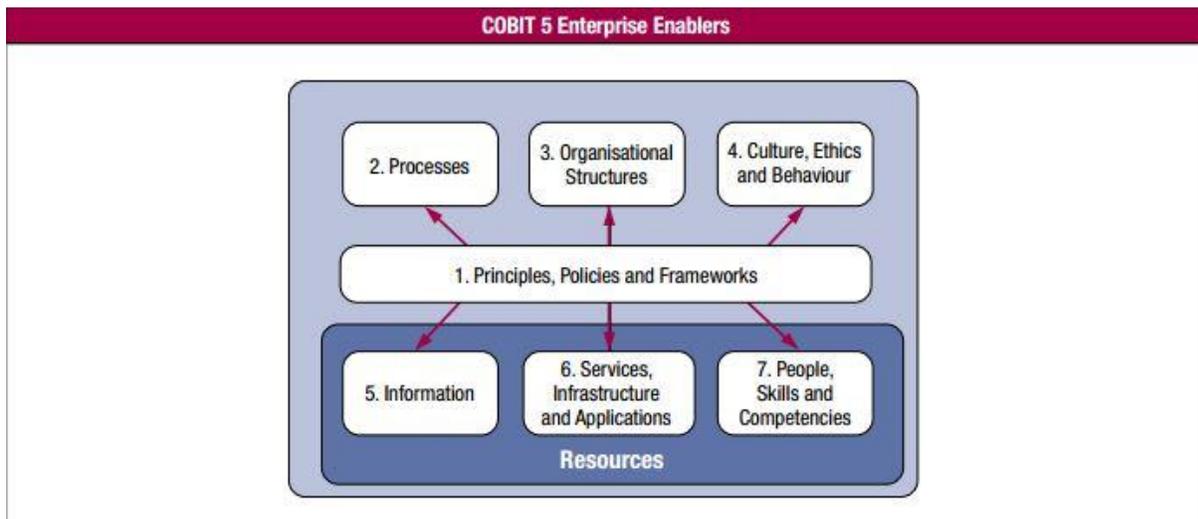
Source: [www.isaca.org](http://www.isaca.org)

**Figure 2-3- COBIT 5 Product Family 1**

The major drivers for the development of COBIT 5 for Information Security include:

1. The need to describe information security in an enterprise context including:
  - The full end-to-end business and IT functional responsibilities of information security.

- All aspects that lead to effective governance and management of information security, such as organizational structures, policies and culture.
  - The relationship and link of information security to enterprise objectives.
2. An ever-increasing need for the enterprise to:
- Maintain information risk at an acceptable level and to protect information against unauthorised disclosure, unauthorized or inadvertent modifications, and possible intrusions.
  - Ensure that services and systems are continuously available to internal and external stakeholders, leading to user satisfaction with IT engagement and services.
  - Comply with the growing number of relevant laws and regulations as well as contractual requirements and internal policies on information and systems security and protection, and provide transparency on the level of compliance.
  - Achieve all of the above while containing the cost of IT services and technology protection.



Source: [www.isaca.org](http://www.isaca.org)

**Figure 2-4- COBIT 5 Enterprise Enablers**

In addition to these major drivers for the development of COBIT 5 for Information Security is the fact that information security is essential in the day-to-day operations of enterprises. Breaches in information security can lead to a substantial impact within the enterprise through, for example, financial or operational damages. In addition, the enterprise can be exposed to external impacts

such as reputational or legal risk, which can jeopardize customer or employee relations or even endanger the survival of the enterprise.

The need for stronger, better and more systematic approaches for information security is illustrated in the following examples:

- A national critical infrastructure depends on information systems, and successful intrusions can result in a significant Impact to economies or human safety.
- Non-public financial information can be used for economic gain.
- Disclosure of confidential information can generate embarrassment to enterprises, cause damage to reputations or jeopardize business relations.
- Intrusion in commercial networks, for example, to obtain credit card or other payment-related data, can lead to substantial reputational and financial damage due to fines, as well as increased scrutiny from regulatory bodies.
- Industrial espionage can enable trade secrets to be imitated and increase competition for manufacturing enterprises.
- Leakage of national or military intelligence can result in damage to political relationships.
- Personal data leaks can result in financial loss and unnecessary efforts to rebuild an individual's financial reputation.
- Significant unplanned costs (both financial and operational) related to containing, investigating and remediating security breaches can impact any enterprise that has suffered a breach.

## **2.5.4 ISO/IEC 27002:2013**

ISO/IEC 27002 is a code of practice - a generic, advisory document, not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information.

Organizations that adopt ISO/IEC 27002 must assess their own information security risks, clarify their control objectives and apply suitable controls (or indeed other forms of risk treatment) using the standard for guidance

### **Structure of ISO/IEC 27002:2013 framework**

#### **Security Control Clauses**

The 114 control objectives are encapsulated in the following 14 sections: Information security policies- Management direction for information security, Organization of information security- internal organization and mobile devices and teleworking, Human resource security- prior to employment, during employment, termination or change of employment, Asset management- responsibility for assets, information classification and media handling, Access control- business requirements for access control, user access management, user responsibilities and system and application control, Cryptography- cryptographic controls, Physical and environmental security- secure areas and equipment, Operations security- operational procedures and responsibilities, production from malware, backup, logging and monitoring, control of operational software, Technical vulnerable management and information systems audit coordination, Communications security- network security management and information transfer, Systems acquisition, development and maintenance- security requirements of information systems, security in development and support process and test data, Supplier relationships—information security in supplier relationships and supplier service delivery management, Information security incident management – management of information security incidents and improvements, Information security aspects of business continuity management –information security continuity and redundancies, Compliance- compliance with legal and contractual requirements and information

## **2.5.5 Regulations Related To Information Security**

### ***The Sarbanes-Oxley Act of 2002***

The Sarbanes-Oxley Act of 2002 has dramatically affected overall awareness and management of internal controls in public corporations. The responsibility for accurate financial reporting has landed squarely on the shoulders of senior management, including the potential for personal criminal liability for CEOs and CFOs. Since modern accounting systems are computer based, accurate financial reporting depends on reliable, and secure, computing environments. (Sarbanes-Oxley Act of 2002)

### **The effect of SOX on information security**

To understand how SOX affects information security, an examination of two specific sections of the act is helpful: section 302, titled “Corporate responsibility for financial reports”, and section 404, titled “Management assessment of internal controls”.

#### **Section 302**

Section 302 of the SOX act states that the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) must personally certify that financial reports are accurate and complete. They must also assess and report on the effectiveness of internal controls around financial reporting. This section clearly places responsibility for accurate financial reporting on the highest level of corporate management. CEOs and CFOs face the potential for criminal fraud liability (Sarbanes-Oxley Act of 2002).

#### **Section 404**

Section 404 of the SOX act states that a corporation must assess the effectiveness of its internal controls and report this assessment annually to the SEC. The assessment must also be reviewed and judged by an outside auditing firm. The impact of section 404 is substantial in that a large amount of resources are needed for compliance. (Sarbanes-Oxley Act of 2002)

### ***Committee of Sponsoring Organizations (COSO)***

For the purpose of internal control guidance, Public Company Accounting Oversight Board

(PCAOB) selected a control framework created by the Committee of Sponsoring Organizations (COSO). The COSO framework provides a structured and comprehensive set of guidelines for creating and implementing internal controls. The use of the COSO framework is not required for SOX compliance, but it is safe to assume that any other framework selected will be similar in scope.

## **2.5.6 Information Security Management Framework for the Government of South Australia- ISMF**

The Information Security Management Framework (ISMF) addresses cyber security in the Government of South Australia, and consists of 40 policies supported by 140 standards. It is a business driven risk-based approach that is aligned with the Australian Government Protective Security Policy Framework and the 27001 international standard for information security management systems. The ISMF applies to South Australian Government agencies and suppliers whose contractual requirements include it.

The objectives of the ISMF are to:

- Support the attainment and realization of three information security objectives across Government: Confidentiality (including information the Government keeps about members of the public), Integrity and Availability of information.
- Provide a framework to enable government to achieve an assured cyber security environment;
- Achieve the assured cyber security environment by using risk management ;
- Prescribe a risk assessment process to identify ICT information assets and the level of risk associated with these assets in a manner that is appropriate to the business of the Agency and that can be consistently applied by Responsible Parties;
- Assist the Responsible Party in developing an Information Security Management System [ISMS] suitable for use with South Australian Government information assets that applies appropriate security controls to permit the efficient and secure access to information assets in a manner that is consistent across all SA Government Agencies;
- Refer Responsible Parties to best practice control processes and measures that are regularly updated to account for new technologies, threats and risks as they may arise;
- Identify management processes to enable Agencies to obtain assurance on an ongoing basis as to the effectiveness of their information security measures;

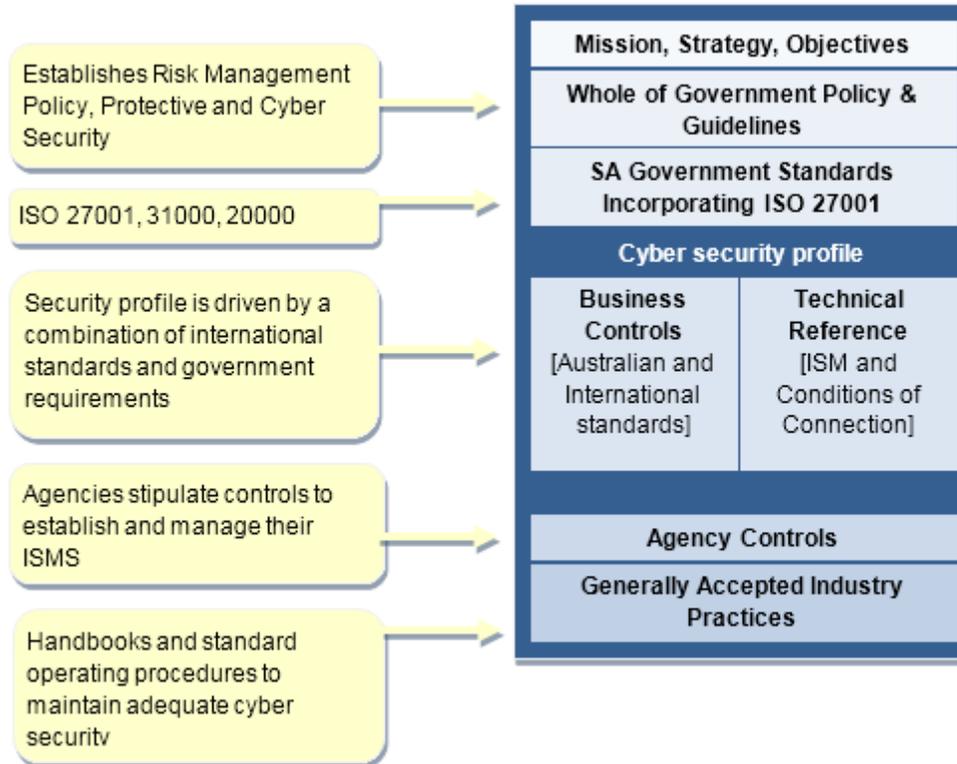
- Establish a communication process to ensure that there is a high level of awareness and commitment to information, particularly ICT based information, security requirements across government;
- Protect the privacy, confidentiality and integrity of all electronic government information including that of SA Government clients and any information the Government keeps about members of the public.

## **Introduction**

This framework for the management of ICT information security (‘cyber security’) has been established as an initiative of the South Australian Government.

The framework presents a consistent approach to information security management and development, regardless of the size, complexity or nature of the Information and Communication Technology [ICT] environment.

The figure below depicts a conceptual model of the South Australian Government ISMF. It is designed in a way that allows an interoperable and consultative process for the agreement, implementation and ongoing management/refinement of a whole of government approach to information security management.



Source: [www.ismfsa.au](http://www.ismfsa.au)

**Figure 2-5 Structure of ISMF of South Australia**

This framework comprises the following key elements:

- **South Australian Government Information Security Policies**

Each major section of this document (sections 4 to 17) contains Policy Statements that apply to Responsible Parties. They are high-level statements of the South Australian Government's position with respect to information security. The policy statements contained herein should be considered a baseline of policy statement applicable to all Responsible Parties that may incorporate additional policy statements applicable to the specific activities and nature of their respective business undertakings.

- **South Australian Government Information Security Standards**

Each sub-section from section 5 onwards contains a number of South Australian Government ISMF Standards in support of that section's policy statements. They describe specific obligations under each of the South Australian Government information security policies. The application of these standards in supporting Policy Statements is the outcome of a risk assessment and the specific nature of the activity being conducted by the Responsible Party.

- **Recommended South Australian Government Agency Information Security Standards and Control Measures**

Additional guidance is provided to assist Responsible Parties in developing their own specific information security standards in order to implement the required South Australian Government standards, based on their risk assessment outcomes. Some of this guidance is general in nature. Each section contains, where appropriate, additional controls for Responsible Parties to consider and/or implement that are based upon the respective classification levels of ICT information assets.

- **Generally-Accepted Industry Practices**

Included in the framework are a set of practices that have been developed to provide additional guidance to Responsible Parties where appropriate. These guidelines constitute the most dynamic part of the framework as additional cyber security issues are addressed or updated. External publications entitled 'ISMF Guidelines' are also available for consultation and implementation to fulfil the stated objectives of South Australian Government cyber security policy and corresponding standards.

## **2.6 Summary of Literature Review**

The literature review consisted of emerging technologies in the public sector and a review of existing frameworks that are in use by institutions and frameworks adopted by governments. Technologies reviewed included IFMIS BYOD, VOIP and E-Procurement. The frameworks adopted by governments of Malaysia, South Australia were also reviewed. ISO/IEC 27002:2013 was discussed with the focus on accountability from Chief Financial Officers and Chief Information Officers. SOX act of 2002 and COSO were described briefly in relation to Information security regulations.

# **CHAPTER THREE: CONCEPTUAL FRAMEWORK**

## **3.1 Conceptual Framework for E-Corruption Control in Public Institutions**

### **3.1.1 Purpose of the Control Framework**

Public institutions are committed to the principles of integrity, respect and accountability which include the prevention, detection and control of corruption (including e-corruption and other forms of criminal conduct, misconduct and maladministration) in the workplace.

The purpose of this framework is to formalize and communicate the processes and strategies for preventing, detecting and responding to actual alleged or suspected conduct of employees or other public officers in the government that is suspected or alleged to be e-fraud, e-corruption or other criminality, misconduct or maladministration.

### **3.1.2 Scope**

This framework applies to all government employees providing services in public institutions.

### **3.1.3 Framework Details**

#### ***STRUCTURE OF THE FRAMEWORK***

The proposed framework is an amalgamation of the following frameworks:

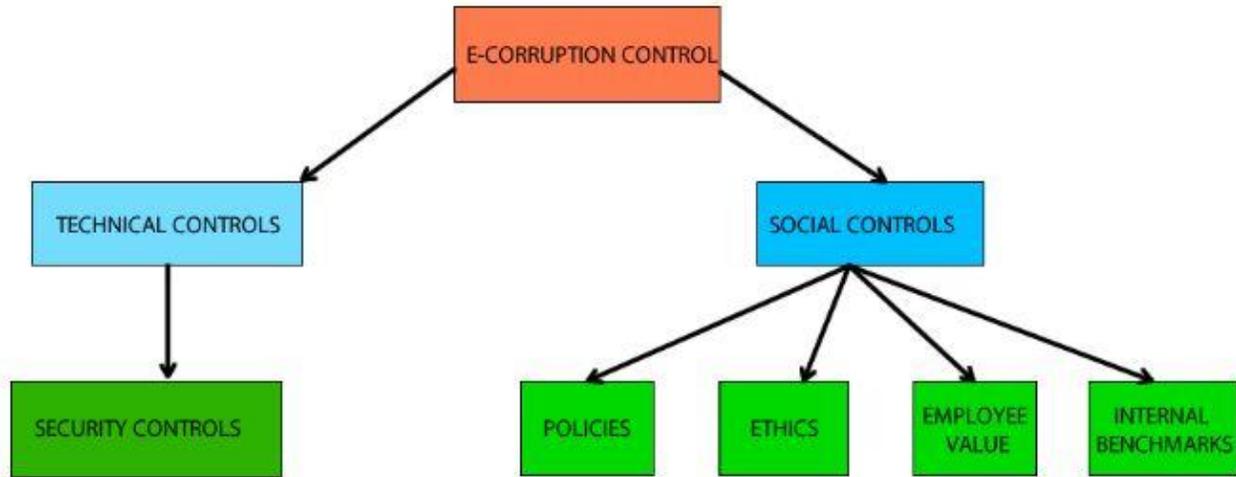
1. Musa et al. 2012, in their assessment of e-corruption level in Malaysia
2. COBIT 5 for information security

Information Security management framework for the government of South Australia (ISMF v 3.2.0)

3. ISO/IEC 27001:2013.

These frameworks were chosen due to their depth in research and the format & breakdown of the report was easy to follow. The format of the structure adopted was borrowed from the ISMF v 3.2.0 that outlines a standard or process and the control objectives that can be applied to ensure the policy will be adopted as prescribed.

The architecture is depicted figure 3-1:



**Figure 3-1 E-corruption control framework**

### **3.1.4 Technical Components**

These are Security methods consisting of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications. The Technical component may vary ranging from hardware, network to software approaches. There are many security controls and counter measures can be employed by government agency to minimize risk relating to IS/IT especially E-Fraud activities. For example, Secure Socket Layer (SSL) can be used to protect sensitive information, firewalls can be used to protect internal networks and data storages, virus scanning software can be used to protect against viruses, security patches should be used to update used software. Other technical solutions including 3D-model based solutions, SET and EMV smart cards, complemented by a real time authorization by the issuer, address and CVV/CVC2 validation, the use of passwords and user Ids, virtual and pseudo card numbers. Apart from that, the security of technology infrastructure of the consumers, merchants, banks and service providers' needs to be taken into consideration as online transactions take place.

The first sub domain from Figure 3-1 follows:

### ***Security Controls***

The following security controls are described:

#### **Physical security perimeters**

##### ***Standard:***

Responsible entities should identify and clearly define security perimeter(s) around the institutions information assets.

##### ***Controls:***

A security perimeter is defined as the physical boundary between an area requiring protection at one level and an area requiring protection at another level (relative to the classification level of information available in each area). This perimeter should be built around the business premises, and could surround key areas within the organization (e.g. information processing facilities) to provide various layers of access controls that protect information assets at levels commensurate with information classification and risk.

#### **Physical Access Controls**

##### ***Standard:***

Physical access (entry) controls for secure areas should be established to restrict access to authorized personnel only.

##### ***Controls:***

C1. Access rights to secure areas should be reviewed and updated on a regular basis. Documented evidence of the review should be retained. These reviews should be performed at least annually, or more frequently based on a risk assessment that takes into account such factors as the level of turnover of personnel and the classification of the information asset being protected.

C2. Dual authentication controls (e.g. Swipe cards plus PIN) should be used to authorize and validate all access.

C3. All personnel should wear Photo ID badges. Time of entry and departure of visitors should be logged. Visitors should be supervised; security requirements and emergency procedures should be conveyed to visitors (excepting those who have already been briefed on prior occasion).

C4. Authentication controls (such as an access card with PIN) should be employed where feasible and an audit log should be maintained commensurate with the access granted.

### **Securing Offices, cubicles**

#### ***Standard:***

Offices, rooms and facilities should be secured in a manner that appropriately protects the information assets stored within the area, relative to its classification and the risk assessment for that information.

#### ***Controls:***

C1. Intruder prevention and detection systems for physical incursions, including alarms should be installed and regularly tested.

C2. Locations of sensitive information processing facilities and other areas should not be included on directories and phone books, with special consideration given to publicly accessible directory information such as that located in lobbies, foyers and stairwells.

### **Access Control**

#### **Access control policy**

#### ***Standard:***

Institutions should establish and document their business requirements using policies and guidelines that implement access control mechanisms for their information assets. Access controls should be implemented such that users are only provided with the level of access required to perform their job function.

### **User Access Management**

#### **User registration**

#### ***Standard:***

Formal registration and de-registration procedures should be implemented for granting and revoking access to all information systems and services.

***Controls:***

C1. Procedures should ensure that user IDs are not reissued to other users, to limit the potential for unauthorized access being inadvertently granted.

C2. Periodically scan for duplicate/redundant user IDs or accounts and remove or block access until resolved.

**User password Management**

***Standard:***

Responsible entities should develop standards to manage the allocation of user passwords.

***Controls:***

C1. Additional technologies for user identification and authentication, such as biometrics and/or hardware tokens, should be considered.

C2. Guidelines on the selection of strong passwords should be included in security awareness briefings and as part of a comprehensive Information Security Awareness Program.

**Password use**

***Standard:***

Responsible entities should inform users of their responsibilities with respect to password selection and use, and in accordance with password management standards.

***Controls:***

C1. All passwords used to gain access to an information system should be treated as though they are classified at least at the same level as the classification of the system they are used to access.

C2. Passwords include all forms of secret authentication information assigned to a user (such as group authentication or individual user id authentication information) for the purposes of this standard.

### **Network access control**

#### ***Standard:***

Access controls should be applied and maintained for both internal and external networked services, connection paths and network-attached resources.

#### ***Controls:***

C1. For shared network infrastructure, clear responsibilities and procedures should be established by the network manager to maintain security in a manner that protects the interests of all institutions that rely on that infrastructure.

C2. Standards should be established regarding acceptable use for Internet services (e.g. web, e-mail, news groups) in terms of business versus personal use, as well as consideration of issues regarding objectionable material.

C3. The standards should also consider issues that relate to capacity implications for specific types of network traffic. This may include limiting the size of e-mail attachments that are acceptable to the institution. It may also include limiting or banning streaming audio and video services and any other identified high-bandwidth services that are not required to support authorized business use.

C4. Users should only be provided with direct access to services that they have been specifically authorized to use. This control is particularly important for network connections to sensitive or critical business applications, or to users in high-risk locations (e.g. public or external areas that are outside the institutions management and control).

## **Dedicated Connection Paths**

### ***Standard:***

Dedicated and secured system and network interconnection paths should be established when multiple or unsecured paths would present an unacceptable risk to the security of information.

### ***Controls:***

C1. In highly sensitive information processing environments, minimizing risk of message interception may be accomplished by restricting the number of alternative routes that are available to users/terminals and/or limiting network traffic to devices that are subject to appropriate physical and logical security.

C2. Systems and/or network interconnections that require dedicated path access controls must not be attached to wireless LAN and/or public broadband services.

C3. Remote access devices (e.g. broadband modems and VPN gateways) should be attached via a secure gateway device that provides appropriate filtering and authentication controls commensurate to the classification of the information assets being accessed.

C4. Encryption and/or cryptographic controls should be enabled where possible per the guidance and requirements described in this framework.

C5. A two factor authentication process at the network perimeter should be adopted for all external connections to an institution server or PC.

C6. Consideration should be given to restricting access for external connections to specific computer systems and/or from specific locations (sources) as well as restricting the time periods that such connections can be used.

C7. A facility should be implemented that can limit the number of unsuccessful attempts at establishing an external connection before the user identifier is suspended.

## **Prevention Of Information Leakage**

### ***Standard:***

Measures and controls should be implemented to protect against unauthorized information disclosure resulting from the presence of embedded covert channels and code exploits (such as Trojans) in applications and systems used to process institution information.

## **External Organizations/Contractors**

### ***Standards:***

Access to information processing facilities by third parties must be controlled and such controls must be agreed to and defined by way of contractual obligation with the external organization.

### ***Controls:***

C1. Responsible entities may embed the use of an assessment tool as a component of the selection process for external organizations.

C2. Responsible Parties should establish individual confidentiality agreements with the staff of contractors.

C3. Third parties and their employees, including sub-contracted service providers, who require access to security classified information must be security cleared to the appropriate level.

C4. Appropriate authorization should be obtained from the relevant manager (typically the Business Owner) before users can obtain remote access.

## **BYOD Controls**

### ***Standard:***

Institutions should have a balance of technical and procedural control over BYOD to minimize their exposure to information risk.

***Controls:***

When deploying a BYOD model, organizations should:

C1. Ensure user education programmes are in place, and users' responsibilities are clear.

C2. Generate acceptable-use policies and security operating procedures for users' devices.

C3. Put processes in place for auditing users' behavior (i.e. trust and verify).

**3.1.5 Social components**

***Policies***

**Policies**

***Standard:***

Institutions should establish a documented Information Security Policy and demonstrate their ongoing support for and commitment to information security incorporating ongoing review and improvement, as required, of the information security policy across the organization.

***Controls:***

C1. Information Security Policy that is developed by an institution must be aligned with Kenya National ICT Master plan.

C2. Information security policies (as distinct from standards and controls) must comply with the Kenyan Government Information Security Manual.

C3. Information security policies that deal with National Security classified information or other highly sensitive information based upon classification must be restricted to audiences on a "need-to-know" basis.

## **Policy Ownership And Review**

### ***Standard:***

Institutions should nominate an owner of their information security policy. The owner of this policy should have approved management authority for the development, maintenance and evaluation of the security policy.

## **Compliance with legal requirements**

### ***Standard:***

Responsible entities should define, document and maintain their compliance with respect to legislative, statutory, regulatory and contractual conditions and requirements for each identified information asset.

## **Intellectual property rights and licensing**

### ***Standard:***

Institutions are accountable for ensuring compliance with legislative, contractual and statutory requirements on the use of material that is the subject of intellectual property rights, such as copyright, design rights or trademarks and software products.

### ***Controls:***

C1. Compliance with software license requirements and terms of use therein should be monitored.

C2. Software should not be copied except for authorized installation and backup purposes.

## **Protection of Government Records.**

### ***Standard:***

Government records, including information that is stored electronically as data, should be protected from loss (including theft), destruction and falsification in accordance with relevant statutory, legislative, regulatory and contractual requirements.

### ***Controls:***

C1. In circumstances where information systems are used to solicit information from members of the public (e.g. in an e-commerce or e-government scenario), informative messages should be included at the point of information capture, to make the individual aware of the intended use of the information, who will use the information and any legal authority or requirements to collect the information.

C2. Institutions that are involved in transmitting, soliciting and collecting personal information via websites should also have regard for the Privacy Guidelines for Kenya Government websites.

C3. Access control lists for electronically stored personal information should be carefully designed such that only those personnel that have a need-to-know are able to access the information, consistent with the stated purpose of collection and disclosure of the information.

C4. Responsible Parties must define 'Authorized Access' for all data, including who has access, the level of authority required, and the level of access allowed.

*Employee Value*  
**Pre-employment**

***Standard:***

Information Security responsibilities should be addressed at the recruitment stage, included in contracts, and monitored during an individual's employment.

***Controls:***

C1. When employing personnel, the Responsible entity should perform appropriate security and / or reference checks to verify their credentials.

C2. A security clearance as defined by the criminal investigations department should be obtained by the applicant.

C3. All personnel should be subject to a security vetting process.

C4. Appropriate checks (e.g. Police security checks) should be carried out upon appointment or promotion to a position where the applicant will have access to sensitive Information Processing Facilities, (e.g. financial information or critical infrastructure). For personnel holding positions of considerable authority these checks should be repeated regularly.

**During Employment**

***Standard:***

Managers and Supervisors, or those acting in supervisory capacities should ensure that personnel under their direction and control, including contractors and temporary staff, apply security practices in accordance with the institutions established policies and procedures.

***Controls:***

C1. Each Responsible Party should ensure that confidentiality and/or non-disclosure agreements are in place for all staff, contractors and/or sub-contractors that seek or have in place access to Kenya Government information, materials and/or intellectual property that is not intended for public access or circulation

C2. Institutions should note that all personnel employed under the auspices of the *Public Service Commission Act 2012* are adequately bound to the confidentiality and non-disclosure requirements of that legislation thus alleviating the requirement for additional non-disclosure undertakings.

**Information Security Awareness and Education**

***Standard:***

Institutions should provide appropriate training in Agency information security policy, standards and procedures to employees and, where necessary, to contractors and other temporary personnel prior to granting access to information assets or services.

***Controls:***

C1. A copy of the Agency's information security policies should be issued to all new personnel as they join and to all existing personnel.

C2. Security reminder messages should be posted in secured areas and/or regularly communicated to personnel according to the intended audience and or classification of the notifications.

C3. Personnel should be made aware of the security classifications of the information assets that they use, and that they handle them appropriately.

**Disciplinary Process**

***Standards:***

A formal disciplinary process should be established by all institution in relation to employees who have violated whole-of-government and/or institution security policies.

Disciplinary processes should aim to be a deterrent to employees who might otherwise be inclined to disregard security policies and procedures.

Where appropriate, discipline should be in line with the relevant employment act conditions. For employees not covered under this, discipline should be in line with contract terms and conditions.

### **Cessation or Change of Employment**

#### ***Standards:***

All Responsible entities should have documented procedures for performing employment termination and/or for the withdrawal of assigned responsibilities resulting from a change in employment status for employees, contractors and other third party users.

#### ***Controls:***

C1. Responsible Parties should implement procedures concerning employment termination, or change of duties in alignment with the implementation guidance.

C2. Responsible Parties should ensure that important knowledge or operational skills have been transferred to other resources prior to departure of the employee and/or contractor.

### **Return of Assets**

#### ***Standard:***

Responsible entities must ensure that all assets belonging to the institution are returned by departing employees, contractors and third-party users.

#### ***Controls:***

C1. Responsible Parties must establish procedures and processes to transfer Official Information contained on personal (home office or BYO) devices such as home computers and mobility devices to agency owned information assets. Such procedures shall include a provision for the secure erasure of all official Information (other than PUBLIC) that is stored on the personal device.

### **Removal of Access Entitlements**

#### ***Standard:***

Responsible entities should have an established and logged procedure for the withdrawal and/or modification of access rights for departing employees, contractors and third-party users. Institutions must implement procedures for the withdrawal or change of access entitlements.

#### ***Internal Benchmarks***

### **Protection from Malicious Software and Scripts**

#### ***Standard:***

This strategy should incorporate use and regular/frequent maintenance of approved virus scanning tools, as well as a user awareness program that will assist users in understanding their roles and responsibilities in relation to malicious software. Only authorized copies of software shall be resident on computer systems and all software licensing requirements must be adhered to.

#### ***Controls:***

C1. Institutions should implement a strategy for scanning or otherwise monitoring ongoing compliance with licensing requirements.

C2. Institutions should establish a formal process for the authorization of software purchases such that records are appropriately maintained and unauthorized software can be identified and actioned.

C3. User awareness and training (Information Security Awareness programs) should be periodically undertaken to inform users of the risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken.

## **Information Backup, Archival and Retrieval**

### ***Standard:***

Essential business information and software should be backed up regularly and information integrity checks should be conducted at random intervals to ensure that backed up information is accurate, available and relevant for recovery following a notifiable Incident (such as disaster, media failure, information theft or system errors that have affected information integrity).

### ***Controls:***

C1. Institution employees are responsible for backing up all data stored on workstations that are not connected to the network (e.g. portables used outside the office) and they should be made aware of this responsibility.

C2. Back-up information may need to be encrypted according to the sum of its classification, sensitivity and/or importance to the business.

## **Protection and Disposal of media**

### ***Standard:***

Media may include any form of information asset that contains information or has previously contained information including but not limited to: paper documents, magnetic media, non-volatile RAM, solid state disks, memory cards etc.

### ***Controls:***

C1. Disposal of information assets must be logged.

C2. Where re-use after media sanitization is impractical, information assets must be disposed of in a secure manner (e.g. secure destruction and/or incineration)

C3. All information and software should be removed totally (i.e. secure-erased (a.k.a. “wiped”) or overwritten, not just deleted from data storage media (e.g. hard drives, discs), which are to be disposed of by the institution.

C4. When equipment is sold, or otherwise disposed of, data on any storage devices should be effectively erased.

### **Information Handling Procedures**

#### ***Standard:***

Institutions should implement documented handling and storage procedures for information to reduce the likelihood of unauthorized disclosure or misuse.

#### ***Controls:***

C1. Personnel should be made aware of the security classifications of the ICT assets that they use, especially the data and documents they deal with, and that they handle them appropriately.

C2. Responsible entities should ensure that documented information handling procedures are communicated to employees and contractors or sub-contractors as part of a comprehensive Information Security Awareness program.

### **Social Media and Messaging Risk Management**

#### ***Standard:***

Responsible entities should implement controls to reduce security risks arising from the use of electronic messaging systems, such as email, electronic data interchange, instant messaging and social networking sites.

***Controls:***

C1. Quarantining messages for closer investigation (policies and procedures need to address the process to follow for quarantined messages).

C2. Limiting the message size (including attachments) to prevent un-necessary resource waste (e.g. Storage and network capacity).

**Electronic Commerce Controls**

***Standard:***

Information used in Electronic Commerce should be protected from fraudulent activity, misuse, breach of privacy and unauthorized access.

***Controls:***

C1. Responsible entities should protect information involved in online transactions using appropriate technical controls.

C2. Liability for fraudulent and erroneous E-Commerce transactions should be risk assessed and may be mitigated through the use of strong Authentication, Authorization, Non-Repudiation, Integrity and Confidentiality controls.

C3. Security and control measures that are adopted by institutions should also take into account the implications of bad publicity that may result from failed security measures that compromise confidential information, or the provision of incorrect or misleading information on the institution web site.

## ***Business Ethics***

### **Acceptable Use Policies**

#### ***Standard:***

Ethical and legal decisions should be defined in the use of electronic systems.

#### ***Control:***

C1. Institutions should have acceptable use policies. Clearly written policies that outline permissions and restrictions will be made known to all employees.

### **Intellectual property rights and licensing**

#### ***Standard:***

Institutions should ensure ethical use of resources owned by the institution and are compliant with legislative, contractual and statutory requirements on the use of the resources that are the subject of intellectual property rights, such as copyright, design rights or trademarks and software products.

#### ***Controls:***

C1. Software should not be copied except for authorized installation and backup purposes.

C2. Software should not be copied for personal use unless it is expressly permitted by the institutions licensing agreements and approved by senior management.

C3. Compliance with software license requirements and terms of use therein shall be monitored.

## **CHAPTER FOUR: METHODOLOGY**

### **4.1 Introduction**

This chapter addressed the methodology, procedures and instruments used by the researcher to gather data and analyze them. The researcher also described the method that was used to select samples and the data collection instruments that were used. The design of the research was described in detail in the last two sections of this chapter.

### **4.2 Sampling**

All public agency professionals working for the government in Kenya would have been the perfect population. However, because, geographical distance and different initiatives, though, such a generalization was not justifiable within the research timeframe and budget. One that was considered justifiable by the researcher was to target the population of all government employees in the major cities-Nairobi, Kisumu and Mombasa.

A total of 70 public sector professionals at the state, local and county level were targeted to participate in the questionnaire-based survey regarding the state of Technology uptake in their respective roles and the risks that are associated with such initiatives. This survey was carried out via questionnaires distributed and recollected between September and October 2014.

Some of the public service sectors that were researched are defense; education; immigration, justice and security; postal; procurement; regulation; procurement; revenue and customs; and transport.

### **4.3 Instrumentation**

A multi-method approach that combines qualitative and quantitative data was used. (Jick,1979). This method was used because data collection from various sources increased the trustworthiness and validity of data (Todd 1979; Yin 2003; Saunders et al 2003).

The instrumentation used on the research questions was a survey of the public officers through questionnaires. Public officers who are key decision makers of the e-Government initiatives were interviewed via telephone and where possible, via face-to-face meetings.

Key demographic information was the respondents role, whether IT or business-related. This important information was required in order to be able to identify the angle of opinion provided by the respondents.

The instrument administered for the first research question was expected to indicate key loopholes used by public officials in carrying out corrupt activities using current technologies that have been implemented. The questionnaire was used to gather empirical data about how systems are secured, policies put in place to determine the level of Information access, confidentiality and integrity.

The research would not be complete if a control framework was not formulated that can be used to tackle the e-corruption menace. Thus, the second research question answered this, where challenges faced by government institutions in terms of information security was extracted through interviews with Security experts. Further interview questions were designed to gather data about how these difficulties are dealt with currently.

#### **4.3.1 Reliability of Data Collected**

Two types of error can occur in sample-based surveys: sampling error and non-sampling error. Sampling error arises because in a sample survey not all of the population is surveyed. Hence a measured sample statistic is not usually identical with the true population behavior. Non-sampling errors cause bias in statistical results and can occur at any stage of a survey and can also occur with censuses (i.e. when every member of the target population is included). Sampling error can be estimated mathematically whereas estimating non-sampling error can be difficult.

On addressing the non-sampling error, the survey response rate excluded responses that were received but were insufficiently complete to provide input into the data generated. However, a response rate of more than 50 percent was considered very creditable for a voluntary survey.

Every effort was made to reduce the non-sampling errors to a minimum by careful survey design and efficient operating procedures. In particular, the paper survey design minimized the possibility of errors made in recording and coding of responses, as the respondents only had to choose from a number of choices when responding to the survey. Whenever the respondents were given subjective questions, a clear guideline was given to guide the response within the scope of the survey.

In addition, identifiable errors made by respondents while completing the survey were removed from the results. For example, blank responses will be generally coded to no response categories.

#### **4.4 Instructional material**

The first set of instructional material consisted of survey questions, in the form of ratings on a Likert scale, directed to public officers who were directly involved in the systems administration, Network administrators, Information system security officials, A list of the suggested questions can be found in Appendix A. Majority of the questions were guided by key selection points to ensure that responses collected are within the scope of this research.

The second set of instructional material consisted of questions in the form of multiple choice answers directed to the same group of individuals. This material was expected to gather empirical data regarding Host Information, Applications Information, Security information, IT Literacy levels, Trainings acquired in Government institutions.

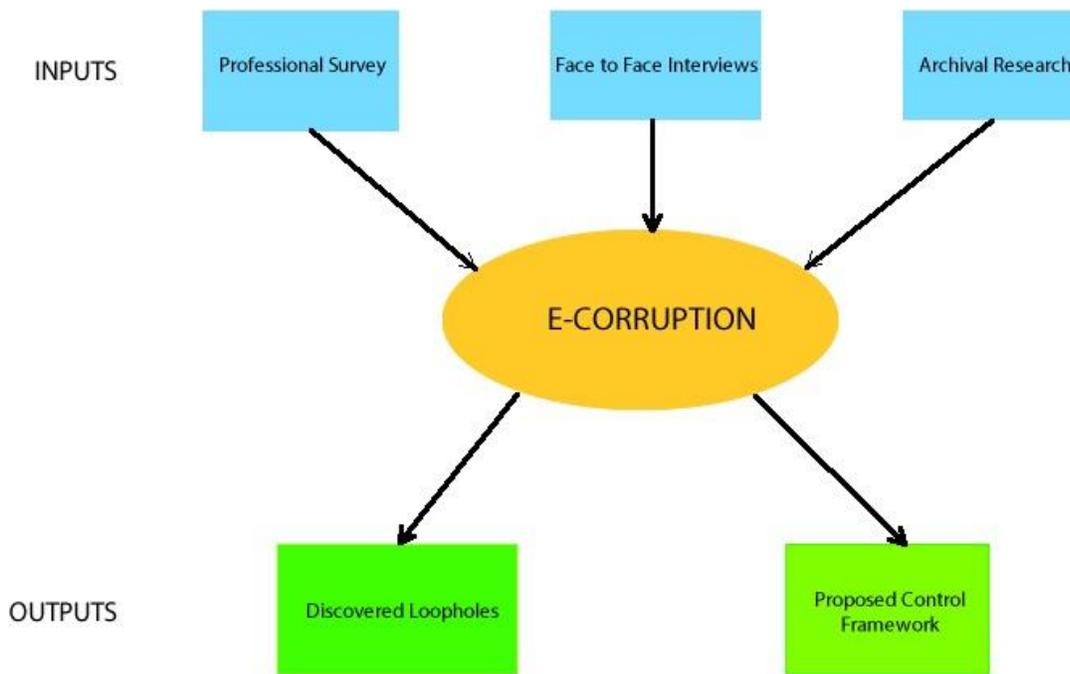
Scales were included in any question that required a respondent to measure the strength or level of a theoretical construct. In its simplest form in the survey, a scale asked a respondent to indicate the frequency of training and refresher courses on a four-point scale. The scales used in the surveys were generally balanced - that is, they allowed the respondents to express one of the two extremes of view (e.g. strongly agree and strongly disagree).

#### 4.5 Research Design

The survey method was used in this research because it has the lowest comparative cost compared to other methods of quantitative data collection methods.

The population of the public sector professionals' targeted in this survey was 70. The agencies were sent the survey in September 2014 and returned in November 2014. This was a paper survey rather than an online survey.

The following work plan methodology in figure 3-1 was used to capture data.



**Figure 4-1- Work plan Methodology**

The researcher used the survey method in order to gather quantitative data via questionnaires to describe the characteristics of emerging technology in the public sector and to detail the corruption risks associated with its adoption.

The findings were expected to contribute towards prioritization of initiatives, formulation of strategies and the development of the implementation framework.

Next, the researcher planned to administer questions during face-to-face and telephone interviews with independent experts in Information systems auditing to support the quantitative data that was collected.

Information was also collected from archived reports and conference papers that were used to analyse the data further. The required outputs were detailed findings on the loop holes that public officers use to carry out corrupt activities proposed control framework for the prevention of e-corruption in the public sector.

#### **4.6 Procedures**

The questionnaire instruments that are directed to the public officers was administered via mail on the first week of September 2014. Samples were given four weeks to complete and submit their response. Public officers were allowed remain anonymous due to the sensitivity of the data collected. Data collected was disposed appropriately to maintain respondents' anonymity.

However, interview slots were pre-booked and therefore it was dependent on the interviewee's available time.

## **4.7 Data analysis**

For analysis presented in this report it was assumed that there was no significant bias between those who responded in the survey and those who did not respond. Results were not presented rounded to the nearest whole percentage point (i.e. 41.8 percent not 42 percent). This was done to maintain accuracy. This non rounding, enabled the percentage results for some questions to add up to exactly 100 percent.

Data collected from the survey was analyzed according to the different research questions. A response to research question one, regarding the methods used in carrying out corrupt activities as a result of technology use in the Kenyan public sector, the characteristics of emerging technologies and the corruption risks in the public sector were generated by computing means and frequency for each survey item after coding the samples.

## **4.8 Summary**

This research thesis target was to investigate and report the methods used in carrying out corrupt activities as a result of technology use, the characteristics of emerging technologies and the corruption risks in the Kenyan public sector.

Thereafter, the results of the survey would pave way for the construction of a control framework.

By administering the instruments described earlier, public officers are surveyed to gather empirical data to show the loopholes used by corrupt public officials to carry out unethical practices. The instruments are also designed to collect demographic data about people, security posture of government institutions, policy and regulatory trends.

Data gathered assisted in the development of a control framework for curbing e-corruption in public institutions, but yet flexible in a sense that it could incorporate any social changes pertaining to state and new county governments.

## **CHAPTER FIVE: RESULTS**

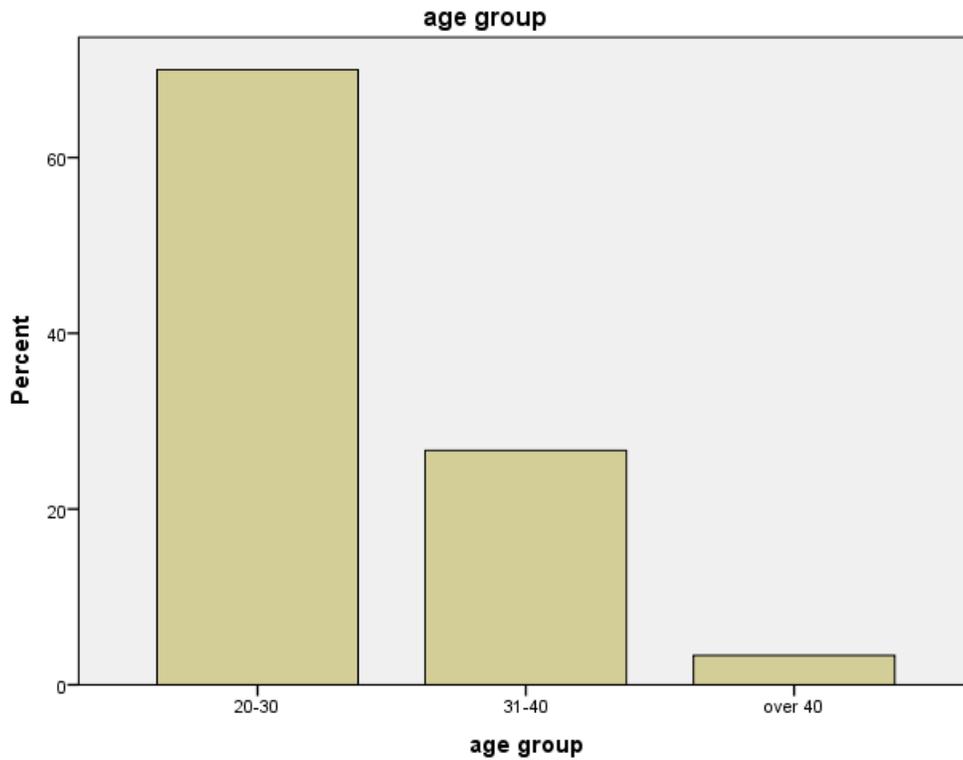
### **5.1 Introduction**

This chapter presents a detailed results of the research findings in an attempt to achieve the objectives of the day. Data was analyzed through two main ways: quantitative analysis by making use of statistical techniques and by qualitative analysis.

The researcher collected 30 questionnaires out of the 50 that were disseminated to the different government agencies and parastatals. The respondents are information security officers/IT officers charged with the responsibility of ensuring the security of the systems that they are in charge of. The respondents were drawn mainly from Nairobi, Mombasa and Kisumu.

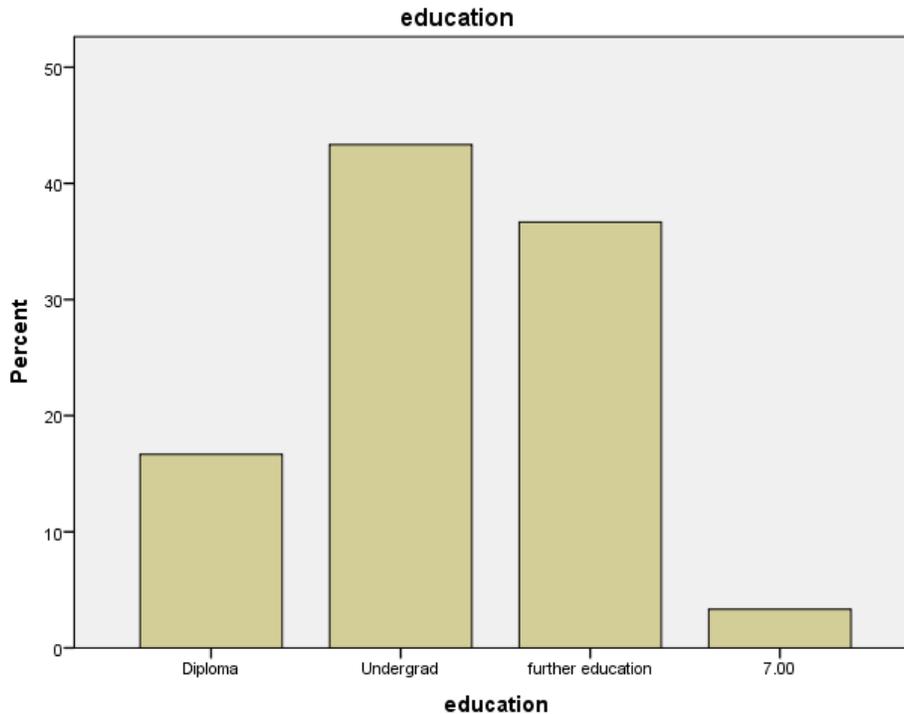
Majority of the respondents were from institutions based in Nairobi because many of the organizations are based in the capital city. First the researcher wanted to know the level of education of the respondents and hence whether there is a direct relationship between the level of e-corruption and the respondents.

## 5.2 Demographics and General information.



**FIGURE 5-1 Age group respondents**

From the demographics of Figure 5-1, those willing to answer the questionnaire were between 20-30 years old. The researcher noted that those older than 40 were not willing to participate in the survey for fear that the information divulged would be used against them. Even after re-assuring them, they were still not willing.



**FIGURE 5-2 Level of education Respondents**

Secondly, the researcher noted from Figure 5-2 that of those of who were over 30 years of age had the least education. Undergraduates were over 45% of the respondents followed by those with further education.

### **5.3 Security Information.**

The researcher further wanted to know, if there were any breaches in information security since the adoption of new technology in the institution and the kind of security measures that have been put in place to prevent a recurrence.

Table 5-1 respondents' views.

**TABLE 5-1 Respondents view on Security status.**

<b>variable</b>	<b>Security information</b>	<b>Yes</b>	<b>%</b>	<b>No</b>	<b>%</b>	<b>Do not know</b>	<b>%</b>	<b>Did not Respond</b>	<b>%</b>
1	Compromised?	11	36.7	13	43.3	6	20	1	3.3
2	Use of Firewalls?	27	90	0	0	2	6.7	1	3.3
3	Use of IDS?	19	63.3	5	16.7	6	20	0	0
4	Use of IPS?	19	63.3	3	10	8	26.7	0	0
5	Dedicated connections to third party providers?	16	53.3	11	36.7	3	10	0	0
6	Remote Access Services?	28	93.3	2	6.7	0	0	0	0
7	Identity Theft Issues?	9	30	10	33.3	10	33.3	1	6.7

The above data shows that there had been breaches in security since the uptake of new technology which in the opinion of the researcher was as a result of failure to tighten security perimeters and as a result was consequential. This was because information is a valuable asset to the organization and thus, needs to be secured. 90 % of the respondents claimed the use of firewall as a physical security feature but still end up being compromised. In the ideal world, there should be a nil breach as it could lead to direct losses to the institution.

Based on the first variable, 36.6% of the respondents indicated that there had been a compromise on their information resources. This comes in the wake of the recent hacking activity of the Kenya government websites.

The second variable indicated that over 90 % of respondents had dedicated third party connections/shared service agreements with various government agencies. A respondent interviewed indicated that there are shared service agreements between the Immigration department and the Kenya Police-Criminal Investigations Department (CID). However with increased connectivity between agencies decreases internal threat and increases external. This is not to say that the internal entity risks are reduced, rather the whole area of risk becomes larger.

When an agencies systems are all in house, under its own control, their reliability was known and well tested. With many more connected systems, agencies may have had to rely on other bodies and their staff to act ethically.

As identity theft was a subject of increasing concern to various law enforcement agencies, the loss of collateral information will doubtless have an impact in that area of e-corruption. Representatives from one institution interviewed believed that identity fraud was closely related to emerging technology corruption, as many more transactions are transacted online or are facilitated through previously registered customer identity.

#### 5.4 Applications information-IFMIS.

The researcher set to find out the perceived level of compliance for business applications that are used by the government agencies. At the time of data collection, IFMIS was the choice of application used by most government organizations. Table 5-2 showed respondents' views.

**TABLE 4-2 Applications Information**

variable	Application information	Yes	%	No	%	Do not know	%	Did not Respond	%
1	The organization uses E-purchasing to	9	30	15	50	6	20	0	0

	buy miscellaneous items?								
2	The organization uses E-procurement to purchase high volume items?	8	26.7	15	50	7	23.3	0	0

Majority of government were still using paper based systems for the procurement of goods and services.

From the respondents the researcher got, 30% were registered with the Integrated Financial management systems-IFMIS where interested bidders are also registered and allowed place tenders for various services and goods. Re-engineering procurement was an opportunity for improving measures for preventing and detecting corrupt purchasing practices. This was an example of how emerging technology can actually decrease the opportunities for corruption.

Further to that, the respondents assessed the software and workstation policies compliance levels using a five point Likert scale with the following units: Strongly agree, agree, neither agree nor Disagree, Disagree, strongly disagree. Maximum points (5) were assigned to the parameter “strongly agree” and the least (0) to the “strongly disagree”. Table 4-3 shows the results of the analysis are shown in the following sections.

**TABLE 5-3 Application Information-IFMIS**

<b>variable</b>	<b>Application information</b>	<b>Strongly agree</b>	<b>Agree</b>	<b>Neither agree nor disagree</b>	<b>Disagree</b>	<b>Strongly disagree</b>
1	Software is properly managed and licenses are well kept.	1	5	5	17	7
2	Password policies are enforced.	0	1	1	14	14
3	Workstation inactivity safeguards (passwords).	1	1	3	17	8
4	Malicious users can access and destroy data.	3	13	5	7	2
5	Antivirus/AntiMalware are up to date	1	10	10	3	6
6	Operating system patches are up to date	1	8	12	3	6

56.7 % of respondents were of the opinion that software purchased by the organization is not properly managed. IT officers interviewed in some institutions openly admitted that they had used company software in their personal machines. Given that the organization buys volume licenses for particular software, they saw no harm in using the product keys in their personal laptops. Some sold to third party individuals.

46.7% of the respondents agreed that there are no password policies that are enforced. A follow up question also indicated that a majority of users share workstations. It was then possible for other users to invade privacy. 56.7 % of the respondents indicated that there are no workstation inactivity safeguards, in case a user goes away for long hours.

## 5.5 BYOD and Email

**TABLE 5-4 Email Respondents.**

<b>variable</b>	<b>Email</b>	<b>Yes</b>	<b>%</b>	<b>No</b>	<b>%</b>	<b>Do not know</b>	<b>%</b>	<b>Did not Respond</b>	<b>%</b>
1	Corporate email accounts?	11	36.7	13	43.3	6	20	1	3.3

As shown in table 5-4, 36.7% of the respondents indicated that they have corporate email accounts. 43.3% indicated they have no email address and 20% do not know if there are corporate accounts issued. This gave an indication that there is still a low uptake of basic but crucial technology.

**TABLE 5-5 Corporate Email Use**

<b>Variable</b>	<b>Email</b>	<b>Strongly agree</b>	<b>Agree</b>	<b>Neither agree nor disagree</b>	<b>Disagree</b>	<b>Strongly disagree</b>
1	Use of personal email for business functions	1	5	11	11	7

The data presented in table 5-5 shows that the use of personal emails for business functions was not allowed in some government institutions. However a section of the respondents were not sure

if it is allowed. This indicated that there were no clear guidelines and policies when making official communications with other agencies.

**TABLE 5-6 WiFi, Enterprise Access systems**

<b>Variable</b>		<b>Strongly agree</b>	<b>Agree</b>	<b>Neither agree nor disagree</b>	<b>Disagree</b>	<b>Strongly disagree</b>
1	Wi-Fi present	5	3	0	10	12
2	Use personal laptops at work?	4	1	1	24	0
3	Access enterprise resources using personal laptops?	2	2	4	21	1
4	Users can access Social media accounts over the corporate network	1	2	3	21	3

From variable one of the table 5-6 above, it shows that a majority of state corporations, parastatals do not have Wi-Fi connections set up. Up to 70% of the respondents indicated this.

The second variable the use of personal laptops at work is strongly prohibited as indicated by the statistics. Up to 80% indicated this in their responses.

The third variable shows that 70% of the respondents are not allowed to use personal laptops/tablets to access corporate enterprise network.

70% of the respondents, according to the fourth variable indicate that accessing social media accounts is not permitted over the corporate network. This includes, Facebook, twitter, YouTube channels.

## 5.6 Literacy, Training and Awareness

**TABLE 5-7. Literacy, Training and Awareness**

<b>variable</b>	<b>Literacy , Training and Awareness</b>	<b>Strongly agree</b>	<b>Agree</b>	<b>Neither agree nor disagree</b>	<b>Disagree</b>	<b>Strongly disagree</b>	<b>Did not Respond</b>
1	Employees are literate.	0	0	3	12	15	0
2	Training includes privacy and security.	0	6	2	18	3	1
3	There is knowledge of HIPAA, COBIT, Sarbanes Oxley frameworks.	3	7	11	5	3	1

Variable one of table 5-7 showed that majority of the users are not computer literate. This is indicated by 50% of the respondents in the institutions. An IT officer in a government hospital interviewed admitted that their immediate supervisor is less computer literate than himself. This shows that there is a knowledge gap within the department especially if the unit relies heavily on technology.

In view of the experts interviewed, the older systems seemed to be less efficient, but more precise. The more IT literate generation appeared to have a greater tolerance to error than before.

63% of respondents disagreed that there isn't enough training given concerning security and privacy. They actually fault the organization for not providing the necessary training.

Variable three showed that 36.7% of the respondents have no idea of any information security frameworks that can be employed to enhance the security posture of the organization.

**TABLE 5-8 Application Training**

<b>variable</b>	<b>Literacy and Training</b>	<b>Quarterly</b>	<b>%</b>	<b>Bi-annually</b>	<b>%</b>	<b>Annually</b>	<b>%</b>	<b>Did not Respond</b>	<b>%</b>
1	Frequency of Application trainings and refresher courses.	8	26.7	4	13.3	15	50	3	10

From the responses, majority -50%- of application training and refresher courses took place on an annual basis followed by quarterly -26.7%- and Bi-annually -13.3%. 10% chose not to respond.

## 5.7 Fraud Deterrence and Prevention

**TABLE 5-9. Fraud Detection and Deterrence responses.**

<b>variable</b>	<b>Fraud Deterrence and Prevention.</b>	<b>Strongly agree</b>	<b>Agree</b>	<b>Neither agree</b>	<b>Disagree</b>	<b>Strongly disagree</b>	<b>Did not Respond</b>
-----------------	---	-----------------------	--------------	----------------------	-----------------	--------------------------	------------------------

				<b>nor disagree</b>			
1	There is an internal IS auditor	2	6	5	11	5	1
2	Employees have meaningful Fraud skill training	1	10	6	12	0	1
3	The organization has an Anti-fraud internal control mechanism.	2	5	7	13	2	1
4	The Institution performs background checks on its employees.	1	4	4	17	3	1
5	Ethics and Anti-corruption Authority are involved in investigations.	1	7	13	8	1	0
6	Whistle blowers are given adequate protection/rewarded	2	3	18	6	1	0
7	Staff morale in the organization is high	2	3	10	12	3	1

In the first variable in table 5-9, the respondents indicated that there was no Information systems auditor known to them. 36.7% disagree and 16.7% strongly disagree.

The second variable indicated that at least 50% of respondents show that there is meaningful training whereas the other half indicates that there was no training.

The third variable, a majority of the respondents disagreed that there is a fraud control mechanism.

The fourth variable showed consensus that in government, there are no background checks were done on new employees. Lack of staff vetting in organizations was central to the e-corruption problem.

The fifth variable showed a majority of respondents were not sure if the ethics and anticorruption authority were involved in the internal investigations.

The sixth variable showed how the respondents answered the questions based on how whistle blowers were treated. 63% of the respondents neither agreed nor disagreed about on how whistleblowers are treated.

The seventh variable shows that staff morale in the organizations was low. 50% of respondents indicate this. Low staff morale are breeding grounds for e-corruption.

**TABLE 5-10 Fraud Deterrence and Prevention**

<b>variable</b>	<b>Fraud Deterrence and Prevention.</b>	<b>Yes</b>	<b>%</b>	<b>No</b>	<b>%</b>	<b>Do not know</b>	<b>%</b>	<b>Did not Respond</b>	<b>%</b>
1	Are there acceptable and unacceptable behavior outlined by the institution?	22	73.3	7	23.3	1	3.3	0	0
2	Do you have hotlines for reporting fraud	8	26.7	20	66.7	2	6.7	0	0
3	Do you use Computer Aided Auditing Techniques?	9	30	7	23.3	14	46.7	0	0

The above data in table 5-10 indicated that from variable one, government agencies have some form of acceptable and non-acceptable behavior (with respect to information systems governance) in its policies.

The second variable showed that government agencies do not have a hotline for reporting fraud. 66.7% gave a negative report concerning hotlines. 8% indicated the presence of a hotline number

The third variable indicated that 23.3% of government agencies did not use Computer aided audit Techniques (CAAT). 46.7% did not know if there exists such auditing techniques or whether the institution has the software for performing auditing.

## 5.8 Physical Protection

**TABLE 5-11. Physical protection of Resources.**

variable	Physical protection	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Did not Respond
1	Sensitive computer resources are locked behind office doors.	0	1	2	16	10	1
2	Individuals leaving the organization return equipment loaned to them.	0	0	1	19	10	0

The first variable in table 5-11 indicated that at least 88% of the respondents are of the opinion that sensitive resources were not well secured.

In the second variable, majority of the respondents indicated that individuals who leave the organization do not return the equipment's loaned to them.

**TABLE 5-12. Access control Types**

variable	Physical protection	Security guards	%	Cipher locks	%	ID badge	%	Biometrics	%	Did not respond	%
1	Access controls	14	46.7	6	20	6	20	3	10	1	3.3

	that apply to the physical protection.										
--	--	--	--	--	--	--	--	--	--	--	--

The data collected in table 5-12 showed that from the respondents, that government agencies preferred to use security guards and locks as opposed to biometrics and RFID badges.

**TABLE 5-13 Disposal of media**

variable	Physical protection	Shredding	%	burning	%	others	%	Did not respond	%
1	Procedures for destroying printed materials.	26	86.7	3	10	0	0	1	3.3

The data collected from table 5-13 indicated that a majority of government agencies prefer shredding as a method of destroying printed information.

## 5.9 Ethics

**TABLE 5-14. Ethics responses**

variable	Ethics	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Did not Respond
1	Senior management demonstrates high ethics.	1	1	6	18	3	1

2	My co-workers demonstrate high ethics.	0	2	4	21	3	0
3	I am aware of allegations involving purchase or sales fraud.	1	15	10	3	1	0

The first variable in table 5-14 indicated that of all the respondents, 60% did not think that management had high ethical behavior.

The second variable showed that the respondents did not trust their fellow coworkers. They demonstrate unethical behavior.70% of the respondents alluded to this.

The third variable showed how a majority of the respondents-50% are aware of fraud activities that are IT related- that take place when systems are in use.

**TABLE 5-15 Ethics.**

<b>variable</b>	<b>Ethics</b>	<b>Yes</b>	<b>%</b>	<b>No</b>	<b>%</b>	<b>Do not know</b>	<b>%</b>	<b>Did not Respond</b>	<b>%</b>
1	Has management requested for an override of an internal control	3		8		18		1	

From table 5-15, the respondents 60% indicated that they do not know if there had been an incidence involving management requesting for an override.10% indicated that they had encountered management interference where as 13.3% indicated that management had not interfered with internal controls.

**Table 5-16 Personnel Involved in fraud**

<b>variable</b>	<b>Ethics</b>	<b>Account s</b>	<b>%</b>	<b>Senior Mgt</b>	<b>%</b>	<b>IT analyst</b>	<b>%</b>	<b>others</b>	<b>%</b>	<b>Did not respond</b>	<b>%</b>
1	Key personnel likely to be involved in unethical activities.	10	33.3	11	36.7	5	16.7	3	10	1	3.3

From the data in table 5-16, senior management was key abusers of technology with 36.7% of respondents alluding to this. They were closely followed by accountants at 33.3%.

## **5.10 Methods used to Perpetuate E-corruption**

### ***5.10.1 Telecommunications***

Current fraud trends in the telecommunications industry.

#### *1. Theft of stored value technology*

Mobile service providers had a loyalty program to reward its customers for its continued use of their services. It is available to both prepaid and postpaid. Customers earned loyalty Points as they use the existing services on offer i.e. voice calls, data, text messaging and mobile money transfer service. As at August 2014 a particular service provider had accumulated 60 billion points from its subscribers.

Insiders hived off reward points from unsuspecting subscribers and transferred them to other accounts for eventual withdrawal for personal use. The rewards in the scheme include Data, Talk time, text messages, MMS bundles, phones, modems, laptops. An interviewee who is an insider noted that majority of those involved preferred to ‘accumulate’ points to buy laptops and tablets rather than redeem for talk time and text messages as they were too cheap.

#### *2. Internet Bundles fraud*

Employees in a telecoms company defrauded the company by selling internet bundles to third parties. An employee needed to know the amount of internet bundles consumed within a specified period in the entire network. This employee colluded with revenue assurance team to know the expected monies. Given that acceptable margins are allowed for accuracy, employees used this margin to sell internet bundles to other parties at cheaper rates. This is best exemplified by the use of ‘Soko nyeusi’ Facebook page. In this page, clients can buy items off the black market at throw-away prices and internet bundles happen to be one of them. A 3GB data bundle that normally retails for 1,999 would cost 1,500 in soko nyeusi.

### ***5.10.2 The Education Sector***

The exploitation of emerging technology in the education sector is at an all-time high. The ease with which fake report cards can be got for a price seems to indicate that the racket is well-oiled

machinery and there's a steady demand for it. The racket is also a pointer to the desperation of the unemployed who needed some papers to ensure they get a job by hook or crook.

*1. Falsification of Continuous Assessment Test (CAT) marks*

This happened when the lecturer did not administer CAT marks and ended up copy-pasting CAT marks from a previous year and giving students undeserving marks.

*2. Examination cheating*

With more lecture notes being presented in PowerPoint and pdf formats, students with high end phones were able to access all class notes which were used for cheating.

*3. Defeating automatic plagiarism detection softwares*

There has been a move away from unseen written examinations and most university degree courses are assessed through term papers, which made it more tempting to commit plagiarism. Increasingly, students and predatory publishers are learnt new tricks to make it more difficult to detect plagiarism in their writings and published articles. A trick used is the find-and-replace feature that converted all spaces in a document to a character from a foreign characters set, and then used find-and-replace to convert that character to the color white, so it appeared as a space again.

*4. Express service websites*

Students accessed websites that offer express services, such as assignment writing, research proposals. All the while many claimed that the work was written by people with post-graduate qualifications. These came in the form of bespoke essays/reports.

### ***5.10.3 The Health Sector***

The abuse of electronic health records was faulted as a key contributor towards e-corruption in the health sector. Fraudulent use of electronic medical records was used to illegally inflate billings.

Two abuses were noted:

One was “cloning,” in which a doctor cuts and pastes information from a patient’s electronic record that suggested that the services were performed again at the later date, or possibly used the same documentation for other patients as well. The other is “upcoding,” in which hospitals exaggerated the intensity of care provided or the severity of a patient’s condition to justify higher billings.

Data held in silos would never be used for insurance purposes, stating that any such actions would represent a criminal offence. Actuaries who obtained the information used it to provide guidance to insurance companies about how to set their prices for critical illness cover, suggesting higher premiums could be justified for most customers below the age of 50.

In another interview, the researcher discovered that unscrupulous providers can bill for extra services if they report false serious diagnoses or procedures performed. For example, if a patient reportedly fell inside a hospital, a crooked provider could intentionally misdiagnose her with head trauma requiring the (unnecessary) use of a computed tomography (CT) scan and/or blood tests.

The reasons an employee took confidential company information varied from being benign and misguided to intentional for the purposes of personal gain. Other reasons cited included the potential usefulness of the data in the future, the employees’ sense of ownership around what they created; the belief that the company cannot trace the theft back to them whereas some claimed it was an accident.

#### ***5.10.4 Energy sector***

##### *1. Metering Ratio adjustment*

This form of fraud was done by unscrupulous meter readers, system analysts and the tenants. The meter readers falsified records which upon reaching the metering department generate a bill based on an adjusted metering ratio. If the bill was say 2 million, the ratio can be halved and the tenant paid only One million. The resulting deficit was used as kickback to the accomplices. This mainly applied to high power consumers.

##### *2. Kenya Power Pre-paid tokens fraud.*

Kenya power recently introduced pre-paid tokens as a way to maximize on revenue collection with minimum defaulters. The pre-paid power meters used a key system. Normally people would visit a shop to put credit on their key, which they then take home and slot into their meter.

For first time installations, contractors colluded with landlords to have the meters installed and bypassed but are not registered in the key generating system. The landlords pay a one-off fee to the contractors who make the installation.

#### ***5.10.5 Financial sector fraud***

##### ***Banking***

###### ***1. Transfer of funds overnight.***

A credit analyst from a local bank interviewed told of a scenario where analysts with high security access level abused their positions to transfer funds overnight from rich dormant accounts to other accounts and then transfer back after the intended purpose for which it was put there. He went on to explain that one of the visa issuance requirements is that the applicant should have a certain amount of monies in their accounts. This scam fits into place with that requirement. Once the visa requirements were met, the money is returned.

###### ***2. Bank tellers and identity theft***

A Bank teller used her position to fraudulently acquire customer information and pass account holders information to conspirators. The bank teller looked up bank account holder information on the computer system without authorization. That information was then disclosed to her co-conspirators who ordered cheque books on account holders' accounts and cashed cheques.

## **CHAPTER SIX. VALIDATED E CORRUPTION CONTROL FRAMEWORK**

The researcher proposed a framework for the control of e-corruption in the public sector based on two domains, 5 Sub-domains, 30 Processes and 73 Control activities.

The framework is an amalgamation of the following frameworks:

1. COBIT 5 for information Security
2. The Information management security framework for the government of south Australia
3. ISO/IEC 27001:2013
4. Musa et.al 2012, in their assessment of e-corruption level in Malaysia

### **6.1 The structure of the validated framework**

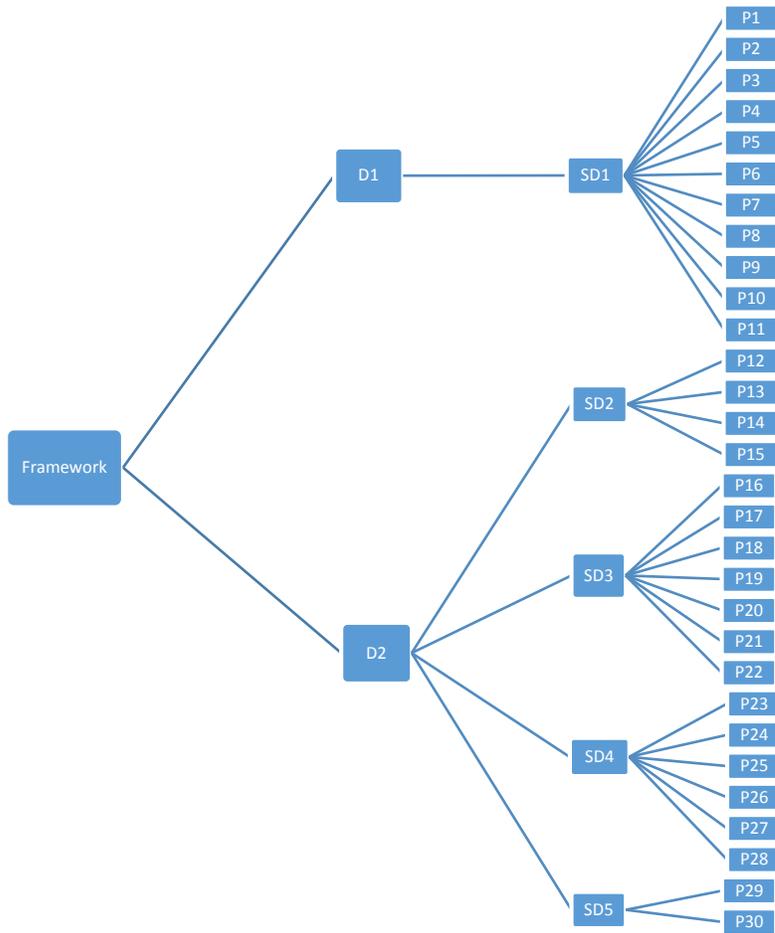
Domain, D1: Technical Control, which highlights the security measures that should be implemented to ensure security of information.

D2: Social Controls, this is composed of four sub domains: Ethics, internal benchmarks, Employee value and policy.

Thirty processes and Seventy three control objectives are defined in relation to the data collected in the questionnaire and specific objectives.

Control is approached by looking at the information necessary to support the government objectives when ensuring information security. Each process summarizes several activities which can be used to design an appropriate control task.

Figure 6-1 shows the E-corruption control framework.



**Figure 6-1 Control framework**

**DOMAIN 1 SUBDOMAIN 1**

<b>DOMAIN</b>	<b>SUB-DOMAIN</b>	<b>PROCESS</b>	<b>ACTIVITY</b>
D1- TECHNICAL	SD1-SECURITY	P1- PHYSICAL SECURITY PERIMETER	A1- Information processing facilities should be well housed and information access levels are to be layered.
		P2-PHYSICAL ACCESS CONTROLS	<p>A2. Access rights to secure areas should be reviewed and updated on a regular basis. Documented evidence of the review should be retained. These reviews should be performed at least annually, or more frequently based on a risk assessment that takes into account such factors as the level of turnover of personnel and the classification of the information asset being protected.</p> <p>A3. Dual authentication controls (e.g. Swipe cards plus PIN) should be used to authorize and validate all access.</p> <p>A4. All personnel should wear Photo ID badges. Time</p>

			<p>of entry and departure of visitors should be logged. Visitors should be supervised; security requirements and emergency procedures should be conveyed to visitors (excepting those who have already been briefed on prior occasion).</p> <p>A5. Authentication controls (such as an access card with PIN) should be employed where feasible and an audit log should be maintained commensurate with the access granted.</p>
		<p><b>P3-SECURING OFFICES,CUBICLES</b></p>	<p>A6. Intruder prevention and detection systems for physical incursions, including alarms should be installed and regularly tested.</p> <p>A7. Locations of sensitive information processing facilities and other areas should not be included on directories and phone books, with special consideration given to publicly accessible</p>

			directory information such as that located in lobbies, foyers and stairwells
		<b>P4- USER REGISTRATION</b>	<p>A8. Procedures should ensure that user IDs are not reissued to other users, to limit the potential for unauthorized access being inadvertently granted.</p> <p>A9. Periodically scan for duplicate/redundant user IDs or accounts and remove or block access until resolved.</p>
		<b>P5-USER PASSWORD MANAGEMENT</b>	<p>A10. Additional technologies for user identification and authentication, such as biometrics and/or hardware tokens, should be considered.</p> <p>A11. Guidelines on the selection of strong passwords should be included in security awareness briefings and as part of a comprehensive Information Security Awareness Program.</p>

		<p>P6-PASSWORD USE</p>	<p>A12. All passwords used to gain access to an information system should be treated as though they are classified at least at the same level as the classification of the system they are used to access.</p> <p>A13. Passwords include all forms of secret authentication information assigned to a user (such as group authentication or individual user id authentication information) for the purposes of this standard.</p>
		<p>P7-NETWORK ACCESS CONTROL</p>	<p>A14. For shared network infrastructure, clear responsibilities and procedures should be established by the network manager to maintain security in a manner that protects the interests of all institutions that rely on that infrastructure.</p> <p>A15. Standards should be established regarding</p>

		<p>acceptable use for Internet services (e.g. web, e-mail, news groups) in terms of business versus personal use, as well as consideration of issues regarding objectionable material.</p> <p>A16. The standards should also consider issues that relate to capacity implications for specific types of network traffic. This may include limiting the size of e-mail attachments that are acceptable to the institution. It may also include limiting or banning streaming audio and video services and any other identified high-bandwidth services that are not required to support authorized business use.</p> <p>A17. Users should only be provided with direct access to services that they have been specifically authorized to use. This control is particularly important for network</p>
--	--	---

			<p>connections to sensitive or critical business applications, or to users in high-risk locations (e.g. public or external areas that are outside the institutions management and control).</p>
		<p><b>P8-DEDICATED NETWORK CONNECTION PATHS</b></p>	<p>A18. In highly sensitive information processing environments, minimizing risk of message interception may be accomplished by restricting the number of alternative routes that are available to users/terminals and/or limiting network traffic to devices that are subject to appropriate physical and logical security.</p> <p>A19. Systems and/or network interconnections that require dedicated path access controls must not be attached to wireless LAN and/or public broadband services.</p> <p>A20. Remote access devices (e.g. broadband modems and VPN gateways) should be</p>

			<p>attached via a secure gateway device that provides appropriate filtering and authentication controls commensurate to the classification of the information assets being accessed.</p> <p>A21. Encryption and/or cryptographic controls should be enabled where possible per the guidance and requirements described in this framework.</p> <p>A22. A two factor authentication process at the network perimeter should be adopted for all external connections to an institution server or PC.</p> <p>A23. Consideration should be given to restricting access for external connections to specific computer systems and/or from specific locations (sources) as well as restricting the time periods</p>
--	--	--	--

			<p>that such connections can be used.</p> <p>A24. A facility should be implemented that can limit the number of unsuccessful attempts at establishing an external connection before the user identifier is suspended.</p>
		<p><b>P9-EXTERNAL CONTRACTORS</b></p>	<p>A25. Responsible entities may embed the use of an assessment tool as a component of the selection process for external organizations.</p> <p>A26. Responsible Parties should establish individual confidentiality agreements with the staff of contractors.</p> <p>A27. Third parties and their employees, including sub-contracted service providers, who require access to security classified information must be security cleared to the appropriate level.</p>

			<p>A28. Appropriate authorization should be obtained from the relevant manager (typically the Business Owner) before users can obtain remote access.</p>
		<p><b>P10-BYOD CONTROLS</b></p>	<p>A29. Ensure user education programmes are in place, and users' responsibilities are clear.</p> <p>A30. Generate acceptable-use policies and security operating procedures for users' devices.</p> <p>A31. Put processes in place for auditing users' behavior (i.e. trust and verify).</p>

## DOMAIN 2 SUBDOMAIN 2

DOMAIN	SUB-DOMAIN	PROCESS	ACTIVITY
D2- SOCIAL	SD2-POLICY	P11-POLICIES	<p>A32. Information Security Policy that is developed by an institution must be aligned with Kenya National ICT Master plan.</p> <p>A33. Information security policies (as distinct from standards and controls) must comply with the Kenyan Government Information Security Manual.</p> <p>A34. Information security policies that deal with National Security classified information or other highly sensitive information based upon classification must be restricted to audiences on a “need-to-know” basis.</p>
		P12-INTELLECTUAL PROPERTY RIGHTS AND LICENSING	A37. In circumstances where information systems are used to solicit information from members of the public (e.g. in an e-commerce or e-government scenario), informative messages should be included at the point of information capture, to make

			<p>the individual aware of the intended use of the information, who will use the information and any legal authority or requirements to collect the information.</p> <p>A38. Institutions that are involved in transmitting, soliciting and collecting personal information via websites should also have regard for the Privacy Guidelines for Kenya Government websites.</p> <p>A39. Access control lists for electronically stored personal information should be carefully designed such that only those personnel that have a need-to-know are able to access the information, consistent with the stated purpose of collection and disclosure of the information.</p> <p>A40. Responsible Parties must define 'Authorized Access' for all data, including who has access, the level of</p>
--	--	--	--

			authority required, and the level of access allowed.
		P13-PROTECTION OF GOVERNMENT RECORDS	<p>A41. When employing personnel, the Responsible entity should perform appropriate security and / or reference checks to verify their credentials.</p> <p>A42. A security clearance as defined by the criminal investigations department should be obtained by the applicant.</p> <p>A43. All personnel should be subject to a security vetting process.</p> <p>A44. Appropriate checks (e.g. Police security checks) should be carried out upon appointment or promotion to a position where the applicant will have access to sensitive Information Processing Facilities, (e.g. financial information or critical infrastructure). For personnel holding positions of</p>

			considerable authority these checks should be repeated regularly.
--	--	--	---

**DOMAIN 2 SUBDOMAIN 3**

<b>DOMAIN</b>	<b>SUB-DOMAIN</b>	<b>PROCESS</b>	<b>ACTIVITY</b>
D2- SOCIAL	SD3-EMPLOYEE VALUE	P14-PRE-EMPLOYMENT	<p>A41. When employing personnel, the Responsible entity should perform appropriate security and / or reference checks to verify their credentials.</p> <p>A42. A security clearance as defined by the criminal investigations department should be obtained by the applicant.</p> <p>A43. All personnel should be subject to a security vetting process.</p> <p>A44. Appropriate checks (e.g. Police security checks) should be carried out upon appointment or promotion to a position where the applicant will have access to sensitive Information Processing Facilities, (e.g. financial information or critical</p>

			<p>infrastructure). For personnel holding positions of considerable authority these checks should be repeated regularly.</p>
		<p>P15-DURING EMPLOYMENT</p>	<p>A45. Each Responsible Party should ensure that confidentiality and/or non-disclosure agreements are in place for all staff, contractors and/or sub-contractors that seek or have in place access to Kenya Government information, materials and/or intellectual property that is not intended for public access or circulation</p> <p>A46. Institutions should note that all personnel employed under the auspices of the <i>Public Service Commission Act 2012</i> are adequately bound to the confidentiality and non-disclosure requirements of that legislation thus alleviating the requirement for additional non-disclosure undertakings.</p>

		<p>P16-INFORMATION SECURITY AWARENESS AND EDUCATION</p>	<p>A47. A copy of the Agency's information security policies should be issued to all new personnel as they join and to all existing personnel.</p> <p>A48. Security reminder messages should be posted in secured areas and/or regularly communicated to personnel according to the intended audience and or classification of the notifications.</p> <p>A49. Personnel should be made aware of the security classifications of the information assets that they use, and that they handle them appropriately.</p>
		<p>P17-DISCIPLINARY PROCESS</p>	<p>A50. Where appropriate, discipline should be in line with the relevant employment act conditions. For employees</p>

			not covered under this, discipline should be in line with contract terms and conditions.
		P18-CESSATION OF CHANGE EMPLOYMENT OR OF	<p>A51. Responsible Parties should implement procedures concerning employment termination, or change of duties in alignment with the implementation guidance.</p> <p>A52. Responsible Parties should ensure that important knowledge or operational skills have been transferred to other resources prior to departure of the employee and/or contractor.</p>
		P19-RETURN OF ASSETS	A53. Responsible Parties must establish procedures and processes to transfer Official Information contained on personal (home office or BYO) devices such as home computers and mobility devices to agency owned information assets. Such procedures shall include

			a provision for the secure erasure of all official Information (other than PUBLIC) that is stored on the personal device.
--	--	--	---

**DOMAIN 2 SUB-DOMAIN 4**

<b>DOMAIN</b>	<b>SUB-DOMAIN</b>	<b>ACTIVITY</b>	<b>PROCESS</b>
D2- SOCIAL	SD4- INTERNAL BENCHMARKS	P20-PROTECTION FROM MALICIOUS SOFTWARE AND SCRIPTS	<p>A54. Institutions should implement a strategy for scanning or otherwise monitoring ongoing compliance with licensing requirements.</p> <p>A55. Institutions should establish a formal process for the authorization of software purchases such that records are appropriately maintained and unauthorized software can be identified and actioned.</p> <p>A56. User awareness and training (Information Security Awareness programs) should be periodically undertaken to inform users of the risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken.</p>

		<p>P21-INFORMATION BACKUP,ARCHIVAL AND RETRIEVAL</p>	<p>A57. Institution employees are responsible for backing up all data stored on workstations that are not connected to the network (e.g. portables used outside the office) and they should be made aware of this responsibility.</p> <p>A58. Back-up information may need to be encrypted according to the sum of its classification, sensitivity and/or importance to the business.</p>
		<p>P22-PROTECTION AND DISPOSAL OF MEDIA</p>	<p>A59. Disposal of information assets must be logged.</p> <p>A60. Where re-use after media sanitization is impractical, information assets must be disposed of in a secure manner (e.g. secure destruction and/or incineration)</p> <p>A61. All information and software should be removed</p>

			<p>totally (i.e. secure-erased (a.k.a. “wiped”) or overwritten, not just deleted from data storage media (e.g. hard drives, discs), which are to be disposed of by the institution.</p> <p>A62. When equipment is sold, or otherwise disposed of, data on any storage devices should be effectively erased.</p>
		<p><b>P23-INFORMATION HANDLING PROCEDURES</b></p>	<p>A63. Personnel should be made aware of the security classifications of the ICT assets that they use, especially the data and documents they deal with, and that they handle them appropriately.</p> <p>A64. Responsible entities should ensure that documented information handling procedures are communicated to employees and contractors or sub-contractors as part of a comprehensive Information</p>

			Security Awareness program.
		P24- SOCIAL MEDIA AND MESSAGING RISK MANAGEMENT	<p>A65. Quarantining messages for closer investigation (policies and procedures need to address the process to follow for quarantined messages).</p> <p>A66. Limiting the message size (including attachments) to prevent un-necessary resource waste (e.g. Storage and network capacity).</p>
		P25- E-COMMERCE CONTROLS	<p>A67. Responsible entities should protect information involved in online transactions using appropriate technical controls.</p> <p>A68. Liability for fraudulent and erroneous E-Commerce transactions should be risk assessed and may be mitigated through the use of strong Authentication, Authorization, Non-Repudiation, Integrity and Confidentiality controls.</p>

			A69. Security and control measures that are adopted by institutions should also take into account the implications of bad publicity that may result from failed security measures that compromise confidential information, or the provision of incorrect or misleading information on the institution web site.
--	--	--	--

**DOMAIN 2 SUB-DOMAIN 5**

<b>DOMAIN</b>	<b>SUB-DOMAIN</b>	<b>ACTIVITY</b>	<b>PROCESS</b>
D2- SOCIAL	SD5-ETHICS	P26-ACCEPTIBLE USE POLICIES	A70. Institutions should have acceptable use policies. Clearly written policies that outline permissions and restrictions will be made known to all employees.
		P27-INTELLECTUAL PROPERTY RIGHTS AND LICENSING	A71. Software should not be copied except for authorized installation and backup purposes.  A72. Software should not be copied for personal use unless it is expressly permitted by

			<p>the institutions licensing agreements and approved by senior management.</p> <p>A73. Compliance with software license requirements and terms of use therein shall be monitored.</p>
--	--	--	--

# **CHAPTER SEVEN: SUMMARY OF RESEARCH, OUTCOMES AND RECCOMENDATIONS**

## **7.1 General Information/Demographics**

Theoretically, education's effect on e-corruption participation is ambiguous. Education has been shown to reduce illegal behavior, increased staff awareness, increased civic responsibility (Heynemann, 2008; Oreopoulos & Salvanes, 2009). All these outcomes suggest that education attainment should lead to less e-corruption participation.

However, more educated individuals are more likely to have better technology skill set to manipulate information and defraud the institution that they work for. This poses a greater risk for the public sector as the increased use of technology offers an opportunity for illegal conducts to arise , moreover with the increased distribution of transactions across jurisdictions, networks and internet sites reduces the potential for systematic regulatory initiatives to be used.

Majority of those with the required technical knowhow are aged between 31-40 years of age. These are considered to be those with the skills to defraud the institutions and are educated to undergraduate level.

For those institutions that are adopting technology but have staff that are not well trained to use the systems, a relentless campaign to train them to use the technology appropriately to avoid accidental or deliberate mishaps on the system.

## **7.2 Security Information**

From the survey carried out, majority of the government institutions do not have a proper security posture. Hosts, networks and applications need to be hardened to ensure confidentiality, Integrity and availability of information.

1. Hardware security

Government agencies need to ensure that computer hardware is adequately protected using appropriate firewalls (hardware or software) to prevent external forms of abuse.

2. Physical security

Government institutions rely mainly on the use security guards for the protection of their premises and RFID locks for areas where servers are stored. In some institutions, machines containing sensitive information were left out in open cubicles .Poor physical security over computer equipment was found to be a common factor in allowing e-corruption to occur.

### 3. Social engineering controls

Social engineering is the art of manipulating people to give up confidential information. Some techniques used to carry out social engineering include shoulder surfing, dumpster diving, mail-outs, forensic analysis.

Core controls that can be implemented (Allen, 2007) include: Security policy, Education/Awareness, Good security architecture, limiting data leakage, and incidence response strategy and security culture.

### 4. Tracking and surveillance

Employees' use of computers and their on-line activities can be monitored through the use of software such as K-9 Web protection by Bluecoat which logs usage and allows managers to know, for example, whether staffs have been using the Internet for non-work-related activities, or if funds are being moved to specified accounts for unauthorized purposes. Ideally, agreed procedures and rules should be established which enable staff to know precisely the extent to which computers are able to be used for private activities, if at all.

### 5. User authentication

Authentication of one's identity is crucial in preventing e-fraud. At present most authentication procedures involve the use of passwords or PINs. Ensuring that these are used carefully and are not able to be compromised is a fundamental fraud control measure.

Implementation of two and three factor authentication methods where biometrics come into play to add more security to systems. Although such systems achieve much greater levels of security than those which rely on passwords, they are expensive to introduce and raise potential issues in terms of privacy and confidentiality of the personal data stored on government computer networks.

### 6. Theft of intellectual property, software, hardware

Government employees have access to and make use of various forms of intellectual property in connection with their employment. In particular the IT officers in government institutions are responsible for using government-owned software on personal computers for private purposes.

### **7.3 BYOD and Email**

The combination of increased data connectivity and the consequent need to be connected anywhere and everywhere has prompted a change in employee attitude towards the use of their devices to access work-related documents. A good example is checking work emails on their mobile device while waiting in a queue.

The I-Phone, blackberry and emerging android phones have enormous storage capacity and are easily connected to the corporate email systems. The combination of storage, data access and ubiquity make a mobile device an ideal method of stealing data.

Email is also an efficient way to take confidential data. Employees can easily mail large amounts of data to personal accounts and then access it from anywhere. By using a personal email account, the employee not only circumvents the corporate email system but the account is beyond control and scope of investigations.

Most government organizations in Kenya have not yet embraced the BYOD program. Despite the perceived benefits of using the program, from the responses in the questionnaire, the respondents seem not to be aware of a BYOD program. In the event that government is to implement such a program, there should be a well-articulated policy in place.

The researcher believes that even though the public sector is largely reluctant to embrace BYOD, many of its agencies will ultimately be later, rather than non-adopters of the policy.

However certain ministries such as the defense may not be adopting such technology soon. This is because of the sensitivity of the agency's operations.

### **7.4 Regulatory Responses**

The government developed a national ICT policy in 2006 to provide a framework for developing and maintaining an effective information technology environment. Some of the organizations examined are not aware of the national ICT policy and have continued to implement ICT systems without referring to the policy. This has exposed the organization to serious vulnerability to information systems security violations.

*Safeguards against E-Corruption and Inefficiencies.*

1. Awareness programmes of National ICT Policy.

The ministry of information and other arms dealing with IT should educate public officers on National IT policy adherence. The policy should address the global e-government strategies and safeguards necessary to prevent e-corruption. The ministry should create awareness on the policy to public institutions. Compliance with the policy is imperative and should be disseminated to public sector employees.

2. Institutional ICT Policy

It is necessary for each department to develop ICT policies that are in line with the national policy. The policies should stipulate disciplinary measures against a member of staff involved in fraud.

3. Codes of Conduct

In addition to having e-corruption control policies in place as part of a general risk management strategy, codes of conduct are able to provide not only a widely disseminated statement of existing laws and acceptable practices which help to create a culture of compliance within specific industries, but also often include dispute resolution procedures and sanctions for non-compliance with the rules in question.

4. Information And Education

Once policies have been established they need to be communicated to staff and fully explained in order to prevent misunderstandings as to their meaning and effect. Often policies are established

but not adequately implemented or publicized. Providing educational material concerning fraud prevention and reporting procedures on internal agency Websites is also now widely used in the public sector.

## **7.5 Conclusion**

This section aims at providing an overall conclusion regarding the findings of this study. This is based on the findings analysis from the previous chapters. The focus of the research was to develop an e-corruption control framework for the public sector.

The main research objectives were to:

- To identify the loopholes used to perpetuate e-corruption in the public sector.

Based on the literature review and Interviews carried out, the researcher discovered various loopholes that are being exploited by public officials. These loopholes are used to defraud the institution. This objective was met by having a series of interviews with industry experts. Findings from the study indicate that insiders with super user privileges use their positions to abuse institution resources. The Ministries outlined were those of Information Communication and Technology, Judiciary, Health, Finance, Energy.

This objective was met and detailed in the chapter 5 and literature review.

- To develop an E-corruption control framework for the public sector.

This research objective was met by drafting the following framework:

Domain, D1: Technical Control, which highlights the security measures that should be implemented to ensure security of information.

D2: Social Controls, this is composed of four sub domains: Ethics, internal benchmarks, Employee value and policy.

Thirty processes and Seventy three control objectives are defined in relation to the data collected in the questionnaire and specific objectives.

Control is approached by looking at the information necessary to support the government objectives when ensuring information security. Each process summarizes several activities which can be used to design an appropriate control task.

- To Test and validate the Framework.

This research objective was met by ethnographic testing of the framework. Once the framework was drafted, two parastatals –Kenya Broadcasting Corporation (KBC) and Kenya Ports Authority were chosen as test beds for the framework. The results of the test proved that the framework can be employed in the public sector and will be useful for policy implementation

## **7.6 Implications for Future Research**

After the research, I found out that a comparative analysis framework for different government agencies can be formulated to draw the levels of e-corruption in the different agencies. I think the research has enough ideas for future researches that can be used for implementing other security frameworks. Of equal concern is the study of BYOD security frameworks for both private and public institutions. As more organizations are adopting technology, the use of personal gadgets in offices will be the norm. A concrete study on this should be done.

## REFERENCES

- Allen, Malcolm.(2007) Social Engineering. A means to violate a computer system .Sans Institute InfoSec Reading Room.
- Ambaye, D. and Hayman A. (1995). Causes of IT failures in teams. In Proceedings of the Third European Conference on Information Systems, 1181-1192, Athens, Greece.
- A.Seetharaman, M. Senthilvelmurugan and Rajan Periyannayagam, “Anatomy of computer accounting frauds”, Managerial Auditing Journal, 2004, Vol 19:8/9, ABI/INFORM Global.
- Arce, I. (2003). The weakest link revisited [information security]. IEEE Security & Privacy, 1 (2), 72-76.
- Atkinson, W.(2000). Strategic Sourcing and E –Procurement. Austin, TX: University of Texas Press.
- Attaran, M and A. Sharmin. (2002). ‘Catch the wave of e –procurement’, Industrial Management, 1 –6.
- Backus, M. 2001. E-Governance and Developing Countries - Introduction and Examples. IICD Research Report No. 3.
- Bowen, B., Devarajan, R. and Stolf, S. (2012). *Measuring the Human Factor of Cyber Security*. Supplement 5, article 2. Homeland Security affairs.
- Center for Applied Philosophy and Ethics, (2001). *eCorruption Vulnerabilities in the NSW Public Sector*. NSW: Independent Commission Against Corruption.
- Computerweekly.com, (2014). *Government approves BYOD for public sector staff*. [online] Available at: <http://www.computerweekly.com/news/2240206170/Government-approves-BYOD-for-public-sector-staff> [Accessed 29 Jun. 2014].
- Chatzidimitriou, Marios and Adamantios Koumpis (2008). “Marketing One-stop E-Government Solutions: the European OneStopGov Project”. *IAENG International Journal of Computer Science*, 35:1, IJCS\_35\_1\_11. (Advance online publication: 19 February). [http://www.iaeng.org/IJCS/issues\\_v35/issue\\_1/IJCS\\_35\\_1\\_11.pdf](http://www.iaeng.org/IJCS/issues_v35/issue_1/IJCS_35_1_11.pdf)
- Connected Kenya – 4 ways Social Media Can Improve Service Delivery in Government . 2014. *Connected Kenya – 4 ways Social Media Can Improve Service Delivery in Government* . [ONLINE] Available at: <http://www.connected.go.ke/4-ways-social-media-can-improve-service-delivery-government/>

Chêne, M. (2009). *The Implementation of Integrated Financial Information Management Systems (IFMIS)*. Transparency International.

Ernst & Young, (2013). *Insight and Governance, Risk and Compliance Report*. Ernst & Young.

Dhillon, G and Moores, S, Computer Crimes: Theorizing about the enemy within, *Computers & Security*, Vol 20, No 8, pp. 715-723, 2001.

Ethics and Anti-corruption Commission, (2009). *ICT and e-corruption*.

Garcia-Murillo, M. & Vinod, H.D. 2005. Opening to the World: The Effect of Internet Access on Corruption. Available from <http://web.si.umich.edu/tprc/papers/2005/478/ppr%20corruption%200.pdf> (Accessed 23 January 2007).

Grabosky, P, Smith RG & Dempsey G 2001, *Electronic theft: unlawful acquisition in cyberspace*, Cambridge University Press, Cambridge.

Grönlund, Å. (2002) *Electronic Government – Design, Applications, and Management*. Hershey, PA: Idea Group.

Grupe, F.H., Hensley, J.M. and Yamamura, J.H. (1998). Watching systems in action: security at the periphery. *Information Management & Computer Security*, 6 (4), 155-159

InformationWeek, (2014). *Social Media In Government: Managing The Risks - InformationWeek*. [online] Available at: <http://www.informationweek.com/regulations/social-media-in-government-managing-the-risks/d/d-id/1112168?> [Accessed 1 Jul. 2014].

K. Mitchell, “Instituting e-procurement in the public sector,” *Public Management*, pp. 21-25, November 2000.

Kaufmann, D., Kraay, A. & Mastruzzi, M. 2003. Governance Matters III: Governance Indicators for 1996-2002. Available from [http://siteresources.worldbank.org/INTWBIGOVANTCOR/Resources/govmatters3\\_wber.pdf](http://siteresources.worldbank.org/INTWBIGOVANTCOR/Resources/govmatters3_wber.pdf) (Accessed 23 January 2007).

Kenya Information and Communication Act, 2009(1998). Communications Authority of Kenya [Kentrade.go.ke](http://www.kentrade.go.ke), (2013). *Objectives - KenTrade* -. [online] Available at: <http://www.kentrade.go.ke/index.php/single-window-system/objectives> [Accessed 31 Jun. 2014].

KICTANET, (2012). *103 Government of Kenya websites hacked overnight*. [online] Available at: <http://www.kictanet.or.ke/?p=5796> [Accessed 28 Jun. 2014].

Kigen P, Kisutsa C, Kimani k., Mwangi, M. and Muchai, C. (2014). *KENYA CYBER SECURITY REPORT 2014*. NAIROBI: SERIANU.

Korongo, B. (2013). *Kenya Country Correspondent*.

Lucian, V. (n.d.). A CONCEPTUAL FRAMEWORK OF E-FRAUD CONTROL IN AN INTEGRATED SUPPLY CHAIN.

N. A. Panayiotou, S.P. Gayialis, and I.P. Tatsiopoulos, "An e-procurement system for governmental purchasing," *International Journal of Production Economics*, no. 90, pp. 79-102, 2004

Moen, V., Inge, K., Klingsheim, A. and Hole, K. (2007). *Vulnerabilities in E-governments*. University of Bergen.

[Marissa Reddy, michelle keeny Eileen Kowalski. \(2004\)](#) Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector .

Musa, N., Mohamed, R., Hanani, D. and Din, I. (2012). E-Government Services: The Formal, Technical and Informal components of E- Fraud Prevention for Government Agency. *International Journal of Research in Management & Technology (IJRMT)*, 2(2), pp.1-7.

National Fraud Center, (2000). *Global Threat Crime Report*.

Sarbanes-Oxley Act of 2002, Section 302, 404.

Shailendra, Sing; Singh Karaulia (2011). "E-Governance: Information Security Issues". *International Conference on Computer Science and Information Technology (ICCSIT'2011)*.

Stc-Egov.IEEE.net, (2014). *e-Government: Security Threats - IEEE Computer Society e-Government STC*. [online] Available at: <http://stc-egov.ieee.net/blog/e-governmentsecuritythreats>

United Nations, Department of Economic and Social Affairs, (2012). E-government Survey, 2012, E-government for the People. United Nations.

Vasiu L. and I.Vasiu, "Dissecting Computer Fraud: From Definitional Issues to a Taxonomy", in the Proc of the 37th Hawaii International Conference on System Science 2004, IEEE, 2004, pp. 170-177.

# APPENDIX A- List of Survey Questions

**Emerging Technologies Abuse in the Public Sector**

**1. General Information**

**What is your Gender?**

Male

Female

**What is your Age Group?**

20-30

31-40

Over 40

**Choose your occupation from the list below**

IT Analyst

Auditing

Legal services

Academia-lecturer

Accountant

Engineer

Other

**What is your level of Education?**

Certificate level

Diploma/Higher Diploma

Undergraduate

Further Studies

**2. Security Information**

**Has your organization ever been compromised (internally or externally)?**

Yes

No

Dont know

## Emerging Technologies Abuse in the Public Sector

**How vulnerable is the network, host, and application(s) to attacks from the internet or intranet?**

	Very Secure	Slightly Secure	Don't Know	No Security
Hosts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Network	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Applications	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Social Engineering controls are effective e.g physical security, limiting data leakage, training staff, incidence response strategies**

Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Operational controls are effective.**

Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Does your organization use a local Firewall(s)?**

- Yes
- No
- Dont Know

**If So(refer to the question above) Which type of Firewalls?**

- Cisco
  - Checkpoint
  - Juniper
  - Other (please specify)
- \_\_\_\_\_

**Does your organization use a local Intrusion Detection System(s) (IDS)?**

- Yes
- No
- I dont Know

**Does your organization use a local Intrusion Prevention System(s) (IPS)?**

- Yes
- No
- I dont Know

## Emerging Technologies Abuse in the Public Sector

**Does your organization have any dedicated connections to other organization's networks (vendors, business partners)?**

- Yes  
 No  
 I dont Know

**Does your organization use any Remote Access services?**

- Yes  
 No

**Specifically, what type of remote access services does your organization use (VPN or Dial-Up RAS)?**

- VPN  
 Dial-Up  
 Not Applicable

**If you use VPN, how many site-to-site VPN tunnels are in use?**

- Less than 5  
 more than 5 but less than 10  
 more than 10

**How many employees use remote access services? approximate**

**Have issues with identity theft arisen in your organization?**

- Yes  
 No  
 Not aware

**An intruder can gain unauthorised access to critical resources**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

### 3. Applications Information

## Emerging Technologies Abuse in the Public Sector

**Does your organization use E-purchasing to buy miscellaneous items?**

- Yes  
 No  
 I dont Know

**Does your organization use E-procurement application in the purchase of high volume items?**

- Yes  
 No  
 Dont Know

**Software is properly managed and licenses purchased by organisations are not used for personal gain**

Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Password policies are enforced in your organisation**

Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Incase of Workstation Inactivity, machines are safeguarded through passwords etc**

Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Malicious users can access, modify and destroy data within the system.**

Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

### 4. Hosts Based Information

**How many computers does your organization have?**

- less than 10  
 grater than 50  
 more than 50 but less than 100  
 more than 100

## Emerging Technologies Abuse in the Public Sector

**Are these workstations connected to the internet?**

- Yes  
 No

**Unnecessary Services are running on the Workstations**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**Workstations running sensitive information are connect to the internet.**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**Antivirus/Malware Signatures are up to date**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**Operating Systems Patches are up to date**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

## 5. BYOD-Bring Your Own Device

**Does your organization have a WiFi connection?**

- Yes  
 No

**Employees are allowed to use their personal laptops/Tablets at work**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**Employees are allowed to access the enterprise network on their devices**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**Users are allowed to access social media accounts over the corporate network**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

## 6. Email and VoIP/PBX Use

## Emerging Technologies Abuse in the Public Sector

**Does each employee have a corporate email account?**

- Yes  
 No

**Employees can use their personal emails for business functions**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**Employees in our organisation make long distance calls that are work related.(using the office line)**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**There is a way of ensuring that employees do not abuse PBX technology to make long distance calls that are not business related.**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**There are incidences that have led to the abuse of email/PBX/VoIP in the office.**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**How is the issue above handled?**

**Those authorized to use VoIP/PBX technology, what formal procedures and safeguards are they trained to follow?**

## 7. LITERACY, TRAINING AND AWARENESS

**The majority of the employees in this organisation are Computer literate**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**How often do employees receive application trainings and refresher courses?**

- Quarterly  
 Bi-annually  
 Yearly

## Emerging Technologies Abuse in the Public Sector

**The training we get includes Topics related to Privacy and security.**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**Employees are aware of Industry Practices/Standards/Laws for Egovernance security programmes such as COBIT/HIPAA/Sarbanes-Oaxley**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

### 8. FRAUD DETERRENCE AND PREVENTION

**Our Organisation has an Information Systems Auditor**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**Employees have meaningful fraud skill training**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**The Organization has an Anti-Fraud internal Control infrastructure**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**The organisation performs background checks on new employees.**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**Do you have acceptable and unacceptable behavior properly defined and communicated to employees?**

- Yes  
 No

**If so, Can you mention one?**

**List some unacceptable behavior referred to above**

**How is evidence handled in the event that the organisation encounters suspicious situations?**

## Emerging Technologies Abuse in the Public Sector

**Do you have hotlines for reporting fraud?**

- Yes  
 No

**Does your organization use Computer Aided Auditing Softwares?**

- Yes  
 No  
 Dont Know

### 9. EARLY FRAUD DETECTION

**Ethics and Anti corruption Authority are involved in our investigations**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**How are investigations carried out in the event of potential fraud detection?**

**Whistle blowers are given adequate protection or rewarded for aiding an investigation**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**Staff morale in our organisation is high**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

### 10. PHYSICAL PROTECTION

**Sensitive computer resources e.g servers, workstations, laptops are locked behind office doors.**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

## Emerging Technologies Abuse in the Public Sector

**Has anyone in management requested an override of an internal control?**

- Yes
- No
- Dont Know

**If overrides of internal control are requested, how are these requests handled?**

\_\_\_\_\_

**I am aware of allegations involving purchasing/procurement/sales fraud within the company.**

Strongly Disagree      Disagree      Neither Disagree Nor Agree      Agree      Strongly Agree

**If anyone wants to commit a corrupt act such as a purchasing/procurement fraud, what key personnel are likely to be involved?**

- Accounts
- Senior Management
- IT analyst
- Other (please specify)

\_\_\_\_\_

## APPENDIX B-Letter of Authorisation.

  
**UNIVERSITY OF NAIROBI**  
**COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES**  
**SCHOOL OF COMPUTING AND INFORMATICS**

Telephone: 4447870/ 4444919/4446544  
Telegrams: "Varsity" Nairobi  
Email: [director-sci@uonbi.ac.ke](mailto:director-sci@uonbi.ac.ke)

P. O. Box 30197  
00100 GPO  
Nairobi, Kenya

Our Ref: UON/SCI/MS/IS/2011 13 February 2015

To Whom It May Concern

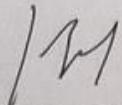
Dear Sir/Madam

**RE: THOMAS KIZITO ODUOR – REG. NO. P56/61643/2013**

The above named is a bona fide student pursuing a M.Sc in Information System degree at the School of Computing and Informatics, University of Nairobi. As part of the course, students are required to undertake a research project. Hence, Mr. Oduor is currently carrying out his research on the project entitled: "**Development of an E-corruption Control Framework for the Public Sector**" under the supervision of Dr. C.K. Chepken.

We would be grateful if you could assist Mr. Oduor as he gathers data for his research. If you have any queries about the exercise please do not hesitate to contact us.

Yours faithfully

  
School of Computing & Informatics  
University of NAIROBI  
P. O. Box 30197  
NAIROBI

**PROF. W. OKELO-ODONGO**  
**DIRECTOR**  
**SCHOOL OF COMPUTING AND INFORMATICS**

WOO/jsn