A Framework to Extend COBIT Security Framework to Overcome Confidentiality Threats in Electronic Commerce

Simon Nderitu Watuthu

A Thesis Submitted in Partial Fulfilment for the Degree of Master of Science in Computer Systems in the Jomo Kenyatta University of Agriculture and Technology

2015

DECLARATION

This Thesis is my original work and has not been presented for a degree in any other University.

Signature:…… Date: ……...

Simon Nderitu Watuthu

This thesis has been submitted for examination with our approval as the University supervisors.

Signature:…… Date: ……...

Dr. Michael Kimwele

JKUAT- Kenya

Signature:…… Date: ……...

Dr. George Okeyo

JKUAT- Kenya

DEDICATION

I dedicate my work to my wife, daughters and mother. My wife and daughters who never left my side encouraging me to push on even when things were becoming harder to tackle. They are so special. A special feeling of gratitude to my late mother Hellen Wanjiku for without her I could not have gone to school. Let this piece of work be a living testimony to everyone that it does not matter where you have come from but what matters is how focused you are to achieve your dreams.

ACKNOWLEDGEMENTS

This thesis saw the light of the day due to advice, support and cooperation from a number of people. My sincere gratitude to my supervisors Dr. Kimwele and Dr. Okeyo for the support, continual guidance, encouragement and positive feedback you gave me throughout this research. These two were more than generous with their expertise and precious time. To my wife Bernice Wangechi thanks for your unending support, encouragement and patience. I extend my heartfelt gratitude to children Gloria Wanjiku and Rejoice Nyambura for their understanding for the sacrificed family time. I would like to thank Tour and Travel companies in Nairobi who participate in this research their excitement and willingness to provide information made the completion of this research an enjoyable experience. Finally I wish to thank God for providing me the energy and the knowledge that enabled me complete this thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS AND ACRONYMS

ATM	:	Automated Teller Machine
CGI	:	Common Gateway Interface
CMM	:	Capability Maturity Model
COBIT	:	Control Objectives for Information and related Technology
DDOS	:	Distributed Denial of Service
DNS	:	Domain Name Server
ERS	:	Economic Recovery Strategy
FTP	:	File Transfer Protocol
HTTP	:	Hypertext Transfer Protocol
IEBC	:	Independent Electoral and Boundary Commission
ISACA	:	Information System Audit and Control Association
ISMS	:	Information security management system
ISO	:	International Standardizations Organization
ISSM	:	Information System Security Management
ITGI	:	IT Governance Institute
ITSM	:	IT Service Management
PA	:	Process area
SLA	:	Service Level agreement
SSE-CMM	:	Systems Security Engineering Capability Maturity Model

OPERATIONAL DEFINITIONS

The following definitions were provided to ensure uniformity and the understanding of these terms throughout the study.

Authentication	Authentication is the ability to identify the identity of a person or entity with whom you are dealing with on the internet.
Authorization	Authorization is the process by which one entity verifies that another entity is who he, she, or it claims to be.
Availability	Preventing denial of authorised access. The ability to use The information resources as desired. Timely, reliable access to data and information services for authorized users.
Confidentiality	Assurance that information is not disclosed to unauthorized persons, processes, or devices.
Information Security	That which protects the integrity, confidentiality, and availability of information on the device that store, manipulate and also transmit the information through products, people and procedures.
Integrity	The property of being whole, Complete, unimpaired, free from interference or contamination, unbroken, in agreement with requirement or expectation.
Privacy	How personal information is collected, used and protected.
Security	Protection against disclosure to unauthorized users confidentiality), improper modification (integrity) and non-access when required (availability).

ABSTRACT

Confidentiality, integrity, availability, non-repudiation, legitimate use, privacy and auditing of critical information being stored, processed and transmitted between parties involved in electronic commerce are of great importance. The main purpose of this research was to extend COBIT security framework to overcome confidentiality threats in electronic commerce. A descriptive survey research design was conducted to gather primary data. A structured questionnaire was used to collect primary data which was used as the inputs of the proposed framework. The data analysis was done using descriptive statistics using SPSS package. The observations made from this research show electronic commerce faces numerous information security challenges. Confidentiality and privacy issues were the top security issue of concern to the respondent's with 60.7% of the respondents admitting to it. The study also revealed that the information security approaches used are ineffective and inefficient. Most of the respondents at 96.4% strongly disagreed with the fact that current approaches adopted by our organization are adequate. Further, the respondents disagreed that current approaches adopted by their organization are efficient as the majority at 82.1% disagreeing. Respondents further considered viruses and malicious software at 46.4%, human errors at 28.6% and also system or software errors at 17.9% as the top three main causes of confidential threat their organizations. Further the study revealed 85.7% of the respondents admitted that their organisation did not use any framework in managing information security. In this research, a security framework adopted from COBIT was developed based on the components adapted from integrated system theory coupled with the use of customised approach or hybrid approach. The framework will among other things to provide guidance in the development of effective measures to counter confidentiality threats in electronic commerce. The framework was qualitatively evaluated and not quantitatively through a theoretical evaluation.

CHAPTER ONE

1.0 INTRODUCTION

1.1 Background to the Study

The internet is causing us to change the way we look at information, the nature and delivery of products and services, and the ways we keep in touch. Internet and multimedia are among the most visible icons in the continuing evolution of the information technology in business. According to Senn (2003), information security technical skills coupled with resources are the principal elements for securing information in an organisation.

According to Comer (2009), although internet crimes, such as scams and identity theft, can affect individuals, they can significantly pose a threat to a business. In addition to outright theft of goods and services, businesses are especially concerned with threats that harm long-term viability of the company. Thus, damage to reputation, loss of customer confidence, stolen intellectual property and prevention of customer access are all important to a business.

News reports also provide some evidence of the impacts from poor Information Security. Information Security has three primary tenets: Confidentiality, Integrity and Availability of information must be preserved. Recently, the Ulster Bank has had to pay compensation to many of its customers following a failure in their systems (King, 2012). In this case, availability was violated, with many customers unable to access their accounts. Another prime example is the SONY password leak, which impacted 100 million customers (Goodin, 2011) - here the confidentiality tenet was violated. Once someone gains access to information, it is relatively easy to compromise its integrity – this was evidenced by Hershey when hackers breached their site and changed one of their recipes (Goodin, 2011b). This is a relatively minor change but the potential is therefore far more serious changes to be made.

The denial of service which is another threat prevents or inhibits the normal use or management of communication facilities (Stallings, 2007). According to survey on cyber crime by Yang (2011), between year 2000 and 2011 there were various websites that have suffered distributed denial of service (DDOS) attacks. Table 1.1 shows the websites that were affected during this period.

Table 1.1: Some Representatives DDOS Attacks between Years 2000 to 2011

WEBSITE	**DATE**
Yahoo	February,7, 2000
Amazon	February 8,2000
Buy.com	February 8,2000
CNN	February 8, 2000
eBay	February 8,2000
E*trade	February 9, 2000
ZDNet	February 9, 2000
Mininova	March 2009
Visa	December 2010
Master card	December 2010
Paypal	December 2010
Word press	March 4,2011

Source: (Yang, 2011)

Some American bank suffered denial of service in 2012. To carry out the cyber attacks, the attackers got hold of thousands of high-powered application servers and pointed them all at the targeted banks. This overwhelmed Bank of America and Chase's Web servers (Goldman, 2012).

Denials of service attacks are an effective but unsophisticated tool that does not involve any actual hacking. No data was stolen from the banks, and their transactional systems --

like their ATM networks -- remained unaffected. The aim of the attacks was simply to temporarily knock down the banks' public-facing websites (Goldman, 2012).

According to Roman (2013), 2.9 million Adobe's customers, were notified that their personal information, including encrypted payment card numbers, had been compromised as a result of a breach of the software company's network. The attackers accessed customers' IDs and encrypted passwords on its systems. The attackers also removed from the system certain information on 2.9 million customers, including names, encrypted credit or debit numbers, cards expiration dates and other information relating to customers order.

In December 2012, Standard Chartered customers in Kenya were hit by a series of attacks where bank accounts for the customers were cleaned out, forcing the bank to tell customers to reset passwords for Automatic Teller Machines (ATM). Insiders' fraud is the leading threat to online banking as well as mobile banking in Kenya; employees sitting in a trusted environment are usually least suspected of committing fraud (Wanjiku, 2013).

According to the cyber crime report of 2012 in Kenya, in February 2012, a leading media house's payroll information for April 2012 was published online. The information published disclosed employee names, titles and monthly salaries. The information was sensitive and was not only embarrassing but also raised questions on what control local organizations put in place to ensure security of sensitive information. According to the same report, in May 2012 sensitive information from a leading Nairobi Stock Exchange listed company was published online. This is a public owned company which holds sensitive information concerning customers, business partners, regulators and shareholders (Serianu, 2012).

While commenting on technological information security challenges encountered by IEBC during the march 4th 2013 general election held in Kenya, the chairman of the

IEBC, Issack Hassan, reported that, a bug in their computer program was multiplying the number of rejected ballots by a factor of eight (Gatehouse, 2013).

In spite of the increasing number of standard and commercial security management methods, various reports, surveys, and related literature indicate that the diffusion of the current security management methods, within organizations has been very limited so far mainly due to lack of awareness, high cost, need for expertise, and long process (Saleh & Alfantookh , 2011).

It is evident that information security is under threat and is not secure despite all the efforts, time and money spent on securing information systems. While this is not a new issue for electronic commerce, the volume and innovation of the attacks on electronic commerce is increasing. Many electronic commerce companies are looking for electronic commerce solutions and IT security to address the problem. However, with this kind of information insecurity, electronic commerce cannot realize its full potential.

1.2 Statement of the Problem

According to Norman and Yasin (2010), development sectors and commercial enterprises in Africa and all over the world have been faced with serious challenges such as theft of data, viruses and saboteurs.

Electronic commerce has continued to face new risks and threats such as, loss of intellectual property rights, network attacks and so on. He further observes that, one of the critical success factors of electronic commerce is its security and without the assurance of security, electronic commerce may not work normally (Yanyan, 2014).

Confidentiality is required during electronic commerce transactions. Sending information should be kept secure against all type of threats. This is important since electronic commerce is conducted on global network that is the internet which is untrusted (Yasin *et al.,* 2012). The attackers accessed customers' IDs and encrypted passwords on the company's systems. Rishabh (2014) observes that there is fear of online transactions caused by hacking. The growth in information has led to identity

theft, credit card stealing and stealing of bank information. Olasanmi (2010) notes that with the heavy reliance of ICT by electronic commerce organisations, there has been an increase of criminal activities like spamming, credit card fraud, ATM fraud, phishing, identity theft and many other types of crime. In effort to secure electronic commerce, organizations tend to concentrate more on technology.

Despite the use of these technologies, companies continue to lose billions due to information security breaches. This suggests that technology alone cannot achieve information security. Companies should therefore compliment these technologies with proper policies, procedures, and standards.

This research aimed at developing a security framework to secure electronic commerce against confidentiality threats. This was developed from the primary data obtained from online travel companies.

This research was also motivated by the fact there are many security standards and frameworks available to help organizations manage these risks. The question which one is best and can address the information security risks adequately warrants further investigation and research (Al-ahmad & Mohammad, 2012).

1.3 Justification of the Study

With an internet penetration of approximately 16 million in Kenya, ICT applications such as e- government and electronic commerce services have become enablers for the country's development. However, cybercrime poses a serious security challenge. Electronic commerce injects billions of shillings into the economy; unfortunately, the gains made are under threat from cyber criminals, whose objective is to illegally compromise online systems. The full potential of electronic commerce is not being realised because of increasing cases of online fraud targeting banks, organisations and even individual shoppers and merchants. Kenya is losing nearly 2 billion Kenya shillings annually to Cybercrime (Ramah, 2012; Murule , 2013).

Information security management is the basis for the development of electronic commerce. The problem of information security in today's networked world has made electronic commerce information security management become outstanding. At present the firewall technology, identity authentication technologies, data encryption technology and calculation system security technology plays an important role. In addition, we need to perfect the legal system, management system and credit system, so that we can guarantee the electronic commerce information security management (Qin & Ge, 2012). Al-ahmad and Mohammad (2012) observe that security management programs needs to be established on solid foundations which are the reasons why enterprises look for standards and frameworks that are widely accepted and common across enterprises. According to Alfawaz (2011), it is important when dealing with information security management to address both technical and non-technical aspects. Protection of information resources requires a sound security policy and a set of controls (Laudon & Laudon, 2008).

This research will provide a support tool to help security managers in establishing security policies, standards and procedure to enhance electronic commerce. The research results can used to formulate more focused information security management policies which could motivate the business organizations to implement Electronic commerce as part of their business. The academics fraternity and researchers in information system security will have an insight and hence build on this research in coming up with gaps that have hindered growth of electronic commerce.

1.4 Research Questions

1. What are the information confidentiality challenges faced by electronic commerce?
2. What are the key confidentiality issues surrounding information security management in electronic commerce?
3. What are the techniques and approaches used in managing Electronic Commerce information confidentiality threats?

4. How can COBIT security Framework be extended to overcome confidentiality threats in electronic commerce?
5. Is the developed framework appropriate for overcoming threats in electronic commerce?

1.5 Research Objectives

1.5.1 General Objective

The general objective of the research was to extend COBIT security framework to overcome confidentiality threats in electronic commerce.

1.5.1 Specific Objectives

The specific objectives of the study were:

1. To identify the information confidentiality challenges faced by electronic commerce and by use of hybrid approach develop a security framework to address them.
2. To identify the key confidentiality issues surrounding information security management in electronic commerce and to provide a means of addressing them.
3. To investigate the techniques and approaches used in managing Electronic Commerce information confidentiality threats.
4. To use findings of 1, 2 and 3 to extend COBIT security framework to overcome confidentiality threats in electronic commerce.
5. To validate the developed framework.

1.6 Scope of the Study

This study mainly focused on electronic commerce information confidentiality threats and challenges faced by tour and travel companies in Nairobi. The study looked at the current status of electronic commerce information security approaches used to manage information confidentiality threats and the impediments of these approaches. The study made recommendations on how electronic commerce information confidentiality can be improved. A security framework was developed to provide a support tool to help security managers to secure information confidentiality in electronic commerce.

1.8 Structure of Thesis

This section provides an overview of the research presented in the following seven chapters.

Chapter one: Background to the Study: The background to the study, Statement of the Problem, Justification of the Study, research objectives, Research questions, Scope of the Study, Definitions of Significant Terms are given.

Chapter two: Literature Review: This chapter provides a critical analysis of background information relied upon in the chapters that follow. In this chapter the dimensions of information security are presented. The challenges facing electronic commerce, issues surrounding electronic commerce and approaches used to secure electronic commerce are discussed. International recognized information security frameworks are also discussed in this chapter.

Chapter three: Research Methodology: In this section we outline the research methodology. Under the methodology we have Research Design, Target Population, Sample Size and Sampling Procedure, Research instruments, Validity, Reliability, Data Collection Procedure, Data Analysis and Limitations of the Study.

Chapter four: Data Presentation, Analysis and Interpretation of Findings: This chapter presents the findings of the research that includes analysis, interpretation of the data gathered from the field**.** This chapter is divided into five sections as follows: Demographic information of the respondents, Information security challenges faced by electronic commerce sector of tour and travel companies, Key issues surrounding electronic commerce information security management and Techniques and approaches used by tour and travel companies in managing Electronic Commerce information security threats.

Chapter five: Development of Proposed Framework Validation: This chapter details the development of the proposed security framework. In the first section, the standard information security frameworks are discussed. In the second section, the challenges of

standard security frameworks are outlined. The research findings discussed in chapter four are summarised and the critical findings are identified using the mean of the responses obtained in chapter four. These findings are then mapped to the standard frameworks in order to provide a level of synchronization between these frameworks and also pick from each the aspect which would address the issues identified in the field. Finally, in the third section the proposed framework is presented.

Chapter six: Framework Validation: this section presents opinion and their analysis concerning the proposed framework. From the results of the validation process a validated framework was generated.

Chapter seven: Conclusions and Recommendations: This chapter concludes the thesis by providing a summary of significant findings from the study. It gives a conclusion to the findings and recommendations.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

This section accounts for what has been credited by scholars on information security. It focuses on the information security issues affecting electronic commerce. This part also has some standard information security framework used in enhancing information security in various sectors.

2.2 Definition of Electronic Commerce

Li Y. and Fan R (2014) state that electronic commerce or electronic commerce refers to a wide range of online business activities for products and services. And it useful to any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact. Electronic commerce is usually related with conducting transaction concerning the transfer of ownership or rights to make use of goods or services through a computer-mediated network, or buying and selling over the internet. Golubova (2012) describes electronic commerce as the selling and buying by means of Internet, or in other words conducting e-transactions over the Internet. Electronic commerce however is really much more than just exchanging products or services for money over the internet. Electronic commerce also include enabling technology that allows business to increase the accuracy and efficiency of business transaction process. Electronic commerce is also a way for organizations to exchange information with customers and vendors to the benefit of everyone involved.

2.3 Security and Information Security

Security is the necessary steps take to protect a person or property from harm (Ciampo, 2012). ISACA defines information security as something that: ensures that within the enterprise, information is protected against disclosure to unauthorised users (confidentiality), improper modification (integrity) and non-access when required (availability) (ISACA, 2012).

Information security is the protection of information assets that use, store or transmit information from risk through the application of policy, education and technology (Whitman & Mettord, 2012). According to Ciampo (2012), information security is that which protects the integrity, confidentiality, and availability of information on the device that store, manipulate and also transmit the information through products, people and procedures.

According to Ciampo (2012), the main goals of information security are to prevent data theft, and thwart identity theft, avoid the legal consequences of not securing information, maintain productivity, and foil cyber terrorism. Computer security depends on a combination of physical barriers, software defences and security procedures.

Electronic commerce security is the protection of electronic commerce assets from unauthorized access, use, alteration, or destruction. Electronic commerce security threats range from intellectual property theft and business disruption to brand and reputation damage.

2.4 Importance of Information Security in Electronic Commerce

Information security is a business enabler that is strictly bound to stakeholder trust, either by addressing business risk or by creating value for an enterprise, such as competitive advantage.

According to Ward (2010), data breaches produce unwelcome publicity that can have a severe negative impact on a retail organization's brand and reputation. The damage from a data breach often extends well beyond losing the trust of only those customers directly impacted by the incident—and negative public perceptions can persist for years after a breach.

The following subsections present examples of the losses caused by malicious codes and hackers.

2.4.1 Financial Losses Due to Hackers

In early 1998, a Mathematician from St Petersburg, Vladimir Levin, transferred US$12 million from Citibank accounts by hacking bank workers' passwords. Levin was later arrested at London's Heathrow Airport. In February 1998, Levin was sentenced to three years in prison by a U.S. judge and ordered to pay Citibank $240,000 in restitution (Goh, 2003).

At a security seminar for the banking industry in Kenya held in September 2013, Col (rtd) Kamenju, director of the Security Research and Information Centre, warned bankers of the increasing incidence of Internet fraud, committed by hackers who are able to overwrite passwords and make unauthorised intrusions into corporate websites. Two years ago, the police anti-banking fraud unit reported that Ksh50 million ($641,000) intended for a firm in Dubai was diverted by hackers. This year, Ksh10 million ($128,000) was also stolen by hackers (Telecoms, 2013).

2.4.2 Financial Losses Due to Viruses

In early 2013, three European men were charged by North American prosecutors with the creation and distribution of a computer virus the 'Gozi' virus that infected more than a million computers worldwide, enabling them to access personal bank information and steal at least 50 million dollars in the period between 2005 and 2011. The virus was introduced in Europe and spread to North America, where it also infected computers belonging to national agencies. This is said to be one of the most financially destructive virus ever witnessed (United Nations, 2013). The table 2.1 shows analyses of viruses by incident.

Table 2.1: Analyses of Viruses by Incident. Source: (United Nations, 2013)

Year	Code Name	Worldwide Economic Impact ($ U.S.)
2001	Nimda	635 Million
2001	Code Red(s)	2.62 Billion
2001	SirCam	1.15 Billion
2000	Love Bug	8.75 Billion
1999	Melisa	1.10 Billion
1999	Explorer	1.02 Billion

From the examples, the importance of information security cannot therefore be under scored.

2.5 Information Security Challenges

2.5.1 Electronic Commerce Competition

According to Kaufmann (2009), competition in electronic commerce has led organization to overlook the confidentiality aspect of information security. Due to this competition, electronic commerce organizations place more value to outsmarting their competitors than securing their systems.

2.5.2 Information Security Attacks

Security is one of the principal and continuing concerns that restrict customers and organizations engaging with Electronic commerce (Niranjanamurthy & Chahar, 2013). According to Kaufmann (2009), security incidents that are related to malicious code (worms, viruses, and Trojans) have grown from slightly annoying to significantly damaging to business operations. Early computer viruses were often contained to individual users' systems, resulting in only a small decline in staff productivity for a given day. However, present-day blended threats, such as Code Red and Nimda, present multiple security threats at the same time, causing major disruptions and billions of dollars of damage to enterprises. A blended threat combines different types of malicious

code to exploit known security vulnerabilities. Blended threats use the characteristics of worms, viruses, and Trojans to automate attacks, spread without intervention, and attack systems from multiple points. The rapid spread of these threats makes it increasingly difficult to respond quickly enough to prevent damage. The threats are expected to continue to grow in magnitude, speed, and complexity, making prevention and clean-up even more difficult. These factors contribute to the need for a proactive plan to address information security issues within every company.

According to Rishabh (2014), despite the fact that internet has come a long way from its 'open' days, the fear of online transactions, be it financial or data transfer, is very high in the consumer's mind. Hacking, identity theft, credit card stealing, bank information stealing, etc. are some of the greatest security issues that hinder the consumer from trusting online businesses. Eventually, this means loss of potential business for organizations.

Electronic commerce security challenges are however, not limited to consumers. Businesses and corporate firms also face security challenges as their vital information, records and most importantly their reputation is at stake.

2.5.3 Immature Information Security Market

The information security market is still in its infancy, with few formal standards established for products or services. The information security industry is at a similar stage today, with several companies offering individual solutions such as firewalls that address only a portion of a company's security needs. As a result, their customers face the challenge of making all these solutions work together. Only early versions of standards exist, forcing companies to complete multiple installations of "point" solutions that provide individual components of their security systems (Ciampa, 2012: Whitman & Mattord 2012).

2.5.4 Information Security Staff Shortage

Finding qualified information security staff is a difficult task, which will likely continue to be the case in the near future. Due to the immature market, lack of standards, and numerous point solutions, training is a problem for security staff. The industry has not had the time to grow the staff necessary for these roles. In addition, the information security challenges keep growing at a rapid pace, constantly expanding the list of technology to be deployed, and the information security staff just cannot keep up. This translates into more time and money to get staff trained on commercially available products. In addition to specific technical training, information security staff members need to develop security enforcement skills that are not part of the traditional IT staff background. This unique requirement makes it difficult for existing IT staff to transition into information security roles without receiving specialized enforcement training (Merkow & Breith, 2014).

2.5.5 Government Legislation and Industry Regulations

Kaufmann (2009) asserts that Government regulations and industry regulations are required controls to ensure that personal information is protected from loss, misuse, unauthorized access, disclosure, and so on as a condition to obtain certification. One major challenge is that certain countries do not place a high priority on protection of personal information or intellectual property. They might have more pressing issues, such as food or medicine, and might be unwilling or unable to police individuals who are engaged in activities such as software piracy. These criminals operate freely in these countries without the fear of law enforcement agencies shutting down their operations. These safe havens for cyber criminals pose additional challenges for legitimate businesses that have little legal recourse to combat the illicit activities of software pirates. Unless business executives put strategies in place to protect their intellectual property and customer information, they run the risk of falling victim to these individuals.

According to Seleanu (2013), to mitigate those risks, security and financial experts have called for an enhanced information-sharing system that would allow firms to provide detailed cyber-attack statistics to the government in exchange for intelligence on emergent threats and mitigation strategies. To date, attempts to establish such a system have had little result.

2.5.6 Mobile Workforce and Wireless Computing

According to Kaufmann (2009), mobile computing devices although convenient have become information security concerns because the confidential information stored on them needs to be protected. In the past, staff members typically used one computer in the office for business purposes and a different one at home for personal use. The challenge from a security perspective is twofold—first, all the protection offered in the company office must now be incorporated on the laptop computer or mobile device, and second, 802.11 protocols have weak security features. When physically in the office, employees can take advantage of the company's security protection such as firewalls and anti-virus software. In addition to the lack of information security tools, mobile devices that might contain valuable intellectual property, customer information, or other sensitive information also run the risk of theft or loss. New technologies often initially focus on features and functionality at the expense of security to obtain critical mass and adoption. This is the case of 802.11, as individual consumers have initially embraced this technology and are less concerned with someone reading their email or obtaining access to their personal address book. Businesses, on the other hand, cannot take those risks because enterprise systems contain vital company records that could disrupt their operations if divulged to unauthorized parties. Companies must give careful consideration before leveraging wireless technology in mainstream business. These information security risks include all the mobile devices such as cell phones, personal digital assistants, and so on that contain valuable information.

Westervelt (2011) supposes that security have cautioned enterprises from ignoring the future risks that smartphones and other mobiles devices pose to corporate data leakage.

The attack surface is much greater on mobile devices and there are far fewer security controls. As a result, companies need to ensure that their information security program extends to all devices that frequently leave the office and that are easily lost or stolen. They can no longer count on safely locking computers in the offices when employees go home at night.

According to Reeder (2011) a recent survey of 100 popular iPhone and Android mobile apps by Via Forensics found that three-quarters of them store sensitive user account information unencrypted on the mobile device. Offending apps include LinkedIn, Netflix, Skype, Gmail, Yahoo Mail and Groupon. The survey examined financial, social networking, productivity and retail apps. It was discovered that the applications store transmit data such as security credentials, personal financial information, private communications and sensitive company data. Usernames were the most common piece of unprotected data with 76 percent of the 100 applications keeping usernames in plain text. Ten percent were storing the user's password in plain text.

2.5.7 Larger User Communities

Larger user communities in electronic commerce is yet another electronic commerce challenge (Oracle, 2002).The sheer size of the user communities which can access business systems by way of the Internet not only increases the risk to those systems, but also constrains the solutions which can be deployed to address that risk. The Internet creates challenges in terms of scalability of security mechanisms, management of those mechanisms, and the need to make them standard and interoperable (Oracle, 2002).

2.5.8 Lack of Trust

Trusting others electronically in electronic commerce transactions is a major concern. Ahmed *et al*. (2012) noted that the problems associated with online shopping are more to consumer's protection in transaction that requires privacy and trust between different geographical locations or countries. There is increasing concern over online shopping because of insecurity, lack of customer's protection and trust which are vital elements for a successful online transaction between countries, organization as well as individual.

Privacy concerns according to Niranjanamurthy and Chahar (2013), has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for electronic commerce providers.

2.5.9 Lack of Security Awareness

Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the electronic commerce security architecture (Niranjanamurthy & Chahar, 2013). While technology is important, organizational and human factors also play a crucial role in achieving information security (Dutta, 2008). The human dimension calls for effective awareness and education to assist in strengthening the 'human firewall' and to ideally cultivate a culture of information security behavior (Frauenstein & Solms, 2009).

2.6 Key Issues Surrounding Electronic Commerce Information Security

Bishop (2003) notes that Computer security rests on confidentiality, Integrity and availability. According to Turban and Jaeler (2006), electronic commerce security involves more than just preventing and responding to cyber attacks and intrusions. The major security issues that can occur in electronic commerce include but not limited to; authentication, authorization, auditing, confidentiality, integrity, availability and nonrepudiation. According to Newnan (2003), Data and Database security can be described by the following three qualities; Availability (Preventing denial of authorised access), Confidentiality (Preventing unauthorised disclosure) and Integrity (Preventing unauthorised modification).

Laudon and Traver (2002) cites six key dimensions of electronic commerce security as integrity, non-repudiation, authenticity, confidentiality, privacy and availability while Turban and King (2006), argues that the major security issues that occur in electronic commerce are authorization, authentication, auditing, confidentiality and integrity.

Otutaye (2003) noted that E-business security consists of six dimensions: confidentiality, integrity, availability, legitimate use, auditing and nonrepudiation.

2.6.1 Confidentiality Issues

Confidentiality is also defined as the avoidance of the unauthorised disclosure of information. Confidentiality involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content (Hoodrick & Temassia, 2011**)**. According to Turban and King (2006), the idea behind confidentiality is that information that is private or sensitive should not be disclosed to unauthorised individuals entities or computer software processes. There several types of threats that affect confidentiality which include: snooping, traffic analysis, eavesdropping, masquerading, internal threats, pharming, malicious codes and identity theft (Forouzan, 2013; Goodrich & Tamassia, 2011; Loudon *et al.*, 2010).

2.6.1.1 Snooping

Forouzan (2013) describes snooping as unauthorized access to or interception of data. A file being transferred through the internet may contain confidential information. Unauthorized entity may intercept the transmission and use its contents for her own benefit. Sniffing and snooping are synonyms. They refer to listening to a conversation. For example, if you login to a website that uses no encryption, your username and password can be sniffed off the network by someone who can capture the network traffic between you and the web site. Goodrich and Tamassia (2011) defined eavesdropping as the interception of information intended for someone else during transmission over a communication channel. Eavesdropping include packet sniffing.

2.6.1.2 Spoofing

According to Goodrich and Tamassia (2011), spoofing involves sending a network data packets that have false return addresses. According to Loudon et al. (2010), hackers attempting to hide their true identities often spoof, or misrepresent themselves by using fake e-mail addresses. Spoofing also may involve redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination. For example, if hackers redirect customers to a fake web site that looks almost exactly

like the true site, they can collect and process orders, effectively stealing business as well as sensitive customer information from the true site.

2.6.1.3 Identity Theft

With the growth of the internet and electronic commerce, identity theft has become especially troubling. Identity theft is a crime in which an imposter obtains key pieces of personal information, such as social security identification numbers, driver's license numbers, or credit card numbers, to impersonate someone else. The information may be used to obtain credit, merchandise, or services in the name of the victim or to provide the thief with false credentials. According to Javelin Strategy and Research, 8.4 million Americans were victims of identity theft in 2007 and they suffered losses totalling to $49.3 billion. One increasingly popular tactic is a form of spoofing called phishing (Loudon et al., 2010).

2.6.1.4 Traffic Analysis

This is where pairs of requests and responses are analysed to help a criminal to guess the nature of transaction (Forouzan, 2013).

2.6.1.5 Masquerading

Goodrich and Tamassia (2011) describe masquerading as the fabrication of information that is purported to be from someone who is not actually the author. Phishing is an example of masquerading. Phishing is creation of a web site that looks like a real electronic commerce site, but is intended for gathering passwords. According to Loudon et al. (2010), Phishing involves setting up fake web sites or sending e-mail messages that look like those of legitimate businesses to ask users for confidential personal data.

2.6.1.6 Internal Threats

Studies have found that user lack of knowledge is the single greatest cause of network breaches. Many employees forget their passwords to access computer systems or allow co-workers to use them, which compromises the system. Malicious intruders seeking system access sometimes trick employees into revealing their passwords by pretending

to be legitimate employees of the company in need of information. This practice is called social engineering (Loudon et al., 2010). Internal threat has been a serious obstacle in managing information security for many organisations recently (Sherif, 2012); he has suggested that internal threat should be dealt with carefully.

2.6.1.7 Malicious Software

According to Loudon et al. (2010), sharing files over peer-to-peer (P2P) networks, such as those for illegal music sharing, may also transmit malicious software or expose information on either information on either individual or corporate computers to outsiders this can occur through Trojan horse. E-mails may contain attachments that serve as springboards for malicious software.

Worms are types of malwares which are self-replicated and are able to spread fast. A worm can designed to collect users' private information such as usernames and passwords or bank account information. The collected information by worms might be handed to illegal and underground organizations. Usually, such information are used for identity fraud or for example, accessing the bank credits (Ali , 2013).

2.6.1.8 Pharming

Pharming is a form of domain spoofing. In simple terms, rather than spamming you with email requests to confirm your financial or personal information, pharmers work invisibly. They change your local DNS server to redirect your Web request to a fake site. This means that when you enter a web address, such as www.iugaza.edu; you will be taken to a fake website rather than the legitimate website. As far as you know, you're connected to the correct site. No email is involved, and if they copied the appearance of the real site well, you would have no way to know that anything was wrong (El-Buhaisi, 2013).

2.6.2 Legitimate Use Issues

Legitimate use has three components: identification, authentication and authorization. Identification involves a process of a user positively identifying itself (human or

machine) to the host (server) that it wishes to conduct a transaction with. The most common method for establishing identity is by means of username and password. The response to identification is authentication (Otutaye, 2003). Laudon and Traver (2014) described authentication as the ability to identify the identity of a person or entity with whom you are dealing on the internet.

According to Otutaye (2003), without authentication, it is possible for the system to be accessed by an impersonator. Once an entity is certified as uniquely identified, the next step in establishing authorization. This may include access to files, manipulation of data, changing system settings, etc. A secured system will establish very well defined authorization policy together with a means of detecting unauthorized activity (Otutaye, 2003).

Authorization is the process by which one entity verifies that another entity is who he, she, or it claims to be. Authorization is done by comparing information about the person or program to the access control information associated with the resources accessed (Laudon & Traver, 2002). According to Hoodrick and Temassia (2011), authorisation is the determination if a person or system is allowed access to resources, based on an access control policy while in Physical security is the establishment of physical barriers to limit access to protected computation resources. Turban and King (2006) explains authorization as the process by which one entity verifies another entity is who he/she or it claims to be. Authentication requires evidence inform of credentials which can take the forms including something known (e.g. a password), something processed (e.g. a smart card), or something unique (e.g. a signature).

2.6.3 Accountability Issues

Accountability issues deal with auditing and traceability**.** In an electronic commerce security context, auditing is the process of examining transactions. Trust is enhanced if users can be assured that transactions can be traced from origin to completion. If there is a discrepancy or dispute, it will be possible to work back through each step in the process to determine where the problem occurred and, probably, who is responsible.

Order confirmation, receipts, sales slips, etc. are examples of documents that enable traceability. In a well-secured system, it should be possible to trace and recreate transactions, including every subcomponent, after they are done. An effective auditing system should be able to produce records of users, activities, applications used, system settings that have been varied, etc., together with time stamps so that complete transactions can be reconstructed (Otutaye, 2003).

2.7 Security Approaches

Researchers and computer security experts have documented various methods that can be used to counter threats against confidentiality, integrity, availability, accountability and nonrepudiation. Laudon and Traver (2014) outline tools available to achieve security include: encryption, firewalls, access control, virtual private networks, authentication, tunneling, Proxy/agent systems, intrusion detection. Hoodrick and Temassia (2011) detailed the tools used to ensure confidentiality as; encryption, access control, authentication, authorisation and physical security.

2.7.1 Encryption

This transformation of information using a secret, called an encryption key, so that the transformed information can only be read using another secret, called the decryption key (Hoodrick & Temassia, 2011).

2.7.2 Firewalls

According to Turban, King and Jaelee (2006), a firewall is a network node consisting of both hardware and software that isolate a private network from a public network. Packet –filtering routers filter data requests moving from the public internet to private network based on the network addresses on the computer sending or receiving the request. The other type of firewall blocks data and requests depending on the type of application being accessed. This type of firewall is called an application- level poxy.

2.7.3 Access Control, Authentication and Authorization

According to Goodrich and Tamassia (2011), access controls consists rules and policies that limit access to confidential information to those people and/or systems with a "need to know". This need to know may be determined by identity, such as a person's name or a computer's serial number, or by a role that a person has, such as being a manager or a computer security specialist. One access control mechanism for preserving confidentiality is cryptography, which scrambles data to make it incomprehensible (Bishop, 2003).

According to Goodrich and Tamassia (2011), authentication is the determination of the identity or the role someone has. This determination can be done in a number of different ways, but it is usually based on a combination of something a person has (such a smart card) something a person knows (like a password) and something a person is (like a fingerprint). Authorization is the determination if a person or a system is allowed access to resources, based on access control policy. Such authorization should prevent an attacker from tricking the system into letting him access to the protected resources.

2.7.4 Intrusion Detection

According to Turban, King and Jaelee (2006), intrusion detectors are a special category of software that can monitor activity across a network or on a host computer to watch for suspicious activity and takes an automated action based on what it sees. Honey nets are a technology that can be used to detect and analyse intrusions.

2.7.5 Security Education and Training

Several years of research from various information security experts have revealed that people still are, and will always be, the weakest link when it comes to organizational security.

Therefore, the organization's information security program will be an ineffective exercise/activity if an adequate level of information security awareness training for example corporate information security policies and procedures is not also implemented.

Generally speaking, almost all security and privacy standards, frameworks, laws and regulations require organizations to educate their personnel in as part of overall policy and security awareness (Khan, 2010).

2.7.6 Policy

According to (Khan, 2010), the formulation, communication and publication of easily accessible information security policies, is by far one of the most critical controls an organization should consider implementing as per the ISO 17799/27002 code of practice for information security management standard. To facilitate effectiveness of information security policy, it is recommended that policies be written in a simple, standardized and a structured format; should be assigned clear business ownership; and lastly, should be a reviewed and updated on a regular basis with appropriate version control. An appropriate policy review and approval process should developed to perform this activity, as it demonstrates that the organization is committed to protecting critical business processes and assets, and has also obtained ongoing executive support for the maintenance of information security policies.

2.7.7 Risk Assessment

Khan (2010) observes that risk assessments play a crucial role in identifying potential threats to the organization and provide a perfect opportunity to implement effective controls to protect critical processes and assets.

2.8 Types of Electronic Commerce Security Threats and Attacks

2.8.1 Threats

Hasan and Sobhan (2012) give the client, server and communications channel as the three key points of vulnerability in electronic commerce. A characteristic of a computer system or network that makes it possible for a threat to occur is called vulnerability. Laudon and Traver (2014) points out that there are about seven most common and most damaging forms of security threats to electronic commerce sites: Malicious code, hacking and cyber vandalism, credit card fraud/theft, spoofing, denial of service attacks, sniffing and insider jobs.

2.8.1.1Client Threats

2.8.1.1.1 Active Content

Active content refers to programs that are embedded transparently in web pages and that cause action to occur. The best known active content forms are Java applets, ActiveX controls, JavaScript and VBScript (Sengupta et al, 2005).

Since active content modules are embedded in web pages, they can be completely transparent to anyone browsing a page containing them. Anyone can embed malicious active content in web pages. This delivery technique, called a Trojan horse, immediately begins executing and taking actions that cause harm. Malicious programs delivered quietly via web pages could reveal credit card numbers, usernames and passwords that are frequently stored in special files called cookies. Malicious active content delivered by means of cookies can reveal the contents of client-side files or even destroy files stored on client computers.

2.8.1.1.2 Malicious Codes

Computer viruses, worms, logic bomb and Trojan horses are examples of malicious code. A computer virus consists of segments of code that perform malicious actions. The code attaches itself to an existing program and takes control of that programs access to the targeted computer. A worm is a malicious program that replicates itself constantly, without requiring another program environment. Trojan Horses are software programs that hide their true nature and reveal their designed behaviour only when activated (Whitman & Mettord , 2012). According to Hoodrick and Temassia (2011), a logic bomb is a program that performs a malicious action as a result of a certain logic condition.

Despite our knowledge and infrastructure defenses, many viruses and worms have broken out regularly in the Internet over the years. By some reports, 5 to 15 new viruses and worms are released every day, although a fraction of that number is not released in the wild and most do not spread well. Still, fast-spreading viruses and worms continue to

appear with regularity. Outbreaks have become so common place that most organizations have come to view them as a routine cost of operation (Chen, 2009).

2.8.1.1.3 Server-Side Masquerading

Masquerading lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one. The user has been spoofed. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but it is usually an active attack (in which the masquerader issues responses to mislead the user about its identity).

2.8.1.2 Communication Channel Threats

Hasan. and Sobhan (2012) observe data transmission security is the most vulnerable place is the network over which data is being transmitted. In electronic commerce, the data is transmitted over the internet and may be accessed by somebody in between. According to Mazundar and Barik (2005), the internet serves as the electronic chain linking a consumer (client) to an electronic commerce resource (commerce server). Messages on the internet travel a random path from a source node to a destination node. The message passes through a number of intermediate computers on the network before reaching the final destination. It is impossible to guarantee that every computer on the internet through which messages pass is safe, secure, and non-hostile.

2.8.1.3 Server Threats

Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information. According to (Hasan, Sobhan, 2012), there are several types of server threats which include: Web-server threats, Commerce server threats, Database threats, Common gate-way interface threats and Password hacking.

2.9 Standard Security Frameworks

Essentially a framework is a collection of controls organized to highlights what needs to be done at various levels of an organisation. An information security framework is a blueprint for assessing your current information security program. According to Kark et al (2007), a comprehensive security framework boils down to three familiar basic components: people, technology, and process. When correctly assembled, the people, technology, and process elements of your information security program work together to secure the environment and remain consistent with your firm's business objectives. A comprehensive security framework must be based on these three components and must also ensure policy definition, enforcement, measurement, monitoring, and reporting for each one of the components. However, because defining and implementing policies alone cannot ensure security, the framework must also:

1) Identify risks to confidentiality, integrity, and availability for different business functions

2) Reduce, transfer, or accept those risks.

2.9.1COBIT

The **C**ontrol **Ob**jectives for **I**nformation and related **T**echnology (**COBIT**) is a set of IT management practices produced by the Information Systems Audit and Control Association (ISACA). Hill and Turbitt (2006) observed that COBIT is an IT-focused governance and control framework created by the IT Governance Institute (ITGI) and Information Systems Audit and Control Association (ISACA).

Rouse (2013) pointed out that COBIT is especially popular with management of information security in organizations. According to Musa (2009), COBIT framework identifies which of the seven information criteria (effectiveness, efficiency, confidentiality, integrity availability, compliance and reliability), as well as IT resources (people, applications, technology, facilities and data) are important for IT processes to fully support business objective.

Olzak (2013) describes COBIT as a framework for developing, implementing, monitoring and improving information technology (IT) governance and management practices. According to According to Susanto et al. (2011), COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, business risks, and security issues.

IT Governance Institute (2007) summarises COBIT process as in figure 2.2

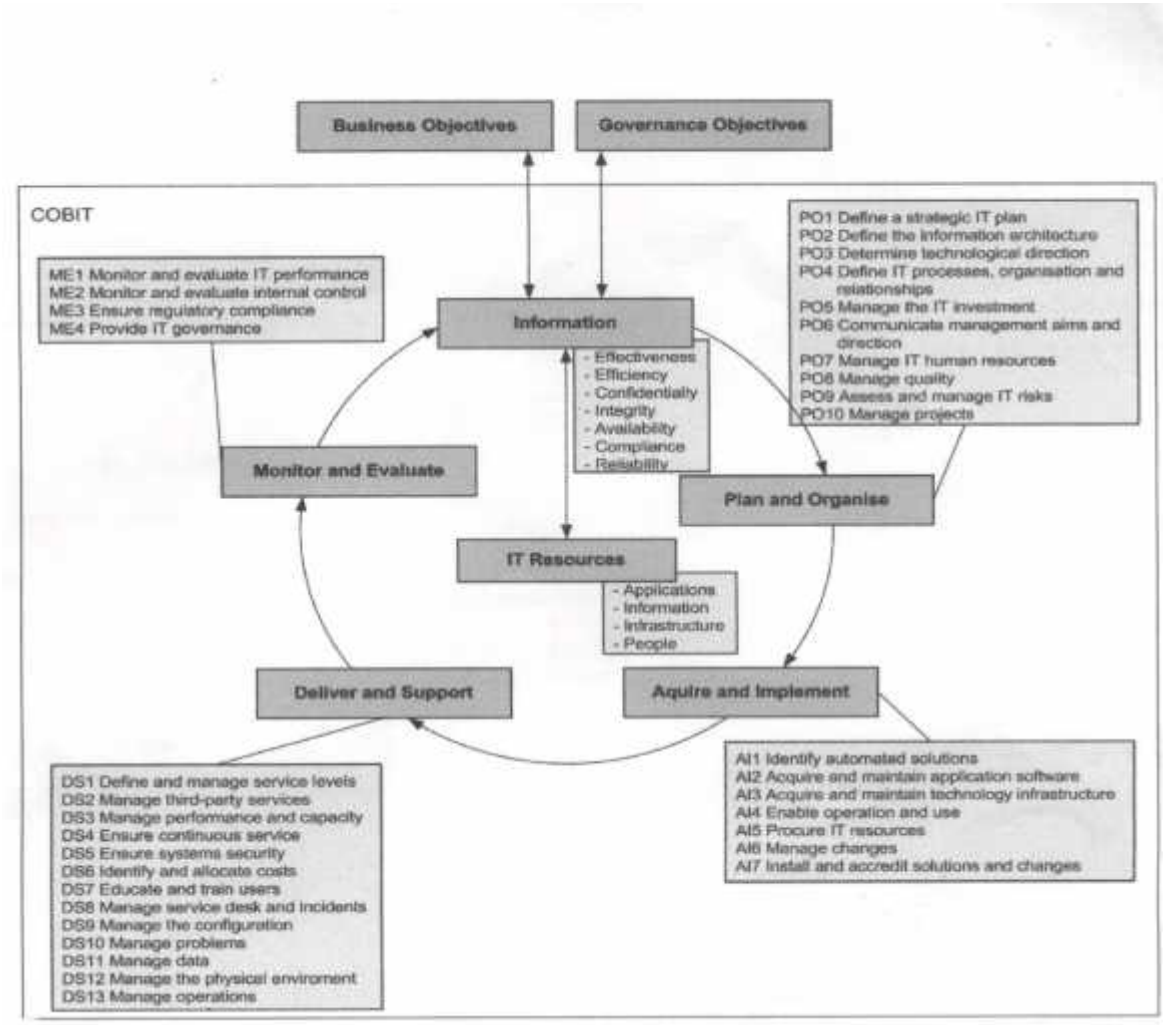


Figure 2.1: COBIT Processes

Source: (IT Governance Institute, 2007)

2.9.2 ISO 27001

According to Sheikhpour and Modiri (2012), ISO 27001 is one of the reference frameworks for information security management to help organizations assess their security risks and implement appropriate security controls. ISO/IEC27001 standard specifies requirements for the design and implementation of an appropriate information security management system in an organization, ensuring that adequate and proportionate controls are selected to protect information assets and to give confidence to interested parties. According to Kosutic (2013), ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. ISO 27001 aims to provide a methodology for the implementation of information security in an organisation.

According to Disterer (2013), there are four phases of information security management system are:

2.9.2.1 The Plan Phase

The Plan phase consists of the following steps: Writing an ISMS Policy, identifying the methodology for risk assessment and determining the criteria for risk acceptance, identification of assets, vulnerabilities and threats, evaluating the size of risks, identification and assessment of risk treatment options, selection of controls for risk treatment, obtaining management approval for residual risks, obtaining management approval for implementation of the ISMS and writing a statement of applicability that lists all applicable controls, states which of them have already been implemented, and those which are not applicable.

2.9.2.2 The Do Phase

This phase consists of the following activities: Writing a risk treatment plan, implementing the risk treatment plan, implementing applicable security controls, determining how to measure the effectiveness of controls, carrying out awareness programs and training of employees, management of the normal operation of the ISMS,

management of ISMS resources and implementation of procedures for detecting and managing security incidents.

2.9.2.3 The Check Phase

The purpose of this phase is to monitor the functioning of the ISMS. This phase includes the following: Implementation of procedures and other controls for monitoring and reviewing in order to establish any violation, regular reviews of the effectiveness of the ISMS, measuring the effectiveness of controls, reviewing risk assessment at regular intervals, internal audits at planned intervals, management reviews to ensure that the ISMS is functioning and to identify opportunities for improvement, updating security plans in order to take account of other monitoring and reviewing activities, keeping records of activities and incidents that may affect the effectiveness of the ISMS.

2.9.2.4 The Act Phase

The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase. This phase includes the following: Implementation of identified improvements in the ISMS, taking corrective and preventive action; applying own and others' security experiences, communicating activities and improvements to all stakeholders and ensuring that improvements achieve the desired objectives.

2.9.3 Capability Maturity Model

Margaret (2007) views the Capability Maturity Model (CMM) as a methodology used to develop and refine an organization's software development process. The CMM establishes a framework for continuous process improvement. Margaret (2007) outlined the levels of Capability Maturity Model as the initial level, repeatable level, defined level, managed level and optimizing level.

According to Phillips (2003), the SSE-CMM defines eleven security-related process areas. They are defined in alphabetical order to avoid implications of a sequence.

PA01 – Administer Security Controls - Security controls are properly configured and used

PA02 – Assess Impact - The security impacts of risks to the system are identified and characterized

PA03 – Assess Security Risk - An understanding of the security risk associated with operating the system within a defined environment is achieved and risks are prioritized according to a defined methodology

PA04 – Assess Threat - Threats to the security of the system are identified and characterized

PA05 – Assess Vulnerability - An understanding of system security vulnerabilities within a defined environment is achieved

PA06 – Build Assurance Argument - The work products and processes clearly provide the evidence that the customer's security needs have been met

PA07 – Coordinate Security - All members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions

PA08 – Monitor Security Posture - Both internal and external security related events are detected and tracked, incident responses are in accordance with policy and changes to the operational security posture are identified and handled in accordance with the security objectives

PA09 – Provide Security Input - All system issues are reviewed for security implications and are resolved in accordance with security goals, all members of the project team have an understanding of security so they can perform their functions and the solution reflects the security input provided

PA10 – Specify Security Needs - A common understanding of security needs is reached between all parties, including the customer

PA11 – Verify and Validate Security - Solutions meet security requirements and solutions meet the customer's operational security needs.

2.9.4 ISO 17799/27002

ISO 27002 (previously known as the ISO 17799 standard) provides a list of operational controls and security considerations which deal specifically with information security

matters. The controls listed provide guidance in protecting the information assets, so as to maintain their confidentiality, integrity and availability criteria (Goosen, 2012).

According to Carlson (2001), the process for implementing information security management using ISO 17799 proceeds as shown in Figure 2.7.

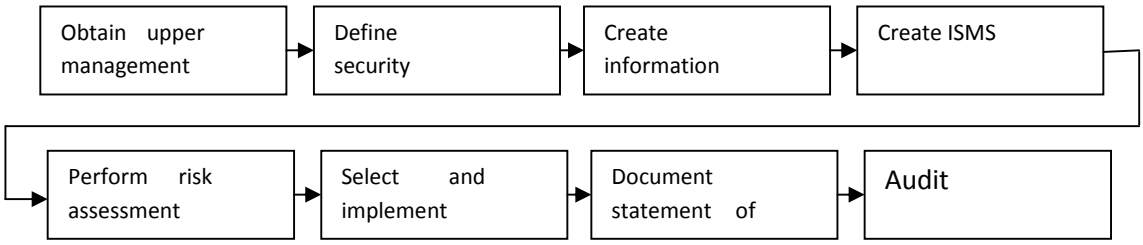


Figure 2.2: ISO 17799 Processes. Source: (Carlson, 2001)

ISO 27002 is not a technical standard, but provides a comprehensive minimum baseline of information security controls that should be in place in all information systems (Carlson, 2008). The following areas of controls form the basis of the ISO 27002 standard: Organisational and human resource management, Asset and physical security management, operations management access controls, information systems' development management, incident and business continuity management and compliance management (Carlson, 2008; ITGI, 2006).

The Information Security Infrastructure category is itself broken into seven sub sections. Asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, system development and maintenance, business continuity management and compliance.

According to Gehrmann (2012), ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management: security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and

maintenance, information security incident management, business continuity management, compliance.

The ISO/IEC 27002 has features to preserve the confidentiality, integrity and availability of the information in organizations (Gehrmann 2012).

2.9.5 COBIT and ISO 17799

The downside of COBIT is that it is not always very detailed in terms of how to do certain things. On the other hand, ISO17799 is exclusive to information security and only addresses that issue; it provides much more guidance on precisely how thing must be done. Despite of its advantages, ISO17799 also suffers the criticism of being very much stand alone. Solms suggests that it is beneficial to combine these two naturally complement frameworks. Organizations can use COBIT as a high level reference framework in which information security governance and use ISO 17799 as a lower level guideline specifically for information security detailed issues (Zhang, 2013).

2.9.6 Challenges of Standard Security Frameworks

None of the standard frameworks discussed that can address the issues of security solely. Again, there is none that is without shortcomings. The shortcomings are summarized in table 5.1 (Rouse, 2013; Chandra, 2012; Wessels & Loggerenberg, 2006; Atwal, 2008; Goosen, 2012).

Table 2.2: Challenges of Standard Security Frameworks

FRAMEWORK	WEAKNESSES
COBIT	❖ It only documents the directions that IT must follow and not how to follow these directions ❖ It does not cater for continuous process improvement ❖ Incongruence exists within COBIT like control objectives not being effectively mapped to process areas and not aligned with business requirements. ❖ Each COBIT domain specifies its own maturity measurement model, based on process areas within that domain. ❖ Does not aid efficient data collection and it does not provide guidelines or options for partial implementation. ❖ The analysis of a COBIT implementation is difficult to achieve and cannot be automated. ❖ Lack of information flow between upper management and implementation teams. ❖ It is complex limiting its adoption in some enterprises that lack the expertise and budgets for its implementation
ISO 27001	❖ It does not provide implementation guidance ❖ Does not specifically address how these processes fit into the overall IT management processes. ❖ Overlook the fact that being certified does not necessarily means that you are secure. Hence if not properly managed, ISMS certifications might lead to a false sense of security ❖ Narrow information security to a particular organisation and ignores outside world.
CAPABILITY MATURITY	❖ Does not specify a particular way of achieving the set goals. ❖ Just because one organisation follows the rules set by the

MODEL	CMM it does not guarantee that it will be successful as there are other factors involved. ❖ CMM only helps if it is put into place early in the software development process. It can't be used as an emergency method of recovering from a difficult position. ❖ CMM is concerned with the improvement of management related activities. Whilst this is a big issue in the software development process it is not necessarily the most important thing to look at. ❖ The CMM ignores the importance of people hence can somehow render individual excellence less important. ❖ The CMM does not effectively describe any information on process dynamics. Instead of modeling these process dynamics, the CMM merely stratifies them.
ISO 17799	❖ Do not deal with financial Issues ❖ Do not deal with corporate governance ❖ Do not deal with ethical conduct ❖ Does not address trust issues

2.10 Summary

The reviewed literature shows that many scholars have found out that there are challenges that face electronic commerce. These challenges include information security staff shortage, lack of security awareness, electronic commerce competition, blended information security attacks lack of government legislation and industrial regulations, mobile work force and wireless computing and immature information security market among others. The literature has cited the issues surrounding information confidentiality. These issues include snooping, spoofing, identity theft, traffic analysis, masquerading, internal threats, malicious software, phishing and pharming. The reviewed literature also shows that there are various approaches that have been used to curb information

confidentiality threats such as encryption, firewalls, access control, authorization, authentication, intrusion detectors, security education and training, use of security policies, antivirus and risk assessment among others.

Further, based on the literature reviewed, there are various existing frameworks and standards which have many weaknesses that limit their adoption. COBIT was found to have weaknesses include: do not cater for continuous process improvement, control objectives not being effectively mapped to process areas and not aligned with business requirements, Lack of information flow between upper management and implementation teams, complex, do not give directions that IT must follow to achieve information security among others and does not deal with the following; ethical values and conduct, privacy issues, internal and external audit for information security program, corporate governance and incident management as reported by Munirul et al. (2011). The literature has also pointed out that for organisations to successfully select an appropriate framework, organizations should understand both the business objectives, requirements and the existing frameworks.

The following were the gaps identified:

(i) There was no specific security standard framework that provides guidance on how to secure ecommerce against information confidentiality threats.

(ii) COBIT which was used as the framework of interest was found to have weaknesses that need to be addressed in order to secure electronic commerce against information security threats effectively.

(iii) The existing COBIT frameworks do not really provide simple and pragmatic guidance needed to secure electronic commerce against information security threats.

The challenges of COBIT were addressed by integrating the framework with ISO 17799 and SSE capability maturity model. The two were found suitable because the areas of weakness in COBIT are security controls addressed in either of them and they are also easy to customize**.**

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

This part covers the methodology that was used in the study. It consists of the research design, target population, sample size and sampling procedures that was be applied, data collection instruments, validity and reliability, procedure for data collection and data analysis.

3.1 Research Design

It is a procedural plan that is adopted by the researcher to answer questions validly, objectively, accurately and economically. Research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedure (Kothari, 2004).

This study used a descriptive survey design. Orodho (2005) observes that a survey is a method of collecting information by interviewing or administering a questionnaire to a sample of individuals. Lokesh (1997) notes that descriptive research studies are designed to obtain information concerning the current situation and other phenomena and whatever possible to draw valid conclusion from facts discussed. Descriptive survey design was appropriate in this research because it enabled the research to explore the information security challenges faced by tour and travel companies practicing electronic commerce and also help in identifying the requirements for the information security framework appropriate for this kind of business.

3.2 Target Population

Population is a group of individuals or events from which the sample will be drawn. According to Cooper and Schindler (2006), a population is the total collection of elements about which we wish to make some inferences. The online travel services segments is the single most successful B2C electronic commerce segment in the sense that it attracts the largest single electronic commerce audience and the largest slice of B2C revenues. The internet is becoming the most common channel used by consumers to search travel options, seek the best possible prices and book reservations for airline

tickets, rental cars, hotel rooms, cruises and tours (Laudon & Traver 2014).The study was carried out in Nairobi where most tour and travel companies are located. There about 57 tour and travel companies in Nairobi (Telkom, 2013). Therefore Nairobi region was purposively selected for this study. The population of this study was obtained from a list that was obtained from the official Nairobi 2013 yellow pages directory published by Telkom Kenya. These 57 tour and travel companies in Nairobi constituted the pollution of this research.

3.3 Sample Size and Sampling Procedure

Sampling is the act, process or technique of selecting a suitable sample or a representative part of a population, for the purpose of determining parameters or characteristics of the whole population (Kombo, 2006). For descriptive studies, 30% of the population is enough (Mugenda & Mugenda, 2003). Stigler (1971) advice of a minimum of 30 for statistical analysis provides a useful rule of the thumb for the smallest number in each category within an overall sample. For the purpose of this study, the researcher used simple random sampling technique. According to Frankel and Wallen (1993), simple random sampling ensures that each element within population has equal and independent chance of being selected.

According to (Kothari, 2004),When field studies are undertaking in practical life, considerations of time and cost almost invariably lead to selection of respondents. The respondents selected should be representations of the total population as possible in order to produce a miniature cross-section. The selected respondents constitute what is technically called ‘sample’ and the selection process is called ‘Sampling Technique ’.
According to Gorard (2003), the purpose of sampling is to use a relatively small number of cases to find out a much larger number. The group you wish to study is termed as the population and the group you actually involve in your research is the sample. This research used random sampling procedure to selected 30 % of the entire population. seventeen tour and travel companies were used in this research.

3.4 Research Instruments

The research was conducted using questionnaires. A questionnaire is a written list of questions, the answers to which are recorded by respondents (Kumar, 2005).

3.5 Validity

Validity is the degree to which an instrument measures what it purports to measure (Borg and Gall, 1989:249). The researcher discussed with colleagues, consulted and got expert judgment from the supervisor to enhance the validity of the data.

3.6 Reliability

3.6.1 Pilot Test Report

Reliability, according Sarantakos (1998), refers to the ability of an instrument to produce consistent results. Reliability is equivalent to consistency.

According to McMillan and Schumacher, (2001), reliability is consistence of measurement thus, the extent to which the results are similar over different form of the same instrument or occasions of data collection. It's the extent to which measures are free from error. To ensure reliability, piloting of the instrument was carried out in three companies which were not involved in the main research. The purpose of the piloting was to find out if the respondents understood the items in the instrument. This enabled the researcher to get a feedback from the research before.

3.6.2 Reliability Analysis

Reliability of the questionnaires was evaluated through Cronbach's Alpha which measures their internal consistency. The Alpha measures internal consistency by establishing if a certain item measures the same construct. Nunnally (1978) established the Alpha value threshold at 0.6 which the study benchmarked against. Cronbach Alpha was established for every objective in order to determine if each scale (objective) would produce consistent results should the research be done later on. The study found that the instrument had reliability (α=0.885). This illustrates that all the four scales were reliable as their reliability values exceeded the prescribed

threshold of 0.6, thus the instrument was reliable to use in collecting data as it helped to achieve the desired research objective.

3.7 Data Analysis

Once all the filled questionnaires were collected, they were validated, edited and then coded. In the validation process, the collected instruments were checked to determine whether an acceptable sample was obtained in terms of proportion of the issued instrument.

Descriptive statistics such as frequency distribution, percentages, means and standard deviations were calculated. This was facilitated by use of the statistical package for social science (S.P.S.S). The data was then presented in tables.

3.8 Research Approach

In order to ensure the security requirements are addressed, this study focused on developing a framework to secure electronic commerce against confidentiality threats based on the components adapted from integrated system theory as suggested by Ismail et al. (2015).

The identified confidentiality challenges and issues were mapped to COBIT, SSE capability maturity model and ISO 17799 to come up with the required Framework. The three frameworks were found to have security controls which complement each other and were flexible for customisation. This was also found necessary to address the weaknesses of COBIT framework.

The proposed Framework was validated using theoretical evaluation through case study. The participants were ICT employees of the organisations sampled whose experience allowed them to provide insight into the **C**ontrol **O**bjectives for **E**lectronic commerce **I**nformation **S**ecurity and related **T**echnologies (**COESIT).**

3.9 Limitations of the Study

There were several limitations that affected the reliability and validity of the findings. The study was not able to control the attitudes of the respondents.

CHAPTER FOUR

4.0 DATA PRESENTATION, ANALYSIS AND INTERPRETATION OF FINDINGS

This research focused on electronic commerce information security threats and challenges faced by tour and travel companies in Nairobi. This chapter presents the findings of the research that includes analysis, interpretation of the data gathered from the field in an attempt to make recommendations on how electronic commerce information security can be improved through the development of a security framework that may provide a support tool to help security managers to enhance security in electronic commerce. This chapter is divided into four sections as follows: Demographic information of the respondents, Information security challenges faced by electronic commerce, Key issues surrounding electronic commerce information security management and Techniques and approaches used in managing Electronic Commerce information security threats. Although the sample consisted of 34 respondents, the researcher was only able to get 28 completed questionnaires were collected for analysis.

4.1 Demographic Information of the Respondents

The background information was sought by the researcher to establish the basis on which the respondents' opinions were based. Hence the researcher sought to establish the gender of the respondents. The findings are summarised in figure 4.1.

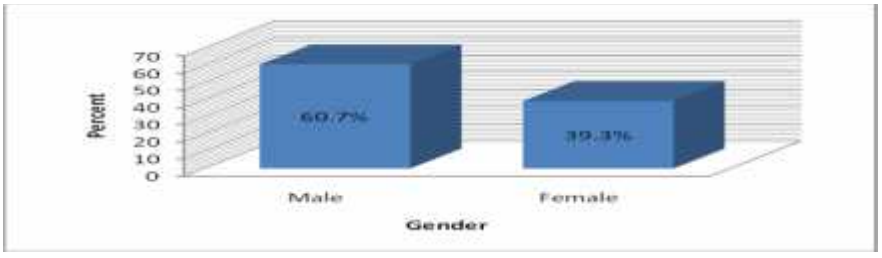


Figure 4.1: Gender of the respondents

Figure 4.1 shows that 60.7% of the respondents were male while 39.3% were female, pointing to the likelihood of the field being male dominated or more preferred by the male gender as compared to the female gender. The researcher further sought to

establish the respondents' length of stay at the organization. Table 4.1 provides a summary of the respondents' length of stay at their respective organizations.

Table 4.1: Length of stay at the organization

How long have you worked in this organization?		
Length of Stay	**Frequency**	**Percent**
1-5 years	11	39.3
6-10 years	8	28.6
11-15 years	5	17.9
Over 15 years	4	14.3
Total	28	100.0

Table 4.1 shows that most (39.3%) of the respondents had stayed in the organization for the least number of years that is 1-5 years while 28.6% had been in the organisation for a period ranging between 6-10 years. A further 17.9% had been in the organization for 11-15 years while the least (14.3%) had worked in their current stations for over 15 years. It was important to find out the experience of the experience of the personnel of those entrusted in maintaining information security in the organizations under study. It has been noted that human factor has a significant role in Information Security. It is confirmed that users' behaviour is linked to technology interaction, data importance perception and security oriented education (Nikolakopoulos, 2009). Information on specific designations or positions held by respondents was also sought and the information is summarised in table 4.2

Table 4.2: Respondents' designation in the IT department

What is your designation in the IT department?		
Designation	**Frequency**	**Percent**
IT Assistant managers	7	25
Information security officer	1	3.6
IT Administrator	1	3.6
IT manager	12	42.6
Network engineer	1	3.6
Data base administrator	2	7.2
IT support staff	4	14.4
Total	28	100.0

Table 4.2 reveals that the positions held by the respondents were varied even though the variation had no effect on the findings of the study. Most (42.6%) of the respondents were IT managers followed by IT assistants and IT support staff at 25 % and 14.4% respectively. The positions of Information Security Officer, IT Administrators and Network engineers were held by an equal but least percentage of only 3.6% of the respondents. The researcher further sought to establish if the organizations had information security officers, the findings are shown in figure 4.2

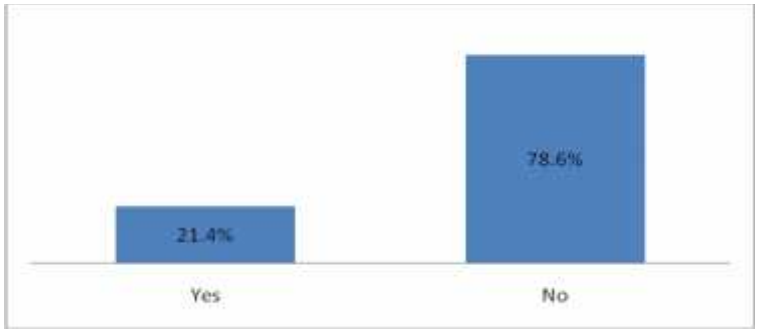


Figure 4.2: Information Security Officers Presence

Figure 4.2 show that only 21.4% of the organizations had information security officers as opposed to the most (78.6%) who did not have them. This may implies that most of

these electronic commerce organizations have not yet taken serious steps to counter the challenges posed by information insecurity. These findings are in line with those of Westervelt (2011). According to him finding qualified information security staff is a difficult task, the industry has not had the time to grow the staff necessary for these roles. Accordingly, information security staff members need to develop security enforcement skills that are not part of the traditional IT staff background. This unique requirement makes it difficult for existing IT staff to transition into information security roles without receiving specialized enforcement training (Westervelt, 2011). Hence a lot still needs to be done to surmount information security challenges faced by these companies. The respondents whose organizations did not have information security officers were further required to state the person who has the responsibility of ensuring that information was secure, figure 4.3 gives a summary of the results

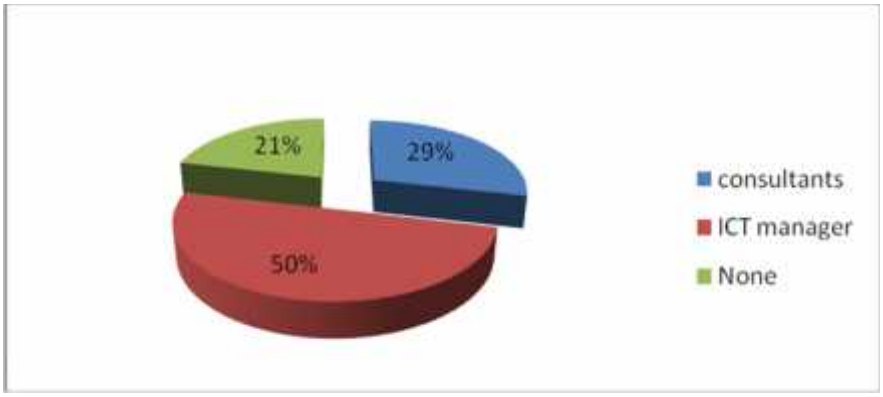


Figure 4.3: Person in charge of Information Security

Figure 4.3 reveals that most (50%) of the respondents mentioned the ICT manager, followed by 29% who indicated that consultants were responsible. The least, (21%) revealed that nobody was responsible for information security in their organizations. This depicts a worrying state of affairs as it is imperative for every organization to bring on board a person who is directly in charge of information security to prevent and limit unwarranted information leakage, or any other confidentiality losses.

4.2 Information Security Challenges Faced by Electronic Commerce

In line with the objectives of the study, the researcher sought to establish the information security challenges faced by electronic commerce. To determine this, the researcher presented a number of items to solicit responses that would address this objective. To start with the researcher sought to establish the budget percentage that organizations spend on security, the findings are summarised in table 4.3

Table 4.3: Budget Set Aside For Information Security

What percentage of your organization budget is spent on information security?		
Security budget	**Frequency**	**Percent**
1-5%	18	64.3
6-10%	5	17.9
11-15%	2	7.1
16-20%	3	10.7
Total	28	100.0

Table 4.3 reveals that most, (64.3%) of the organizations where the respondents are stationed only allocate 1-5% of their budgets to security followed by 17.9% who allocate 6-10% while only 10.7 % allocate 16-20% of their budget to information security. This is a very worrying state of affairs as organizations ought to prioritize information security so as to prevent, loss, leakage and disclosure of confidential information. Kaufmann (2009) observes that electronic commerce organizations place more value to outsmarting their competitors than securing their systems. As result of this very little finances are set aside to cater for information security management while advertisement budget to make these organisations reach more clients continues to grow day by day.

Respondents were further asked to indicate the extent to which they agreed with statements on a five-point Likert scale (strongly agree, agree, don't know, disagree, and strongly disagree). Based on their responses on each item, an average score was computed to establish the extent to which the respondents agreed with the statements.

Figure 4.4 shows the ratings of the respondents on whether electronic commerce organizations place more value on outsmarting competitors than securing information.

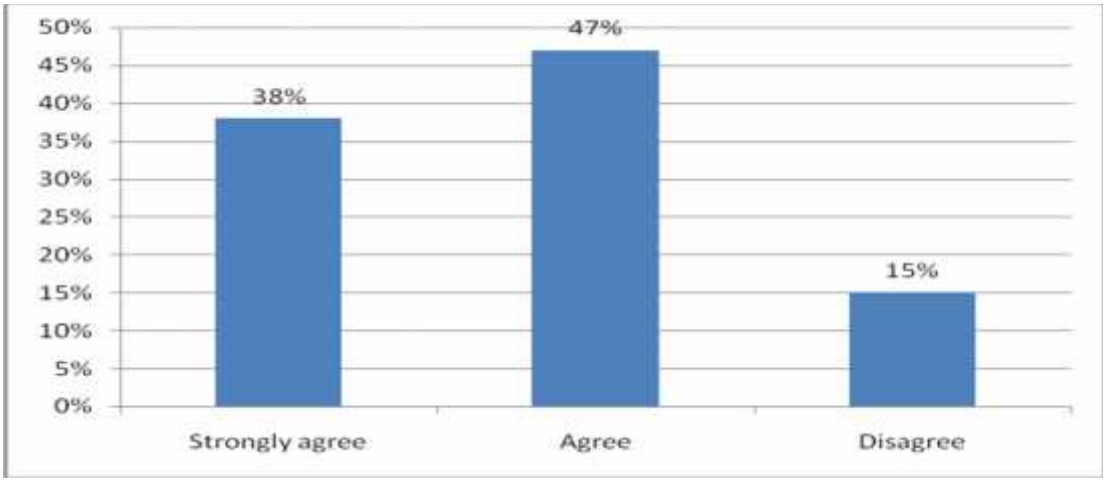


Figure 4.4: Priority on Information System Security

Most, (47%) of the respondents agreed while 38% strongly agreed that most electronic commerce organizations place more value outsmarting competitors than securing their information. The least, only 15% disagreed with this statement. This implies that indeed, most electronic commerce organizations place more value outsmarting competitors than securing their information systems. The lack of emphasis on securing information might be the reason why information in this organisations easily leaks, is accessed by authorised people or even lost. Ideally companies should always strive to secure their information systems. These findings are also in agreement with Niranjanamurthy and Chahar (2013), who observes that competition in electronic commerce has led organization to overlook of the aspect of information security.

The researcher further sought to establish the respondents opinion on finances set aside to secure information as compared to those set aside for advertisements. The findings are presented in table 4.4

Table 4.4: Views on Finances Set Aside to Secure Information

Little finances are set aside to secure information compared to finances set aside for advertisements		
	Frequency	**Percent**
strongly agree	15	53.6
Agree	11	39.3
Disagree	2	7.1
Total	**28**	**100.0**

The findings in table 4.4 reveal that electronic commerce organizations set aside less money for information security in comparison to what they set aside for advertisements as an overwhelming majority of the respondents (53.6%) strongly agreed and 39.3% agreed to this statement. The least, only 7.1% disagreed with the statement. Thus there is a big challenge as concerns budget allocation for information security by electronic commerce organizations that needs to be addressed urgently. Apparently, the organizations do not recognize the need to invest in information security. Loveland and Lobel (2012) observed that insufficient funding for capital expenditures has been a problem in securing information in many organisations.

Table 4.5 shows the response obtained when the respondents were asked to what extent they consider security as the principal concern that restrict customer and organisation not to engage in electronic commerce.

Table 4.5: Opinion on how insecurity restricts customers in electronic commerce

Security is the principal concern that restrict customers and organizations engage in electronic commerce		
	Frequency	**Percent**
Strongly agree	15	53.6
Agree	10	35.7
Disagree	2	7.1
Strongly disagree	1	3.6
Total	**28**	**100.0**

Table 4.5 shows that the majority of the responds (53.6%), strongly agree that security is the principal concern that restrict customer and organisation not to engage in electronic commerce, with 35.7% agreeing with the statement, 7.1% of the respondent disagree and with the least.3.6% strongly disagreeing with it. Hence it is evident that most of the respondents feel that information security is important in electronic commerce. This means that they feel that improved security will attract more audience in electronic commerce. These funding are in agreement with Nivan et al. (2013), who observes that security is one of the principal concern that restrict customers and organizations engaging in electronic commerce.

Further the researcher sought to establish if growth in magnitude, speed and complexity of information security threats has made prevention and clean up more difficult.
The responses are summarized in figure 4.5

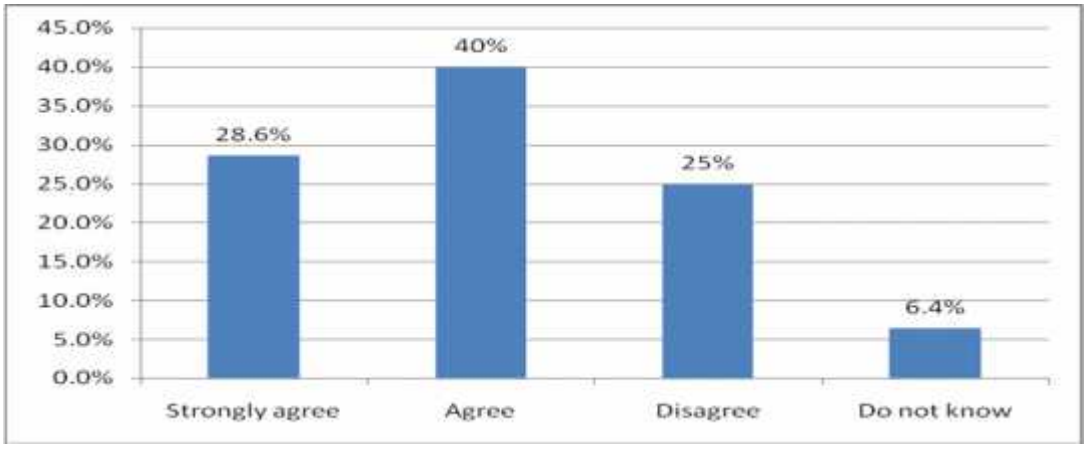


Figure 4.5: Opinion on Difficulty in Cleaning Up Threats

From the responses, majority of the respondents (40 %) and a further 28.6% of the respondents agreed and strongly agreed respectively that growth magnitude, speed and complexity of information security threats has made prevention and clean up more difficult, with 6.4% saying they do not know. the least, 25% disagreed with the statement. This implies that, indeed growth in magnitude, speed and complexity of information security threats has made prevention and clean up more difficult. The researcher further sought respondents' opinion on whether blended threats have made prevention and clean up more difficult. The findings are summarized in figure 4.6

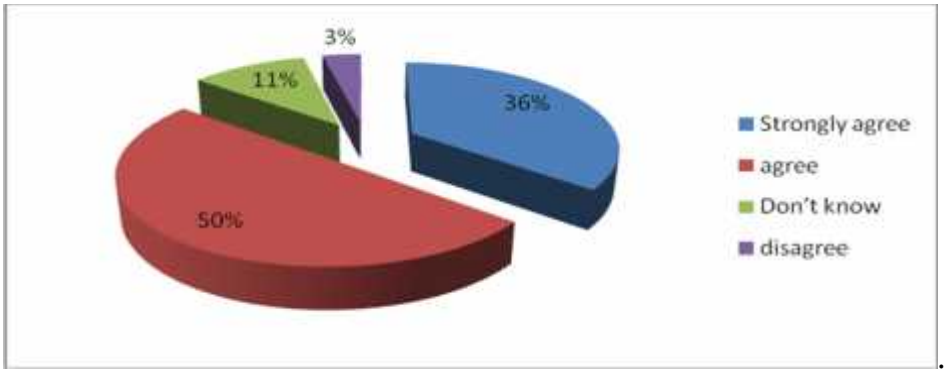


Figure 4.6: Views on Blended Threats

Figure 4.6 reveals that indeed blended threats have made prevention and clean up more difficult with half (50%) of the respondents agreeing and 36% strongly agreeing to the statement. Only 11% of the respondents reported they didn't know while the least, 3%

disagreed with the statement, thus blended threats pose a challenge to information security. According to Rishabh (2014), present-day blended threats, such as Code Red and Nimda, present multiple security threats at the same time, causing major disruptions and billions of dollars of damage to enterprises. Accordingly, blended threats combine different types of malicious code to exploit known security vulnerabilities. The respondents also agreed with the fact that one of the biggest information security challenges is that the information security market is still in its infancy with few formal standards established for products or services. Figure 4.7 summarizes the responses

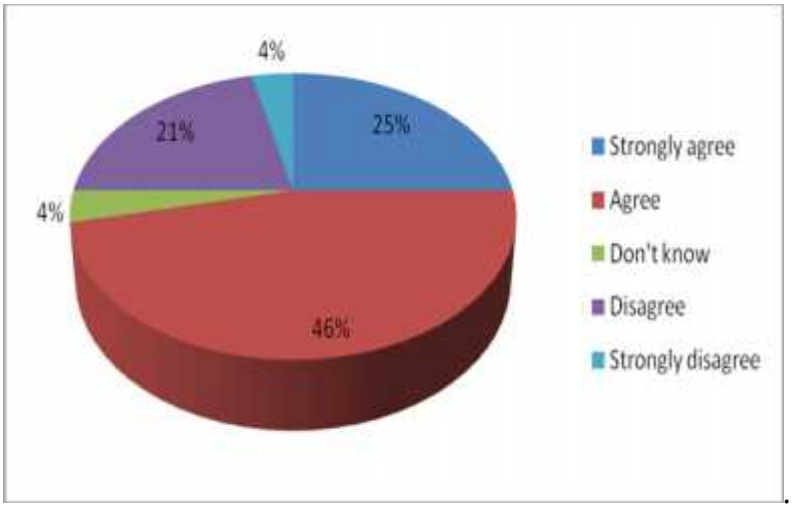


Figure 4.7: View on Information Security Market

Of all the respondents, most, 46% agreed, 25% strongly agreed with a few, 21% disagreeing with the statement. The least, 4% reported that they did not know. Hence the fact that the information security market is still in its infancy with few formal standards established for products or services is a major challenge as reported by the respondents. According to Rishabh (2014), the information security market is still in its infancy, with few formal standards established for products or services. Furthermore, only earlier versions of standards exist, forcing companies to complete multiple installations of "point" solutions that only provide individual components of their security systems. The researcher further sought respondents' opinion on whether information security techniques available in the market address only a portion of a company's security needs

forcing companies to have multiple installations. The findings are summarized in Table 4.6

Table 4.6: Views on Information Security Techniques Available In the Market.

Information security techniques available in the market address only a portion of a company's security needs forcing companies to have multiple installations		
	Frequency	**Percent**
Strongly agree	15	53.6
Agree	8	28.6
Don't know	2	7.1
Disagree	2	7.1
Strongly disagree	1	3.6
Total	28	100.0

The responses in table 4.6 reveal that the respondents agreed with the statement, with the most, 53.6% strongly agreeing followed by 28.6 % simply agreeing to it. Only 7.1 percent disagreed with the statement. The respondents were further required to state whether they agreed or disagreed with the fact that there is no unified approach that can be used to secure information, their responses are summarized in figure 4.8

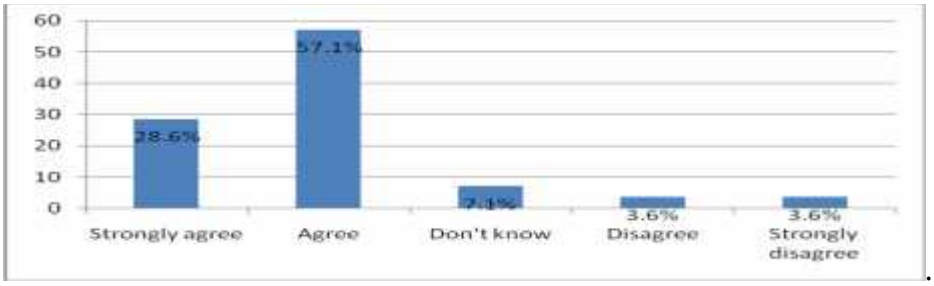


Figure 4.8: Opinions on Availability of a Unified Approach

Of all the respondents, the most 57.1% and 28.6% agreed and strongly agreed respectively with the statement. The least 3.6% disagreed with the fact that there is no unified approach that can be used to secure information. Hence lack of unified approach that can be used to secure information is a big challenge to information security amongst organizations in Kenya. However, the respondents disagreed with the fact that finding qualified information security staff is difficult. Their responses are summarized in table 4.7.

Table 4.7: Views on Availability of Information Security Staff

Finding qualified information security staff is difficult		
	Frequency	**Percent**
Strongly agree	3	10.7
Agree	11	39.3
Don't know	1	3.6
Disagree	12	42.9
Strongly disagree	1	3.6
Total	**28**	**100.0**

From the responses in table 4.7, most, 42.9% of the respondents disagreed with the fact that finding qualified information security staff was difficult; however a closer percentage, 39.3% and 10.7% agreed and strongly agreed respectively with the statement. This constitutes a total of 50% of the respondents agreeing that finding a qualified information security staff is a problem. These findings disagree with those of Kauffman (2009) who indicated that Finding qualified information security staff is a difficult task for many organisations, according to the author, driving the hiring challenge is the immaturity of the solutions from information security vendors, the limited number of qualified staff available, and the unique blend of information security skills required. Thus business executives will need to invest more in this area to

overcome these challenges. The respondents were further required to either agree or disagree with the fact that information security challenges keep growing at a rapid pace hence continuous awareness training are necessary which electronic commerce organizations find hard to cope. Table 4.8 provides a summary of the responses:

Table 4.8: Respondent's Views on Continuous Awareness Training

The information security challenges keep growing at a rapid pace hence continuous awareness trainings are necessary which electronic commerce organizations find hard to cope		
	Frequency	**Percent**
Strongly agree	13	46.4
Agree	13	46.4
Don't know	2	7.1
Total	28	100.0

Most (46.4%) of the respondents strongly agreed with the statement while a similar percentage(46.4%) agreed with the statement. None of the respondents disagreed with the statement as no response was capture under disagreed or strongly disagreed. Hence the fact that information security challenges keep growing at a rapid pace hence continuous awareness training are necessary which electronic commerce organizations find hard to cope. These findings are consistent with what Olsen (2013) observed. He noted that training and education is a key piece of puzzle that is often neglected. Companies do not communicate with employees enough about why they are making the changes and what is expected of them as they adopt these technologies, end users are basically the first and the last firewall, so it is critical that they understand their role and responsibilities in safe guarding the data on the network (Olsen, 2013).

The researcher further sought to establish whether unique requirements for information security officers makes it difficult for existing IT staff to transition information security

without receiving specialized enforcement training. The responses are presented in table 4.9

Table 4.9: Views on why Enforcement Training To Existing ICT Staff Difficulty.

Unique requirements for information security officers makes it difficult for existing IT staff to transition into information security personnel without receiving specialized enforcement training		
	Frequency	**Percent**
Strongly agree	3	10.7
Agree	11	39.3
Don't know	1	3.6
Disagree	8	28.6
Strongly disagree	5	17.9
Total	**28**	**100.0**

Table 4.9 shows that the respondents agreed with the statement with the most 39.3% and 10.7% of the respondents agreeing and strongly agreeing respectively. On the other hand, 17.9 % strongly disagreed with the statement. Hence the unique requirements for information security officers makes it difficult for existing IT staff to transition information security without receiving specialized enforcement training. These findings are also in line with Kauffman (2009) who indicated that the unique requirements for information security officers makes it difficult for existing IT staff to transition into information security roles without receiving specialized enforcement training.

The researcher further sought the respondents opinions on whether there are inadequate government and industry regulations to ensure personal information was protected from

loss, misuse, unauthorized access or disclosure, the responses are summarized in figure 4.9.

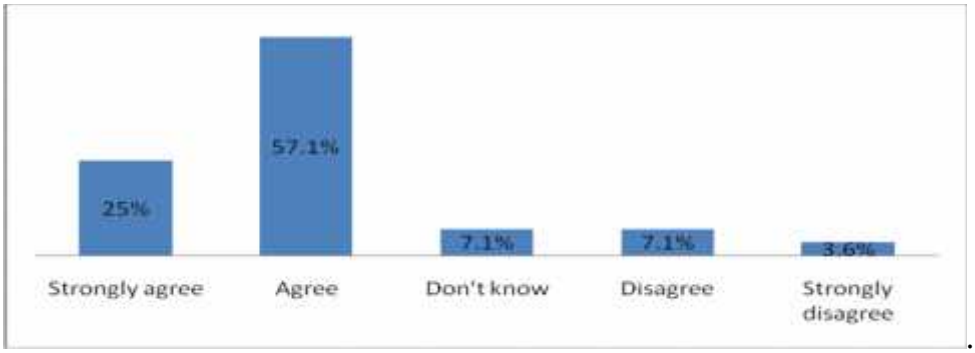


Figure 4.9: Views on regulations on information confidentiality

Figure 4.9 shows that most(57.1%) of the respondents agreed with a further 25% strongly agreeing with the fact that there were inadequate government and industry regulations to ensure personal information was protected from loss, misuse, unauthorized access or disclosure. Only 7.1% disagreed with the least 3.6%, strongly disagreeing to the statement. According to Saleanu (2013) legitimate businesses face the challenge of lack or little legal recourse to combat illicit activities of software pirates in their countries. According to Saleanu (2013), unless business executives put strategies in place to protect their intellectual property and customer information, they run the risk of falling victim to these individuals. These finding are also consistent with what Mutung'u (2012) noted. She noted that although in Kenya the right to privacy is guaranteed in the Constitution, this right has not been translated into national legislation. For instance, there are no data protection laws to guarantee that data collected in the online realm is protected from unauthorized access. To a large extent, the Kenyan online community does not concern itself with intellectual property rights. Users share content freely, many times without attribution. Many rights holders have also disseminated some of their content through social media. This has mostly worked positively for these people by promoting their content to a wider audience.

The researcher also sought to determine whether the Kenyan government placed priority on protection of personal information or intellectual property. The information is summarized in table 4.10.

Table 4.10: Kenyan Government Protection of Personal Information

Kenyan government does not place high priority on protection of personal information		
	Frequency	**Percent**
Strongly agree	5	17.9
Agree	8	28.6
Disagree	10	35.7
Strongly disagree	5	17.9
Total	28	100.0

Table 4.10 shows that the respondents disagree that the Kenyan government placed priority on protection of personal information or intellectual property with 35.7% and 17.9% disagreeing and strongly disagreeing respectively. On the other hand only 28.6% agreed with the statement. Thus it is evident from the findings that the Kenyan government placed priority on protection of personal information or intellectual property. Saleanu (2013) indicated that one major challenge facing information security was that certain countries did not place a high priority on protection of personal information or intellectual property.

Further the researcher sought to determine if mobile computing devices owned by organization employees are a threat to information security. The information is summarized in table 4.11.

Table 4.11: Views on Mobile Computing Devices and Information Security

Mobile computing devices such as flash disks, laptops, iPods, tablets, Smartphone's and USB cables owned by organization employees are a threat to information security		
	Frequency	**Percent**
Strongly agree	17	60.7
Agree	7	25
Strongly disagree	4	14.3
Total	28	100.0

Table 4.11 shows that the majority at 60.7 % strongly agreed closely followed by 25 % who simply agreed to the statement. The least, 14.3% strongly disagreed. Hence mobile computing devices such as flash disks, laptops, iPods, Smartphone's and USB cables owned by organization employees are a threat to information security. These findings are in agreement with Olsen (2014), who observes that two thirds of employees regularly use two or more devices at work. It is predicted that number of employee-owned smartphones and tablets used in enterprise will grow to 350 million in 2013. All this does not even begin to take into account the threats posed by lapses in physical security. Olsen (2014) observes that mobile phones are frequently lost or left behind, this is a threat to confidential corporate data when become exposed by someone circumventing a password. This would be relatively an easy task to a seasoned hacker. Stolen devices can comprise even the most protected encrypted data, as well as to lead to unauthorized access to corporate services, as email and the VPN. Olsen (2014), further reports that, malware for Android rose by 400% between 2010 and 2011. According to Westervelt (2011), security experts have cautioned enterprises from ignoring the future risks that smartphones and other mobiles devices pose to corporate data leakage. According to the author the attack surface is much greater on mobile devices and there are far fewer security controls. As a result, companies need to ensure that their

information security program extends to all devices that frequently leave the office and that are easily lost or stolen. Moreover, they can no longer count on safely locking computers in the offices when employees go home at night. Thus controls must be put in place to control wireless communications USE to ensure that the company's most valuable secrets are secure. Long W. (2013) points out that the use of personal devices in the workplace continues to rise, as do the potential legal and data protection risks, and so businesses oganisations need to think carefully about BYOD and put in place appropriate policies and processes to tackle these issues and thereby minimise the risks with bring your own device (BYOD).

Further, the researcher established that in Kenya there is little legal recourse to combat the illicit activities of software pirates and cyber crimes as presented in Table 4.12.

Table 4.12: Kenyan Government Fight On Cyber Crimes

In Kenya there is little legal recourse to combat the illicit activities of software pirates and cyber crimes		
	Frequency	**Percent**
Strongly agree	10	35.7
Agree	14	50
Don't know	1	3.6
Disagree	3	10.7
Total	28	100.0

Table 4.12 shows that the statement is true with a majority at 50% and 35.7% agreeing and strongly agreeing with the statement respectively. The least 3.6% disagreed with the statement, hence the findings justify that in Kenya there is little legal recourse to combat the illicit activities of software pirates and cyber crimes.

Further the researcher sought to establish the respondents' opinion on whether there is a lack of consumer education on security threats; the responses are summarized in table 4.13.

Table 4.13: Views on Consumer Education on Security Threats

There is lack of consumer education on security threats		
	Frequency	**Percent**
strongly agree	13	46.4
Agree	11	39.3
Disagree	3	10.7
strongly disagree	1	3.6
Total	28	100.0

A majority of the respondents, at 46.4% and 39.3 % agreed and strongly agreed respectively with the statement that there is lack of consumer education on security threats. Only 10.7% disagreed with the least at 3.6% strongly disagreeing with the statement. Hence the findings reveal that there is lack of consumer education on security threats. Reeder (2011), three-quarters of mobile applications store sensitive user account information in an unencrypted form on the mobile device. Offending apps on mobile devises include LinkedIn, Netflix, Skype, Gmail, Yahoo Mail and Groupon. Researchers discovered that the applications store on mobile devises transmitted data such as security credentials, personal financial information, private communications and sensitive company data. According to the research, username was the most common piece of unprotected data with 76% of the 100 apps keeping usernames in plain text. Ten percent were storing the user's password in plain text. Also these finding are line with what Ackerman and Davis (2013) that educating the consumers on security issue is still in the infancy stage but still prove most critical element of the electronic commerce security architecture.

Suggestion given by respondents on to Address the Challenge Facing Electronic Commerce

The respondents were further asked to give their opinion on what should be done in order for electronic commerce organizations to overcome the mentioned challenges, the responses included: enactment of strict laws strict laws governing handling of confidential information in electronic commerce organizations, conducting consumer education on information security, development of electronic commerce regulation, constant monitoring of information security threats, promotion of international information security standards, increase in security budget allocation and employment of information security officers in all electronic commerce organizations.

4.3 Key Issues Surrounding Electronic Commerce Information Security Management

In line with objective two of the research, the researcher sought to determine key issues surrounding electronic commerce information security management. The researcher presented a number of items to solicit responses that would address this objective. Firstly, the researcher sought to establish what the respondents' considered the top security issue of concern to their organisations, the responses are summarised in figure 4.10.

Figure 4.10: The top security issue of concern to your organisation

Figure 4.10 shows that the respondents considered confidentiality and privacy as the top security issue of concern to their organisations at 60.7% followed by integrity at 21.4%.

The issue of availability was mentioned by the least, 17.9% of the respondents. This implies that indeed confidentiality and privacy is an important security issue in electronic commerce organizations, hence a lot emphasis ought to place on addressing it. These findings echo what Nivan et al. (2013) observed. They observed that Privacy and security are major concern for electronic commerce.

The researcher further sought to establish what the respondents considered to be top three main causes of security incidents in their organizations table 4.14 presents the findings.

Table 4.14: Views on the Main Causes of Security Incidents

What do you consider to be top three main causes of security incidents in your organization?		
	Frequency	**Percent**
Viruses and malicious software	13	46.4
Human errors and omissions	8	28.6
System or software errors	5	17.9
Hardware failure	2	7.1
Total	28	100.0

Table 4.14 reveals that the respondents considered viruses and malicious software at 46.4%, followed by human errors also at 28.6% and lastly system or software errors at 17.9% as the top three main causes of security incidents in their organizations. Loudon et al. (2010), indicate that sharing files over peer-to-peer (P2P) networks, such as those for illegal music sharing, may transmit malicious software or expose information on either information on either individual or corporate computers to outsiders this can occur through Trojan horse. Furthermore E-mails may contain attachments that serve as springboards for malicious software. These findings reflect what was observed by Nivan et al. (2013). They observed that Trojan horse programs launch against client systems

pose greatest threat to electronic commerce because they by pass or subvert most of the authentication an authorization mechanisms used in an electronic commerce transaction. Viruses are a nuisance threat in electronic commerce.

This implies that any effort geared towards address information insecurity security should lay emphasis on these three issues. Further the respondents were required to state whether their organizations' network has ever experienced any of the following problems since they began using it. The first problem was unauthorized access or interception of data. Their responses are summarized in table 4.15.

Table 4.15: Views on occurences of unauthorized access

Unauthorized access to or interception of data		
	Frequency	**Percent**
Yes	17	60.7
Never	6	21.4
Do not know	5	17.9
Total	28	100.0

Table 4.15 shows that majority(60.7%) of the respondents reported that their networks had experienced the problem of unauthorized access to or interception of data with 21.4% reporting they had never while the least 17.9%, reporting they didn't know if such a problem had occurred. Hence from the responses, unauthorized access to or interception of data is a security threat to electronic commerce organizations. These findings reflect what was observed by Nivan et al. (2013).They observed that Trojan horse programs launch against client systems pose greatest threat to electronic commerce because they by pass or subvert most of the authentication an authorization mechanisms used in an electronic commerce transaction.

Further the respondents were required to sate if the username or password leakage had been a problem in their organizations. The finding are summarized in figure 4.10

Figure 4.11: Username and Password leakage

Figure 4.11 shows that an overwhelming majority (89%) of the respondents' organizations had experienced username or password leakage with a just 11% reporting not to have experienced this problem. These finding are consistent with what was observed by Keanini (2014). He observed that more individuals on the net are having their email, social media and other accounts compromised because of weak passwords.Web link to an address being different to an intended one was evidently not a big challenge as shown in table 4.16.

Table 4.16: Experiences of Web Link to Different Addresses

Web link to an address different from the intended one		
	Frequency	**Percent**
Yes	5	17.9
Never	18	64.3
Do not know	5	17.9
Total	**28**	**100.0**

Majority, (64.3%) of the respondents reported never having experienced web links to different sites other than the intended ones while only 17.9% reported having

experienced it. A similar percentage 17.9%, reported that they did not know if such a problem had ever been experienced in their organizations. Hacking was reported to have occurred as an overwhelming majority reported that their organization networks had been hacked before, figure 4.12 provides a summary of the results

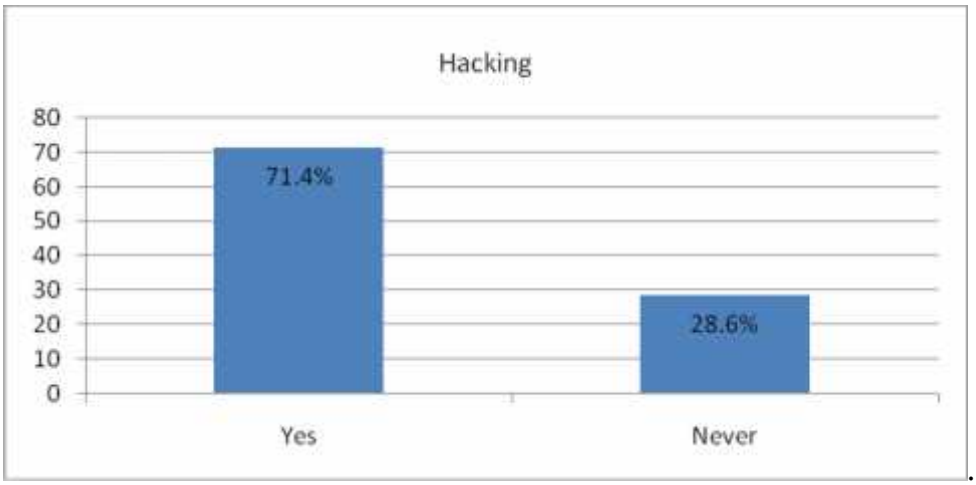


Figure 4.12:Views on Occurrence of Hacking

Figure 4.12 shows that an overwhelming majority (71.4%) of the respondents reported having had their organizations' networks hacked while the least, 28.6% reported never having had their networks hacked. These responses imply that hacking is a big information security issue as it has been experienced by an overwhelming number of electronic commerce organizations; hence emphasis has to be placed on finding ways of addressing it. These finding echoes what happened in Kenya where a leading media house's payroll information for April 2012 was published online. Soon after in May, 2012 sensitive information from a leading NSE listed company were also published online after their systems were hacked (Serianu, 2012).

In an effort to establish key issues in information security, the researcher further sought to determine whether the respondents had experienced theft of business as well as sensitive customer information from their organizations' websites. The responses are summarized in figure 4.13.

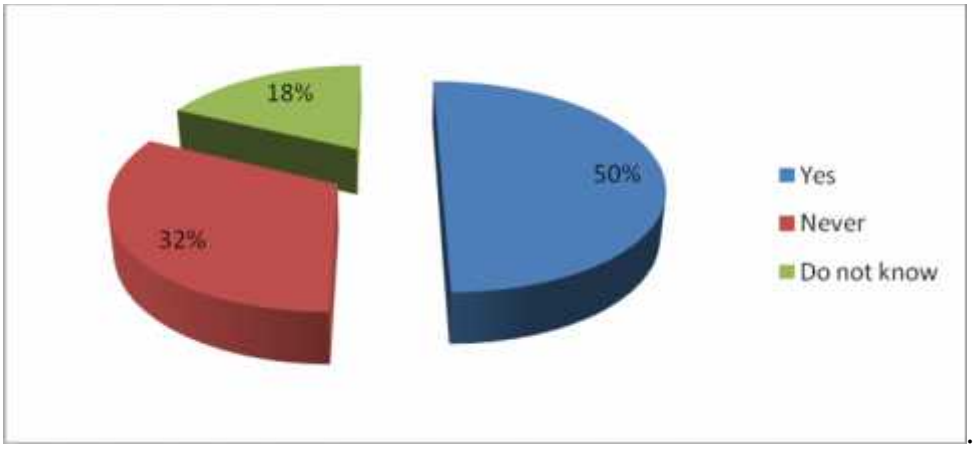


Figure 4.13: customers' information Theft from websites

Figure 4.13 reveals that indeed theft of business as well as sensitive customer information from respondents' organization websites takes place with a majority at 50% admitting it had happened followed by 32% who said this has never happened to their networks. The least at 18% reported that they did not know if such a thing had ever occurred. This findings are in line with what Manktelow (2013) reported. He observed that data theft and security issues are increasing each year, leading to financial losses, intellectual property theft, identity fraud, and compromised reputations. According to Roman (2013), Adobe's 2.9 million customers' personal information, including encrypted payment card numbers were accessed by attackers. The respondents further reported that indeed it was true that they had received e-mail messages that looked like those of legitimate business partners or financial institution they bank with yet in the real sense they were fake. Table 4.17 gives a summary of the responses.

Table 4.17: Experiences on Phishing in Organisations

Receiving e-mail messages that look like those of legitimate business partners or financial institution you bank with but in the real sense they are fake		
	Frequency	**Percent**
Yes	18	64.3
Never	9	32.1
Do not know	1	3.6
Total	28	100.0

Table 4.17 reveals that receiving e-mail messages that look like those of legitimate business partners yet in real sense they are fake had occurred with a majority at 64.3% agreeing with it. Only 32.1 % said this had not happened to them with the least, 3.6% reporting that they did not know if such a thing had ever taken place in their organizations. Hence this is a real issue that affects electronic commerce organizations as shown by the overwhelming majority who said it has happened to them. This is in line with a report by Telecoms (2013). According to the report, a research and information centre director has warned bankers of the increasing incidence of internet fraud, committed by hackers who are able to overwrite passwords and make unauthorised intrusions into corporate websites.

The researcher also sought to establish if employees have ever been tricked to give confidential information about their organizations or about their customer by people claiming to be legitimate authorities. The responses are presented in table 4.18

Table 4.18: Experiences of Social Engineering

Employees being tricked to give confidential information about your organization or about your customer by people claiming to be legitimate authorities		
	Frequency	**Percent**
Yes	13	46.4
Never	10	35.7
Do not know	5	17.9
Total	28	100.0

Table 4.18 shows that the majority of the respondent's organizations, at 46.4% had encountered this problem while 35.7 % reported not having encountered this problem. Only 17.9% reported that they did not know if such a problem had been encountered by their organizations. This findings are consistent with what Mwakalinga (2011), noted that information security systems that use only technical security measures have a hard time keeping up with attackers who use both social and technical measures. He noted that attackers can design new social and technical methods of attacking information security systems.

The study wanted also to find out whether sacked employees have ever revealed customers' confidential information. A majority of the respondents at 64% further reported not being aware of the fact that sacked employees reveal confidential information about their organizations and customers. The results are summarized in figure 4.14.

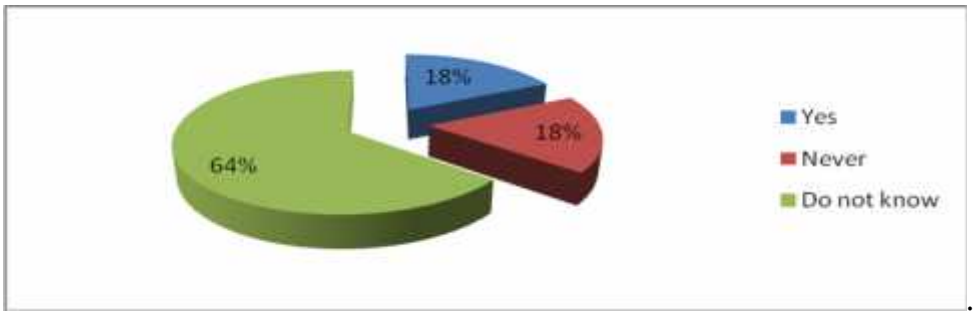


Figure 4.14: Threat of Sacked Employees

From figure 4.14 only 18% of the respondents agreed that sacked employees reveal confidential information about their organizations or about customers with another 18 % saying they did. Hence this is not a major information security concern as only a small percentage thought it was an information security problem with a majority, 64%, reporting they are not aware of it. These findings disagree with those Patil, (2008), who revealed that in an effort to secure electronic commerce, organizations tend concentrate more on technology.

Further, most respondents, at 53.6% reported that their organizations had never encountered disgruntled employee revealing confidential information about a customer. Table 4.19 gives a summary of the responses.

Table 4.19: Disgruntled employees and information security

Disgruntled employees revealing confidential information about your customer		
	Frequency	**Percent**
Yes	7	25.0
Never	15	53.6
Do not know	6	21.4
Total	28	100.0

Most respondents, at 53.6% reported that their organizations had never encountered with only 25% of the respondents saying they had witnessed it while the least, 21.4% reported they did not know if disgruntled employees had ever revealed confidential information about a customer. The findings also do not agree with (Norman & Yasin, 2010) who reported that employee/people issues in electronic commerce is one of the research gaps that need to be address in researches (Norman & Yasin, 2010).

Further the researcher sought from the respondents if the electronic commerce organizations had experienced attacks using malicious software such as viruses, worm or Trojan horse, the responses are summarized in table 4.20.

Table 4.20: Attacks of Malicious Software

Attacks using malicious software such as viruses, worm or Trojan horse		
	Frequency	**Percent**
Yes	18	64.3
Never	9	32.1
Do not know	1	3.6
Total	28	100.0

Table 4.20 reveals that the most, 64.3% of the respondents, agreed that attacks using malicious software such as viruses, worm or Trojan horse was an information security issue while the least 32.1% reported that this had never been an issue. The least, 3.6% reported they did not know if this was an issue. These observations are consistent with what Nivan et al. (2013) observed that Trojan horse programs launch against client systems in electronic commerce are on the increase.

The resercher further sought to determine if users of respondents' organization web sites would be redirected to bogus web pages even when they typed in the correct webpage into their browser. The responses are summarized in figure 4. 15.

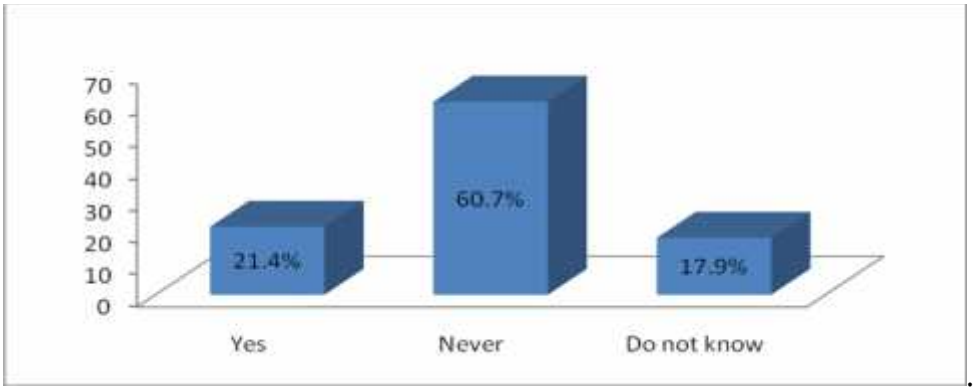


Figure 4.15: Incidences of Pharming in Respondents' Organizations

From figure 4.16, majority (60.7%) of the respondents reported that they had never encountered such a problem with only 21.4% reported that such a problem had been encountered. The least, 17.9% said they did not know if such a problem had ever occurred. Thus the issue of users of respondents' organization web sites being redirected to bogus web pages was not a major problem encountered by electronic commerce organizations.

4.4 Techniques and Approaches Used in Managing Electronic Commerce against Information confidentiality Threats

In line with objective 3 of the study, research sought to determine techniques and approaches used in managing electronic commerce information security threats. The research presented a number of items to solicit responses that would address this objective. Firstly, the research sought to establish if the respondent's organisations use firewalls information security approach to overcome electronic commerce information security threats, the responses are summarised in figure 4.16.

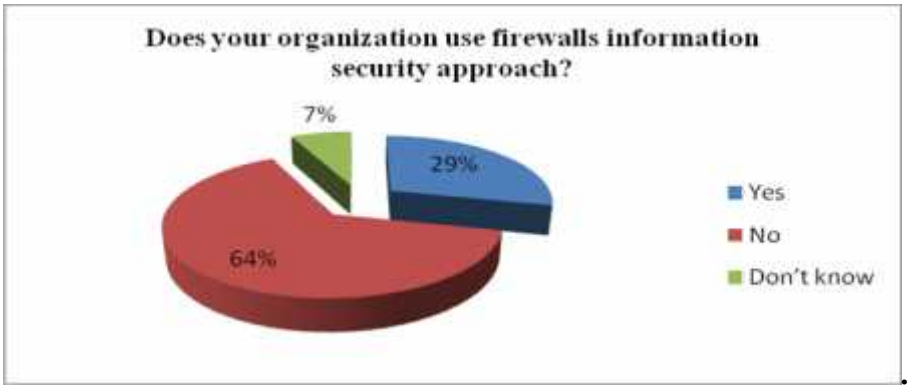


Figure 4.16: View of Uses of Firewalls

Figure 4.16 shows that the majority, 64% of respondents reported that their organizations did not use firewalls to overcome electronic commerce information security threats, just 29% said their organizations employed the use of firewalls, the least, 7% reported that they did not know if their organizations employed the use of firewalls information security approach to overcome electronic commerce information

security threats. Hence there is need for electronic commerce organizations to embrace firewalls in combating information security. Although firewalls are an essential part of any information security system being the first defense line against security attacks, Hayajneh et al. (2013) found that there is limited usage of fire walls and lack of awareness regarding the importance. This concurs with the findings of this study.

Further the researcher sought to determine if the organizations used authentication control information security approach to overcome information security threats. Figure 4.17 presents the findings

Figure 4.17: Vies on Uses of Authentication control

Figure 4.17 reveals that a majority, at 71% used authentication control information security approach with only 25% of the respondents reporting that their organizations did not use this approach. The least, 4% reported they did not know if authentication control information security approach was used by their organizations to guard against information security threats.

The respondents were further required to state whether their organizations used authorization control information security approach. Table 4.21 presents the findings.

Table 4.21: Views on use of authorization

Does your organization use authorization control information security approach?		
	Frequency	**Percent**
Yes	9	32.1
No	19	67.9
Total	28	100.0

Table 4.21 reveals that, most respondents' organizations, at 67.9% did not employ the use of authorization control, with the least 32.1% agreeing that their organizations use this technique. Hence there is need for more of these electronic commerce organisations to embrace this technique. Further the researcher sought to determine if the organization use international standard framework to manage information security, the responses are summarized in table 4.22.

Table 4.22: Views on the uses of frameworks

Does your organization use standards/framework information security approach?		
	Frequency	**Percent**
Yes	3	10.7
No	24	85.7
Don't know	1	3.6
Total	28	100.0

The finding in table 4.22 show that most, 85.7% of the respondents did not use standard/framework to manage information security with only 10.7 % of them admitting to using them. Hence there is need for these organizations to embrace the use of standard/framework information security approach in order to reduce or overcome information security threats. This is also a pointer to the fact that there is a need to develop a framework to guide security implementation in electronic commerce

organisations. The study also established that organizations employed antivirus information security approach with the majority at 89.3% admitting while only 10.7% of the respondents reported that their organizations did not use antivirus information security approach. The information is summarised in table 4.23.

Table 4.23: Views on the uses of antivirus

Does your organization use antivirus information security approach?		
	Frequency	**Percent**
Yes	25	89.3
No	3	10.7
Total	28	100.0

The respondents were further required to state whether their organizations updates the antivirus regularly. Table 4.24 summarises the response obtained.

Table 4.24: Uses of Updated Antivirus

Does your organization updates antivirus used regularly?		
	Frequency	**Percent**
Yes	15	53.6
No	13	46.4
Total	28	100.0

The responses indicate that 53.6% of the organizations used in the research do not update their antivirus regularly. This means that although majority of the organizations use antivirus this approach is not effective. Its only 46.4% of the organizations update their antivirus.

The respondents were further required to state whether their organizations used intrusion detectors in their effort to secure information. Figure 4.18 gives a summary of the responses.

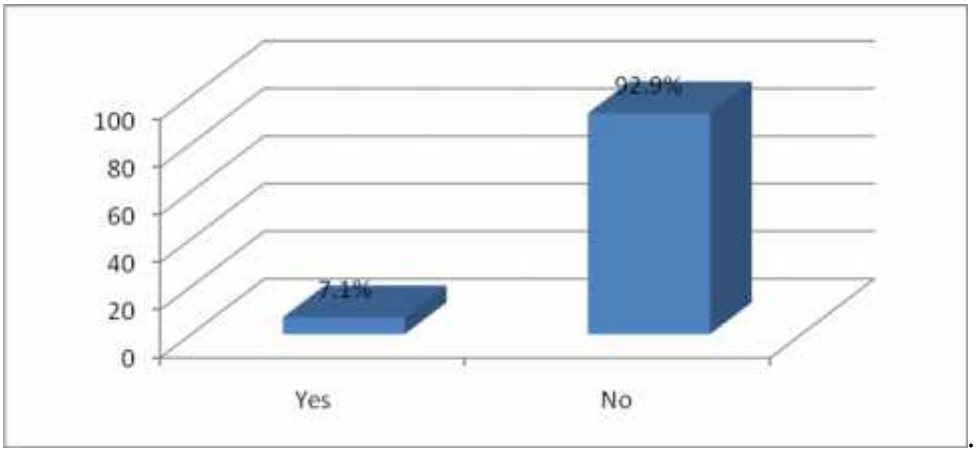


Figure 4.18: Views on Uses Intrusion Detectors

Figure 4.18 reveals that the majority at 92.9% of the companies do not use intrusion detectors in managing information security, the least, 7.1% of the respondents employed this method. This depicts a sorry state of affairs as concerns information security. Hence these organizations need to be encouraged to embrace this approach to improve information security. Further the respondents were required to indicate whether their organizations used security education and training information security approach. Table 4.25 presents the findings.

Table 4.25: View on Use Security Education and Training

Does your organization use security education and training information security approach?		
	Frequency	**Percent**
Yes	4	14.3
No	24	85.7
Total	28	100.0

Most, (85.7%) of the respondents denied that their organizations used this approach with the only 14.3% admitting that their organizations make use of this approach, thus, there is need to sensitize these organizations on the benefits of this approach in enhancing information security. Further, most (82.1%) of the respondents indicated that their organizations did not use risk assessment information security approach as indicated in table 4.26.

Table 4.26: Use of risk assessment in security management

Does your organization use Risk Assessment information security approach?		
	Frequency	**Percent**
Yes	5	17.9
No	23	82.1
Total	28	100.0

Table 4.26 indicates that just 17.9% of the respondents reported that their organizations used risk assessment information security approach; however a whooping majority at 82 % did not. This implies that a lot needs to be done to encourage all these companies to incorporate this approach in their information security strategies. In response to whether their organizations used activity monitoring and audit using system logs or otherwise information security, the respondents reported as indicated in figure 4.19.

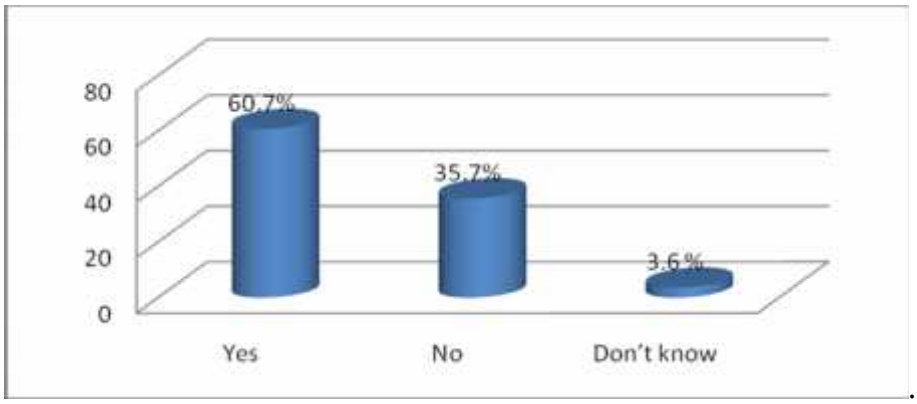


Figure 4.19: views on Uses System Logs

Figure 4.19 reveals that most (60.7%) of the respondents admitted that their organizations employed the approach while 35.7% indicated they did not use the approach. The least 3.6% indicated that they did not know if their organizations used the above approach. Hence there is need to bring on board all the electronic commerce organizations especially those that don't use the approach so that they can benefit from it. The respondents were further required to state the extent to which they agreed with given statements about their organizations: Firstly, they were asked to either agree or disagree with the statement: Senior, management regularly received reporting on the status of the information security, their responses are summarized in figure 4.20.

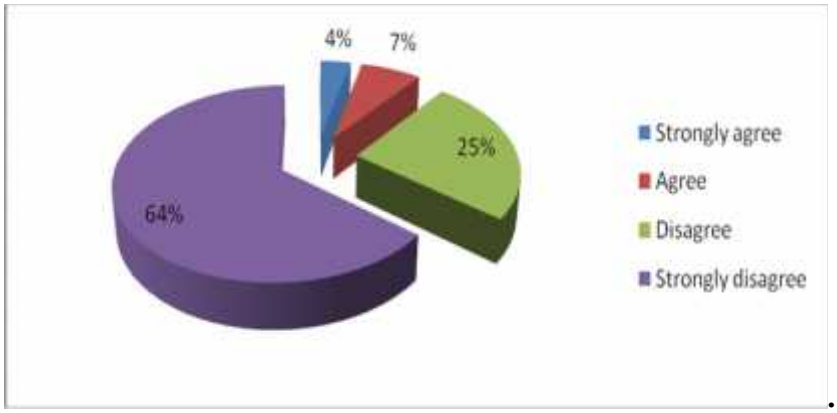


Figure 4.20: Views on Information Security Reporting

Figure 4.20 shows that 64% of the respondents strongly disagreed that Senior, management regularly received reporting on the status of the information security, Followed by 25% who just disagreed. On the other hand only 25% agreed that their senior, management regularly received reporting on the status of the information security, with the least 4% saying they did not know if it that takes place. The respondents were further required to indicate whether their organization employees understood the importance of information security. Their responses are summarized in table 4.27.

Table 4.27: Opinion on Awareness on Information Security

Our organization employees understand the importance of information security		
	Frequency	**Percent**
Strongly agree	12	42.9
Agree	6	21.4
Disagree	2	7.1
Strongly disagree	8	28.6
Total	28	100.0

Table 4.27 shows that the majority (42.9%), strongly agreed with the fact that their organization employees understood the importance of information security, with 28.6% strongly disagreeing with the statement. 21.4% agreed with the statement with the least 7.1% disagreeing with it. Hence it is evident that most of the organization employees understand the importance of information security. The respondents were then asked if senior management provided the required level of support for information security. Figure 4.21 presents a summary of the responses.

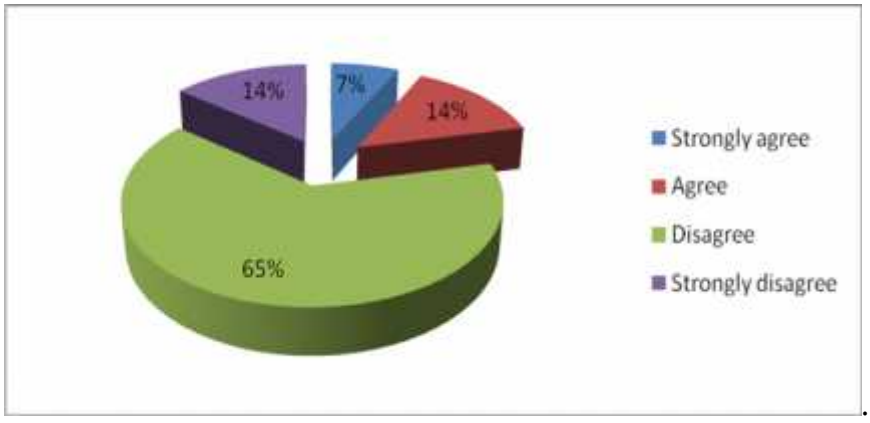


Figure 4.21: Views on Support of Senior Management

Majority (65%) of the respondents disagreed with 14 % strongly disagreeing with the statement. Only 14% of the respondents agreed with the statement with 7% strongly agreeing. This depicts a bad state of affairs in these electronic commerce organizations

as under normal circumstances senior management staff are required to offer all the necessary support for any task to be accomplished. Hence a lot need to be done to correct this situation in order to realize improved information security. Further the respondents were required to indicate whether they agreed or disagreed with the fact that the current approaches adopted by their organizations are adequate and if the approaches were efficient. Table 4.28 and 4.29 provide a summary of the responses on adequacy and efficiency of approaches adopted by organizations respectively.

Table 4.28: Adequacy of Approaches Adopted by Our Organization

Current approaches adopted by our organization are adequate		
	Frequency	**Percent**
strongly agree	1	3.6
agree	1	3.6
disagree	8	28.6
strongly disagree	18	64.3
Total	28	100.0

Most of the respondents (64.3%) strongly disagreed with the fact that Current approaches adopted by their organization are adequate with 28.6% also disagreeing. The least 3.6% agreed with the statement. Thus, from the responses, the current approaches adopted by organizations are indeed inadequate. Further, the respondents disagreed that current approaches adopted by their organization are efficient as shown in table 4.29.

Table 4.29: Efficiency of Approaches Adopted by Organizations

Current approaches adopted by our organization are efficient		
	Frequency	**Percent**
strongly agree	2	7.1
agree	5	17.9
disagree	17	60.7
strongly disagree	4	14.3
Total	28	100.0

From table 4.26, a majority at 60.7% disagreed with the fact that current approaches adopted by our organization are efficient. Only 17.9 % of the respondents agreed with the statement. This implies that indeed the current information security approaches adopted by the e commerce organization are in adequate and as such the situation needs urgent redress. The respondents also disagreed with the fact that their employees received frequent training on information security as shown in figure 4.22.

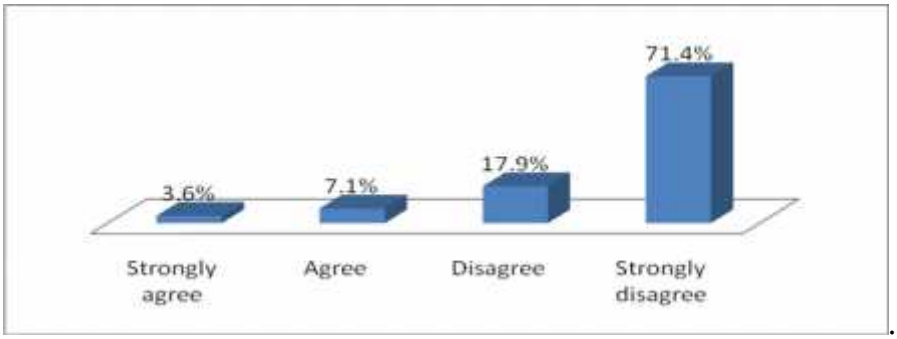


Figure 4.22: Views on Frequency of Training

From figure 4.22, most of the respondents (71.4%) strongly disagreed with the fact that employees received frequent training on information security with only 7.1% of the respondents agreeing with the statement. Hence it is evident that the employees hardly receive any training on information security, if any. Thus there is need for structured training on information security for employees in all electronic commerce organization

in order for information security to be enhanced. The respondents were further required to indicate if their organizations had policies that could enhance information security. The first policy was access control and apparently, access control as a policy was not in most of the sampled electronic commerce organizations. Findings from respondents are summarized in table 4.30.

Table 4.30: Policy on Access Control

Does your organisation have access control policy?		
	Frequency	**Percent**
Yes	13	46.4
No	12	42.9
Don't know	3	10.7
Total	**28**	**100.0**

Most of the respondents (46.4%) indicated they have such a policy with the 46.4 % of the respondents admitting to having it. The least, 10.7% indicated they did not know if this policy existed in their organizations. The second policy was authorization and as indicated in table 4.31, not all organizations had it.

Table 4.31: Policy on Authorization

Does your organisation have a policy on authorisation control?		
	Frequency	**Percent**
Yes	15	53.6
No	13	46.4
Total	**28**	**100.0**

Table 4.30 shows that 46.4% of the respondents reported that they did not have such a policy in their organizations while only 53.6% indicated they had authorization policy. Hence there is need for all electronic commerce organizations to embrace this policy in order to secure their information. Most 85.7% of the respondents also indicated that they did not have a policy on education training and security awareness as shown in figure 4.23.

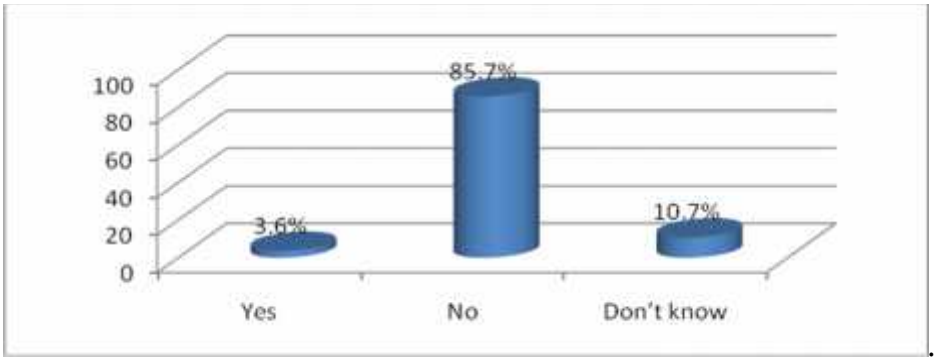


Figure 4.23: Policy on Education Training and Security Awareness

Figure 4.28 shows that only 3.6 % of the respondents indicated they had such a policy while 10.7% reported that they did not know if their organizations had education training and security policy. Most of respondents also reported that their organizations did not have email access control policy as indicated in table 4.32.

Table 4.32: Policy on Email Usage Control

Does your organisation have policy on usage of Email?		
Response	**Frequency**	**Percent**
Yes	7	25
No	21	75
Total	**28**	**100.0**

Only 25% of the respondents acknowledged that they had email access control policy in their organization as opposed to the majority at 75% who indicated that they did not have such a policy. On being asked if their organizations had mobile devices control policy, the respondents reported as indicated in Table 4.33.

Table 4.33: Policy on Mobile Devices Control

Does your organisation have mobile devices control policy?		
Response	**Frequency**	**Percent**
Yes	2	7.1
No	25	89.3
Don't know	1	3.6
Total	**28**	**100.0**

Table 4.33 indicates that a whooping majority at 89.3% of the respondents' organizations did not have any mobile devise control policy with only 7.1% indicating that they had such a policy. Concerning an antivirus policy, the respondents indicated as shown in table 4.34.

Table 4.34: Policy on Antivirus

Does your organisation have antivirus policy?		
	Frequency	**Percent**
Yes	7	25
No	21	75
Total	**28**	**100.0**

Most, (75%) of the respondents reported that they do not an antivirus policy as opposed to 25% who indicated they did have such a policy in their organizations. This implies

that most organizations still do not take information security threats posed by viruses seriously. Further, the respondents were required to indicate if they had a policy on separation of duties in management of information security.

Figure 4.24 presents a summary of the responses.

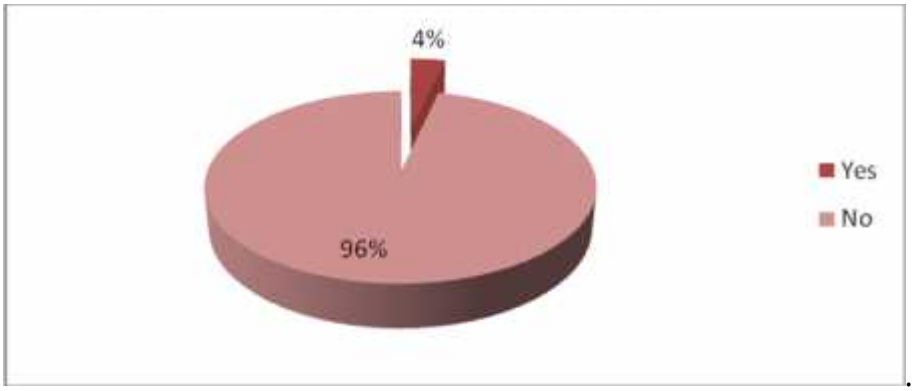


Figure 4.24: Policy on Separation of Duties

From figure 4.24, 96% of the respondents indicated they lacked a policy on separation of duties in management of information security, only 4% of the respondents' confirmed that their organizations had such a policy. This implies that claiming or assigning responsibility for mistakes or omissions committed might be difficult as it will be hard to tell who specifically committed the mistake since separation of duties in the management of information security does not exist. The respondents were further required to indicate if they had physical information security policy in their organizations. Table 4.35 provides a summary of the findings.

Table 4.35: Policy on Physical and Environment Security

Does your organisation have physical and environmental policy?		
	Frequency	**Percent**
Yes	6	21.4
No	22	78.6
Total	**28**	**100.0**

Table 4.35 indicates that most, 78.6% of the respondents' organizations do not a policy on physical and environmental security while only 21.4 % on the other hand reported that their organizations had policy on physical and environmental security, this implies that most organizations had not embraced physical security policy as required in order to help guard against information security threats, hence there is need for all electronic commerce organizations to lay emphasis on physical and environmental security by developing a policy on this. The respondents were also required to indicate if they had a policy on security reporting. Table 4.36 provides a summary of the findings.

Table 4.36: Policy on Security Reporting

Does your organisation have a policy on security reporting?		
	Frequency	**Percent**
Yes	6	21.4
No	22	78.6
Total	28	100.0

Most of the respondents at 78.6% reported not having security reporting policy in their organizations with just 21.4 % reporting that such a policy existed in their organizations. This implies that security reporting channels may not be well defined in these organizations. Further, the respondents were required to indicate if they had a security incidents recovery policy in their organizations, the findings are presented in figure 4.25.

Figure 4.25: Policy on Security Incidents Recovery

Figure 4.25 reveals that 60.7% of the respondents' organizations lacked security incidents recovery policies with only 35.7% of them indicating that their organizations had such a policy. The least, 3.6 %, indicated they did not know if their organizations had such a policy. Hence there is need for all electronic commerce organizations to adopt or formulate a policy on security incidents recovery in order to secure their information.

4.5 Changes Respondents Thought Would Improve Information Security in Electronic commerce Organizations

The respondents were lastly, required to propose changes they thought would improve information security in their organizations, the proposals they made included: emphasis on the importance of information security, devices not in use for a long time to be logged off, secure disposal of confidential customer information, use of strong and simple passwords that do not require to writing them down, use of correct security permissions based on job roles, avoidance of anonymous file sharing software, access accounts for sacked employees should be disabled immediately, penalizing staff members who fail to comply with security procedures, updating defensive tools like antivirus, firewalls etc, use of licensed software, regular application of security patches, servers should be installed in a secure place, back up and offsite data storage be encouraged, encryption of stored confidential customers information to protect data in case of theft of hardware, conducting risk analysis, regular review of lists of users who have been granted access of systems that contain confidential information, employee screening, employees should frequently receive training on information security, enactment of government and industry regulation to enforce compliance, awareness of information security measures amongst entire staff, physical information security, information security incidents recovery measures, separation of sensitive data from other data and storing sensitive data independently in a non-networked device.

4.6 Conclusions

A conclusion of the findings is presented under themes derived from research objectives.

4.6.1 Information Security Challenges Faced By Electronic Commerce

The main security challenges as revealed by the findings are inadequate budget allocation, presence of blended threats, infancy of the information security market with few formal standards and lack of unified approach that can be used to secure information. The fact that information security challenges keep growing at a rapid pace was also cited together with the fact that there is inadequate government and industry regulations to ensure personal information was protected from loss, misuse, unauthorized access or disclosure. Another challenge was the fact that unique requirements for information security officers makes it difficult for existing IT staff to transit to information security without receiving specialized enforcement training. Furthermore, the fact that the Kenyan government did not place priority on protection of personal information or intellectual property and lack of consumer education on security threats were also mentioned as challenges.

4.6.2 Key Issues Surrounding Electronic Commerce Information Security Management

Confidentiality and Privacy were the top security issues of concern to the respondents followed by integrity. Respondents further considered viruses and malicious software, system or software errors and human errors as the top three main causes of security incidents in their organizations. Unauthorized access, username or password leakage, hacking and theft of business as well as theft of sensitive customer information from respondents' organization websites were also cited as issues. Other issues included: Receiving e-mail messages that look legitimate yet they are fake, employees being tricked to give confidential information about their organization or about a customer by people claiming to be legitimate authorities and attacks using malicious software such as viruses and worm or Trojan horse.

4.6.3 Techniques and Approaches Used in Managing Electronic Commerce Information Security Threats

The study established that organizations employed antivirus information security approach in managing Electronic Commerce Information security threats. Further, activity monitoring and audit using system logs were reported as some of the approaches used by tour and travel companies to manage information threats.

The research found out that most of the organisation has antivirus policy although they reported that this is not documented. However most respondents' organizations, did not employ the use of authorization control information security approach, nor did they use a standard/framework. Furthermore, majority of the companies did not use intrusion detectors information security approach.

Respondents also denied that their organizations used security education and training information approach and risk assessment information security approaches. Respondents also denied that senior, management regularly received reporting on the status of the information security. Findings further revealed that the respondents thought that the current approaches adopted by their organization were inadequate and inefficient.

One of the objectives of this study was to develop a security framework to guard electronic commerce against confidentiality threat. Therefore, the significant findings in this chapter were mapped against the processes of COBIT framework along side with the ISO 17799 and the SSE capability maturity frameworks in order to come up with the desired framework.

CHAPTER FIVE

5.0 DEVELOPMENT OF THE SECURITY FRAMEWORK

A security framework is important because it provides a roadmap for implementation, evaluation and improvement of information security practice, Conner et al (2003). One of the important features of a security framework is that it establishes security policy and practice for an organisation. Policies provide general guidance on matters affecting security that state what methods and minimum compliance activities appropriate to ensure that the security objectives of an organisation.

5.1 Development of the Proposed Security Framework

From the reviewed literature the existing information security standards have been for to exhibit weaknesses that may limit their adoption by electronic commerce organizations. In view of this, this study we intend to propose a framework that could be the solution to the confidentiality threats experienced by the organisations used in this research.

Although a selection of various elements of standard best practice can be aligned to suit the organisation invariably the use of best practices needs to be applied in context to organizational needs. The implementation of best practices tends to be costly, complex and unfocused if treated as purely technical guide. Implementation of best practices should be consistent with the organisation's business risk management and control framework.

According to Mohammed (2012), to successfully select an appropriate framework, organisations should understand both business objectives and the requirements and the exiting frameworks. Further Mohammed (2012) suggests use of a customised approach or hybrid approach when adopting security framework. In customised approach the firm can build its own inventories of threats, vulnerabilities, and risks specific to its own business type. Associated control and control objectives need also to be customised based on the firm's objective need also to be customised based on the firm's objectives and risk appetite. In hybrid approach, more than one standard or framework to be used on bases of selecting which parts achieve the enterprise risk management objectives.

In this research, we have used both the customised approach and the hybrid approach to develop the proposed framework. The data used to develop the framework were both primary and secondary data. For the primary data, the researcher developed a criterion which was used to filter the research findings and identify the critical factors that are necessary to in corporate in the proposed framework. The summary of the findings are summarised in tables 5.2 to 5.5.

Table 5.1: Challenges faced by electronic commerce

Response	**Percentage (%)**
Lack of security officer	78.6
Little finance for security	92.9
Necessity for Training	92.8
Lack of government regulations	85.7
Lack of consumer education	85.7
Electronic commerce organizations place more value on outsmarting competitors than securing information system	85
Security is a principal that restrict customer and organisation not to engage in electronic commerce.	89.3
growth in magnitude, speed and complexity of information security threats has made prevention and clean up more difficult	68.6
Blended threats have made prevention and clean up more difficult.	86
Mobile computing devices belonging to employee is a security threat	85.7
TOTAL	***850.3***

$$\text{Mean} = \frac{\sum x}{N}$$

$$= \frac{850.3}{10}$$

$$= 85.03$$

$$= 85\%$$

A threshold of 85% which is the mean for the responses was used in identifying the challenges that should be used in the proposed framework. Any response equal or

greater than the calculated mean was considered critical. The critical information security challenges facing electronic commerce identified by the researcher using the set criterion are as follow:

- Blended threats have made prevention and clean up more difficult
- Electronic commerce organizations place more value on outsmarting competitors than securing information system
- Our organizations set aside little finances to secure information compared to finances set aside for advertisement
- There is lack Consumer education on security issues
- There are no enough Government and industry regulations to ensure that personal information is protected from loss, misuse, unauthorized access or disclosure.
- The information security challenges keep growing at a rapid pace hence continuous awareness trainings are necessary which electronic commerce organizations find hard to cope.
- Mobile computing devices such as flash disks, lap tops, iPods, tablets, smartphones and USB cables owned by organisation employees are a threat to information security

Table 5.2: Issues surrounding electronic commerce security management

Response	Percentage (%)
Attacks by viruses and malicious codes	64.3
Human errors and omission	28.6
System and software errors	17.9
Unauthorised access	60.7
User name and password leakage	89
Hacking	71.4
Theft of Business information	50
Phishing	64.3
Social engineering	46.3
TOTAL	***492.5***

$$\text{Mean} = \frac{\sum x}{N}$$

$$= \frac{492.5}{9}$$

$$= 54.7\%$$

A threshold of 54.7% which is the mean was applied to identify the techniques and approaches that should be used in the proposed framework. Any response equal or greater than the calculated mean was considered critical. The key issues surrounding electronic commerce information security management identified by the researcher using the set criterion are as follow:

Username and password leakage, hacking, stealing of business as well as sensitive customers' information from your organization's website, unauthorized access to or interception of data, attacks using malicious software as such viruses, worm or Trojan horse.

The following were the research findings on the Techniques used in managing electronic commerce information security by the organisations under the research.

Table 5.3: Techniques used in managing information security

Response	Percentage (%)
Do not use firewalls	64
Do not authentication control	25
Do not have authorisation control	67.9
Do not have standard security framework	85.7
Do not use anti-virus	10.7
Do not use intrusion detectors	92.9
Do not have awareness Trainings	85.7
Do not assess risk	82.1
Do not use activity log in security management	35.7
No security reporting mechanisms	64
Employees do not understand importance of information security	35.7
Senior management do not support in security management	79
TOTAL	***728.4***

$$\text{Mean} = \frac{\sum x}{N}$$
$$= \frac{728.4}{12}$$
$$= 60.7$$

A threshold of 60.7% which is the mean was applied in identify the techniques and approaches that should be used in the proposed framework for managing Electronic Commerce information security threats. Any response equal or greater than the calculated mean was considered critical. Using the set criterion it found that the proposed framework should include the following techniques and approaches: Firewalls, authorisation control, use of intrusion detectors, security education and training, risk assessment, involvement of senior management in management of information security,

regularly security reporting on the status of information security and use of information security framework.

The following were the research findings on the security policies in the organisations under the research.

Table 5.4: Finding on the usage of various security Policies

Response	Percentage (%)
Do not have Policy on access control	42.9
Do not have Policy on authorisation	46.4
Do not have Policy on education training and awareness	85.7
Do not have Policy on use of email	75
Do not have Policy on mobile device control	89.3
Do not have Policy on antivirus	75
Do not have Policy on separation of duties	96
Do not have Policy on physical and environmental	78.6
Do not have Policy on security reporting	78.6
Do not have Policy on security incident recovery	60.7
TOTAL	***728.2***

$$\text{Mean} = \frac{\sum x}{N}$$

$$= \frac{728}{10}$$

$$= 72.8$$

To design the information security framework the researcher used the study finding. Any response which rated above or is equal the mean (72.8%) was considered an important component of the proposed framework. The following policies were identified by use of the 72.8% threshold and ought to be included in the proposed framework: Policy on education training and awareness, Policy on the use of email, Policy on use of mobile

devices, Policy on antivirus, Policy on separation of duties, Policy on physical and environmental security and Policy on security reporting.

It is worthy noting that some of the responses which might have been rated lowly but the researcher feel that they are critical to be ignored. The researcher also feels that the suggestions on how to improve information confidentiality in electronic commerce offered by the respondents are worthy to consider when developing the framework. Such suggestions include: Devices not in use for a long time should be logged off, Secure disposal of confidential customer information, Avoidance of anonymous file sharing software, Access accounts for sacked employees should be disabled immediately, Regular application of security patches, Regular review of lists of users who have been granted access of systems that contain confidential information, Storing sensitive data independently in a non-networked device, Use of licensed software, Back up and offsite data storage be encouraged, Enactment of government and industry regulation to enforce compliance, Security incidents recovery, Use of updated antivirus and Use audit logs.

The challenges and issues identified were mapped against COBIT, ISO 17799 and SSE capability maturity model. The reasons for the mapping were to provide a level of synchronization between these frameworks and also pick from each the aspect which would address the issues identified in the field. The aspect identified, would form a process or a domain for the proposed framework.

The results of the mapping are presented in table 5.6.

Table 5.5: Mapping research findings to security frameworks

RESEARCH FINDINGS	*COBIT*	*ISO 17799*	*SSE Capability maturity model*	*How the Issue is Addressed by COEIST*
Many tour and travel Companies lacked information officers.	**Planning and Oganisation** *PO7-Manage human resource*	**Personnel security** *Security in job definition and resourcing* **Communications and Operations management** *operational procedures and responsibilities*	**PA01 – Administer Security Controls** ***BP.01.01*** *Establish Security Responsibilities*	Planning and organisation **PO6**
Little Finances are set aside for securing information	**Delivery and Support** *DS6- Identify and allocate cost*		**PA09 – Provide Security Input** ***BP.09.02*** *Determine Security Constraints and Considerations*	Acquisition and Development **AD2**
Employees of tour and travel companies lack education and training on information security.	**Delivery and Support** *DS7- educate and train users*	**Personnel security** *User training*	**PA01 – Administer Security Controls** ***BP.01.03*** *Manage Security Awareness, Training, and Education Programs*	Operations and Maintenance **OM3**
Adherence to laws regulating use of confidential customers' information	**Planning and organisation** *PO8 – ensure compliance with external requirements*	**Compliance Management** *Policies and procedures to ensure compliance with relevant laws and regulations*	**PA10 – Specify Security Needs** ***BP.10.02*** *Identify Applicable Laws, Policies, and Constraints*	Planning and Organisation **PO4**
There lack in consumer education on information security.	**Delivery and services** *DS8 – assist and advise customers*		**PA01 – Administer Security Controls** ***BP.01.03*** *Manage Security Awareness, Training, and Education Programs*	Operations and Maintenance **OM3**
More value placed in out smarting Competitors than Securing information systems.	**Delivery and service** *DS5 – ensure system security*			Acquisition and Development **AD2**

Growth in magnitude, speed and complexity of information security threat make prevention and clean up more difficult.	**delivery and support** *DS10- manage problems and incidents*		**PA08 – Monitor Security Posture** ***BP 08.02*** *Monitor Changes* ***BP 08.04*** *Monitor Security Safeguards* ***BP 08.05*** *Review Security Posture*	Risk Management **RM4**
Blended threats have made prevention and clean up more difficult.		**System development and maintenance** *Security requirement of systems*	**PA04 – Assess Threat** ***BP 04.05*** *Assess Threat Likelihood* ***BP 04.06*** *Monitor Threats and Their Characteristics* **PA05 – Assess Vulnerability** ***BP.05.01*** *Select Vulnerability Analysis Method* ***BP.05.02*** *Identify Vulnerabilities* ***BP.05.03*** *Gather Vulnerability Data* ***BP.05.05*** *Monitor vulnerabilities*	Risk Management **RM2**
Leakage of user name and password.	**Monitoring** *M2- Assess internal control adequacy*	**Access controls** *User access management and user responsibilities*	**PA11 – Verify and Validate Security** ***BP.11.02*** *Define Verification and Validation Approach* ***BP.11.03*** *Perform Verification* ***BP.11.04*** *Perform Validation* ***BP.11.05*** *Provide Verification and Validation*	Technical and Control **TC6**
Hacking of electronic commerce websites.	**Monitoring** *M2- Assess internal control Adequacy*	**Access controls** *Network access control and monitoring system access and use access and use*	**PA08 – Monitor Security Posture** ***BP 08.01*** *Analyze event records* ***BP 08.03*** *Identify security incidents* **PA04 – Assess Threat** *BP 04.02* ***Identify Man-made Threats***	Technical and Control **TC4**
Stealing of business as well as sensitive customer information from organisation website		**System development and control** *Control of interactions between internal and third parties at information exchange and cryptographic controls*	**PA10 – Specify Security Needs** ***BP.10.01*** *Gain Understanding of Customer's Security Needs*	Technical and Control **TC4**

		Communications and Operations management *Exchanges of information and software*		
Attack using malicious Software such as viruses, worms or Trojan horse.		**Communications and Operations management** *Protection against malicious software and Exchanges of information and software with other organisations*	**PA08 – Monitor Security Posture** ***BP 08.04*** *Monitor Security Safeguards*	Technical and Control **TC4**
Careless disposal of customers' confidential information.	**Delivery and support** *DS11- Manage data*	**System development and maintenance** *security of file systems* **Communications and Operations management** *Media handling*		Acquisition and Development **AD2**
Use of uncertified and unlicensed software.	**Acquisition and Implementation** *AI5- install and accredit system* **Planning andorganisation** *PO8- ensure compliance with external requirements*	**Organisational security** *Implementing controls on acquisition and testing* **Communications and Operations management** *system planning and acceptance*		Acquisition and Development **AD4**
Lack of proper management of access rights of current employees	**Acquisition and Implementation** *AI6- manage changes*	**Access controls** *User access management and user responsibilities*	**PA01 – Administer Security Controls** ***BP.01.02*** *Manage Security Configuration* ***BP.01.04*** *Manage Security Services and Control Mechanisms*	Technical and Control **TC6**
Poor Storing customers' sensitive information. Some	**Delivery and support**	**System development and maintenance**		Planning and organisation

organisation store confidential information in networked devices	*DS11- Manage data*	*security of file systems* **Communications and Operations management** *Media handling*		**PO3**
Access accounts of sacked Employees are not disabled	**Acquisition and Implementation** *AI6- manage changes*	**Personnel security** *Policies and procedures surrounding terminating employees*	**PA08 – Monitor Security Posture** ***BP 08.02*** *Monitor Changes*	Technical and Control **TC6**
Lack of use of security patches	**Acquisition and Implementation** *AI2- acquire and maintain application software*	**Compliance** *Review of security policy and technical compliance*	**PA10 – Specify Security Needs** **BP.10.06** Define Security Related Requirements	
Many tour and travel companies do not use firewall to manage information security		**Communications and operations management** *Network security management.*	**PA08 – Monitor Security Posture** ***BP 08.04*** *Monitor Security Safeguards*	Technical and Control **TC4**
Many organisation lack proper and co-ordinated authorisation control.	**Acquisition and Implementation** *AI4- develop and maintain procedures*	**Access controls** *Application access controls, user access management and monitoring system access and use*		Technical and Control **TC6**
Intrusion detectors/ logical detectors are not used to secure confidential information.	**Acquisition and Implementation** *AI1- identify automated solutions*	**Communications and operations management** *Network security management.*	**PA09 – Provide Security Input** ***BP.09.03*** *Identify Security Alternatives*	Technical and Control **TC6**
Many organisations do not assess risk and manage risk.	**Planning and organisation** *PO9 – assess risks*	**Business continuity management** *An IT disaster recovery plan should be developed.*	**PA03 – Assess Security Risk** ***BP.03.01*** *Select Risk Analysis Method* ***BP 03.02*** *Exposure Identification* ***BP 03.03*** *Assess Exposure Risk* ***BP 03.04*** *Assess Total Uncertainty* ***BP 03.05*** *Prioritize Risks* ***BP 03.06*** *Monitor Risks and Their*	Risk Management **RM2**

			Characteristics	
Seniors managers do not support in securing information.	**Planning and organisation** *PO5- communicate management aim and direction*	**Personnel security** *Responding to security incidents and malfunctions*	**PA09 – Provide Security Input** ***BP.09.02*** *Determine Security Constraints and Considerations* ***BP.09.05*** *Provide Security Related Guidance* ***BP.09.06*** *Provide Operational Security Guidance*	Operations and Maintenance **OM4**
Many of the visited do not have a procedure of security reporting.Rarely do they have security incident reporting.	**Delivery and support** DS1- define and manage service levels		**PA07 – Coordinate Security** ***BP.07.01*** *Define Coordination Objectives* ***BP.07.02*** *Identify Coordination Mechanisms* ***BP.07.03*** *Facilitate coordination* ***BP.07.04*** *Coordinate Security Decisions and Recommendations*	Operations and Maintenance **OM4**
Lack of policy on education training and awareness	**Planning and organisation** *PO7- manage human resources*	**Personnel security** *Developing policies and procedures surrounding training*	**PA01 – Administer Security Controls** ***BP.01.03*** *Manage Security Awareness, Training, and Education Programs*	Planning and Organisation **PO1**
Lack of policy on use of email communication	**Planning and organisation** *PO7- manage the IT investment*	**Communications and Operations management** *Exchanges of information and software with other organisations*		Planning and Organisation **PO1**
Lack of policy on use of Mobile devices		**Access control** *Mobile computing and teleworking*		Planning and Organisation **PO1**
Lack of policy on antivirus	**Acquisition and Implementation** *AI- acquire and maintain application software*			Planning and Organisation **PO1**

Lack of policy on separation of duties	**Planning and organisation** *PO7- manage human resources*	**Security policy** *policies and procedures establishing the roles and responsibilities*	**PA01 – Administer Security Controls** ***BP.01.01*** *Establish Security Responsibilities*	Planning and Organisation **PO1**
Lack of policy on physical and environmental security	**Delivery and support** DS12 –manage facilities	**physical and environmental security** *Policies and procedures should be put in place against physical and environmental hazards*		Planning and Organisation **PO1**
Lack of policy on security reporting	Planning and organisation *PO3 – manage the information architecture*	**Communication and Operations Management** *Operational procedures and responsibilities*	**PA07 – Coordinate Security** ***BP.07.01*** *Define Coordination Objectives* ***BP.07.02*** *Identify Coordination Mechanisms* ***BP.07.03*** *Facilitate coordination* ***BP.07.04*** *Coordinate Security Decisions and Recommendations security*	Planning and Organisation **PO1**

5.2 Proposed Information Security Framework

As mentioned earlier customised approach and the hybrid approach was used to develop a framework to secure electronic commerce against confidentiality threats. The researcher derived the Framework from COBIT. The derived framework was referred to as **C**ontrol **O**bjectives for **E**lectronic commerce **I**nformation **S**ecurity and related **T**echnologies (**COEIST).**

The proposed framework has five domains obtained by grouping the related processes to implement information security in an organisation thereby enhancing confidentiality of information in an electronic commerce environment or other sectors. These domains are namely:

- Planning and organizing which has six processes (PO1 –PO6)
- Acquisition and development management which has five processes (AD1 – AD5)
- Operation and Maintenance has seven processes (OM1- OM7)
- Technical and control has seven processes (TC1 – TC7)
- Monitoring and Control has four processes (MC1-MC4)

Each domain has other primary processes, many of which are derived from other internationally recognized security frameworks. A process is what has to happen to achieve information security objectives. There are twenty nine (29) processes in the proposed framework. Each primary process has activities that give direction of how information security will be implemented within a process.

The Proposed framework can be summarized by the figure 5.1

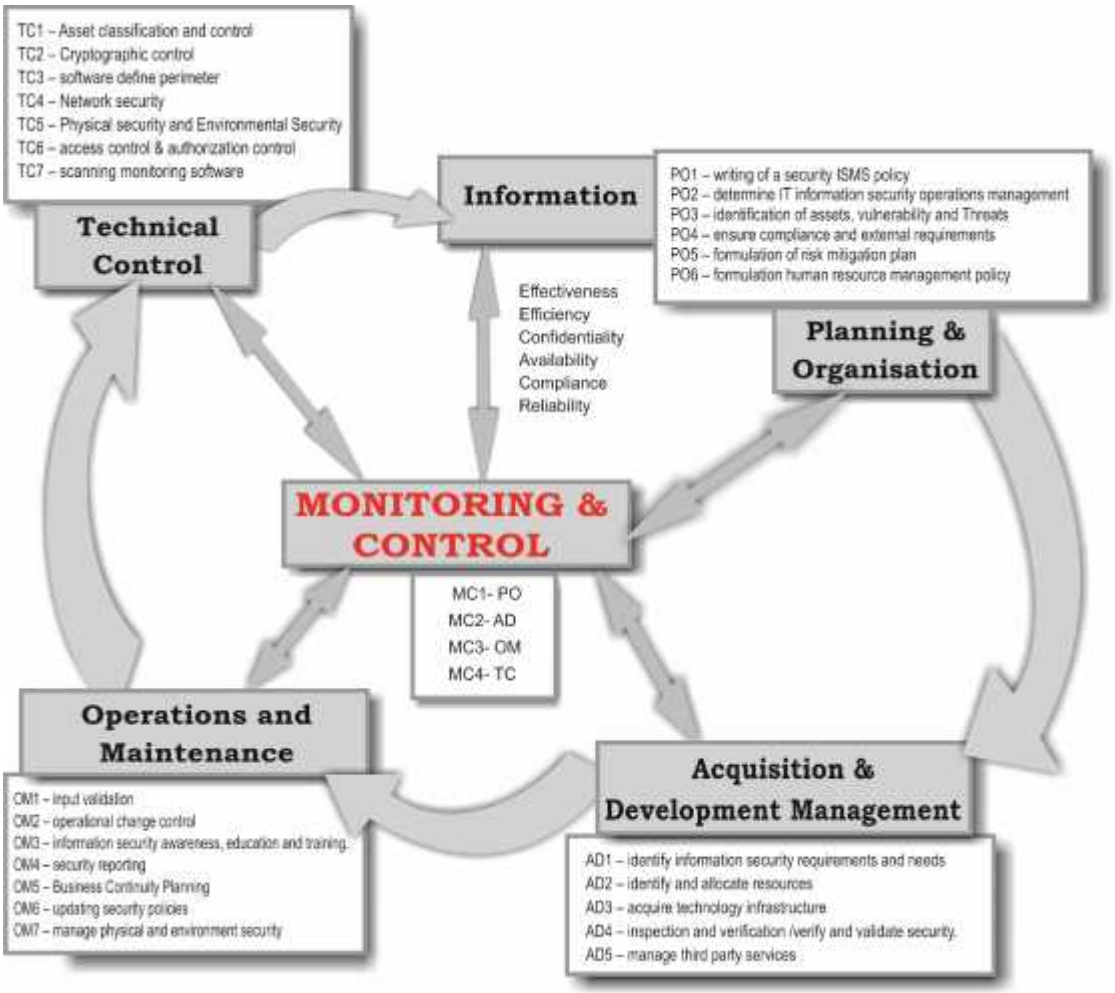


Figure 5.1: The Unvalidated Framework

CHAPTER SIX

6.0 FRAMEWORK VALIDATION

Evaluation is the most important step in framework development. It provides essential feedback to the framework development and the quality assurance process.

There are a number of evaluation methods that could be used for evaluating a proposed framework. These are observational, descriptive, analytical, testing and experimental method. Observational and descriptive evaluation methods appear to be more suitable for theoretical evaluation approach. The practical evaluation approach requires implementing a framework in a real - world environment. This approach would demand much time as well as resources (Karokola, 2012). A case study was selected for conducting the study in the same organisations studied earlier and other participants the researcher found to be of importance in the validation process. Such an approach was been used by scholars (Karokola 2012; Ireri, 2012; Atieno 2011; Munirul et al. 2011; Bechan 2008).

In order to validate the usefulness of the **COESIT**, test cases were carried out. The profile of the participants required for the case study were ICT employees at the organisations considered to have experience allowed them to provide insight into the **COESIT.**

The participants of the validation process were purposefully selected. The participants were considered good test cases based on they use online electronic commerce transactions, they are faced by information security challenges the researcher wish to address or have valuable information security expertise which would benefit this research.

The data collected during was used to verify the completeness and usefulness of the **COESIT** framework. To satisfy the quality of completeness the framework the interviewee was asked to confirm that the **COEIST** framework has all the necessary controls and that none of the controls listed are extraneous.

6.1 Validation Results Presentation and Analysis

The responses obtain from the test cases are summarised in tables 6.1 to 6.11 table.

Table 6.1: Views on proposed framework and information confidentiality.

statement	Frequency	Percent (%)	Valid percent
Agree	6	60	60
Strongly agree	4	40	40
Total	**100**	**100**	**100**

60% of the respondents agree that the framework will improve information confidentiality, 40% of the respondents strongly agreed with this statement. This means that all the respondents believed that the proposed framework will improve information confidentiality in electronic commerce.

On the issue of whether the framework can be applicable in real life situation, the responses obtained are summarises in table 6.2.

Table 6.2: Views on proposed framework in real life application

statement	Frequency	Percent (%)	Valid percent
Agree	2	20	20
Strongly agree	8	80	80
Total	**100**	**100**	**100**

Table 6.2 shows that most 80% of the respondents strongly agreed that the proposed framework is applicable in real life while 20% agreed with the statement. From the response obtained it is an indication that all the respondents believed that the framework is applicable to real – life situation.

Table 6.3 shows the responses obtained when the respondents were asked whether the tasks in the proposed framework are clear and are easy to implement.

Table 6.3: Opinions on proposed framework clarity and ease

statement	Frequency	Percent (%)	Valid percent
Do not know	2	20.0	20.0
Agree	6	60.0	60.0
Strongly agree	2	20.0	20.0
Total	**10**	**100.0**	**100.0**

It is noted that 60% of the respondents agreed that the tasks in the proposed framework are clear and are easy to implement, 20% of the responds strongly agreed that the tasks in the proposed framework are clear and are easy to implement. 20% of the respondents do not know whether the tasks in the framework are clear and easy to implement. Based on the mean obtained for this response (4.0) which corresponds to agree on the likert scale used, it can be conclude that most of the respond agreed that the task in the proposed framework are clear and easy to implement.

The respondents were also asked whether the suggested framework is economical the responses are presented in table 6.4.

Table 6.4: Views on economy of suggested framework

statement	Frequency	Percent (%)	Valid percent
strongly disagree	1	10.0	10.0
disagree	7	70.0	70.0
agree	2	20.0	20.0
Total	10	100.0	100.0

80% of the respondents disagreed with the statement that the suggested framework is economical. To deal with this issue the researcher suggested that instead of having a supervisor for each of the department suggested in the framework, all the suggested departments will be co-ordinated by the company's security officer. This will reduce the cost of implementation.

Table 6.5 shows the responses obtained when the respondents were asked whether the proposed framework is clear and easily understandable to the intended users. It is noted that 70% agreed with this statement while 30% strongly agreed with this statement. A mean of 4.30 which corresponds with agree on the likert scale for used was obtained. From this means it can be concluded that most of the respondents agreed that the proposed framework is clear and easily understandable to the intended users.

Table 6.5: Opinions on suggested framework ease to understand

statement	Frequency	Percent (%)	Valid percent
Agree	7	70.0	70.0
Strongly agree	3	30.0	30.0
Total	**10**	**100.0**	**100.0**

Table 6.6 shows the response obtained for the statement on whether the framework adequately addresses the technical and non-technical related security.

Table 6.6: Views on suggested framework address to threats

statement	Frequency	Percent (%)	Valid percent
Disagree	2	20.0	20.0
Agree	4	40.0	40.0
Strongly agree	4	40.0	40.0
Total	**10**	**100.0**	**100.0**

Table 6.8 shows that 40% of the respondents agreed that the proposed framework adequately addresses the technical and non technical related security. It is also noted that 20% of the respondents disagreed with this statement while 40% strongly agreed with this statement. The mean obtained concerning whether the suggested framework addresses the technical and non-technical related security was 4.0. This means that most of the respondent agreed that the framework adequately addresses the technical and non-technical related security.

As to whether the suggested framework is aligned with the current security standards and practice, the responses obtained are as shown in the table 6.7.

Table 6.7: Views on Framework alignment with current security standards

statement	Frequency	Percent (%)	Valid percent
Agree	5	50.0	50.0
Strongly agree	5	50.0	50.0
Total	**10**	**100.0**	**100.0**

From the table it is noted that the proposed framework got 100% approval. This was also depicted by the mean for this response which stood at 4.5 this mean is approximately 5.0 indicating that the respondents strongly agreed that the framework is aligned with current standards and practice.

The researcher also required to establish whether the respondents considered the framework flexible enough to deal with possible future confidentiality threats. The table 6.8 shows that 10% of the respondents do not know, 70% agreed and 20% strongly agreed with the statement. The mean for these responses was found to be 4.10 which correspond to agree.

Table 6.8: The framework is flexibility to deal with future threats

statement	Frequency	Percent (%)	Valid percent
Do not know	1	10.0	10.0
Agree	7	70.0	70.0
Strongly agree	2	20.0	20.0
Total	**10**	**100.0**	**100.0**

These findings shows that the proposed framework is flexible to deal with possible future confidentiality threats.

On the issue of adoptability, table 6.9 indicates that 60% strongly agreed that the proposed framework is easy to adopt. Those who agreed with this statement were at 30%

while 10% of the respondents did not know whether the proposed framework is easy to adopt. The mean for these responses was 4.50. This is a strong indication that most of the respondents believed that the framework is easy to adopt.

Table 6.9: Views on whether the proposed framework is easy to adopt

statement	**Frequency**	**Percent (%)**	**Valid percent**
Do not know	1	10.0	10.0
Agree	3	30.0	30.0
Strongly agree	6	60.0	60.0
Total	**10**	**100.0**	**100.0**

Table 6.10 is the summary of the means of responses of the respondents.

Table 6.10: Descriptive Statistics

Statement	**Mean**	**Std. Deviation**	**Variance**
The framework developed will improve information confidentiality	4.40	.516	.267
The tasks in the framework are applicable in real life situation	4.80	.422	.178
The tasks in the framework are clear and are easy to implement	4.00	.667	.444
The suggested framework is economical to use	2.30	.949	.900
The framework is clear and easily understandable to the intended users	4.30	.483	.233
The framework adequately addresses the technical and non-technical related security	3.50	1.080	1.167
The framework is aligned with current security standards and practice	4.50	.527	.278
The framework is flexible enough to deal with possible future confidentiality threats	4.10	.568	.322
The framework is easy to adopt	4.50	.707	.500

6.2 Validated Security Framework

To come up will the validated information security framework, the researchers considered the recommendations given by the participants used to evaluate the initial proposed framework. For the purposes of differentiating what was added to the framework after the validation, an asterisk (*) symbol was used.

The validated security framework will consist of five domains. These domains are namely:

- Planning and organizing has five processes (PO1 – PO5)
- Acquisition and development management has five processes (AD1 – AD5)
- Operation and Maintenance has seven processes (OM1 – OM7)
- Technical and control (TC1 – TC8)
- Risk Management (RM1-RM4)

The developed framework can be summarized in the figure below:

Figure 6.1: Validated Framework

6.3 Discussion of the Proposed Framework

1. Planning and organization

PO1- writing of a security ISMS policy

Under this process the activities that should be undertaken are writing the policies that will govern;

- Access control
- Authorization control.
- Education training and security awareness
- Physical and environmental security
- Email management
- Protection from Malicious Software
- Duties and responsibilities of each information security personnel
- Information Security reporting
- Information security Incidents recovery and business recovery
- Policy on use of mobile devices
- Policy on use, storage and disposal of confidential information *

PO2– determine IT information security operations management

In this process the activities that govern operations are spelt out. These should include

- Plans on how system upgrading should be carried out
- How often antivirus software should be upgraded.
- Portable computing devices management and control

When using portable computing devices (e.g. laptops, smart phones, personal data assistants) to access information special care must be taken to ensure that device and information accessed by that device is not compromised (unauthorized persons viewing information on the screen).When accessing databases containing confidential information the mobile device user must be careful never to save data to the local hard-drive or other mobile storage device.

PO3 – Privacy and confidentiality of information *

- Safeguarding of an organisation's Records

Organization's records must be protected from theft or unauthorized access. Some records may need to be retained in a secure manner for extended periods to meet and may be required support essential business operations. Records containing customer's confidential information should be stored in encrypted form in storage media. Such media must be kept in restricted areas.

- Data.

Separation of sensitive data from other data and storing sensitive data independently in a non-networked device. Anonymous file sharing software should be avoided. Data should be categorized according to its sensitivity and its value; Non-sensitive (Public data); moderately sensitive (Internal Business use only data); highly sensitive (Confidential data). Sensitive data should be stored independently in a non-networked device.

- Disposal of confidential information

For electronic wastes, Media such as tapes, diskettes, servers, mainframe and PC hard drives which contain sensitive data must be disposed of in accordance with laid down organizational policy. Sensitive information could be leaked to outside persons through careless disposal of such media. Formal processes must be established to minimize this risk. Media containing sensitive organisation's data must be destroyed by incineration, shredding, or electronic erasure of data before disposal consistent with record retention laws.

PO4 – ensure compliance of external requirements

The process that is meant to avoid breaches of any criminal and civil law, statutory or state regulatory or contractual obligations, and security requirements, the design, operation, use and management of information systems. Advice on specific legal requirements should sought Legal from a Counsel and necessary actions taken to ensure

compliance with the regal requirements governing confidentiality of personal information.

- Prevention of Misuse of Information Technology Resources

The information technology resources and the data processed by these resources are provided for business purposes. Management should authorize their use. Any use of IT facilities for non-business or unauthorized purposes, without management's consent, should be considered a misuse of facilities. Controls must be implemented to detect and report such activity to the appropriate responsible officer.

- Compliance with Security Policy

ICT manager or supervisors should ensure that all security processes and procedures within their areas or responsibility are followed. In addition, all business units within an organisation will be subject to regular reviews to ensure compliance with security policies and standards.

This process relates to the management and ongoing monitor of compliance with laws, regulations, contractual requirements, internal policies and standards or other requirements. The process involves conducting reviews to ensure obligations are appropriately complied with to reduce occurrence of risks of noncompliance such as fines and public embarrassment. An effective compliance management process prevents the organization's system, application and information from internal and external threats. Enactment of government and industry regulation to enforce compliance should be done within the government ministry dealing with electronic commerce.

PO5 – Formulation of human resource management policy

The Human Resources Information Security Program is intended to reduce the risks of human error, theft or misuse of an organization's information and facilities. Security responsibilities must be defined and addressed at the employee hiring stage.

The policy should include;

- Security roles and responsibilities. These include any general responsibilities for implementing or maintaining the security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of specific security processes. Use of correct security permissions based on job roles should be embraced by an organization. All staff should comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

- Personnel Screening. This should include: Previous employment; Criminal records as authorized by state laws; A check for completeness and accuracy of the applicant's information as indicated in the curriculum vitae; Confirmation of claimed academic and professional qualifications.

2. Acquisition and development management

AD1 – identify information security requirements and needs

- Requirements

Requirement for new systems or a new version of software must be established and documented before a requisition is made. The requirements must be need driven. Such a requirement may be to address a certain confidentiality threat or to mitigate a risk identified in the process of risk assessment.

- Capacity demands

Capacity demands should be monitored and projections of future capacity requirements made to ensure that adequate processing capability and storage are available. This information will be used to identify and avoid potential bottlenecks that might present a threat to system security or user services.

- Upgrades and new versions

Upgrades and new versions of existing systems must be established. Such upgrades or a new version are necessary to ensure information confidentiality.

AD2 – identify and allocate resources

- Budget allocation. The budget include cost of acquisition of IT infrastructure, installation cost, capacity building and security maintenance.
- Human resources. Human resource is required for the development of the IT infrastructure, capacity building as trainers. IT staff with the necessary skills should be engaged and capacity building should be done regularly.

AD3 – acquire technology infrastructure

There are a number of factors that should be considered at this level such as:

compatibility of the infrastructure, capability of doing all that is required, if it is a software, does it have any known problems or bugs, does the supplier offer any technical support?

AD4- inspection and verification /verify and validate security

- Acceptance criteria

Acceptance criteria based on best practices for new information systems, management will ensure that the requirements and criteria for acceptance are clearly defined, agreed and documented. Infrastructure or software which can compromise information confidentiality should not be accepted.

- System test

Suitability and vulnerability tests should be performed to ensure confidentiality security requirements have been met prior to formal system acceptance.

- Verification

Verifications may comprise such checks as:

- Whether works or services meet the technical standards
- Whether all required manuals or documentation have been received

- Intellectual Property Rights

Appropriate procedures must be implemented to ensure compliance with legal restrictions on the use of copyrighted material, or material that may have design rights or trademarks. Proprietary software products are generally supplied with license agreements that limit the use of the product to a specific machine or number of users. Controls must be implemented to ensure all aspects of license agreements are met and can be audited. Copyright infringement can lead to legal action which may involve criminal proceedings. Majority of the pirated software do not meet the required standards and may contain malicious codes that can be used to harvest information in the internet. Use of licensed software should be adhered to.

- Configuration management

It refers to a practice to protect and manage the system and network devices from unauthorized users exploiting the configuration weaknesses. The configuration management deals with managing configuration of IT infrastructure and resources. An effective configuration management facilitates the integrity of software and hardware, provides greater system availability and resolves issues more quickly.

AD5- manage third party services

- Test data

Test data must be protected and controlled. Live operational data must never be connected to a testing environment. Acceptance testing usually requires large volumes of test data that closely resembles operational data. The use of test data populated from operational databases containing sensitive information requires that those performing the tests are authorized by the appropriate data custodians to access such information. Test data should be done on test servers but not active servers.

- Support programmers

Support programmers are given access only to those parts of a system necessary to perform their jobs, and that formal agreement and approval processes for changes are implemented as specified by the organisation management.

3. Operations and maintenance

Operations management includes maintaining operational service of data processing and monitoring IT infrastructure.

OM1- input validation

Data input must be validated. Checks will be applied to the input of business transactions. Where feasible the applications should apply the controls as part of the system to ensure consistent, complete, and accurate implementation of the controls in the most efficient manner. This activity is necessary in order to manage the human errors. The following controls must be considered:

Dual input or other input checks to detect the following errors:

1. Out-of-range values;
2. Invalid characters in data fields;
3. Missing or incomplete data;
4. Exceeding upper and lower data volume limits;
5. Unauthorized or inconsistent control data.

OM2- operational change control

To minimize the possibility of corruption of administrative information systems, strict controls over changes to information systems must be implemented. Formal change control procedures must be enforced. They must ensure that security and control procedures are not compromised, that IT staffs are given access only to those parts of a system necessary to perform their jobs. These change control procedures should apply to Organization's applications as well as systems software used to maintain operating systems, network software, hardware, etc. In addition, access to source code libraries for both Organization's applications and operating systems must be restricted to ensure that only authorized individuals have access to these libraries and where an IT staff has logged on an application, audit log is done to establish the credibility of such logs.

OM3- information security awareness, education and training.

This process involves management of security, awareness, training and education programs. Information security awareness training should be included in the staff induction process. An ongoing awareness programme should be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary. Information in such training should include:

- Personal roles on information security
- Information on known information security threats
- Channels for communicating information security threats
- Organizational security policies
- Identification of risk and risk assess.

OM4- security reporting

The Information Security Officer should keep the executives informed of the information security status of the organisation by means of regular reports and presentations. In event of equipment failure, theft or a site disaster, data backup and storage would enable the organisation to retrieve information with minimal business interruptions. In the event of a security incident, there should be a procedure which is clearly defined what to do and who to call for assistance. All information security events should be investigated to establish their cause and impact with a view to avoiding similar events.

OM5- Business Continuity Planning

Business continuity management must include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. Business continuity management begins with a business impact analysis and a threat analysis that identifies events that could cause an interruption of business operations and processes. Following the threat identification, a risk assessment must be performed to determine the impact of the threat on the business, likelihood of occurrence, and recovery time necessary for essential for business applications and

processes. This assessment will consider only those business processes that are information technology related. A business continuity plan must be developed by each business unit that addresses each of the following key elements: Threat analysis, Risk identification, Risk mitigation, System recovery, Business impact analysis and Identification and prioritization of business processes and supporting applications

OM6- updating security policies

- Review the policy when new attack vectors become known.
- Review the policy after a breach of confidentiality occurs.

OM7– manage physical and environment security

- Knowledge of existence of high valuable ICT devices
- Appropriate of physical and environmental security procedures should be put in place to prevent information confidentiality being compromised.
- Staff who travel with portable computers should be made aware of the risks relating to theft and potential liability through compromised data
- Visitors to the organisation should be always escorted around the building and are never left to wander on their own.
- Back up and offsite data storage be encouraged. Use of shadow backup servers with real time back up.
- Installation of access control devices such as smart cards or biometric identifications
  should be encouraged to control restricted areas.
- Use of firewalls and domain oriented LANS should be encouraged
- Use of mobile computing devices in public places should be prohibited.

4. Technical control

According to Munirul et al. (2011), it is essential that technology environment be monitored on constant basis and that risk of technology changes in the market should be

addressed. At this level, the technology controls applicable to the organisation's environment are identified. The activities for this process are:

TC1- Asset classification and control

Activities within this process are: Ability for the organisation to locate asset, ability to control local and remote access, management of information.

TC2 – Cryptographic control

Highly sensitive (confidential) data should never be in unencrypted format on portable computing devices and information storage media. Customer detail database and file transmission should be encrypted. Encryption access credentials should be implemented.

TC3 – Software define perimeter

In this case, the activities would include application of security concepts such as; Security standards such as PKI, TLS, SAML, XML. Such technology ensures that device security posture and identification are verified before access is granted.

TC4 – Network security

- Firewall and security gates

A firewall is a network node consisting of both hardware and software that isolate a private network from a public network. Packet –filtering routers filter data requests moving from the public internet to private network based on the network addresses on the computer sending or receiving the request. The other types of firewall block data and requests depending on the type of application being accessed. This type of firewall is called an application- level proxy. Firewalls should be used to protect information against confidentiality threats. Security gate can be used to validate source and destination addresses. Routing control should be based on positive source and destination address (checking mechanism).

- IPSec and Virtual Private Network

When data moves from one network to another across a third, perhaps untrusted, network, Virtual Private Networks should be used.

- Intrusion detectors

Intrusion detectors are a special category of software that can monitor activity across a network or on a host computer to watch for suspicious activity and takes an automated action based on what it sees should be installed. Honey nets are a technology that can be used to detect and analyses intrusions.

- Protection from Malicious Software

An organisation should use up date antivirus software and management procedures to protect itself against the threat of malicious software. Such antivirus should be updated periodically. Any portable storage medium must be scanned for the presence of malicious codes before plugging them in the organisation's computers. All staff are expected to co-operate fully with this policy. Users should not install software on the organisation's property without permission. Users breaching this requirement may be subject to disciplinary action.

- Emails

The policy for the email management may contain the following:
It is strictly prohibited to:

  - Forge or attempt to forge email messages.
  - Disguise or attempt to disguise your identity when sending mail (Spoofing)
  - Send email messages using another person's email account
  - Copy a message or attachment belonging to another user without permission of the originator
  - Security. In Security, users are responsible for safeguarding their password. Password should be obscure and a minimum of 8 characters in length. They should not be printed, stored on line or given to others. Email account and password obtained from IT department are solely intended for your individual use and should not be shared. If a user must temporarily share his or her password, then they user must change the password as soon as possible afterward. Password should be change on regular basis.

- Confidential Information. Never send any confidential information via email. If you are in doubt as to whether to send certain information via email, check this with your supervisor first.

- Online transactions

The use of electronic signatures by each of the parties involved in the online transaction. Care must be taken to ensure that communications path between all involved parties in electronic commerce transactions is encrypted. Ensure that the storage of confidential information is located outside of any public accessible environment.

TC5- Physical security and Environmental security

- Physical security perimeters

Physical security perimeters should be established. Such areas include areas where the server is stored or area where printers are to print confidential information. Physical security for machines which are left unattended. Use of computer screen savers or similar technology is required to ensure that confidential information is not displayed after a specified period of inactivity. All the computers must be screen locked. The IT resources should be protected against physical and environmental hazards. The server and other critical asset should be kept in strong room with limited access.

- System logs

System logs are used to detect physical access to the computer system. System log is an indication that someone was physically present at the system. The following should be checked while examining system physical access: Short or incomplete logs, Logs missing entirely, Strange timestamps, Logs with incorrect permissions or ownership, System reboots and Services restarting. The file containing system logs should be encrypted to avoid being tampered with or being accessed by unauthorized people.

TC6- access control and authorisation Control

- Access control

Only authorised personnel who have a justified and approved business need should be given access to restricted areas containing information systems or stored data. Access to information should be restricted to authorised users who have a bona-fide business need to access the information. Access to computer facilities should be restricted to authorised users who have a business need to use the facilities. Access to data, system utilities and programme source libraries should be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Access accounts for sacked employees should be disabled immediately. Regular review of lists of users who have been granted access of systems that contain confidential information should be done to ensure that each staff has access to information that is within their duties and responsibility.

The following measure should be implemented;

- ❖ Limit the number of unsuccessful log-on- attempts *****
- ❖ Recording unsuccessful and successful log-on-attempts *****
- ❖ Sending an alarm message to the system console if maximum number of log-on-attempts are reached *****
- ❖ Make use to automatically expiring passwords which will expire after the expiry of the period specified in the password policy *****

- Authorization control.

This includes use of password or PIN or token card. Privileges should be given to each employee depending on the security role they play in the organisation.

- Verify and validate security *

In this case verification and validation approach are defined. Verification and validation are performed.

TC7- scanning monitoring software

The company management reserves the right to scan any device attached to the organisation network on a periodic basis to ensure that IT infrastructures are protected against known vulnerabilities. This includes the scanning of any mobile devices owned by the organisation or its employees. Avoidance of anonymous file sharing software should be encouraged. Regular application of security patches should be done.

TC8 – Anti-phishing measures *

To overcome phishing it is proposed that domain Keys infrastructure can be used. Domain Keys infrastructure verifies the domain of an email sender. This verification helps in the war against phishing by helping to curb the proliferation of spam. Scam blockers can also be used.

5. Risk Management *

The risk management cycle is an iterative and continuous process, constantly reinforced by the changing risk landscape, as well as by organizational priorities and functional changes. The risk management cycle provides four elements that structure an organization's approach to risk management, as represented in Figure 6.2: Frame, Assess, Respond and Monitor.

Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization.

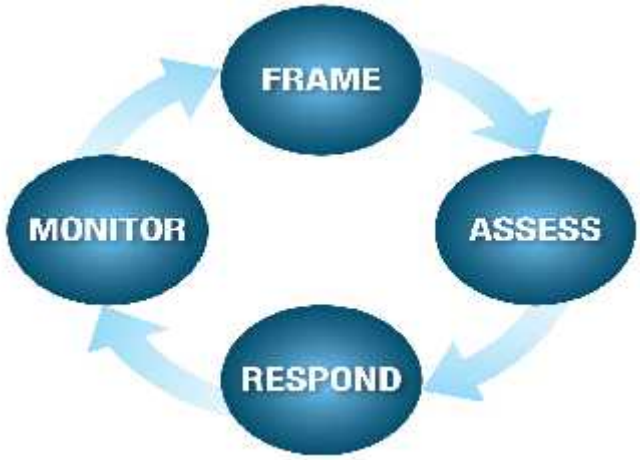


Figure 6.2: Risk Management Process

Source: [Risk Management Process]

In the proposed framework each of these elements will form processes.

RM1- Risk Frame

The risk framing element describes the environment in which risk-based decisions are made.

Establishing a realistic and credible risk frame requires that organizations in the electronic commerce, identify:

- Assumptions about threats, vulnerabilities, impacts, and likelihood of occurrence;
- Constraints imposed by legislation, regulation, resource constraints (time, money, and people) and other factors identified by the organization;
- Risk tolerance, which identifies the level of acceptable risk;
- Priorities within mission and business processes, and trade-offs between different types of risk; and
- Trust relationships, such as physical interconnections, third-party service providers, reciprocity agreements, or device vendors

RM2 – Risk assessment

The risk assessment element identifies, prioritizes, and estimates risk to an organization's operations, assets, individuals, and other interconnected organizations. The purpose of the risk assessment element will be to identify the following components of risk and evaluate these against mission and business processes: Threats; Vulnerabilities; Impact (consequence or opportunity); and Likelihood (probability or frequency an event will occur).

RM3- Risk Response

The risk response element will addresses how an electronic commerce organization responds to risk once that risk is assessed.

The risk response element provides a consistent, organization-wide response to risk consistent with the organization's risk exposure. In this process, organizations:

- Develop alternative courses of action for responding to risk;
- Evaluate the alternative courses of action;
- Determine appropriate courses of action consistent with the organization's risk tolerance level; and
- Implement the courses of action.

RM4- Risk monitoring

The risk monitoring process addresses how risks will be monitored and communicated over time in electronic commerce organization. During the risk monitoring element, organizations will: Verify that risk response measures are implemented and that the information confidentiality requirements derived from the Risk Management Strategy are satisfied; Evaluate the on going effectiveness of risk response measures; Identify changes that may impact risk to an organization's assets and the Operational environments; and Define the monitoring process to assess how change impacts the effectiveness of risk responses.

6.4 Summary of Additions after Validation

Table 6.11 shows the amendment done to the initial proposed framework after the process of validation. There were number of proposal from the respondents that were found to be useful and therefore they were infused in the framework.

Table 6.11: Results for the Validation

Domain	Process	Remarks
Planning and organisation	PO1 - writing of a security ISMS	Activity policy on use, storage and disposal of confidential information was added
	PO3 - Privacy and confidentiality	A domain Privacy and confidentiality was added
Technical Control	TC6 - Access and Authorisation Control	Activity access was expanded to include; - Limit unsuccessful log-on- attempts - Recording log-on-attempts - Alarm message once Maximum log-on-attempts are exceeded - Automatically expiring passwords
		An activity Verify and Validate Security was added
	TC6 – Anti-Phishing Measures	A new Domain named Anti-Phishing Measures was added
Risk Management	RM1 – RM4	A domain Risk management introduced to replace the domain Monitoring and control in the former framework which was considered inferior to Risk Management
		Process RM1 to RM4 in the domain Risk Management were introduced

From 6.11 the following can be noted for each domain:

Plan and Organise

- This domain has been rebranded to Planning and organizing
- Tuned to suit information confidentiality and other information security requirements such as compliance with external requirements.
- The processes reduced from ten to five

Acquire and Implement

- The domain has been aligned to suit the problems identified in this study
- The domain has been rebranded to acquisition and development management
- The processes reduced from seven to five
- Inspection and verification /verify and validate security as a process was introduced

Deliver and Support

- The domain was rebranded to operations and maintenance
- Processes reduced from thirteen to seven
- Domain was reinforced with strong security controls such as security reporting Monitor and Evaluate
    - This domain was rebranded to Technical control. It was completely reorganised to suit information confidentiality security.
    - This domain has the core processes where the information confidentiality control is anchored

It is important to note that a new domain that did not exist in COBIT was created. This is the domain Risk Management.

Table 6.12 is a comparison between the COBIT security framework and the proposed security framework. The table shows the difference between the COBIT and the proposed framework in terms of what was removed and what was injected in coming up with the new framework.

Table 6.12: Comparison of COBIT and COEIST

COBIT		PROPOSED FRAMEWORK (COEIST)	
DOMAIN	**PROCESSES**	**DOMAIN**	**PROCESSES**
PLAN AND ORGANISE	PO1: Define a strategic plan	Planning and organizing	PO1: Writing of a security ISMS policy
	PO2: Define the information architecture		
	PO4: Define IT process, organizations and relationships		PO2: Determine IT information security operations management
	PO5: Manage the IT investments		PO3: Privacy and confidentiality of information
	PO6 :Communicate management aims and direction		PO4: Ensure compliance of external requirements
	PO7: Manage IT human resources		PO5: Formulation of human resource management policy
	PO8: Manage quality		
	PO9: Asses and mange IT risks		
	PO10: Manage projects		
ACQUIRE AND IMPLEMENT	AI1: Identify automated solutions	development and Acquisition management	AD1: Identify information security requirements and needs
	AI2: Acquire and maintain application software		AD2: Identify and allocate resources
	AI3: Acquire and maintain technology infrastructure		AD3: Acquire technology infrastructure
	AI4 : Enable operation and use		AD4: Inspection and verification /verify and validate security
	AI5: Procure IT resources		AD5: Manage third party services
	AI6 : Manage changes		
	AI7: Install and accredit solutions and changes		
DELIVER AND SUPPORT	DS1: Define and manage service level	Operations and maintenance	OM1: Input validation
	DS2: Mange third party services		OM2: Operational change control
	DS3: Manage performance and capacity		OM3: Information security awareness, education and training
	DS4: Ensure continuous service		OM4: Security reporting

	DS5: Ensure system security		OM5: Business continuity planning
	DS6 : Identity and allocate costs		OM6: Updating security policies
	DS7: Educate and train users		OM7:Manage physical and environment security
	DS8: Manage service desk and incidents		
	DS9: Manage the configuration		
	DS: 10 Manage problems		
	DS: 11 Manage data		
	DS: 12 Manage the physical environment		
	DS: 13 Manage operations		
MONITOR AND EVALUATE	ME1: Monitor and evaluate IT performance	Technical control	TC1: Asset classification and control
	ME2: Monitor and evaluate internal controls		TC 2: Cryptographic control
	ME3: Ensure regulatory compliance		TC3: Software define perimeter
	ME4: Provide IT governance		TC4: Network security
			TC5: Physical and Environmental security
			TC6: Access control and authorisation Control
			TC7: scanning monitoring software
			TC8 :Anti-phishing measures
		Risk Management	RM1: Risk Frame
			RM2: Risk assessment
			RM3: Risk Response
			RM4: Risk monitoring

CHAPTER SEVEN

7.0 CONCLUSIONS AND RECOMMENDATIONS

This section provides a summary of significant findings from the study. It gives a conclusion to the findings and recommendations.

7.1 Summary of Significant Findings of the Study

The research was intended to identify the challenges faced by electronic commerce, to identify the key issues surrounding electronic commerce information security management, to investigate the techniques and approaches used in managing Electronic Commerce information security threats and to develop a security framework for securing electronic commerce against confidentiality threats.

This research points out electronic commerce faces numerous information security challenges and also the information security approaches used are ineffective and inefficient. Most of the respondents at 96.4% strongly disagreed with the fact that current approaches adopted by our organization are adequate with 28.6% also disagreeing. Further, the respondents disagreed that current approaches adopted by their organization are efficient as the majority at 82.1% disagreeing. Confidentiality and Privacy issues was the top security issue of concern to the respondent's with 60.7% of the respondents admitting to it. Respondents further considered viruses and malicious software at 46.4%, human errors at 28.6% and also system or software errors at 17.9% as the top three main causes of confidential threat their organizations. Further the study revealed 85.7% of the respondents admitted that their organisation did not use any framework in managing information security.

7.2 Conclusion

As business and financial sectors increasingly continue to heavily rely on the internet and computer technologies to operate their business and market interactions, the threats and security breaches have highly increased in the recent years. Confidentiality and privacy attacks both internally and externally have caused electronic commerce institutions trillions dollars annually. Thus, it is believed that the developed security framework will secure electronic commerce against confidential threats and increases effectiveness and efficiency of information security management in electronic commerce.

The specific research objectives and how they were achieved are summarized in Table 7.1.

Table 7.1: Mapping the Objectives on to the Research findings

Research objectives	How they were achieved
To identify the information confidentiality challenges faced by electronic commerce and by use of integration approach develop a security framework to address them	Questionnaires were used to collect data on services from the tour and travel companies electronic commerce B2C sector
To identify the key confidentiality issues surrounding information security management in electronic commerce and to provide a means of addressing them.	The Key issues surrounding electronic commerce were identified through literature review and confirmed through collection of data from the service providers and the clients.
To investigate the techniques and approaches used in managing Electronic Commerce information confidentiality threats.	The findings from the data collected also showed the techniques and approaches used in tour and travel companies a sector of B2C electronic commerce.
To use findings of 1, 2 and 3 to develop a security framework for securing electronic commerce against confidentiality threats.	A framework was derived from Control Objective for Information and related technology (COBIT) framework, the secondary and primary data obtained from the research was developed. It has also borrowed from other existing information security management frameworks of best practices. The framework referred to as **C**ontrol **O**bjectives for **E**lectronic commerce **I**nformation **S**ecurity and related **T**echnologies (**COEIST)** has five domains namely: Planning and organizing, Acquisition and development management, Operation and Maintenance, Technical and control and Risk Management.
To validate framework the developed framework.	This was achieved through analysis of the collected data. The findings confirmed the elements of the framework and newer elements were also added.

7.3 Recommendations of the Study

The recommendations of the study based on the findings:

- Organisations practicing electronic commerce should formulate policies that promote information confidentiality. Such policies were found lacking.
- Each organisation practicing electronic commerce should increase the funds allocated for managing threats against information confidentiality.
- A Risk assessment framework should be developed necessary to assess confidentiality threats in electronic commerce.
- Information security experts globally should come up with a unified approach to fight threats against confidentiality.
- Creation of awareness and train staff and consumers on information security services.

7.4 Recommendations for Further Research

- Research could be done to determine the characteristics of effective security managers.
- This study suggests that research should be done to find out whether the framework proposed by this research can be used to address integrity issues.

Study should be done to evaluate the proposed framework in a real - world environment.

REFERENCES

Al-Ahmad, W. and Mohammad, B. (2012). Can a Single Security Framework Address Information Security Risks Adequately? *International Journal of Digital Information and Wireless Communications (IJDIWC)*, 2(3), 222-230.

Alfawaz, S. M. (2011). Information security management: A case study of an information security culture. Retrieved from: http://eprints.qut.edu.au/41777/1/Salahuddin_Alfawaz_Thesis.pdf

Ali, K. (2013). Web Mediated Communications – Positive and Negative Effects. Retrieved from: http://bada.hb.se/bitstream/2320/12623/1/2013MAGI05.pdf

Atwal, H. (2008). Capability Maturity Model. Retrieved from: http://www.cs.nott.ac.uk/~cah/G53QAT/Report08/hsa06u-WebPage/hsa06u-WebPage/disadvantages.html

Bechan, U. (2008). Towards a Framework for Securing Business against Electronic Identity Theft. Retrieved from: http://uir.unisa.ac.za/bitstream/handle/10500/1304/dissertation.pdf?sequence=1

Bishop, M. (2002). Computer Security. Art and Science. Boston: Addison –Wesley

Bishop, M. (2003). Computer Security. Art and science. Delhi: Pearson Education

Borg,W.R., and Gall,M.D (1989). Education Research. Newyork: Longman

Bragg, R. (2004). Network security. The complete reference. New Delhi: Tata McGRAW-Hill publishing Company Limited

Carlson,T. (2008). Understanding ISO 27002. Retrieved from: http://www.orangeparachute.com/documents/Understanding_ISO_27002.pdf.

Carlson, T. (2001). Information Security Management: Understanding ISO 17799. Retrieved from: http://www.netbotz.com/library/ISO_17799.pdf.

Chen, T. M. (2009). Trends in Viruses and Worms. Retrieved from: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/virus_trends.html.

Ciampo, M. (2012). Security and Guide to Network Security Fundamental, International Edition. Mexico: Cengage Learning

ICT Authority (2014). Campaign to sensitize Kenyans on online safety launched. Retrieved from http://www.icta.go.ke/kaa-ridhoo-campaign-launched/

Commer, D. E. (2009). Computer Networks and Internets. 2nd Ed. New Delhi: Pearson Education, Inc.

Conner, B. (2003). Information Security Governance: Towards a Framework for Action, Business Software Alliance New Jersey: John Wiley & Sons, Inc.

Cooper, D.R. and Schindler, P., S. (2008).Business Research Methods. London: Mcgraw Hill Higher Education.

Curtis, G. and Cobham. D. (2005*).* Business Information System: Analysis, design and Practice, 5th ed.. England: Pearson Education Limited Edinburgh hate Harlow.

Disterer, G. (2013). *ISO/IEC 27000, 27001 and 27002 for Information Security Management Journal of Information Security, 4*. Retrieved from http://www.scirp.org/journal/jis

Dutta, A., Roy, R. (2008). *Dynamics of organizational information security*, *System Dynamics Review, vol.24, Issue 3.*, Wiley Interscience, Retrieved from: http://www3.interscience.wiley.com/journal/121518999/abstract?CRETRY=1 andSRETRY=0

El-Buhaisi, A.N. (2013). Detection Model for Pharming Attack Based on IP- Address Check and Website Predictability. Retrieved from: http://library.iugaza.edu.ps/thesis/111679.pdf

Frankel and Wallen (1993). Research Methodology 2nd ed.. New York: Mcgraw-Hill

Frauenstein E. D. and Solms R. V. (2009). Phishing: How an Organisation Can Protect Itself. Retrieved from: http://icsa.cs.up.ac.za/issa/2009/Proceedings/Full/12_Paper.pdf

Forouzan, B.A (2013) Data communication and networking 5E Mc , 5th Ed. New York: Graw-Hill.

Gatehouse, G. (2013). Kenya election: Tech hub hopes take polling day blow. Retrieved from: http://www.bbc.co.uk/news/world-africa-21712715

Gehrmann, M. (2012). Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations. Retrieved from: http://www.spell.org.br/documentos/ver/32517/combining-itil--cobit-and-iso-iec-27002-for-structuring-comprehensive-information-technology-for-management-in-organizations/i/en

Goldman,D. (2012). Major Banks hit with biggest cyber-attacks in history. Retrieved from:http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/

Goh, R. (2003). Information Security: The Importance of Human Element. Unpublished PhD. Thesis. Retrieved from: http://www.ritagoh.com/Academia/thesis.pdf

Golubova, S. (2012). Electronic commerce Adoption and Implementation Strategy for a High- Tech Firm. Retrieved from: http://essay.utwente.nl/62992/1/ Master_Thesis_Electronic commerce_Adoption_and_Implementation_ Strategy_Svetlana_Golubova_%281%29.pdf

Goodin, D. (2011). Sony says data for 25 million more customers stolen. Retrieved from: http://www.theregister.co.uk/2011/05/03/sony_hack_ exposes_more_customers/

Goodin, D. (2011b). Hackers breach chocolate recipe on Hershey website. Retrieved from: http://www.theregister.co.uk/2011/08/08/hershey_website_hacked/

Goodrich,M. T. and Tamassia, R. (2011). Introduction to computer security. New York: Pearson

Goosen, R. (2012). The Development of an Integrated Framework In Order To Implement Information Technology Governance Principles at a Strategic and Operational Level for Medium-To-Large Sized South African Businesses. Retrieved from:http://scholar.sun.ac.za/bitstream/handle/10019.1/20279/goosen _development_2012.pdf?sequence=2

Gorard, S. (2003).Quantitative methods in social science. New York: Continuum.

Hasan, R. and Sobhan, M. A. (2012). Study on electronic commerce Threats and Security. Retrieved from: http://daffodilvarsity.edu.bd/nccis/pdf/TS2 _Paper_06.pdf

Hayajneh, T. (2013). Performance and Information Security Evaluation with Firewalls. Retrieved from: http://www.sersc.org/journals/IJSIA/vol7_no6_2013/37.pdf

Hill, P. and Turbitt, K. (2006). Combine ITIL and COBIT to Meet Business Challenges. Retrieved from: http://www.ualberta.ca/~vpit/frameworks/pdf/itil_cobit.pdf

Himi, A. and Mustapha, E. (2011). The IT Service Management according to the ITIL framework applied to the enterprise value chain. Retrieved from: http://ijcsi.org/papers/IJCSI-8-3-2-515-522.pdf

Hoodrick, M.T. and Temassia, R. (2011). Introduction to Computer Security. Delhi : Pearson Education

Horak, R. (2002). Communications Systems and Networks, 3rd ed. New Delhi: Wiley Dreamtech India (P) Ltd.

Humphreys, E. J (2013). The new cyber warfare. Retrieved from: http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1785

Hurst, S. (2013). Top to security challenges for 2013. SC magazine. Retrieved from: http://www.scmagazine.com/top-10-security-challenges-for-2013/article/281519/

Ismail, S. (2015). Studying Scada Organisations Information Security Goals: An Integrated System Theory Approach. Retrieved from: http://pacis2015.comp.nus.edu.sg/_proceedings/PACIS_2015_submission_476.pdf

IT Governance Institute (2011). COBIT Security Baseline—An Information Security Survival. Kit. Rolling Meadows. Retrieved from: http://trygstad.rice.iit.edu:8000/Policies%2520%26%2520Tools/COBITSecurityBaselie-ISACA.pd

IT Governance (2006). COBIT Mapping: Overview of International IT guidance, 2nd ed. Retrieved from: http:www.sox-expert.com/uploads/file/COBT%20mapping%202nd%20edition.pdf.

Kanapathy, K. and Lumpur, K.(2012). Assessing the Relationship between ITIL Implementation Progress and Firm Size: Evidence from Malaysia. Retrieved from: http://repository.um.edu.my/14369/1/IJBM_Vol7_2_KK.pdf

Keanini, T.K (2014). The evolution of security and Challenges that come with IT in 2014. Retrieved from: http://www.scmagazine.com/the-evolution-of-security-and-challenges-that-come-with-it-in-2014/article/323302/

Kaufmann, M. (2009). Computer and Information Security. New Jersey: Pearson education Upper Saddle River

Kenyon, T. (2002). Data networks. Rerouting, security, and performance optimization. Amsterdam: Digital press

Khan, R. (2010). Practical Approaches to Organizational Information. Security Management. Retrieved from: http://www.sans.org/reading-room/whitepapers/leadership/practical-approaches-organizational-information-security-management-33568

King, M. (2012). RBS IT Fallout: Ulster Bank Customers Still Without Account Access. Retrieved from: http://www.guardian.co.uk/money/2012/jul/02/ rbs-it-ulster-bank-customers-without-access

Kark, K. (2007). Defining a High-Level Security Framework. Putting Basic Security Principles to Work. Retrieved from: http://www.forrester.com/Defining+A+ HighLevel+Security+Framework/fulltext/-/E-RES40996

Kombo, D. and Tromp, D (2006), Proposal and Thesis Writing An Introduction. Nairobi: Paulines Publications,

Kosutic, D. (2011). *ISO 27001 Basics*. http://www.iso27001standard.com/en/what-is-iso-27001

Kothari, C.R. (2004). Research Methodology. Methods and Techniques. New Delhi: New Age International (P) Limited.

Kumar, R. (2005). Research Methodology. A step-by-step Guide for Beginners. New Delhi: Sage Publications.

Laudon, K. C. and Trever, C. G. (2002). E- Commerce Business Technology Society. Delhi:Pearson Education

Li ,Y. and Fan, R. (2014). The coordination of Electronic commerce and Logistics: A case study of Amazon.com. Retrieved from: http://www.diva-portal.org/smash/get/diva2:685599/fulltext01.pdf

Long, W. (2013). *BYOD: Data Protection and Information Security Issues*. Retrieved from: http://www.computerweekly.com/opinion/BYOD-data-protection-and-information-security-issues

Lokesh, K. (1997). Research Methodology and Educational Statistics 3rd ed. New Delhi: Vikas Publishing

Loudon, K.C. and Laudon, J. P. (2010). Management information systems. Managing digital firm, 11th ed. Upper Saddle River, New Jersey: Pearson Education, INC

Laudon, K.C. and Traver, C.G. (2014). Electronic commerce: Business. Technology. Society. Saddle River, New Jersey: Pearson Education, INC

Loveland,G. and Lobel, M. (2012). Cybersecurity: The new business priority. Retrieved from: http://www.pwc.com/us/en/view/issue-15/cybersecurity-business-priority.jhtml

Manktelow, J. (2013). Data and Information Management. Protecting an Important Organizational Asset

McMillan, J. H., and Schumacher, S. (2001). Research in Education. New York: Longman.

Meadows, C. (1999). A Formal Framework and Evaluation Method for Network Denial Of Service, Proceedings of the 1999 IEEE Computer Security Foundations Workshop, IEEE

Merkow, M.S. and Breith, J. (2014). Information Security: Principles and Practices, 2nd Ed. USA: Pearson Education inc.

Moftah A.A.A. et al. (2012). Challenges of Security, Protection and Trust on Electronic commerce: A Case of Online Purchasing In Libya. *International Journal of Advanced Research in Computer and Communication Engineering 1*(3), May Retrieved from :http://www.ijarcce.com/upload/may/

electronic commerce%20a%20casE%20OF%20ONLINE%20PURCHASING%20IN%20LIBYA.pdf 2012

Mohammad, N, A. (2012). Security electronic transactions to support electronic commerce. Retrieved from: arxiv.org/pdf/1207.4292

Mugenda, M, and Mugenda, G. (2003) Research Methods: Quantitative and Qualitative Approaches. Nairobi: African Centre for Technology Studies.

Munirul, U, and Zuraini,I. (2011). A Framework for Governance of Information Security In Banking Systems. Retrieved from: http://www.ibimapublishing.com/journals/JIACS/2011/726196/726196.pdf

Murule , R. (2013). Cybercrime to cost Kenya almost $23mn in 2013. Retrieved from: http://www.itwebafrica.com/security/515-kenya/232053-cybercrime-to-cost-kenya-almost-23mn-in-2013#sthash.96e5xW6m.dpuf

Musa, A., A. (2009). Exploring the importance and implementation of COBIT processes in Saudi organizations. Retrieved from: http://www.emeraldinsight.com/journals.htm%3Farticleid%3D1793523

Mutung'u, G. (2012). New media in Kenya: Time for regulation. Retrieved from: http://www.article19.org/join-the-debate.php/72/view/

Mwakalinga, J. (2011). A Framework for Adaptive Information Security Systems – A Holistic Investigation. Retrieved from: http://www.diva-portal.org/smash/get/diva2:417888/FULLTEXT01.pdf

Myers, D. H. (1983). Social Psychology. New York: Mc-Hraw- Hill Book Company.

Mzekandaba, S. (2013). Kenyan businesses face cyber security threat. Retrieved from: http://www.itwebafrica.com/security/515-kenya/231726-kenyan-businesses-face-cyber-security-threat-says-kaspersky#sthash.cKcLKgIN.dpuf

Newnan, R. C (2003). Enterprise Security. Delhi: Pearson Education

Nikolakopoulos, T. (2009). Evaluating the Human Factor in Information Security. Retrieved from: https://oda.hio.no/jspui/bitstream/10642/444/2/Nikolakopoulos_Theodoros.pdf

Niranjanamurthy, M. and Chahar, D. (2013). The study of Electronic commerce Security Issues and Solutions. *International Journal of Advanced Research in Computer and Communication Engineering 2(7),* Retrieved from: http://www.ijarcce.com/upload/2013/july/69-o-Niranjanamurthy%20-The%20study%20of%20Electronic commerce%20Security%20Issues%20and%20Solutions.pdf

Nivan, J.M et al. (2013). The study of electronic commerce security issues and solutions. *International journal of advanced research in computer and communication engineering, 2 (*7).

Norman, A. A.and Yasin, N.M. (2011). An Analysis of Information Systems Security Management (ISSM): The Hierarchical Organizations vs. Emergent Organization. *International Journal of Digital Society (IJDS), 1 (*3). Retrieved from http://www.infonomicssociety.org/IJDS/An%20Analysis%20of%20Information%20Systems%20Security%20Management%20%28ISSM%29_The%20Hierarchical%20Organizations%20vs.%*20Emergent*%20Organization.pdf

Nunnally, J. C. (1978). Psychometric Theory. New York: McGraw-Hill Book Company.

Olsen, K. (2013). Top three data security challenges for IT mangers. Retrieved from: http//www. Information-management.com/news/top-3-data-security-challenges-for-it-managers- 10024093-1.html.

Olzak ,T. (2013), COBIT 5 for information security: The underlying principles. Retrieved from:http://www.techrepublic.com/blog/it-security/cobit-5-for-information-security-the-underlying-principles/

Oracle (2002). Security Overview: Oracle9i Security Overview, Release 2 (9.2) Retrieved from: http://docs.oracle.com/cd/B10501_01/network.920/a96582/part1.htm

Orodho, J.A (2005). Elements of Education and Social Science Research Methods. Nairobi: Harlifax Printers and General Supplies.

Otuteye, E. (2003). A systematic approach to E-business security. Retrieved from:

http://ausweb.scu.edu.au/aw03/papers/otuteye/paper.html

Paquet, C. (2013). Network Security Concepts and Policies. Retrieved from: http://www.ciscopress.com/articles/article.asp?p=1998559

Patil J. (2008). Information Security Framework: Case Study of a Manufacturing Organization. Retrieved from: https://legacyweb.mercy.edu/ias/patil.pdf

Pfleeger, C. P. and Pfleeger, S. L. (2009). Security in Computing, 3rd ed. New Jersey: Prentice Hall Upper Saddle River.

Phillips, M. (2003). Using a Capability Maturity Model to Derive Security Requirements GSEC Practical v1.4b Option 1. Retrieved from: http://www.sans.org/reading-room/whitepapers/bestprac/capability-maturity-model-derive-security-requirements-1005?show=capability-maturity-model-derive-security-requirements-1005 andcat=bestprac

Qin, Q. and Ge, L. (2012). Information Security Management in Electronic commerce. China: Shanghai ocean university

Ramah, R. (2012). Kenya to set up online identity-verification system. Retrieved from: http://sabahionline.com/en_GB/articles/hoa/articles/features/2012/12/06 /feature-01

Raggad, B. G. (2010). Information Security Management. Concepts and Practise. New York: CRC Press Taylor and Francis Group, ILC

Rashid, R.M. and Zakaria, O.M.(2013). The Relationship of Information Security Knowledge (Isk) and Human Factors: Challenges and Solution

Rayport, J. F and Jaworski, B. J. (2003). Introduction to Electronic commerce, 2nd ed. New Delhi: Tata Mchraw-Hill Edition.

Rayport. J F. and Jaworski B. J. (2002). Cases in electronic commerce. New York: Mc Graw-Hill.

Reeder K. (2011). Survey: Mobile Apps Exposing Sensitive Data. Retrieved from: http://www.enterprisenetworkingplanet.com/netsecur/survey-mobile-apps-exposing-sensitive-data

Rishabh (2014). Electronic commerce Challenges – 1: Security Concerns. Retrieved

from: http://www.rishabhsoft.com/blog/electronic commerce-challenges-1-security-concerns.

Rhodes, M and Strassberg, K (2004). Network Security.The Complete Reference. New Delhi:McGraw-Hill Professional.

Roman, J. (2013).Testing Cyber-Attack Responses.National Drill to Help Banks Improve Communications. Retrieved from: www.bankinfosecurity.com/new

Rouse, M. (2007). Capability Maturity Model (CMM). http://searchsoftwarequality.techtarget.com/definition/Capability-Maturity-Model

Saleh, M.S. and Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. Applied Computing and Informatics 9 (2), 107–118. Retrieved from: http://ac.els-cdn.com/S2210832711000287/1-s2.0-S2210832711000287-main.pdf?_tid=ec592ef8-2577-11e5-98a6-000aab0f01&acdnat=1436363450_3d6a6957b4997243bc70eae8125da1b3

Sarantakos, S. (1998). Social Research, 2nd ed. Australia: Charles Sturt University.

Sante, T. V. and Ermers J. (2013) ITIL® and TOGAF® 9.1: Two frameworks Retrieved from: https://shop.axelos.com/gempdf/ITIL_and_TOGAF_White_Paper_v0_3.pdf

Sengupta, A, Mazumdar,C and Bariki, M. (2005). Electronic commerce Security. A life Cycle Approach.Sadhan, 30 (2 &3), 119–140. © Printed in Indi

Seleanu, D. (2013). Cybersecurity in Canada: Finance industry, government seek ways to share Data. Retrieved from: http://blogs.reuters.com/financial-regulatory-forum/2013/07/18/cybersecurity-in-canada-finance-industry-government-seek-ways-to-share-data/

Senn. J A. (2003). Information Technology in Business. Principles, Practices and Opportunities. New Jersey: Prentice Hail upper saddle River.

Serianu (2012). Kenya cyber security report 2012. Nairobi: Serianu.

Sharma, V. and Sharma, R. (2000). An integrity Approach. Delhi: Pearson Education

Sheikhpour, R. and Modiri, N. (2012). An Approach to Map COBIT Processes to ISO/IEC 27001Information Security Management Controls .international. *Journal of Security and Its Applications,* 6(2). Retrieved from*:* http://www.academia.edu/1587532/An_ Approach_to_ Map_COBIT_Processes_to_ISO_IEC_27001

Sherif, E. (2012). Information Security Policy: The National Payment System in Libya. Retrieved from: http://uobrep.openrepository.com/uobrep/bitstream/ 10547/235594/1/SherifXF-1032226.pdf

Stahl, S. and Kimberly, A (2007). Effectively Managing Information Security Risk. A guide for executives. Los Angelas: Citadel Information Group, Inc

Stallings, W. (2007). Network Security Essentials, Applications and Standards, 3rd Edition. New Jersey: Pearson Education, Inc.

Stallings, W. and Brown, L. (2011). Cryptography and Network Secutity. Principle and Practice. New York: Pearson education limited

Stallings, W. and Brown, L. (2012). Computer security. Principles and practice (2nd ed). Edinburgh Gate: Pearson education limited

Stigler, G. (1971). The Social Science Research Methods. *Bell Journal of Economics and Management Science, 2,* 3-21.

Susanto, H. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical and Computer Sciences IJECS-IJENS 11 (05) Retrieved from: http://www.ijens.org/vol_11_i_05/113505-6969-ijecs-ijens.pdf

Talib, A.M. and Barachi, M.E. (2012). Guide to ISO 27001: UAE Case Study. Issues in InformingScience and Information Technology, *7.* Retrieved from: http://iisit.org/Vol9/IISITv9p331- 349Talib041.p.

Tariq, U. (2011*).* Electronic commerce: security challenges and solutions. Retrieved fromhttp://usmantariq.org/blog/homepage/wp-content/uploads/2011/02/ Electronic commerce-Security-Challenges-and-Solutions-25-April-2011.ppt

Telecoms (2013). Lack Of Security Fears Slows Down Uptake of Electronic commerce in Kenya. Retrieved from: http://www.balancingact-africa.com/news/en/issue-no-185/web-and-mobile-data/lack-of-security-fea/en.

Telkom Kenya (2013). Kenya Telephone directories. The Official Yellow Pages. Postel Directories, Kenya

Tipton, H.F. and Krause M. (2002). Information Security Management. Newyork: C.R.C Press LLC.

Tomoda, K. (2010). IT Infrastructure of Data Center Services.Based on ITIL344 FUJITSU Sci. Tech. J., 46(4), 344–351.

Traver. C. G. and Laudon K. C. (2002). Electronic commerce: Business technology society.New York: Pearson education.

Trepper, C. (2000). Electronic commerce Strategies. Asoke K Ghosh, Prentice – Hall of India Private Limited, Connaught Circus, New Delhi.

Turban, E., King D. and Jaeler D. V. (2006). Electronic Commerce. A managerial perspective. Upper saddle River: Pearson Prentice Hait

United Nations (2013). Comprehensive Study on Cybercrime . New York, 2013 Retrieved from: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Vivek, S. and Rajiv, S. (2000). Developing Electronic commerce Sites. An integrity Approach. Delhi: Pearson Education.

Wanjiku, R. (2013). Kenyan banks face challenges with secure online transactions International banks are not as successful as in other markets. Retrieved from: http://www.pcadvisor.co.uk/news/enterprise/3453739/kenyan-banks-face-challenges-with-secure-online-transactions/#ixzz2h7ieqP57

Ward, T. (2010). Strategies for Reducing the Risk of electronic commerce Fraud. First Data. Retrieved from: https://www.firstdata.com/downloads/thought-leadership/ecommfraudwp.pdf

Westervelt, R. (2011). Top 5 mobile phone security threats in 2012. Retrieved from: http://searchsecurity.techtarget.com/news/2240112288/Top-5-mobile-phone-security-threats-in-2012.

Wessels, E. and Loggerenberg, J.V. (2006). IT Governance: Theory and Practice. Proceedings of the Conference on Information Technology in Tertiary Education,Pretoria, South Africa, 18 – 20 September 2006. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.2838andrep=rep1andtype=pdf

Whitman, M. E. and Mettord, H. J. (2012). Principles of Information Security, 4th Edition.Course technology, Cengage learning.

William, S. (2011). Cryptography and network security. Principles and practice, 5th ed.Upper Saddle River: Pearson education

Wilson, D. A. (2006). Management information .IT for business processes, 3rd ed. Oxford: Elsevier Butterworth Heinemann.

Yang, Z. (2011). A Survey of Cybercrime. Retrieved from: http://www.cs.wustl.edu/~jain/cse571-11/ftp/crime/index.html

Yeo, K. T. and Ren, Y. (2011). Risk Management Capability Maturity Model for Complex Product Systems (CoPS) Projects. Retrieved from: http://www-scf.usc.edu/~yingtaor/publications/RM_CMM_SysEng.pdf

Zhang, S. (2013). An Exploratory Examination of the Practicability of COBIT framework. Retrieved from: http://liacs.leidenuniv.nl/assets/Masterscripties/ICTiB/Zhang-non-confidential.pdf

APPENDICES

APPENDIX A

STUDY INSTRUMENT

INSTRUCTIONS:

I am a post graduate student pursuing Masters of Science in Computer Systems and carrying out a study on information security in electronic commerce. Your organisation has been sampled for this study. Kindly co-operate and assist in filling the questionnaire as correctly and honestly as possible. The information you will give will be treated with great confidentiality and will not be used for any other purpose other than this research. This questionnaire has four parts. Please, indicate the correct option by putting a tick (√) on the options. For the questions that require your own opinion use the provided spaces. Kindly respond to all items.

SECTION A

1. Indicate your gender
2. Male ( ) Female ( )
3. How long have you worked for this organisation?

   (a) 1-5 years ( ) (b) 5-10 years ( )

   (c) 10-15 years ( ) (d) over 15 years ( )
4. What is your designation in the IT department?

   ……
5. Does your organisation have an information security officer?

   Yes ( ) No ( )
6. If no to question 4 above state who is responsible of taking care of information security. Tick (√) where applicable.

Consultants	( )
Data entry clerks	( )
ICT Manager	( )
None	( )
Others	( )

If your response above is others, state who takes care of the information security.

……

SECTION B

Information Security Challenges Faced by Electronic Commerce.

7. **What percentage of your organisation budget is spent on information security? Tick (√) where applicable.**

1- 5%	( )
5-10%	( )
10-15%	( )
15-20%	( )
Greater than 20%	( )

8. **To what extent do you agree with the following statements? Tick (√) where applicable**

Statement	**Strongly Agree**	**Agree**	**Disagree**	**Strongly Disagree**	**Do not know**
Our organizations place more value to outsmarting our competitors than securing our information systems.					
Our organizations set aside Little finances to secure information compared to finances set aside for advertisement.					
Security is the principal concerns that restrict customers and organizations in engaging in online business transactions.					
Growth in magnitude, speed, and complexity of Information security threats has made prevention and clean-up more					

difficult.					
Blended threats have made prevention and clean-up more difficult.					
One of the biggest information security challenges is that the information security market is still in its infancy with few formal standards established for products or services.					
Information security techniques that are available in the market address only a portion of a company's security needs forcing companies to have multiple installation.					
There is not unified approach that can be used to secure information.					
Finding qualified information security staff is a difficult.					
Due to the immature market, lack of standards, and numerous security solutions, training is a problem for security staff.					
The information security challenges keep growing at a rapid pace hence continuous awareness trainings are necessary which electronic commerce organizations find hard to cope.					
Unique requirements for information security officers makes it difficult for					

existing IT staff to transit into information security personnels without receiving specialized enforcement training.					
There are no enough Government and industry regulations to ensure that personal information is protected from loss, misuse, unauthorized access or disclosure.					
Kenyan government does not place high priority on protection of personal information or intellectual property.					
Mobile computing devices such as flash disks, lap tops, iPods, tablets, smartphones and USB cables owned by our employees are a threat to our information security.					
In Kenya there is little legal recourse to combat the illicit activities of software pirates and cyber crimes.					
Our organisation ignores the human dimension of information security while enforcing information security.					
In Kenya, there is lack Consumer education on security issues.					

9. In your own opinion what do you think should be done in order for electronic commerce organisations to overcome these challenges?

SECTION C

Key issues surrounding electronic commerce information security management.

1. What do you consider the top information security issue of concern to your organisation?

   Confidentiality and privacy issues ( )
   Integrity issues ( )
   Availability issue ( )
   Non-repudiation ( )

2. **What do you consider to be top three main causes of security incidents in your organisation?**

   Viruses and malicious software ( )
   Cyber attacks ( )
   System or software errors ( )
   Internal based attacks ( )
   Hardware failure ( )
   Human errors and omissions ( )

3. **Has your organisation network ever experienced any of the following problems since you started using it?**

Problem	**Yes**	**Never**	**Do not know**
Unauthorized access to or interception of data			
Username and password leakage			
Web link to an address different from the intended one			
Hacking			
Stealing of business as well as sensitive customers' information from your organization's website			
Receiving e-mail messages that look like those			

of legitimate businesses partners or financial institution you bank with but in the real sense they are fake			
Employees being tricked to give confidential information about your organization or about your customer by people claiming to be legitimate authorities.			
Sacked Employees revealing confidential information about your organization or about your customers.			
Disgruntled employees revealing confidential information about your organization or about your customer.			
Attacks using malicious software as such viruses, worm or Trojan horse.			
Competitor hacking into your organisation website			
users of your organisation's website being redirected to bogus web pages, even when they types the correct web page address into his or her web browser			

SECTION D

Techniques and approaches used in managing Electronic Commerce information security threats.

1. **Does your organisation use the following information security approaches?**

Statement	**Yes**	**No**	**Do not know**
Firewalls			
Authentication control			
Authorisation control			
International information security management Standards/framework.			
Antivirus			
Updating antivirus regularly			
Intrusion detectors			
Security Education and training			
Risk Assessment			
Activity monitoring and audit using system logs			

2. **To what extent do you agree with the following statement about your organisation?**

Statement	**Strongly Agree**	**Agree**	**Disagree**	**Strongly Disagree**	**Do not know**
Senior management regularly receive reporting on the status of information security status					
Our organisation employees understand the importance of information security.					
Our organisation top management					

understand the importance of information security.					
Senior management provides the required level of support for information security.					
Current approaches adopted by our organisation are adequate.					
Current approaches adopted by our organisation are efficient.					
Our employees frequently receive training on information security					

3. Does your organisation have the following policies

Statement	**Yes**	**No**	**Do not know**
Access control			
Authorization			
Statement	**Yes**	**No**	**Do not know**
Education training and security awareness			
Email access control			
Mobile devices control			
Antivirus			
Separation of duties in management of information security			
Physical security and environmental			
Security reporting			
Security incidents recovery			

4. What changes would you propose in order to improve information security in your organisation?

Thank you for your co-operation

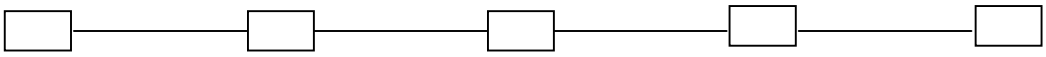
APPENDIX B

VALIDATION QUESTIONNARE

Instructions

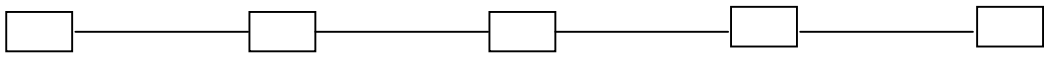
Please rate how strongly you agree or disagree with each of the following statements by placing a check mark in the appropriate box where applicable.

1. The framework developed will improve information confidentiality in electronic commerce business transactions.



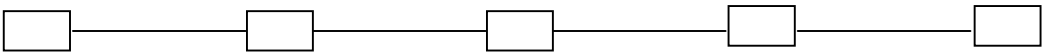
Strongly disagree | Disagree | Undecided | Agree | Strongly agree

2. The tasks in the Framework are applicable in real life situation.



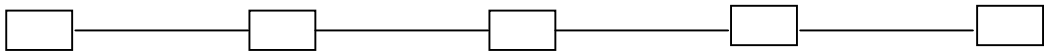
Strongly disagree | Disagree | Undecided | Agree | Strongly agree

3. The tasks in the framework are clear and are easy to implement.



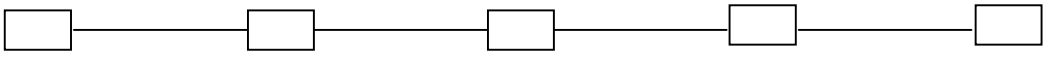
Strongly disagree | Disagree | Undecided | Agree | Strongly agree

4. The suggested framework is economical to use.



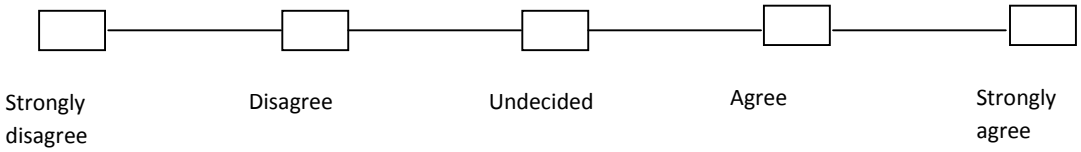
Strongly disagree | Disagree | Undecided | Agree | Strongly agree

5. If you strongly disagree with question 4 above, what do you suggest to be included in the Framework to make it more economical?
6. The framework is clear and easily understandable to intended users.

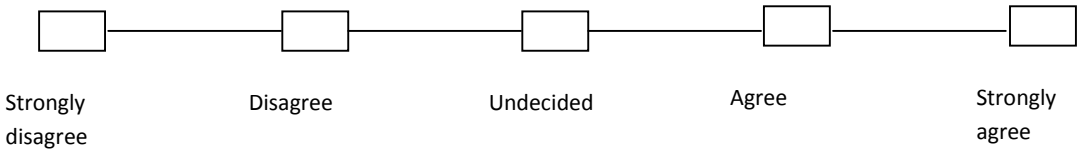


Strongly disagree | Disagree | Undecided | Agree | Strongly agree

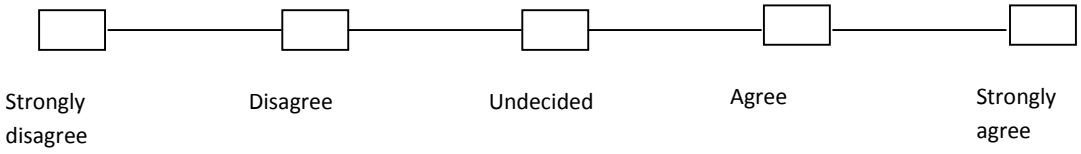
7. If you strongly disagree with question 6 above, is there anything that could be added to or taken away from the Framework to make it clear and easily understandable?
8. The framework adequately addresses the technical and non- technical related security issues.



9. If you strongly disagree with question 8 above make recommendations of how it can be improved.
10. The framework is aligned with current security standards and practice.



11. The framework is flexible enough to deal with possible future confidentiality threats.



Thank you for your cooperation

APPENDIX C

FINANCIAL BUDGET

No.	ITEM	COST
1.	Proposal Preparation	10,000
2.	Stationery	25,000
3.	Final Proposal	15,000
4.	Pilot Study	10,000
5.	Traveling	5,000
6.	Field Work	30,000
7.	Data Analysis	10,000
8.	Report Writing	10,000
9.	Final Report	15,000
10.	Binding and others	10,000
	Total	**130,000**

APPENDIX D

ACTIVITY SCHEDULE

ITEMS OF WORK/ACTIVITIES	MONTHS											
	1	2	3	4	5	6	7	8	9	10	11	12
Proposal writing and submission to BPS												
Proposal Departmental defence												
Corrections												
Preparation for and data collection												
Data analysis												
Thesis writing												
Departmental Presentations												
Preparing journal papers for publication												
Submission of draft thesis for review												
Submission of final thesis to BPS												
Thesis defense												
Corrections and final submission												