CYBER THREATS AND CYBER SECURITY IN ISO CERTIFIED ORGANIZATIONS IN KENYA

BY

MWANIA KASYUMA

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF BUSINESS ADMINISTRATION DEGREE, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

OCTOBER, 2016

DEDICATION

First, I dedicate this research to the Almighty God, without whom this research would have been impossible to conduct.

Secondly I dedicate with love this research to my family, who offered me unconditional love and support throughout the course of this research.

DECLARATION

I declare that this research project is my original work and has not been presented for any academic award in any university

SIGNED_________________________________DATE______________________

Mwania Kasyuma

Registration No.: D61/P/7094/2003

This project has been submitted for examination with my approval as the University Supervisor.

SIGNED_____________________________DATE____________________________

Joel Lelei
Department of Management Science,
School of Business,
University of Nairobi

ABSTRACT

This research is about cyber threats and cyber security in ISO certified organizations in Kenya. The research was motivated by the need to establish the cyber threats facing the ISO certified organizations in Kenya, the cyber threat countermeasures these organizations have implemented and how effective the implemented countermeasures are in managing the cyber threats faced and the overall cyber security of the organizations. ISO certified organizations in Kenya are under a lot of pressure to give their customers quality products and services efficiently. So as to meet their customers' expectations on quality products and services efficiently, the ISO certified organizations have had to rely heavily on the use of ICT systems which are networked and connected to the internet through the national fibre network. With networked ICT Systems, the organizations have become more vulnerable to cyber attacks. The objectives of this research were to establish the cyber threats being faced by ISO certified organizations in Kenya, the cyber threat countermeasures these organizations have implemented and the effectiveness of the countermeasures implemented to managing or counter the cyber threats and ultimately the overall cyber security. A descriptive survey targeting ICT officers, ICT Managers, IT Managers, ICT officers, Information security officers, chief information officers, Heads of ICT as well as ICT Directors was carried out in 45 ISO certified organization in Kenya selected randomly from a population of 175 ISO certified organizations. Overall 35 respondents returned fully completed survey questionnaire resulting in a total response rate of 77.8%. The main instrument for the survey was a questionnaire and descriptive statistics was used for data analysis. The study found out that ISO certified organizations in Kenya face the following cyber threats: insider threats, VOIP PBX Fraud, social media, denial of service (DoS), botnet attacks, online and mobile banking fraud, mobile money fraud and cyber espionage. The study findings also indicate that although most ISO certified organizations have implemented effective cyber threat countermeasures to the cyber threats facing them, some of the organizations have not. Some of the organizations that have not implanted effective countermeasures lack even a cyber security policy which is a crucial blue print guideline and source of reference for managing cyber security.

ACKNOWLEDGEMENTS

I would like to express my deep appreciation to my supervisor Joel Lelei for his support, guidance and encouragement during the entire period of this research. Special thanks to Dr. Kate Litondo and Dr. Kariuki J. T. for their support and recommendations, which helped improve this thesis.

I would also like to thank all Lecturers, IT professionals and all other individuals in the various ISO certified organizations who participated in this study, for their help and co-operation; without them I would not have been able to complete the research.

Last but not certainly not least, I am forever indebted to my wife Hilda Wavinya and my sons Ian, Mark and Moses for their endless patience and support.

Thank you all.

Mwania Kasyuma

Registration No.: D61/P/7094/2003

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

BERR	:	Business, Enterprise and Regulatory Reform
CERT	:	Computer Emergency Response Team
COBIT	:	Control Objectives for Information and related
DOS	:	Denial of Service
IEEE 802.1Q	:	Networking standard that supports virtual LANs (VLANs) on an Ethernet network
ICT	:	Information and Communication Technology
ISACA	:	Information Systems Audit and Control Association
ISO	:	International Organization for Standardization
ISP	:	Internet Service Provider
LAN	:	Local Area Network
PBX	:	Private branch Exchange
VOIP	:	Voice over Internet Protocol

CHAPTER ONE

INTRODUCTION

1.1 Background

Spontaneous information and communication technology (ICT) advancements have resulted in numerous new areas of opportunities and efficiencies for organizations in Kenya and globally. However, while these new technologies have brought the said benefits, they have also brought unprecedented cyber threats (IT Governance Ltd, 2015). To exploit the mentioned ICT benefits, organizations have to put in place ICT infrastructures that consist of networked computers and other communications systems. With the advent of the use of these networked computers both within Local Area Networks (LANs) and internet, organizations worldwide are on a continual basis being faced with the challenge of maintaining their information systems and data in cyberspace secure. Probes of corporate networks by hackers have increased dramatically and new strains of computer viruses that can be used by hackers to launch cyber attacks are being released rapidly and on a continual basis. This calls for organizations to protect their networks and websites with proper security measures because the threat of destructive denial of service attacks has increased significantly (O'Brien 2002).

In Kenya there is improved bandwidth availability as a result of the arrival of the submarine fibre optic cable. Kenyan organizations are using the increased bandwidth and ICT capabilities brought about by the deployment of the national fibre network to efficiently deliver services and collaborate across organizational, social, and geographic boundaries (Government of Kenya, 2014). The result of this is the dissolution of network boundaries so that organizations allow their stakeholders access to their information and data in order to push collaboration and innovation. In so doing, organizations have become more exposed to the likelihood of their data and information getting misused or stolen. Cloud computing has put even more strain on what is left of enterprise network boundaries and also introduced new cyber risks and threats (Curry, 2013).

1.2 Cyber Threats

Cyber threats may be defined as those actors or adversaries exhibiting the strategic behaviour and capability to exploit cyberspace with an intention of harming life, information, operations, the environment and or property (Robinson et al, 2013). Cyber threats have a huge potential to cause serious harm because cyber applications permeate most places including governments, vital infrastructure, businesses and also private space. Cyber threats may be broadly categorized into two, cyber warfare and cyber crime. Cyber warfare is any malevolent activity which poses a threat to the security, defence mechanisms or vital installations of a state or a geographical region (Saulius, 2012). On the converse, cyber crime alludes to criminal activities done using ICT infrastructure (Jethwani & Surbhi, 2015).

1.3 Cyber Security

Cyber security may be defined as the defence of ICT infrastructure, data and information in cyberspace against threats such as cyber crime and cyber war. The required protection involves the implementation of one or a matrix of countermeasures to the cyber threats. A cyber threat countermeasure may be defined as a mechanism that completely eliminates cyber threat attack(s) or reduces the effects of a cyber attack (Carnagie Mellon University, 2016). Common cyber threat countermeasures include but not limited to training of employees on cyber security policy issues, access controls to ICT assets to counter insider and social media threats and patching software vulnerabilities to harden ICT Systems (Paula et al, 2014).

Other countermeasures include: use of virtual LAN to segregate voice and data traffic to counter VOIP PBX fraud (Wei, 2012), continuous monitoring of system capacity; traffic type of any critical infrastructure like firewalls and sand boxes, segmentation of internal and external networks to counter denial of Service (DOS) attack threat (European Broadcasting Union, 2015), cooperation with internet service providers to gain access and shutdown central components and remote cleaning up of infected machines in case of botnet attacks (Leder & Martini, 2009), two-factor authentication to counter online banking, mobile banking and mobile money fraud (Ferguson, 2015), legislation and diplomatic cooperation on the part of governments, and use of advanced threat analyzers by private organizations to counter cyber espionage (Threat Track Security, Inc, 2013).

The effectiveness of a cyber threat countermeasure is to deter cyber attackers by reducing an organization’s cyber attack surface. However, the efficacy of cyber threat countermeasures upon the deterrence of cyber attackers has not yet been examined critically. As a result organizations spend large sums of money upon countermeasures without knowledge of their effects upon the hackers who are behind the attacks.

Given the exponential growth of cyber threats and vulnerabilities, effective models are needed to aid in the implementation of the right security mechanisms so as to achieve the desired objectives of attack prevention, vulnerability reduction, and threat deterrence at a good return on investment for the organization (Gurvirender, 2012).

Establishing effective cyber threats countermeasures is not an easy exercise to do. Largely, this is due to the ever-evolving threat landscape and the fact that hackers can easily and almost effortlessly make their hacking tools more sophisticated. Unfortunately organizations cannot predict with precise accuracy what hackers' will do next. However, countermeasures that minimize an organization's exposure to cyber attacks either by removing vulnerabilities or blocking them are regarded as more effective compared to those that require interpretation or analysis to operate (Cyberedge Group, 2014).

A number of studies have been done in the area of cyber threats and countermeasures including: Rjaibi (2015) researched on monitoring the effectiveness of security countermeasures in a security risk management model. The objective of the study was to extent the value based cyber security metric namely the Mean Failure Cost (MFC) into information security management to aid in highlighting what constitutes security priorities for an organization. The extended model was also to assist in implementing cyber threat countermeasures and in the monitoring and evaluating how effective the implemented countermeasures are using return on investment (Rjaibi, 2015). Gurvirender (2012) did a research on investigating the effectiveness of information sstem security countermeasures towards cyber attacker deterrence whose aim was to develop a better model to aid organizations choose and implement cost effective cyber threat countermeasures (Gurvirender, 2012).

1.4 ISO Certified Organizations

The scope of this study is within ISO certified organizations. These are organizations that have implemented and are certified for ISO 9001 quality management system (QMS). An ISO 9001 quality management system is a systematic and process driven approach to managing an organization’s processes. Its main objective is to aid the organization in meeting the requirements of its stakeholders at a consistent quality and satisfaction level (ISO Quality Systems Limited, 2015). The quality management system gives the certified organization benefits such as providing efficient management processes, defining responsibility dockets in the organization, aiding in setting up the right communication strategy or strategies to staff and customers, helping in the identification and implementation of more efficient processes, highlighting gaps in business processes, reducing costs of doing business and providing continuous assessment and improvement of business systems and processes. Customers of the ISO certified organizations benefit from improved quality products and services, delivery on time of products and services, fewer returned products and less complaints. Independent audits of the ISO quality management system ensures commitment to quality of products and services (ACS Registrars, 2010). A complete list of the organizations that were sampled and studied is found in appendix 2 of this study.

To give their customers quality products and services, these ISO certified organizations rely heavily on the use of ICT systems which are networked and connected to the internet through the Kenya national fibre network. In so doing, these organizations have become more vulnerable to cyber attacks (Curry, 2013). This situation brings the need to put in place effective cyber threat countermeasures in order to comply with the stringent requirements they are expected to meet by virtue of being ISO certified. Hence the need for this study in the ISO certified organizations in Kenya.

1.5 Research Problem

Cyber security is critical to organizations because they need to secure their information systems and data in cyber space to ensure uninterrupted provision of quality products and services efficiently to their customers (Kumar, 2011). Increasingly organizations are more reliant on information stored in cyberspace for the efficient execution of their business transactions. Should confidentiality, integrity or availability, which attributes are critical to reliability of the information be breached, the aftermath could be seriously damaging to the organizations. The effects could include but not limited customer loss, dented organizational image and monetary losses. Robust cyber security is a necessity for reliable information needed for conducting business reliably (Zegers, 2006).

Numerous researches have been carried out globally on cyber security, cyber threats and cyber threats countermeasures. In United States, Vatis (2009) did a study on trends in cyber vulnerabilities, threats and countermeasures. He recommended for improvement in the detection, investigation and response to cyber security incidents and exploration for more effective ways to foster greater security of networks so that they are less vulnerable to cyber attacks. In Australia, Heidi (2009) carried out a research on countering social engineering through social media: an enterprise security perspective. The research found out that social engineering cannot be managed by traditional security measures due to its mode of attack which relies heavily on human error. In Germany, Leder (2009) did a study on proactive botnet countermeasures an offensive approach. The study recommended an approach that combines both defensive and offensive countermeasures in response to botnet attacks. He also recommended cooperation as an important aspect to successful and sustainable botnet mitigation.

These global studies have been done in the context of their different countries and also not in the context of ISO certified organizations in Kenya. Therefore they are not very relevant in the context of Kenya as a country and also the ISO certified organizations in Kenya. In Kenya ISO certified organizations are under a lot of pressure to meet the standards of quality of goods and services they provide to their customers and other stakeholders by virtue of being ISO certified.   To meet the stringent standards of giving quality products and services, the ISO certified in Kenya organizations rely heavily on the use of ICT systems which are networked and connected to the internet. In so doing, these organizations have become more vulnerable to cyber attacks. Hence the need for this study whose findings are expected to be more relevant in the context of Kenya as a country and Kenyan ISO certified organizations.

In Kenya, Njiiru (2013) did a study on a framework to guide information security initiatives for banking information systems in the Kenyan banking sector. The results of the study showed that human stakeholders were the biggest threat to information systems security (Njiru, 2013). Kitheka (2013) did a study on information security management systems in public universities in Kenya. The study showed that the information security controls in public universities were not strong enough to deal effectively with information security threats (Kitheka, 2013). Ngalyuka (2013) did a study on the relationship between ICT utilization and fraud losses in commercial banks in Kenya. The study found out that ICT utilization has exposed commercial banks in Kenya to more fraud (Ngalyuka, 2013).

Despite there being local studies conducted in the area of information systems security, they have not addressed the subject matter with a focus on cyber security in ISO certified organizations in Kenya. Therefore there exists a knowledge gap on how ISO certified organizations in Kenya are managing cyber security hence the need for this research to find answers to the questions: What cyber security threats are being faced by Kenyan ISO certified organizations? What cyber security countermeasures have been put in place by these ISO certified organizations in Kenya? What is the perceived effectiveness of the countermeasures these organizations have put in place in countering cyber security threats?

1.6 Research Objectives

The objectives of this research project are to:

1. Establish the cyber security threats faced by ISO certified organizations in Kenya.
2. Establish the cyber threat countermeasures that ISO certified organizations in Kenya have put in place.
3. Determine the effectiveness of the cyber threat countermeasures used by ISO certified organizations in Kenya in countering cyber security threats.

1.7 Value of the Study

The findings of this research are expected to be of great value to Kenyan organizations both ISO certified and not yet certified ones. It will give practical insights in cyber threats and cyber security management, especially the need to implement more effective cyber threat countermeasures. It will give cyber security chiefs, security supervisors and different ICT partners with a superior comprehension of how their recognitions, concerns, needs and in particular how their current guarded stances stack up against those of other cyber security experts and associations. It will lead to Kenyan organizations getting better returns on investment in their cyber security investments and avoid losses that can result from cyber attack eventualities.

The study will also contribute to the body of knowledge on cyber security threats; cyber threats countermeasures and cyber security. It will avail to academicians, scholars and researchers with additional written material on the concepts of cyber security threats, cyber threats countermeasures and cyber security. The study is also expected to give cyber security development engineers with better answers to take care of the worries and necessities of their clients.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter explores related researches conducted on cyber threats and cyber security in ISO certified organizations. The review aims at bringing out good insights into the concepts of cyber threats, countermeasures to cyber security threats, and effectiveness of countermeasures to cyber threats. The chapter also discusses theories of managing cyber security.

2.2 Theoretical Review

Cyber security may be defined as the protection of systems, networks and data in cyber space against threats such as cyber crime and cyber war. Cyber crime is generally defined as any illegal behaviour directed electronically at the security of ICT systems and data these systems process. Cyber warfare includes the activities by a state or worldwide organization to attack and endeavour to harm another state's or organization's computers or data and information stored in their computers and ICT network through, for instance, computer malware infections (IT Governance Ltd, 2015). Theoretically numerous models to the management of cyber security have been advanced. This study will use the Chain-of-Events Model, the Business Model for Information Security by ISACA, the ISO/IEC 17799 Information Security Management and the EMC Corporation's Intelligence Driven Information Security Model to get more insights into the theory of cyber security management.

2.2.1 The Chain of Events Model

Chain of Events Model sequentially organizes causal components shaping an occasion chain, where different occasions are incorporated to comprehend causal variables behind a loss. The objective of Chain of Events Model is to manage the danger of a future cyber attack by executing countermeasures, for removing an event(s) or potentially mediating between occasions in a chain, so that the chain is broken. In this model, a few occasions or environmental aspects are assigned as proximate, root, or contributory. Unsafe practices and conditions prompting to such practices are utilized to comprehend basic causal components, which resulted in a loss (Salim, 2014).

2.2.2 The Business Model for Information Security

Conceptually the Business Model for Information Security is best depicted as an adaptable, three dimensional, pyramid formed structure made up of four components connected up by six element interconnections. The dynamic interconnections go about as strains, applying a push and draw constraints in response to changes in the venture, permitting the model to adjust as required. The four components of the model are: organizational strategy and design, processes, people and technology. The interconnections are governance, culture, enabling and support, emergence, human factors and architecture (ISACA, 2009).

2.2.3 ISO/IEC 17799 Information Security Management

ISO 17799 is an exhaustive information systems security management model that avails to organizations the benefits of an internationally accepted and tested methodology that defines a clear process for evaluating, implementing, maintaining, and managing information systems security. It also defines a set of targeted policies, procedures and guidelines and standards for information systems security management. ISO certification allows organizations to evaluate their own information security standing and also that of their business partners. The model consists of ten ICT security tenets, which are used as a baseline reference for security risk assessment in organizations. The ICT security tenets are: the overall security policy, organizational security, asset classification and control, human resources security, physical and environmental security, communications and operations management, access control, systems development and maintenance, business continuity management and compliance (Tom, 2001).

2.2.4 Intelligence Driven Information Security Model

An industry initiative sponsored by RSA Security LLC, the security division of EMC Corporation under the umbrella of the Security for Business Innovation council of the United Kingdom formulated a six step road map to developing an intelligence driven information security (EMC Corporation, 2012). The six steps are: one, carry out an inventory of strategic or mission critical information assets that need protection and their locations. Two, present a value proposition to the appropriate stakeholders who could include the executive management, the board of directors and the various organizational departments. Three, putting in place a team of people with the right cyber intelligence skills. Four, build sources of cyber risk data. Five, develop a standard methodology that produces significant intelligence thus guaranteeing proper reaction to security breaches or incidents and six, implement automation that assists in making big data set easier to manage and access. Automation also makes it easier to identify relationships, connections and any patterns of activities forming among disparate data types (EMC Corporation, 2012).

2.3 Cyber Threats

The Kenya Cyber security report 2014 found the following cyber threats as topping the list of the cyber threats facing Kenyan organizations; insider threats, VOIP PBX Fraud, social media, denial of service (DoS), botnet attacks, online and mobile banking fraud, mobile money fraud and cyber espionage (Paula et al, 2014).

2.3.1 Insider Threats

This type of threats are characterised by employees deliberately attacking the organizational cyberspace assets. High level access users, for example system administrators look for system loop holes so as to gain unauthorized access, ride on other users' access privileges without their authority to attack the organizational systems for reasons ranging from but not limited to disgruntlement, revenge and blackmail (Paula et al, 2014). Insider threats can be categorized into three, malicious insiders who purposely take data or cause harm, insiders who are unwittingly abused by external parties and insiders who are reckless and so commit unintended errors (Zegers, 2006). Insider threats may likewise originate from privileged systems users or regular system users with authorized access to sensitive data. System administrators in most cases possess full access to conduct basically any operation on many vital organizational systems. Also employees of all cadres more often accumulate access levels than they need for their job roles generating higher security risk levels that are preventable with proper access review systems (Miller et al, 2015).

2.3.2 VOIP / PBX Fraud

This type of fraud involves parties external to the organization making unauthorized calls through the organization's VOIP/PBX systems at the expense of the organization. The external parties hack into the organization's VOIP/PBX phone system and make money by using the phone system to make calls to premium rate numbers, and leave the owner organization to pay the bills of the hackers' calls (Paula et al, 2014).

2.3.3 Social Media

Social media cyber threats include online fake offers that are designed to trick users to give away their access credentials. Subtle online malware install buttons are availed to user with the ultimate aim of gaining access to the user's computer(s) or system(s). The hackers may provide fake plug-ins posing as legitimate internet extensions to trick users to download them and therefore infect their computer and steal information from it (George, 2015).

2.3.4 Denial of Service (DoS)

Many denial of service (DoS) attacks come from compromised ICT systems at hosting service providers sites especially the ones that are slow to respond to malware attack clean ups and also from installations that cannot be reached by international authorities. Denial of service attacks present themselves in various forms, some attack the ICT infrastructure at a site. Others take advantage of vulnerabilities in applications and network communication protocols in use at a site. The attacks are intended to make websites, servers and ICT infrastructures unavailable to their legitimate users (Blagov, 2015).

2.3.5 Botnet Attacks

These attacks emanate from compromised computers (referred to as botnets) in cyberspace. The rapidly expanding usage of high speed internet exposes more computers, routers and other ICT gadgets to the world-wide-web and in this manner expanding the quantity of computers, routers and other ICT gadgets that can be compromised by cyber crooks especially if these gadgets are not properly secured. The compromised gadgets can be utilized to spread viral infections, produce spam and carry out different sorts of online crime and fraud. The assailants then use this very distributed system to launch attacks on targets such as, monetary establishments and government institutions with the aim to defraud, cripple or steal information (Leder, 2009).

2.3.6 Online and Mobile Banking Fraud

Kenyans who have subscribed to mobile banking services run the risk of exposing their money to fraudsters (Mukinda, 2014). The growing implementation and use of online and mobile banking services has brought to the fore a new frontier of cyber threats to financial institutions and their customers. This is due to the fact that most of these financial institutions are implementing already vulnerable web and mobile applications. In a Kenyan study of online banking applications, it was revealed that out of the thirty three online banking applications sampled, only two online banking sites had adequate online security deployed on their web applications. Most of the online applications studied lacked strong encryption and are prone to phishing attacks (Paula et al, 2014).

2.3.7 Mobile Money Fraud

The sustained popularity of mobile money usage in Kenya and the East Africa region in general has attracted cyber criminals who have shifted their focus to this new money transfer service. In particular the year 2013 recorded an increase in mobile money fraud targeting individual users and organizations in Kenya. The criminals involved are getting sophisticated and are fast in finding exploitable vulnerabilities in new controls implemented by mobile money merchants, financial institutions and individual users (Paula et al, 2014).

2.3.8 Cyber Espionage

Cyber espionage may be defined as the theft of secret or confidential information stored digitally on computers and ICT networks. Cyber criminals financed by states or organizations deploy high level and carefully crafted techniques to access networks and steal information in a stealthy manner. Cyber espionage is being advanced by the ongoing political and economic changes in most countries in the world. Also, competing organizations are using cyber espionage attacks to obtain strategic information from their competitors (Lotrionte, 2015).

2.4 Cyber Threat Countermeasures

A cyber threat countermeasure can be viewed as an action, process, technology, device or system that serves to prevent or mitigate the effects of a cyber attack against a computer, server, and network or associated device (Carnagie Mellon University, 2016).

2.4.1 Countermeasures to Insider Threats

Measures to counter insider threats include awareness training for employees to be able to identify phishing and other social media threat techniques (US Government, 2014). Give training to employees regularly to maintain high levels of knowledge skills and abilities to prevent or mitigate insider threats and to improve risk perception. Constant and targeted training will also improve usability of available security tools to minimize the incidents of system induced human errors. The training will also raise the level of employee knowledge on how they can guard themselves against becoming unintentional threats. The organization should implement adequate security practices such as two-factor authentications for system logon and inculcate employee culture that highly resonates with organizational information security mission (US Government, 2014).

2.4.2 Countermeasures to VOIP /PBX Fraud

As a countermeasure to VOIP/PBX fraud an organization needs to use virtual LAN (IEEE 802.1Q) to segregate voice and data traffic (Wei, 2012). Also implement quality of service (802.1p) to give priority to voice traffic over data traffic. This design prevents internal hackers from sniffing voice traffic. The network administrator could also monitor traffic on individual voice ports on the Ethernet switch. If a voice port has unusual traffic spike, it would trigger a security alert for further investigation. Other countermeasures include disabling non-service related ports as a way of hardening the PABX/Server, restricting international calls to designated phone numbers and constantly monitor call detail records (CDRs) to identify unusual usage patterns (Yu, 2015).

2.4.3 Countermeasures to Social Media Threat

Countermeasures to social media cyber security threat can be implemented from two fronts, the people front and the policy front. People front constitutes awareness training for employees on how to handle the various social media cyber threat vectors when online. A general consensus by the public and private sectors is that strong cooperation between governments and businesses is needed to maximize cyber security effectiveness (Wilcox, 2015). From the policy perspective, countermeasures involve including measures in the organizational security policy on how to handle social media threats such as phishing and social engineering while online (Wilcox, 2015).

2.4.4 Countermeasures to Denial of Service

A denial of service (DoS) attack is a network based attempt to make a website, a service or a complete infrastructure unavailable to users in most cases by simultaneously attacking a victim from several compromised systems. To counter

DoS attack, detective security in the form of continuous monitoring of system capacity and traffic type of critical infrastructure, and services like firewalls with a view to improving detection capabilities of cyber attack is needed. Strengthen the detective security measures with preventive security measures such as segmentation of internal to external networks, segmentation of any network containing critical broadcast systems, automation of the scanning and patching of potential DoS vulnerabilities in internet facing services and load balancing and defining a DoS protection agreement with the internet service provider (ISP) (European Broadcasting Union, 2015).

In the event of an attack use corrective security measures such as DoS protection services that allow traffic cleaning. These services can be implemented internally or outsourced from external ISP or a different third party. Security gateways should include DoS detection and protection capabilities. Additional network based countermeasures may also be considered, for example black holing., blocking attackers IP addresses, stopping IP announcing, domain name service (DNS) reconfiguration and isolation (disconnect from internet access) (European Broadcasting Union, 2015).

2.4.5 Countermeasures to Botnet attacks

Countermeasures to botnet attacks can be classified into two, classical and offensive countermeasures. Classical countermeasures entails identifying a central weak point in the botnet infrastructure which is then manipulated, disrupted or blocked to incapacitate the botnet. Mostly cooperation with an ISP is required so as to access and shut down the central component of the botnet, which then leads to the owner losing control of the botnet (Leder & Martini, 2009).

Offensive countermeasures can be categorized into three: mitigation, manipulation and exploitation. Mitigation entails technical methods that slow botnets down by restricting the bandwidth available to it. Manipulation strategies make use of the command interface to issue commands that will cripple or disrupt the botnet. The likely solution here is to remove the DoS commands as well as the download and execute programs commands so as to allow the cleaning of infected computers. Exploitation involves finding vulnerabilities or bugs in the botnet then use them to cripple or shutdown the botnet (Leder & Martini, 2009).

2.4.6 Countermeasures to Online Banking and Mobile Money Fraud

A common countermeasure to online and mobile banking fraud is two-factor authentication. Two-factor authentication entails an identification name and a password consisting of a known and fixed part and an additional piece of information that is dynamically generated and used once with each session. The dynamically generated part can be a session code or a set of single use identifiers sent at regular intervals to each customer or automatically generated at the time of logon into a session. Some financial institutions use session codes sent to user mobile phone while others issue hardware tokens that generate random codes which customers then use in their logon sessions. Still others provide bank card reading devices which first require users to use a personal identification number (PIN) to generate confirmation codes. In most cases the codes are needed when making money transactions (Ferguson, 2015).

Mobile money fraud countermeasures would involve training staff so that they could identify customers who are at higher risk and provide adequate advise on risk mitigation for example Personal Identification Number (PIN) generator versus static passwords, transaction limits, SMS alerts and such (Omuga, 2014), raising awareness through sustained communication campaign warning customers about con schemes and other financial crime risks and sharing experiences and exchanging information about account moles within the industry and with other stakeholders for instance, law enforcement (Omuga, 2014).

2.4.7 Countermeasures to Cyber Espionage

At government levels cyber espionage is being countered using legislation and diplomatic cooperation. As for business organizations, they have to defend themselves against persistent threats to their private data and intellectual property. Advanced tools such as threat analyser provide enterprises with the protection they need to keep cyber threats at bay, protect their data and keep their reputations intact (Threat Track Security Inc, 2013).

2.5 Cyber Security Measurement

The effectiveness of cyber threats countermeasures implemented by an organization can measured by the perceived level of cyber Security. The perceived level of cyber security is a sentimental measure of cyber security risk to the private sector organizations and governmental information systems from known cyber security threats which is computed by aggregating the opinions and views of information security practitioners over a time period (Geer Dan, 2016). It is sentiment based in recognition of the rapid change in cyber security threats and postures, the state of cyber security metrics as a practical art, and also the degree of uncertainty in any risk centred field, like in this case, cyber security.

2.6 Empirical Review

The empirical review looks at the findings of studies addressing cyber threats and cyber security in organizations that have been done in Kenyan and other countries internationally.

2.6.1 International Review

Baino (2001) from Australia did a study on evaluation of security risks associated with networked information systems. The study results showed that a big portion of security lapses are as a result of system administrators not updating software patches and not keeping abreast with developments in their trade. He attributed this ineffectiveness of system administrators to culture and workload, stating that the systems administrators are in most cases responsible for taking care of numerous disparate systems. He also found out that the system administrators are also expected to be experts in increasingly complex systems comprising of various technologies, which are often beyond the comprehension of most of them.

Kreicberga (2010) in Sweden did a study on internal threat to information security countermeasures and human factor in small and medium enterprises (SMEs). The results for the research were that formal policies that lack proper maintenance and awareness do not impact employee behaviour, whereas informal norms within organization have the greatest influence on information security behaviour. Technological security countermeasures are more effective and undertaken seriously if their necessity is explained as a benefit to the end users.

Tarino et al (2006) in Sweden did a study on social – technical view of ICT security issues, trends and challenges towards a culture of ICT security – the case of Tanzania. The results of the study showed that, to cultivate a culture sensitive to ICT security is not an easy task and it is not an issue that can be addressed solely by organizations. There are factors external to the organizations that also need addressing when it comes to ICT security. For instance, when it comes to training and creating awareness for ICT security, aspects such as the overall education system of a country and its support structures need to be put into consideration.

2.6.2 Local Review

Makumbi et al (2012) carried out a research entitled an analysis of information technology (IT) security practices a case study of Kenyan small and medium enterprises (SMEs) in the financial Sector. The objectives of the research were to establish the level of reliance Kenyan SMEs are on ICT, establish the most prevalent security threats among Kenyan SMEs and to establish how Kenyan SMEs are protecting their computers, data, and networks from information security risks. The findings of the study were that there is awareness among the organizations investigated on the importance of information systems security and they have endeavoured to put security measures in place based on their reliance on IT systems (Makumbi, 2012). Because of the nature of these organizations, financial fraud seems to feature prominently among the incidents that are reported, loss of computer assets seemed to be a recurring problem and systems user threat was common among the organization studied. Firewalls are the common defence employed against hacking. The study recommendations were that, such organizations should put various measures in place including segregation of duties, physical security controls and inventories of IT assets. He also recommended awareness campaigns for users to sensitize them on ICT security (Makumbi, 2012).

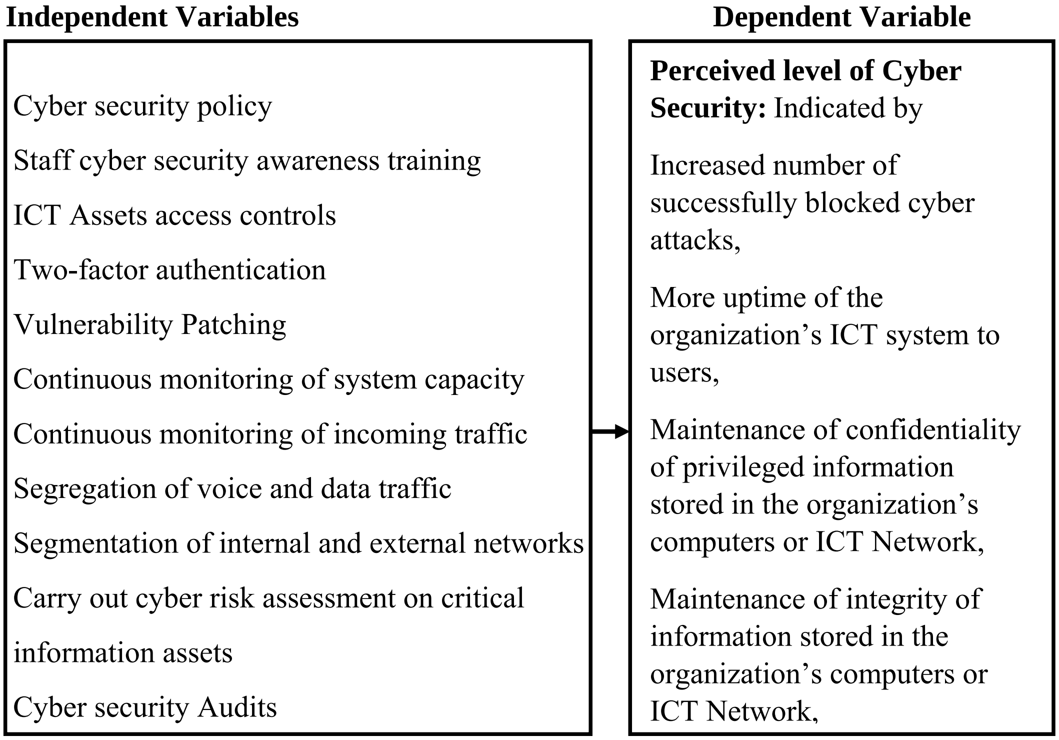
Nyamongo (2012) did a study on information systems security management, a case study of private chartered universities in Kenya. The findings of the research were that institutions of higher learning in Kenya are ready to adopt and improve on their information systems security management by regularly updating management on security updates. Staff training on information systems security management will go a long way in improving the university's information security system management (Nyamongo, 2012). The major challenges facing information security system management were viruses, user errors, theft of computers, system and software errors, the study concluded that institutions of higher learning should rethink their ways of handling security of their most valued assets. Therefore, there is need to adopt an effective strategy that will help institutions higher learning to achieve effective information security management (Nyamongo, 2012).

Njiru (2013) carried out a study on a framework to guide information security initiatives for banking information systems, Kenyan banking sector case study. The aims of the research were to identify common vulnerabilities affecting the banking information systems, to analyse existing frameworks used to evaluate security programs and initiatives of banking systems, to define the gaps in the existing security investment frameworks, to develop a framework that will be used for evaluating security programs for banking industry and to validate the security investment framework (Njiru, 2013). The findings of the study showed that people are the largest threat to information systems while lack of proper communication, lack of skilled labour and security awareness by customers were cited as major obstacles to security effectiveness. Fraud, careless or unaware employees and internal attacks were cited as the threats that have increased banks' risk exposure. The study concluded that leadership and the alignment of people, processes and technology is what is most important in the transformation of information security (Njiru, 2013).

2.7 Conceptual Framework

The conceptual framework for this research looks at the relationship(s) between the variables being researched on. The variables being studied can be classified into two; the independent variables and the dependent variable. The independent variables are cyber threats countermeasures that the Kenyan ISO certified organizations implemented. These include cyber security policy, staff cyber security awareness training, ICT assets access controls, two-factor authentication, vulnerability patching, continuous monitoring of system capacity, continuous monitoring of incoming traffic, segregation of voice and data traffic, segmentation of internal and external networks, carry out cyber risk assessment on critical information assets and security audits.

The dependent variable is perceived level of cyber security that is indicated by increased number of successfully blocked cyber attacks, more uptime of the organization’s ICT system to users, maintenance of confidentiality of privileged information saved in the organization’s computers or ICT network, maintenance of integrity of information saved in the organization’s computers or ICT network and maintenance of availability of information saved in the organization’s computers or ICT network as shown in Figure 2.7.



Independent Variables

Cyber security policy

Staff cyber security awareness training

ICT Assets access controls

Two-factor authentication

Vulnerability Patching

Continuous monitoring of system capacity

Continuous monitoring of incoming traffic

Segregation of voice and data traffic

Segmentation of internal and external networks

Carry out cyber risk assessment on critical information assets

Cyber security Audits

Dependent Variable

Perceived level of Cyber Security: Indicated by

Increased number of successfully blocked cyber attacks,

More uptime of the organization’s ICT system to users,

Maintenance of confidentiality of privileged information stored in the organization’s computers or ICT Network,

Maintenance of integrity of information stored in the organization’s computers or ICT Network,

Figure 2.7: Conceptual Framework

2.8 Literature Review Summary

This chapter has explored the available literature on cyber threats, cyber threat countermeasures and cyber security. It has explored theoretical models that are available for guiding implementation of effective cyber security. These models show that cyber security and information systems security in general is a must do for organizations so as to safeguard their cyber space and assets in it.

The chapter also explored relevant previously done studies on the topic which covered generally information systems or bits of the topic in different contexts to the one being studied. Literature on existing cyber threats facing organizations, the countermeasures in use by these organizations in Kenya and other parts of the world was explored. Also, literature on effectiveness of countermeasures was reviewed.

At the time of this study no known similar research has been done in the context of ISO certified organizations in Kenya.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter explains the methodology that was applied in conducting this study. It explains the research design employed, the population studied, the targeted population sampling technique used and the sample size that was drawn from the population. The chapter also explains the research instruments that were used in data collection and data analysis techniques used.

3.2 Research Design

This research is a descriptive study. A descriptive study is one in which information is collected without changing the environment to answer the question *what is?* The reason for the descriptive study design is because it involved the systematic empirical investigation of cyber threats that ISO certified Kenyan organizations are faced with, the countermeasures these organizations have implemented and establishing the level of perceived effectiveness these countermeasures are achieving.

3.3 Population

A population is a total collection of all the subjects that are studied and from which, if need be, a sample is e drawn. The study covered all the ISO certified organizations in Kenya that were certified by the Kenya Bureau of standards certification body. At the time of this research Kenya Bureau of standards certification body had certified 175 organizations per their website. A random sample of 45 ISO certified organizations was taken and studied. The source of the list of ISO certified organizations is Kenya Bureau of Standards certification body (KEBS, 2016). A complete list of the 175 organizations that comprised the population of this study is in appendix 2 of this report.

3.4 Sample Design

A simple random sample of 45 organizations was selected. The reason for choosing 45 organizations is to ensure a representative sample which is supposed to be equal to or greater than 30 organizations per statistical standards (N>=30) (Cooper, 2013). The 45 organizations were randomly picked from the sampling frame of 175 ISO certified organizations in Kenya per the Kenya Bureau of Standards certification body at the time of this research (KEBS, 2016).

3.5 Data Collection

Primary data was collected through a questionnaire sent to respondents in the chosen organizations. "Drop-and- pick-later" method was used in the administration of the questionnaire for the organizations geographically near the researcher and by email to those far away. The respondents of the questionnaire were ICT managers, IT managers, Chief Information Officers (CIOs), ICT Officers, Information Security Officers, Heads of ICT and ICT Directors depending on staff responsible in each chosen organization and the knowledge they have on cyber security.

The questionnaire consisted of four sections A, B, C and D. Section A collected demographic information on the individual respondents and also information on their organizations. Section B of the questionnaire contained list of cyber threats and respondents were o rate whether their organizations have faced the threats and extent to which they have faced such cyber threats. Section C had a list of cyber threat countermeasures that the respondent organizations are expected to have implanted. The respondents were required to indicate whether their organizations have implemented such cyber threat countermeasures and if implemented, to what extent they have implemented them. Section D had a list of cyber threat risk objectives that the cyber threat countermeasures are expected to achieve. The respondents were supposed to rate based on their opinion to what extent are the implemented cyber threat countermeasures effective in achieving the cyber threat risk objectives listed.

3.7 Data Analysis

The completed copies of the questionnaire generated both quantitative and qualitative data. The returned copies of questionnaire were checked for completeness coded and summarized. The summarized data was then used to generate frequencies, percentages, weighted averages and cumulative percentages which were thereafter tabulated. Demographic data was analyzed using frequencies and percentages. Organizational data was also analyzed using frequencies and percentages. Data on cyber threats facing ISO certified organizations in Kenya was analyzed using means and standard deviations. The data on cyber threat countermeasures was analyzed using means and standard deviations. The data on effectiveness of cyber threat countermeasures implemented was analyzed using multiple regression analysis. The model used for regression analysis is as follows:

3.7.1 Analytical Regression Model

$$Y_1 = a+\beta_{1X1} + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_{4+} \beta_5 x_{5+} \beta_6 x_{6+e}$$

Where Y_1 represents perceived cyber security level

a - represents constant or intercept

x1 - Increased number of successfully blocked cyber attacks

x2 - More uptime of the organization’s ICT system to users

x3 - Maintenance of confidentiality of privileged information stored in the organization’s computers or ICT network

x4 - Maintenance of integrity of information stored in the organization’s computers or ICT network

x5 - Maintenance of availability of information stored in the organization’s computers or ICT network

e – Error

The β coefficient represents the strength and direction of the relationship between the variables assuming the error e will be independent of x and is normally distributed with zero mean and constant variance.

3.7.2 Test of significance

It is expected that significant relationship between x and Y will be at 0.05 significance level by testing the null hypothesis β =0. If p-value is much less that 0.05, the null hypothesis will be rejected and therefore there will be no relationship between the variables.

CHAPTER FOUR

DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

This chapter contains the analysis of the data that was collected from the respondent organizations. The questionnaire administered was mainly completed by ICT security officers, chief information officers, ICT managers, IT Managers, ICT officers, ICT directors who are basically the staff charged with cyber security issues in the organizations studied (see table 2). Copies of the questionnaires were administered personally by the researcher to respondents geographically near the researcher and by email to those far away. The overall response rate was 77.8% (see table 1). Analysis was done on individual respondent demographic data, respondent organizational data, cyber threats facing ISO certified organizations in Kenya data, cyber threats countermeasures implemented by Kenyan ISO certified organizations and the effectiveness of cyber countermeasures implemented by ISO certified organizations data.

Table 1: Questionnaire Response Rate

	Response Percent	**Response Count**
Number of copies completed and returned	77.8%	35
Number of copies not returned	22.2%	10
Total Copies Sent to Respondents		**45**

4.2 Demographic Information

From the respondent data summary it can be seen that the sample population had the following characteristics. The minimum work experience of the respondents was six years (see table 6). The respondents were ICT officers, ICT Managers, IT Managers, ICT officers, Information security officers, chief information officers, and heads of ICT as well as ICT directors (see Table 2).

Table 2: Job Title of Respondents

Job Title	Number of Respondents	Percentage
Chief Information Officer (CIO)	3	9%
IT Manager	5	14%
ICT Manager	10	29%
ICT Officer	6	17%
Information Security Officer	4	11%
Head of ICT	5	14%
ICT Director	2	6%
Total	**35**	**100%**

4.2.1 Gender of Respondents

83% of the respondents surveyed were male while 17% were female (see Table 3).

Table 3: Gender of Respondents

Gender	Response Percent	Response Count
Female	17.1%	6
Male	82.9%	29

4.2.2 Age of Respondents

The ages of the respondents were between 31 years and 50 years (see Table 4).

Table 4: Respondents Age

Answer Options	Response Percent	Response Count
25 years or less	0.0%	0
26– 30 years	0.0%	0
31 - 35 years	57.1%	20
36 - 40 years	28.6%	10
41 - 45 years	8.6%	3
46 - 50 years	5.7%	2
Over 50 years	0.0%	0

4.2.3 Respondents Education Levels

The respondents surveyed either had graduate degrees or postgraduate degrees (See table 5).

Table 5: Respondent Education Level

Educational Level	Response Percent	Response Count
Postgraduate	57.1%	20
Graduate	42.9%	15
Diploma	0.0%	0
Other (please specify)		0

4.2.4 Respondent Work Experience

The minimum work experience of the individual respondents was 6 years (See table 6).

Table 6: Respondent Work Experience

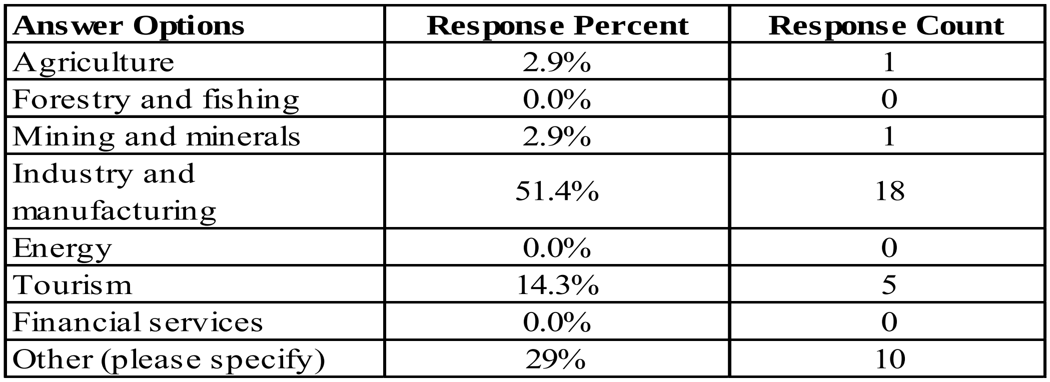
Answer Options	Response Percent	Response Count
5 years or less	0.0%	0
6 -10 years	57.1%	20
Above 10 years	42.9%	15

The demographic information shows that the respondents surveyed had the right knowledge, work experience, education levels and were of the right seniority in the organization to handle cyber security matters.

4.3 Organizations Surveyed Information

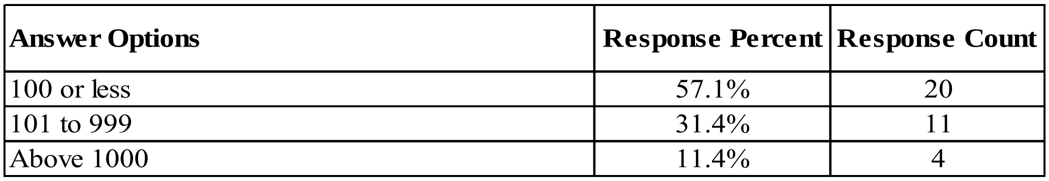
The majority of the organizations surveyed were from the industry and manufacturing sector of the Kenyan economy, 51%, (see table 7). The number of employees in these organizations is between 100 and 999 (see table 8). The asset base of the organizations surveyed is between less that 5 billion to above 10 billion (see table 9). This means that the sizes of the organization ranged from small to large organizations. The majority of the organizations surveyed were locally owned at 85.7% (see table 11) and have operated in Kenya for more than 10 years (see table 10).

Table 7: Organization Industry of Operation



Answer Options	Response Percent	Response Count
Agriculture	2.9%	1
Forestry and fishing	0.0%	0
Mining and minerals	2.9%	1
Industry and manufacturing	51.4%	18
Energy	0.0%	0
Tourism	14.3%	5
Financial services	0.0%	0
Other (please specify)	29%	10

Table 8: Number of Employees in Organization



Answer Options	Response Percent	Response Count
100 or less	57.1%	20
101 to 999	31.4%	11
Above 1000	11.4%	4

Table 9: Organization Asset Base

Asset Base	Response Percent	Response Count
Less than KES 5 billion	48.6%	17
Above KES 5 billion but less than KES 10 billion	37.1%	13
Above KES 10 billion	14.3%	5

Table 10: Years of Operation in Kenya

Answer Options	Response Count
5 years or less	0
6 -10 years	5
Above 10 years	30

Table 11: Organization Ownership

Answer Options	Response Percent	Response Count
Locally owned	85.7%	30
Foreign	14.3%	5
Both	0.0%	0

4.4 Cyber Threat s that are Faced by ISO Certified Organizations in Kenya

The Likert scale used here should be interpreted as follows: 1 no extent, 2 little extent, 3 Moderate extent, 4 large extent, 5 very large extent. The means and standard deviations should be interpreted per this scale. From the respondent data in Table 12 it can be deduced that the following cyber threats are being faced by the organizations surveyed from a moderate to a large extent.

4.4.1 Insider Threats

Insider cyber threats have been confirmed by the following situations being experienced by the organization from moderate to very large extent with corresponding ratings: Employees unintentionally or carelessly making mistakes that compromise cyber security (mean of 2.71 standard deviation of 0.69, employees being tricked by parties external to the organization to give out their security information for example passwords (mean of 2.14 standard deviation of 0.98, and privileged users for example, IT administrators, attacking the organization's information system for any reason, mean of 1.57 and standard deviation of 0.72 (see table 12).

4.4.2 Social Media Threats

Social media cyber threats have been confirmed by the following situations being experienced by the organization from moderate to very large extent with corresponding ratings: fake offers on the internet to share user security credentials (mean 3.28 standard deviation 1.03) and fake plug-ins posing as legitimate extensions that trick users to download and install them leading to infection and stealing of information from the infected computers, mean 3.00, standard deviation 1.19, and fake applications, that appear to be integrated for use with a social network tricking users to install them resulting in the stealing of user access credentials, mean 2.71 and standard deviation 1.27 (see Table 12).

4.4.3 VOIP/PBX Fraud Threats

These cyber threats have been confirmed the findings that external parties hacking into the organizations' PBX and making calls through it. This cyber threat is not common place as respondents indicated they have not experienced it mean of 1.28 and standard deviation of 0.69 (see table 12).

4.4.4 Denial of Service (DoS) Threat

This is a common place cyber threat experienced by most organizations that were surveyed. This can deduced from the finding that they have experienced attacks that resulted in websites and servers being unavailable to legitimate users with a rating mean of 2.00 and a standard deviation of 0.53 (see Table 12)

4.4.5 Botnet Attacks

This cyber threat is being experienced by the respondent organizations by the findings that computers in the organizations were spamming and or spreading viruses, mean 2.14 and standard deviation 0.83, and computers in the organization being used by third parties to conduct online fraud activities, mean 1.28 and standard deviation 0.45. (see table 12)

4.4.6 Online and Mobile Banking Fraud

This cyber threat is being faced by the ISO certified organization in Kenya. This is confirmed by the findings that attempts to access online or mobile banking platform by non authorized users have been made, mean 1.42 standard deviation 0.49, and money has been lost fraudulently through mobile money service, mean1.42 standard deviation 0.72. (see table 12)

4.4.7 Cyber Espionage

The cyber espionage report is confirmed by the findings that attempts to access secret or confidential information stored in the organization's computers or ICT network by unauthorized users have been experienced by the respondent organizations, mean 1.85 and standard deviation 0.63, breach of access to secret or confidential information stored either in the organizations' computers or ICT network has happened, mean 1.71 and standard deviation 1.03 and confidential information stored in the organization's computers or ICT network been stolen at any one time mean 1.28 and standard deviation 0.45.

Table 12: Cyber Threats Facing Respondent Organizations

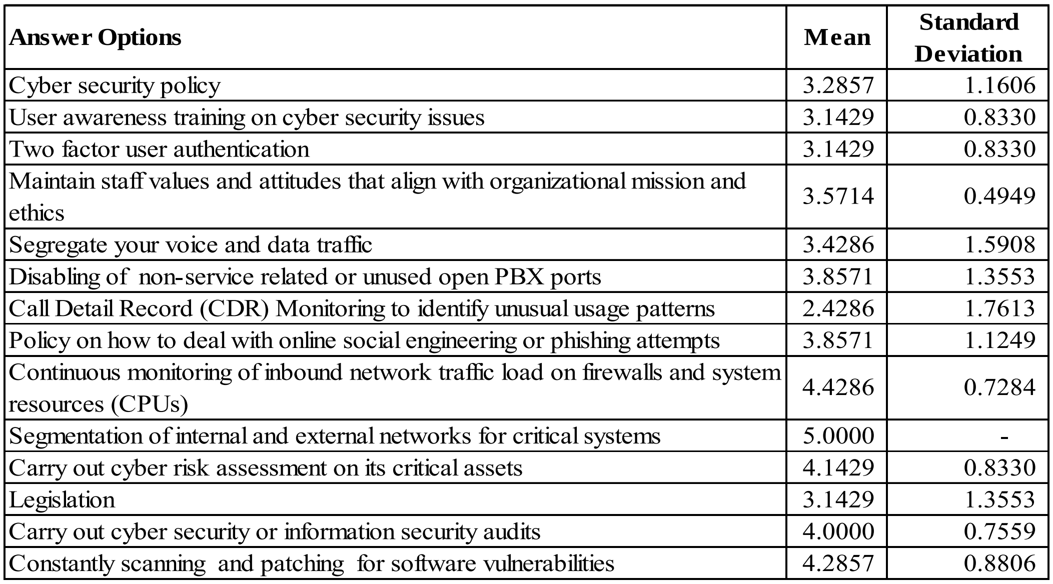
The Likert scale used should be interpreted as follows: 1 no extent, 2 little extent, 3 Moderate extent, 4 large extent, 5 very large extent. The means and standard deviations should be interpreted per this scale

Answer Options	Mean	Standarad Deviation
Employees unintentionally or carelessly making mistakes that compromise cyber security	2.714	0.6999
Employees being tricked by parties external to the organization to give out their security information for example passwords	2.143	0.9897
Privileged users for example, IT administrators, attacking the organization's information system for any reason	1.571	0.7284
Fake offers on the internet to share user security credentials	3.286	1.0302
Fake plug-ins posing as legitimate extensions that trick users to download and install them leading to infection and stealing of information from the infected machine(s)	3.000	1.1952
Fake applications, that appear to be integrated for use with a social network tricking users to install them resulting in the stealing of user access credentials	2.714	1.2778
External parties hacking into your PBX and making calls through it	1.286	0.6999
An attack that resulted in websites and servers unavailable to legitimate users	2.000	0.5345
Computers in your organization spamming and or spreading viruses	2.143	0.8330
Computers in the organization used by third parties to conduct online fraud activities	1.286	0.4518
Attempts to access your online or mobile banking platform by non authorized users	1.429	0.4949
Lost money fraudulently through mobile money service	1.429	0.7284
Attempts to access secret or confidential information stored in the organization's computers or ICT network by unauthorized users	1.857	0.6389
Breach of access to secret or confidential information stored either in the organization's computers or ICT network	1.714	1.0302
Confidential information stored in the organization's computers or ICT network been stolen at any one time	1.286	0.4518

4.5 Cyber Threat Countermeasures Implemented by ISO Certified Organizations in Kenya

From the respondents data in table 13 it can be deduced that the organizations that were surveyed have implemented the following cyber threat countermeasures: based on the percentage that rated "little extent" to "very large extent" for the countermeasure implementation as follows: cyber security policy, user awareness training on cyber security issues, two-factor user credentials (authentication), maintain employee values and attitudes that align with organizational mission and ethics , segregation of voice and data traffic , disabling of non-service related or unused open PBX ports, Call Detail Record (CDR) Monitoring to identify unusual usage patterns, policy on how to deal with online social engineering or phishing attempts, continuous monitoring of inbound network traffic load on firewalls and system resources (CPUs) , segmentation of internal and external networks for critical systems , carrying out cyber risk assessment on critical assets, Legislation, carrying out cyber security or information security audits and constantly scanning and patching for software vulnerabilities All responses had a mean of more than 3.0 and standard deviation of more than 0.4.

Table 13: Cyber Threat Countermeasures Implemented by Respondent Organizations



Answer Options	Mean	Standard Deviation
Cyber security policy	3.2857	1.1606
User awareness training on cyber security issues	3.1429	0.8330
Two factor user authentication	3.1429	0.8330
Maintain staff values and attitudes that align with organizational mission and ethics	3.5714	0.4949
Segregate your voice and data traffic	3.4286	1.5908
Disabling of non-service related or unused open PBX ports	3.8571	1.3553
Call Detail Record (CDR) Monitoring to identify unusual usage patterns	2.4286	1.7613
Policy on how to deal with online social engineering or phishing attempts	3.8571	1.1249
Continuous monitoring of inbound network traffic load on firewalls and system resources (CPUs)	4.4286	0.7284
Segmentation of internal and external networks for critical systems	5.0000	-
Carry out cyber risk assessment on its critical assets	4.1429	0.8330
Legislation	3.1429	1.3553
Carry out cyber security or information security audits	4.0000	0.7559
Constantly scanning and patching for software vulnerabilities	4.2857	0.8806

4.6 Effectiveness of Cyber Threat Countermeasures

From the multiple regression results in table 14 it can be deuced that the variable x4 which represents the objective maintenance of integrity of information stored in the organization’s computers or ICT Network and variable x5 representing maintenance of availability of information stored in the organization’s computers or ICT Network are distorting the results of the model when included in the regression model because of similar data and therefore they need to excluded in the analysis resulting in regression analysis results in table 15.

4.6.1 Analysis of Variance

From the adjusted multiple regression results in table 15, it can be deduced that 97.55 % of variation in effectiveness of cyber threat countermeasures can be accounted for by the model with adjusted R^2 of 0.8 (80%) of the terms falling into the regression line. The P=Values of all the variables are greater than 0.05 meaning that we reject the null hypothesis $\beta = 0$ and conclude that $\beta > 0$ meaning it has effect on the model. The t statistics are great than the corresponding coefficients meaning that the coefficient are great than 0 and therefore we again reject the null hypothesis that $\beta = 0$ and conclude the independent variables have effect on the dependent variable. This leads to the conclusion that the cyber threat countermeasures implemented by the ISO certified organizations in Kenya have effect on the perceived cyber security level.

4.6.2 Regression Coefficients and Regression Model

From the regression analysis results (Table 15) the cyber security level can be predicted as follows:-

$$Y_1= 1.5+0.15_{X1} -0.071x_2 + 0.135\ x_3$$

Where Y_1 represents perceived cyber security level

a - represents constant or intercept

x1 - Increased number of successfully blocked cyber attacks

x2 - More uptime of the organization’s ICT system to users

x3 - Maintenance of confidentiality of privileged information stored in the organization’s computers or ICT network

Table 14: Regression Analysis for Effectiveness of Cyber Threat Countermeasures with all Objectives

Regression Statistics	
Multiple R	0.9747
R Square	0.9500
Adjusted R Square	-2.2000
Standard Error	0.7071
Observations	5.0000

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	6.0000	9.5000	1.5833	6.3333	#NUM!
Residual	1.0000	0.5000	0.5000		
Total	7.0000	10.0000			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	1.5000	0.5000	3.0000	0.2048	-4.8531	7.8531	-4.8531	7.8531
X Variable 1	0.0821	0.0971	0.8461	0.5530	-1.1515	1.3158	-1.1515	1.3158
X Variable 2	-0.0036	0.0519	-0.0688	0.9562	-0.6627	0.6556	-0.6627	0.6556
X Variable 3	0.1357	0.0585	2.3212	0.2590	-0.6072	0.8786	-0.6072	0.8786
X Variable 4	0.0000	0.0000	65535.0000	#NUM!	0.0000	0.0000	0.0000	0.0000
X Variable 5	0.0000	0.0000	65535.0000	#NUM!	0.0000	0.0000	0.0000	0.0000

Table 15: Adjusted Regression Analysis for Effectiveness of the Cyber Threat Countermeasures:

Regression Statistics	
Multiple R	0.9747
R Square	0.9500
Adjusted R Square	0.8000
Standard Error	0.7071
Observations	5.0000

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	3.0000	9.5000	3.1667	6.3333	0.2823
Residual	1.0000	0.5000	0.5000		
Total	4.0000	10.0000			

	Coefficient	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	1.5000	0.5000	3.0000	0.2048	-4.8531	7.8531	-4.8531	7.8531
X Variable 1	0.1500	0.0866	1.7321	0.3333	-0.9504	1.2504	-0.9504	1.2504
X Variable 2	-0.0714	0.0606	-1.1785	0.4480	-0.8415	0.6987	-0.8415	0.6987
X Variable 3	0.1357	0.0585	2.3212	0.2590	-0.6072	0.8786	-0.6072	0.8786

4.7 Discussion

It is of utmost importance that Kenyan ISO certified organizations implement robust cyber security systems as they rely heavily on the use of ICT systems to serve their customers efficiently per the stringent requirements of ISO certification. The ICT systems they use are networked and connected to the internet through the high speed national and ultimately international fibre optic network exposing them to cyber attacks. The first objective of this study was to establish the cyber security threats faced by ISO certified organizations in Kenya. Based on the findings of this study, Kenyan ISO certified organizations are faced by insider cyber threats, social media cyber threats, VOIP/PBX fraud, denial of service (DoS), botnet attacks, online and mobile banking fraud, mobile money fraud and cyber espionage.

Faced by the cyber threats established in this study, the Kenyan ISO certified organizations have to implement and maintain effective cyber threat countermeasures as advocated for by available cyber security literature and theory. The results of this study show that most ISO certified organizations have implemented from “little extent” to “very large extent” cyber threat countermeasures for the cyber threats identified by this research. The findings to support this are summarized in table 13. However, there are some organizations that do not have a cyber security policy, have not segregated their voice and data traffic in their networks, have not disabled non-service related or unused open PBX ports do not carry out call detail record (CDR) monitoring to identify unusual usage patterns and do not use legislation as a cyber threat countermeasure.

The study results also show that the cyber threat countermeasures that the organizations have implemented are effective in increasing the number of successfully blocked cyber attacks, reduction in number of successful cyber attack incidences, ensuring more uptime of the organization’s ICT system to users, maintenance of confidentiality of privileged information saved in the organization’s computers or ICT Network, maintenance of integrity of information saved in the organization’s computers or ICT Network and maintenance of availability of information saved in the organization’s computers or ICT Network. This is based on the fact that the respondents rated that the cyber threat countermeasures implemented in their organizations were able to achieve the listed risk mitigation objectives.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter contains a summary of the conclusions drawn from the data analysis, contributions the study has made to theory and practice, recommendations for further research and limitations of the study.

5.2 Contributions

This research work has immensely contributed to achieving the objectives it was designed for. The study is of importance to ISO certified and even the non ISO certified organizations in Kenya as it gives these organizations practical insights into cyber threats and cyber security management, especially in the area of implementing more effective cyber threat countermeasures. The insights, if adopted, will give the organizations better returns on investment in their cyber security investments and also avoid losses that can result from a cyber attack eventuality.

The study provides cyber security decision makers, cyber security managers and other cyber security stakeholders with a better insight of how their perceptions, concerns, priorities and most importantly how their current defensive postures stack up against those of other security professionals in the industry.

The study contributes to the body of knowledge on cyber threats and cyber security. It avails to academicians, scholars and researchers additional written material on the concepts of cyber threats, cyber threat countermeasures, cyber security and effectiveness of cyber threat countermeasures that organizations implement or plan to implement.

The study also provides developers of cyber security technologies and products with some of the answers they need to better align their solutions with the concerns and requirements of their potential customers.

5.3 Conclusions

The main objective of this study was to establish the cyber threats that Kenyan ISO certified organizations face. The study has brought to the fore the cyber threats that ISO certified organizations are facing. This information is useful to both ISO certified and non certified organizations in knowing the threats they are up against.

Another objective of the study was to establish the cyber threat countermeasures that the Kenyan ISO certified organizations have implemented. The study has clearly identified the cyber threat countermeasures that these organizations have implemented. This information is useful to both ISO certified and non ISO certified organizations when it comes to implementing cyber threat countermeasures for effective cyber security levels.

The last but certainly not the list objective was to establish how effective the countermeasures implemented by ISO certified organizations in Kenya. The study has brought out the information on the effectiveness of the cyber threat countermeasures implemented by these organizations. This information is important to the ISO certified and non ISO certified organizations in Kenya when it comes to making decisions on what countermeasures to implement to get a good return on investment in their cyber security investments.

The study findings indicate that although the ISO certified organizations in Kenya are faced by the identified cyber threats, some of them have not implemented adequate cyber threats countermeasures. Some of the ISO certified organizations in Kenya do not have in place a cyber security policy which is a critical and must have guideline and source of reference point for implementing and maintaining a robust cyber security system.

5.4 Limitations of the Study

This research was conducted on a sample of the ISO certified organizations in Kenya and not in all ISO certified organizations due to budget and time constraints. Another constrain to this research is that it focused mainly on key cyber threats in ISO certified organizations in Kenya. The research did not look at cyber threats associated with the acquiring of ICT systems and applications development which are also critical for effective cyber security management.

5.5 Recommendations

Although most of the Kenyan ISO certified organizations have implemented cyber threat countermeasures to moderate, large and very large extent, there are still a number that have not adequately implemented the countermeasures. This study research has established that there are weaknesses and or omissions in the implementation of cyber threat cyber countermeasures and therefore the study recommends the following:

Cyber security policy is the blue print which gives guidelines and acts as reference for strong cyber security system. Therefore all the ISO certified organization s in Kenya should have a comprehensive and current cyber security policy which also has a section or chapter on how to deal with online social engineering and phishing.

ISO certified organizations in Kenya should have a comprehensive, active, current and continuous user training awareness on cyber security issues program. The program is a very strong and vital countermeasure against insider threats.

The fact that a significant number of ISO certified organizations in Kenya have implemented the two factor authentication cyber security measure to a little extent is a demonstration of weak access controls to their ICT assets. These organizations should implement this countermeasure to a large or very large extent so as to harden the access to their ICT assets in cyber space.

The ISO certified organizations should separate their voice and data traffic in and out of their cyber space so as to have better monitoring of the two to identify unusual patterns that could indicate cyber attacks and therefore be able to take remedial measures in time.

Call Detail Record (CDR) monitoring is a crucial safeguard against VOIP and PBX fraud. The research recommends that all the ISO certified organizations in Kenya implement this cyber threat countermeasure to curb the VOIP/PBX fraud threat and also to avoid losses that can be caused by such an eventuality.

A number of the ISO certified organizations surveyed have not included legislation as a cyber threat countermeasure. Legislation is a critical safeguard especially against cyber espionage. Therefore there is need for the ISO certified organizations in Kenya to implement legislation as a cyber threat countermeasure and also partner with the relevant government departments and agencies for the countermeasure to work effectively.

5.6 Suggestions for Further Research

Given the time constraint at hand for the researcher, the research could not cover a detailed study on cyber threats as well as the cyber threat countermeasures as topics. The researcher therefore recommends further detailed research into the two topics jointly or separately to obtain further insights into cyber threats and cyber threat countermeasures implemented by the ISO certified organizations in Kenya.

The research could not also carry out detailed study on individual cyber threats as well as individual cyber threat countermeasures and their individual effectiveness to countering the cyber threats. Therefore the researcher recommends further detailed study on individual cyber threats and also individual cyber threat countermeasures and their individual contributions to cyber security effectiveness.

REFERENCES

ACS Registrars. (2010). *ISO 9001- Benefits of ISO 9001Certicatio, ISO Acreditation*. Retrieved from http://www.iso9001.com/benefitsofiso9001.asp

Anderson, J. P. (1972, October). *Computer Security Technology Planning Study*. Retrieved 08 10, 2010, from National Institute of Standards and Technology, Information Technology Laborartory: http://csrc.nist.gov/publications/history/ande72.pdf

Baino, P. (2001). *Evaluation of Security Rrisks Associated with Networked Information Systems*. Melbourne: Royal Melbourne Institute of Technology University.

BERR. (2008). *2008 Information Security Breaches Survey*. London: Department for Business Enterprise and Regulatory Reform, United Kingdom.

Blagov, M. (2015). *What is a Distributed Denial of Service (DDoS) Attack:DoS and DDoS Explained: Incapsula*. Retrieved from www.incapsula.com: https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html

Businesslink.gov.uk. (2010). *IT security: the basics*. Retrieved June 30, 2010, from Business Link: http://www.businesslink.gov.uk

Carlson, T. (2001, October). *Information Security Manangement: understanding ISO 17799*. Retrieved from http://www.gta.ufrj.br/ensino/cpe728/03_ins_info_security_iso_17799_1101.pdf

Carnagie Mellon University. (2016). *CERT Division*. Retrieved from http://www.cert.org/

Combs, O. (2013). *ISO 9001 As A business Management Tool | Quality Digest*. Retrieved from Quality Digest: http://www.qualitydigest.com/inside/quality-insider-article/iso-9001-business-management-tool.html

Computer World. (2001, February 19). *Suspicious server probles multiply*. Retrieved from www.computerworld.com: http://www.computerworld.com/article/2591768/security0/suspicious-server-probes-multiply.html

Cooper, D. P. (2013). *Business Research Methods.* McGraw Hill.

Curry, S. e. (2013). *Big data fuels intelligence driven security.* Security Division. San Diego: EMC Corporation.

Cyberedge Group. (2014). *2014 Cyberthreat Defense Report, North America & Europe.* Annapolis: Cyberedge Group.

EMC Corporation. (2012). *Getting Ahead of Advanced Threats, Achieving Inrtelligence-Driven Information Security.* Massachusetts: EMC Corportaion.

European Broadcasting Union. (2015). *Mitigation of Distributed Denial of Service (DDoS) (DDoS) Attacks.* Geneva: The European Broadcasting Union.

Ferguson, R. (2015). *The Word Is Not Enough – Online banking fraud.* Cork, Ireland: Trend Micro Incorporated.

Geer Dan, P. M. (2016, August 31). *The Index*. Retrieved from Cyber Security Iindex Organization: http://www.cybersecurityindex.org/index.php

George, T. (2015, October). *Next Big Cybercrime Vector: Social Media*. Retrieved from Security Week: www.securityweek.com

Government of Kenya. (2014). *Cyber Security Startegy.* Ministry of Information Communications and Technology. Nairobi: Govenment Press.

Gurvirender P.S. Tejay, S. M. (2012). Investigating the Effectiveness of IS Security Countermeasures Towards Cyber Attacker Deterrence. *2012 45th Hawaii International Conference on System Scienc* (pp. 1-10). Hawaii: Nova Southeastern University.

Gurvirender, P. T. (2012). Investigating the Effectiveness of IS Security Countermeasures Towards Cyber Attacker Deterrence. *2012 45th Hawaii International Conference on System Scienc* (pp. 1-10). Hawaii: Nova Southeastern University.

Heidi, W. M. (2015). *Countering Social Engineering through Social Media: An Enterprise Security Perspective.* Australia: Charles Sturt University.

ISACA. (2009). *An Introduction to the Business Model for Information Security.* Illinois: ISACA.

ISO Quality Systems Limited. (2015). *ISO 9001 certification, Quality Mnangement System, ISO Quality Systems Limited*. Retrieved from www.isoqsltd.com: http://www.isoqsltd.com/iso-certification/iso-9001-quality-management-certification/

IT Governance Ltd. (2015). *what-is-cybersecurity.aspx*. Retrieved from http://www.itgovernance.co.uk: http://www.itgovernance.co.uk/what-is-cybersecurity.aspx

IT News Africa. (2010, January 25). *New Security Threats Invade Africa in 2010*. Retrieved 08 04, 2010, from IT News Africa: http://www.itnewsafrica.com/

Javanainen, M. (2015). *ISO 9001:2015 and Enterprise Information Management | Quality Digest*. Retrieved from Quality Digest: http://www.qualitydigest.com/inside/standards-column/090115-iso-90012015-and-enterprise-information-management.html

Jethwani, K., & Surbhi, G. (2015). *Cyber Crime: Issues and Challenges.* Delhi: International Journal of Emerging Research in Management &Technology.

KEBS. (2016, August 19). *KEBS - Standards, Training, Testing and Certification*. Retrieved from Kenya Bureau of Standards Web site: http://www.kebs.org/index.php?opt=certification&view=qms_firms

Kitheka, P. M. (2013). *Information Security Management Systems in Public Universities in Kenya: A Gap Analysis Between Common Practices and Industry Best Practices.* Nairobi: University of Nairobi.

Kreicberga, L. (2010). *Internal Threat to Information Security-Countermeasures and human factor within SME.* Kiruna: Lulea University of Technology.

Kumar, D. A. (2011). A study on ISO 9001 Quality Management System: Reason behind the failure of ISO Certified Organizations,. *Global Journal of Management and Business Research, Vol. XI (XI),* , 43-50.

Leder. (2009). *Proactive Botnet Countermeasures An Offensive Approach.* Bonn: Institute of Computer Science IV, University of Bonn, Germany.

Leder, F., & Martini, W. (2009). *Proactive Botnet Countermeasures An Offensive Approach.* Bonn: Institute of Computer Science IV, University of Bonn, Germany.

Letiwa, P. (2010, June 20). Cyber Criminals on the prowl target unsuspecting victims. *Daily Nation* , 6-7.

Lotrionte, C. (2015). Countering State-Sponsored Cyber Economic Espionage Under International Law. *Journal of Law Cyber Warfare* , 443 - 540.

Makumbi, e. a. (2012). *An Analysis of Information Technology (IT) Security Practices: A Case Study of Kenyan Small and Medium Enterprises (SMEs) in the Financial Sector.* Nairobi: University of Nairobi.

Miller et al, R. M. (2015). *Dealing with insider threats to cyber-security.* Atlanta: CA Technologies, Security Management.

Mukinda, F. (2014). *Fraudsters find easy cash in mobile banking.* Nairobi: DAILY NATION Newspaper.

Murdoch University - IT Security. (2010). Retrieved June 30, 2010, from Murdoch University in Perth Australia: http://www.murdoch.edu.au/

Ngalyuka, C. (2013). *The Relationship Between ICT Utilization and Fraud Losses in Commercial Banks in Kenya.* Nairobi: University Of Nairobi.

Ngunjiri, P. (2010, March 22-28). Beware Kenyans, hackers are on the prowl. *The East African* , 41.

Njiru, S. W. (2013). *A Framework to Guide Information Security Initiatives for Banking Information Systems, Kenyan Banking Sector Case Study.* Nairobi.

Nyabiage, J. (2010, May Tuesday 22). Kenya Records upsurge in cybercrime. *Daily Nation* .

Nyamongo, D. M. (2012). *Information Systems Security Management A Case Study of Private Chartered Universities in Kenya.* Nairobi: Strathmore University.

Omuga, S. (2014). *Mobile money fraud.* Nairobi.

Paula, e. a. (2014). *Kenya Cyber Security Report 2014, Rethinking Cybersecurity – "An Integrated Approach:Processes, Intelligence and Monitoring."*. Nairobi: Serianu Limited.

PriceWaterHouseCoopers. (2008, April). *eng/publications/berr_information_security_breaches_survey_2008.html*. Retrieved 08 04, 2010, from Security_Survey: http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html

Rjaibi, N. R. (2015). Monitoring the Effectiveness of Security. *Institut Supérieur de Gestion de Tunis publication* (pp. 327 -336). Tunis: Institut Supérieur de Gestion de Tunis.

Robinson et al, N. L. (2013). *Cyber-security threat characterisation, A rapid comparative analysis.* Stockholm: RAND Corporation.

Salim, H. (2014). *Cyber Safety:A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks.* Massachusetts : Massachusetts Institute of Technology.

Saulius, P. (2012). *What factors explain why there is not a common and comprehensive global response to cyber threats?* Leiden University.

Tarimo, C. N. (2005). An Approach To Enhance ICTInfrastructures' Security Through Legal, Regulatory Influence. In J. E. HS Venter (Ed.), *ISSA 2005 New Knowledge Today Conference.* Sandton, South Africa.

Threat Track Security Inc. (2013). *Enterprises Must Prepare to Combat Cyber Espionage.* Clearwater, Florida: hreatTrack Security, Inc.

Threat Track Security, Inc. (2013). *Enterprises Must Prepare to Combat Cyber Espionage.* Clearwater, Florida: hreatTrack Security, Inc.

Tom, C. (2001). *Information Security Management: Understanding ISO 17799.* Santa Clara: International Network Services.

US Government. (2014). *Combating the Insider Threat.* New York: National Cybersecurity and Communications Integration Centre.

Vatis, M. (2009). *Trends in Cyber Vulnerabilities, Threats, and Countermeasures.*

Wei, X. K. (2012). Security Implementation for a VoIP Server. *Conference on Computer Science & Service System*, (pp. 983 -985).

Wilcox, H. M. (2015). *Countering Social Engineering through Social Media: An Enterprise Security Perspective.* Sydney: Charles Sturt University, Australia.

Yu, J. (2015). Prevention of Toll Frauds against IP-PBX. *International Conference on Security and Management*, (pp. 259 - 254). Chicago.

Zegers, N. (2006). *A Methodolgy for Improving Information Security Incident Identification and Response.* Rotteram: Erasmus Universiteit Rotterdam.

APPENDIX 1: QUESTIONNAIRE

This questionnaire is designed to assist in collecting data to determine cyber threats, countermeasures and effectiveness of countermeasures in ISO certified organizations in Kenya. Kindly note that the findings of this research are solely for academic purposes and all the responses will be treated with utmost confidentiality

SECTION A:

(i) Demographic Information

Tick as appropriate

1. Gender Male □ Female □
2. Age bracket 25 years or less…….. □
   26– 30 years………... □
   31 - 35 years………. □
   36 - 40 years………. □
   41 - 45 years………. □
   46 - 50 years………. □
   Over 50 years............. □
3. Education Level : Postgraduate □ Graduate □ Diploma □
   Other Specify____________________
4. Job Title : ________________________________
5. Years of work experience: 5 years or less □ 6 -10 years □
   Above 10 years □

(ii) Organization Information

1.0 In which industry does your organization operate? Tick as appropriate

Agriculture……………………………….. □

Forestry and fishing…………………….. □

Mining and minerals……………………... □

Industry and manufacturing…………….. □

Energy…………………………………… □

Tourism…………………………………... □

Financial services……………………….. □

Other Specify_____________________________

2.0 Number of employees in your organization (Tick as appropriate)

100 or less...………………………………………………... □

101 to 999………….……………………………………..…. □

Above 1000………………………………………………..... □

3.0 Asset base

3.1 Less than KES 5 billion………………………………. □

3.2 Above KES 5 Billion but less than KES 10 Billion……. □

3.3 Above KES 10 Billion………………………………... □

4.0 How long has the organization been operating in Kenya? _________years

5.0 Is the organization locally owned or foreign multi-national subsidiary?

Locally owned……………………………………………. □

Foreign …………………………………………………... □

Both…………………………………………………………. □

SECTION B: Cyber Threats

To what extent has your organization experienced each of the following situations? Tick to indicate using the scale given.

		No Extent	Little Extent	Moderate Extent	Large Extent	Very large Extent
1.	Employees unintentionally or carelessly making mistakes that compromise cyber security					
2.	Employees being tricked by parties external to the organization to give out their security information for example passwords					
3.	Privileged users for example, IT administrators, attacking the organization’s information system for any reason					
4.	Fake offers on the internet					

	to share user security credentials					
5.	Fake plug-ins posing as legitimate extensions that trick users to download and install them leading to infection and stealing of information from the infected machine(s)					
6.	Fake applications, that appear to be integrated for use with a social network tricking users to install them resulting in the stealing of user access credentials					
7.	External parties hacking into your PBX and making calls through it					
8.	An attack that resulted in websites and servers unavailable to legitimate users					
9.	Computers in your organization spamming and or spreading viruses					
10.	Computers in the organization used by third parties to conduct online fraud activities					
11.	Attempts to access your online or mobile banking platform by non authorized users					
12.	Attempts to access mobile money points of service by unauthorized users					
13.	Lost money fraudulently through mobile money service					
14.	Attempts to access secret or confidential information stored in the organization's computers or ICT network by unauthorized users					
15.	Breach of access to secret					

	or confidential information stored either in the organization’s computers or ICT network					
16.	Confidential information stored in the organization’s computers or ICT network been stolen at any one time					
17.	Other: specify and rate					

SECTION C: Cyber threat Countermeasures

To what extent has your organization implemented each of the following cyber security countermeasures? Tick as appropriate using the scale given

	Countermeasure	No Extent	Little Extent	Moderate Extent	Large Extent	Very large Extent
1.	Cyber security policy					
2.	User awareness training on cyber security issues					
3.	Two factor user authentications					
4.	Maintain staff values and attitudes that align with organizational mission and ethics					
5.	Segregate your voice and data traffic					
6.	Disabling of non-service related or unused open PBX ports					
7.	Call Detail Record (CDR) Monitoring to identify unusual usage patterns					
8.	Policy on how to deal with online social engineering or phishing attempts					
9.	Continuous monitoring of inbound network traffic load on firewalls and system resources (CPUs)					
10.	Segmentation of internal and external networks for critical systems					

11.	Carry out cyber risk assessment on its critical assets					
14.	Legislation					
15.	Carry out cyber security or information security audits					
16.	Constantly scanning and patching for software vulnerabilities					
17.	Other : specify and rate					

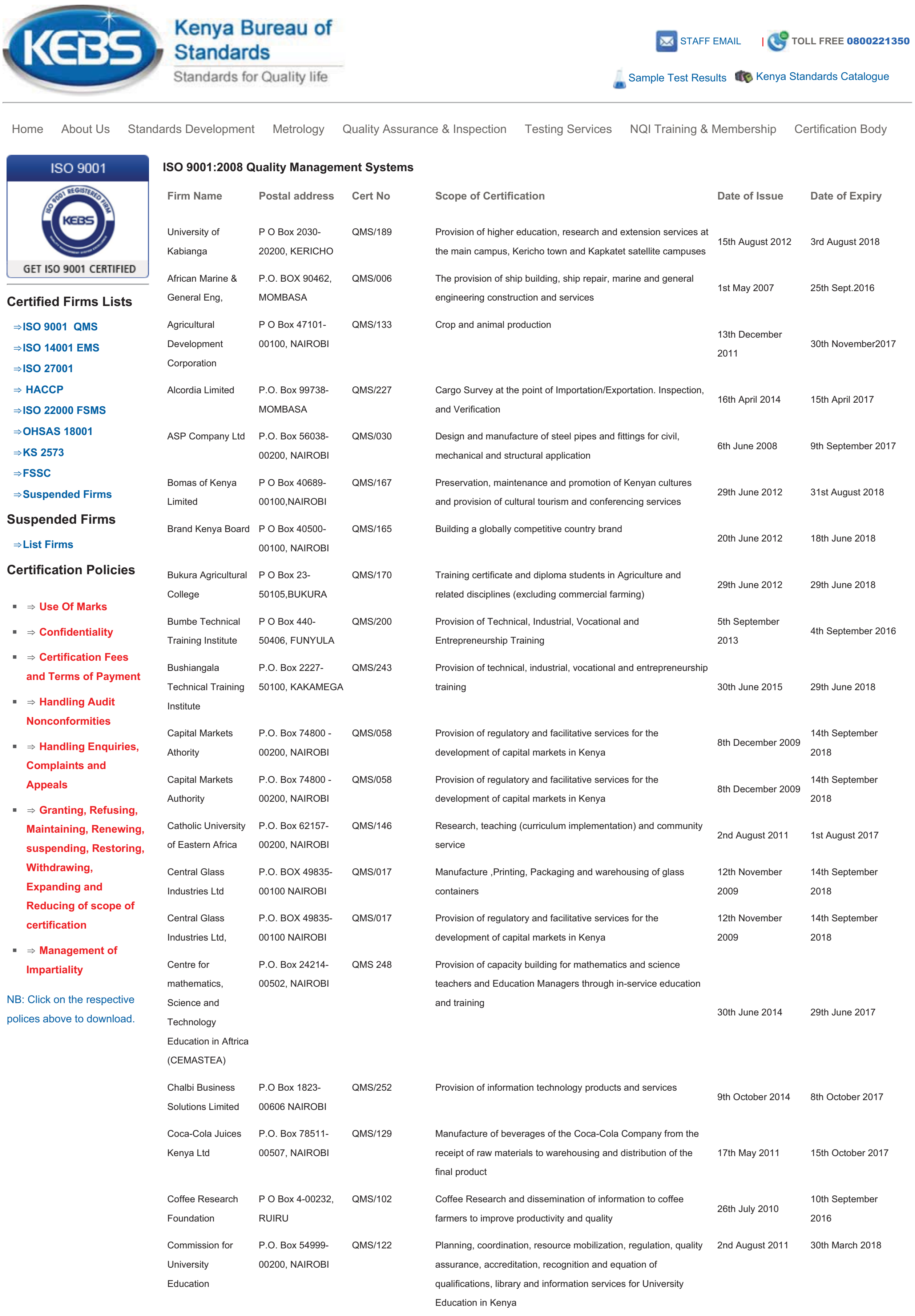
SECTION D: Effectiveness of cyber threat countermeasures implemented by organization

To what extent has the cyber threat countermeasures applied in the organization been effective in achieving each of the following risk mitigation objectives?

		No Extent	Little Extent	Moderat e Extent	Large Extent	Very large Extent
1.	Increased number of successfully blocked cyber attacks					
2.	More uptime of the organization's ICT system to users					
3.	Maintenance of confidentiality of privileged information stored in the organization's computers or ICT Network					
4.	Maintenance of integrity of information stored in the organization's computers or ICT Network					
5.	Maintenance of availability of information stored in the organization's computers or ICT Network					
6.	Other: Specify and rate					

Thank you for completing the questionnaire

APPENDIX 2: LIST OF KENYAN ISO CERTIFIED ORGANIZATIONS



Kenya Bureau of Standards
Standards for Quality life

STAFF EMAIL | TOLL FREE 0800221350

Sample Test Results Kenya Standards Catalogue

Home About Us Standards Development Metrology Quality Assurance & Inspection Testing Services NQI Training & Membership Certification Body

ISO 9001
GET ISO 9001 CERTIFIED

Certified Firms Lists

- ⇒ISO 9001 QMS
- ⇒ISO 14001 EMS
- ⇒ISO 27001
- ⇒ HACCP
- ⇒ISO 22000 FSMS
- ⇒OHSAS 18001
- ⇒KS 2573
- ⇒FSSC
- ⇒Suspended Firms

Suspended Firms

- ⇒List Firms

Certification Policies

- ⇒ Use Of Marks
- ⇒ Confidentiality
- ⇒ Certification Fees and Terms of Payment
- ⇒ Handling Audit Nonconformities
- ⇒ Handling Enquiries, Complaints and Appeals
- ⇒ Granting, Refusing, Maintaining, Renewing, suspending, Restoring, Withdrawing, Expanding and Reducing of scope of certification
- ⇒ Management of Impartiality

NB: Click on the respective polices above to download.

ISO 9001:2008 Quality Management Systems

Firm Name	Postal address	Cert No	Scope of Certification	Date of Issue	Date of Expiry
University of Kabianga	P O Box 2030-20200, KERICHO	QMS/189	Provision of higher education, research and extension services at the main campus, Kericho town and Kapkatet satellite campuses	15th August 2012	3rd August 2018
African Marine & General Eng,	P.O. BOX 90462, MOMBASA	QMS/006	The provision of ship building, ship repair, marine and general engineering construction and services	1st May 2007	25th Sept.2016
Agricultural Development Corporation	P O Box 47101-00100, NAIROBI	QMS/133	Crop and animal production	13th December 2011	30th November2017
Alcordia Limited	P.O. Box 99738-MOMBASA	QMS/227	Cargo Survey at the point of Importation/Exportation. Inspection, and Verification	16th April 2014	15th April 2017
ASP Company Ltd	P.O. Box 56038-00200, NAIROBI	QMS/030	Design and manufacture of steel pipes and fittings for civil, mechanical and structural application	6th June 2008	9th September 2017
Bomas of Kenya Limited	P O Box 40689-00100,NAIROBI	QMS/167	Preservation, maintenance and promotion of Kenyan cultures and provision of cultural tourism and conferencing services	29th June 2012	31st August 2018
Brand Kenya Board	P O Box 40500-00100, NAIROBI	QMS/165	Building a globally competitive country brand	20th June 2012	18th June 2018
Bukura Agricultural College	P O Box 23-50105,BUKURA	QMS/170	Training certificate and diploma students in Agriculture and related disciplines (excluding commercial farming)	29th June 2012	29th June 2018
Bumbe Technical Training Institute	P O Box 440-50406, FUNYULA	QMS/200	Provision of Technical, Industrial, Vocational and Entrepreneurship Training	5th September 2013	4th September 2016
Bushiangala Technical Training Institute	P.O. Box 2227-50100, KAKAMEGA	QMS/243	Provision of technical, industrial, vocational and entrepreneurship training	30th June 2015	29th June 2018
Capital Markets Athority	P.O. Box 74800 - 00200, NAIROBI	QMS/058	Provision of regulatory and facilitative services for the development of capital markets in Kenya	8th December 2009	14th September 2018
Capital Markets Authority	P.O. Box 74800 - 00200, NAIROBI	QMS/058	Provision of regulatory and facilitative services for the development of capital markets in Kenya	8th December 2009	14th September 2018
Catholic University of Eastern Africa	P.O. Box 62157-00200, NAIROBI	QMS/146	Research, teaching (curriculum implementation) and community service	2nd August 2011	1st August 2017
Central Glass Industries Ltd	P.O. BOX 49835-00100 NAIROBI	QMS/017	Manufacture ,Printing, Packaging and warehousing of glass containers	12th November 2009	14th September 2018
Central Glass Industries Ltd,	P.O. BOX 49835-00100 NAIROBI	QMS/017	Provision of regulatory and facilitative services for the development of capital markets in Kenya	12th November 2009	14th September 2018
Centre for mathematics, Science and Technology Education in Aftrica (CEMASTEA)	P.O. Box 24214-00502, NAIROBI	QMS 248	Provision of capacity building for mathematics and science teachers and Education Managers through in-service education and training	30th June 2014	29th June 2017
Chalbi Business Solutions Limited	P.O Box 1823-00606 NAIROBI	QMS/252	Provision of information technology products and services	9th October 2014	8th October 2017
Coca-Cola Juices Kenya Ltd	P.O. Box 78511-00507, NAIROBI	QMS/129	Manufacture of beverages of the Coca-Cola Company from the receipt of raw materials to warehousing and distribution of the final product	17th May 2011	15th October 2017
Coffee Research Foundation	P O Box 4-00232, RUIRU	QMS/102	Coffee Research and dissemination of information to coffee farmers to improve productivity and quality	26th July 2010	10th September 2016
Commission for University Education	P.O. Box 54999-00200, NAIROBI	QMS/122	Planning, coordination, resource mobilization, regulation, quality assurance, accreditation, recognition and equation of qualifications, library and information services for University Education in Kenya	2nd August 2011	30th March 2018

ISO 9001

GET ISO 9001 CERTIFIED

Certified Firms Lists

- ⇒ISO 9001 QMS
- ⇒ISO 14001 EMS
- ⇒ISO 27001
- ⇒ HACCP
- ⇒ISO 22000 FSMS
- ⇒OHSAS 18001
- ⇒KS 2573
- ⇒FSSC
- ⇒Suspended Firms

Suspended Firms

- ⇒List Firms

Certification Policies

- ⇒ Use Of Marks
- ⇒ Confidentiality
- ⇒ Certification Fees and Terms of Payment
- ⇒ Handling Audit Nonconformities
- ⇒ Handling Enquiries, Complaints and Appeals
- ⇒ Granting, Refusing, Maintaining, Renewing, suspending, Restoring, Withdrawing, Expanding and Reducing of scope of certification
- ⇒ Management of Impartiality

NB: Click on the respective polices above to download.

ISO 9001:2008 Quality Management Systems

Firm Name	Postal address	Cert No	Scope of Certification	Date of Issue	Date of Expiry
Cooperative University College of Kenya	P.O. Box 24814-00502, NAIROBI	QMS 246	Provision of cooperative education, training, research, consultancy and conference facilities at the main campus	11th July 2014	10th July 2017
CPF Financial Services Ltd (Formerly Laptrust Administration Services Ltd)	P.O. Box 28938-00200, NAIROBI	QMS/145	Retirement benefits and financial services	30th June 2011	29th June 2018
Dalcom Kenya Limited	P.O. Box 17491-00100, NAIROBI	QMS/276	Manufacture, assembly, distribution and installation of motor vehicle speed limiters and recorders	18th December 2015	17th December 2018
Dalcom Kenya Limited	P.O. Box 17491-00100, NAIROBI	QMS/276	Manufacture, assembly, distribution and installation of motor vehicle speed limiters and recorders	18th December 2015	17th December 2018
Defence Forces Memorial Hospital	P O Box 62938-00200, NAIROBI	QMS/216	Administration and Clinical Services	15th January 2014	14th January 2017
East African Breweries Ltd	P.O. BOX 30161-00100 NAIROBI	QMS/004	Production and marketing of alcoholic and non-alcoholic beverages	20th July 2006	17th June 2016
East African Maltings Ltd	P.O. Box 41412-00100, NAIROBI	QMS/015	Production of barley seed, malting barley, barley malt and barley varieties	20th July 2006	24th November 2017
East African Portland Cement Company Limited	P.O. Box 20-002004, ATHI RIVER	QMS/085	Limestone and Kunkur mining and Clinker and Cement Production	26th June 2009	30th June 2018
East African School of Aviation	P.O. Box 30689-00200, NAIROBI	QMS/142	Aviation Training	1st April 2011	30th March 2018
Egerton University	P O Box 536 Egerton	QMS/111	Provision of Higher Education, research, Consultancy, Medical Services, Hotel and Conferencing facilities at the Njoro Campus	16th June 2010	25th September 2016
Egoji Teachers College	P O Private Bag, Egoji	QMS/191	Provision of training for P1 Teachers	14th May 2013	14th September 2018
Eldoret Polytechnic	P.O. Box 4461-30100, ELDORET	QMS 159	Provision of training services in technical, industrial, vocational and entrepreneurship at the Main Campus located along Eldoret-Kapsabet Road	30th June 2014	29th June 2017
Embu University College	P.O. Box 6-60100, EMBU	QMS/261	Provision of training, research and extension	2nd December 2014	1st December 2017
Energy Regulatory Commission	P O Box 42681-00100 NAIROBI	QMS/116	Regulation of the electric power, Petroleum and Renewable Energy sectors in Kenya	28th June 2010	18th August 2016
Ewaso Ng'iro South Development Authority	P.O. Box 213-20500, NAROK	QMS/245	Basin planning actities, coservation, water projects and community projects	20th June 2014	19th June 2017
Friends College Kaimosi (Kaimosi Institute of Research & Technology	P O Box 150-50309, KAIMOSI	QMS/207	Provision of Technical, Industrial, Vocational and Entrepreneurship Training at the main campus (excludes the farm)	25th March 2013	14th September 2018
General Motors East Africa Ltd	P.O. BOX 30527-00100, NAIROBI	QMS/013	Motor vehicle manufacturing, sales and distribution and associated after sales services	16th June 2009	10th August 2018
Geothermal Development Company	P O Box 100746-00101,NAIROBI	QMS/149	Exploration, resource assessment, drilling reservoir management and steam harnessing	26th June 2012	25th June 2018
	P O Box 100746-00101,NAIROBI	QMS/149	Exploration, resource assessment, drilling reservoir management and steam harnessing	26th June 2012	25th June 2018

Geothermal Development Company					
GlaxoSmithKline	P.O. BOX 78392 - 00507, NAIROBI	QMS/005	Manufacture of analgesic, nutritional and oral healthcare products	8th December 2009	6th May 2016

FIRST | PREVIOUS (Page 2 of 9) NEXT | LAST

Total number of firms: 175

Physical Location:
Certification Body
Kenya Bureau of Standards Headquarters
Popo Road, Off Mombasa Road
South C area, Nairobi

Postal Address:
P.O. Box 54974-00200
Nairobi
Email – General enquiries
cbstaff@kebs.org

Telephone:
Office:(254 20) 6948506

Specific Contacts
Caroline Outa
Head of the KEBS Certification Body
Tel: (254 20) 6948324/263
E-mail: outac@kebs.org

Useful links

- Codex
- PVoC
- Standards Levy
- Bio-Safety
- Non-Destructive Testing
- Banned Products
- Upcoming Training
- Entropy Login

Our services

- Standards Development and Harmonization
- Testing
- Measurments (Calibration)
- Enforcment of Standards
- Product Inspection
- Education and Training
- Management System Certification
- Product Certification
- Training Courses

Industry sectors

- Technical Committees
- Food and Agriculture
- Chemical
- Textile and Leather
- Civil
- Electrotechnical
- Mechanical
- Services
- Trade Affairs

About KEBS

- Corporate Responsibility
- Careers
- News and Events
- Press Release
- Public Notices
- Media Center
- Speeches
- Bids Tenders Expression of Interests
- Service Charter
- Complaints Contacts

Other KEBS websites

- ISO Webstore
- Notify Kenya TBT
- Car Inspection Details

Contact us

Landline : (+ 254 20)6948000
Mobile :
+ 254722202137
+ 254734600471
PVoC : + 254724255242
Email : info@kebs.org
Fax : (+254 20) 6948575

| Frequently Asked Questions | Compliments and Complaints | Other KEBS contacts

chss business translation business financeaccounting managementscience economics ids idis awsc arts african-studies arabic confucius french geography history kiswahili languageskills linguistics literature philosophy politicalscience journalism psychology sociology koreanstudies dlis acfrn law-school commerciallaw privatelaw publiclaw psri caselap kisumu mombasa

Kenya Bureau of Standards
Standards for Quality life

STAFF EMAIL | TOLL FREE **0800221350**

Sample Test Results Kenya Standards Catalogue

Home About Us Standards Development Metrology Quality Assurance & Inspection Testing Services NQI Training & Membership Certification Body

ISO 9001

GET ISO 9001 CERTIFIED

Certified Firms Lists

- ⇒**ISO 9001 QMS**
- ⇒**ISO 14001 EMS**
- ⇒**ISO 27001**
- ⇒ **HACCP**
- ⇒**ISO 22000 FSMS**
- ⇒**OHSAS 18001**
- ⇒**KS 2573**
- ⇒**FSSC**
- ⇒**Suspended Firms**

Suspended Firms

- ⇒**List Firms**

Certification Policies

- ⇒ **Use Of Marks**
- ⇒ **Confidentiality**
- ⇒ **Certification Fees and Terms of Payment**
- ⇒ **Handling Audit Nonconformities**
- ⇒ **Handling Enquiries, Complaints and Appeals**
- ⇒ **Granting, Refusing, Maintaining, Renewing, suspending, Restoring, Withdrawing, Expanding and Reducing of scope of certification**
- ⇒ **Management of Impartiality**

NB: Click on the respective polices above to download.

ISO 9001:2008 Quality Management Systems

Firm Name	Postal address	Cert No	Scope of Certification	Date of Issue	Date of Expiry
Tanzania Steel Pipes Ltd	P.O. Box 5476, Dar es salaam TANZANIA	QMS/078	Design and manufacture of steel pipes and fittings for civil, mechanical and structural applications	18th May 2009	25th May 2018
Tea Research Institute - Kenya Agricultural and Livestock Research Organization (KALRO)	P O Box 820-20200,KERICHO	QMS/160	Tea research and dissemination of information to tea farmers	20th June 2012	21st September 2018
The Mater Hospital	P.O. BOX 30325-00100 NAIROBI	QMS/042	The provision of healthcare services at the main hospital and at Development house, Buruburu, Thika and Embakasi satellite clinics	3rd February 2010	14th September 2018
The Nairobi Hospital	P O Box 30026-00100, NAIROBI	QMS/163	Provision of Health Care Services and nursing Education	13th April 2012	12th April 2018
Thika Technical Training Institute	P.O. Box 91-00100, THIKA	QMS/126	Provision of technical, industrial, vocational and entrepreneurship training (TIVET)	25th July 2011	26th January 2018
Trident Plumbers Ltd	P.O. Box 7335-00300, NAIROBI	QMS 237	Mechanical services for constrution within Nairobi	30th June 2014	29th June 2017
Tropikal Brands (Africa) Ltd	P.O. Box 49465-00100, NAIROBI	QMS/235	Manufacture and trade in household care products, foods, personal care and auto care products	31st July 2014	30th July 2017
University of Nairobi	P.O. BOX 30197-00100, NAIROBI	QMS/064	Provision of Higher Education	6th April 2009	22nd July 2017
University of Nairobi Enterprises and Services Ltd	P O Box 68241-00200 NAIROBI	QMS/097	Provision of Financial management services, restaurant and conferencing facilities, consultancy services and the operation of bookstores	14th May 2010	18th July 2016
Vermont Flowers (EPZ) Ltd	P.O. Box 27719-00506, NAIROBI	QMS/51	Perservation of natural flowers, foliages and creation of floral arrangements	1st August 2007	14th October 2017
Water Resources Management Authority	P O Box 45250-00100, NAIROBI	QMS/180	Management and regulation of water use	21st February 2013	14th May 2018
Water Services Regulatory Board	P.O. Box 41621-00100, NAIROBI	QMS/076	Regulation of Water services in Kenya	18th May 2009	11th Sept. 2016
Water Services Trust Fund	P.O. Box 49699-00100, NAIROBI	QMS/123	Financing of water services and water resources to underserved rural and urban areas in Kenya	30th May 2011	21st June 2018
Wote Technical Training Institute	P.O. Box 377-90300, MAKUENI	QMS 247	Provision of technical industrial, vocational and entrepreneurship training located at Wote, Makueni County	30th June 2014	29th June 2017
Youth Enterprise Development Fund Board	P.O. Box 48610-00100, NAIROBI	QMS/266	Empowering the Kenyan Youth through provision of affordable financial services, business development services and facilitating employment opportunities	21st September 2015	20th September 2018

FIRST | PREVIOUS (Page 9 of 9) NEXT | LAST

Total number of firms: 175

Physical Location:
Certification Body
Kenya Bureau of Standards Headquarters
Popo Road, Off Mombasa Road
South C area, Nairobi

Postal Address:
P.O. Box 54974-00200
Nairobi
Email – General enquiries
cbstaff@kebs.org

Telephone:
Office:(254 20) 6948506

Specific Contacts
Caroline Outa
Head of the KEBS Certification Body
Tel: (254 20) 6948324/263
E-mail: outac@kebs.org

Kenya Bureau of Standards
Standards for Quality life

STAFF EMAIL | TOLL FREE **0800221350**

Sample Test Results Kenya Standards Catalogue

Home About Us Standards Development Metrology Quality Assurance & Inspection Testing Services NQI Training & Membership Certification Body

ISO 9001

GET ISO 9001 CERTIFIED

Certified Firms Lists

- ⇒**ISO 9001 QMS**
- ⇒**ISO 14001 EMS**
- ⇒**ISO 27001**
- ⇒ **HACCP**
- ⇒**ISO 22000 FSMS**
- ⇒**OHSAS 18001**
- ⇒**KS 2573**
- ⇒**FSSC**
- ⇒**Suspended Firms**

Suspended Firms

- ⇒**List Firms**

Certification Policies

- ⇒ **Use Of Marks**
- ⇒ **Confidentiality**
- ⇒ **Certification Fees and Terms of Payment**
- ⇒ **Handling Audit Nonconformities**
- ⇒ **Handling Enquiries, Complaints and Appeals**
- ⇒ **Granting, Refusing, Maintaining, Renewing, suspending, Restoring, Withdrawing, Expanding and Reducing of scope of certification**
- ⇒ **Management of Impartiality**

NB: Click on the respective polices above to download.

ISO 9001:2008 Quality Management Systems

Firm Name	Postal address	Cert No	Scope of Certification	Date of Issue	Date of Expiry
Pest Control Products Board	P.O. Box 13794-00800	QMS/130	Regulation of pest control products in importation, exportation, manufacturing, distribution, sale, use and disposal	26th June 2012	14th September 2018
Polucon Services Ltd	P.O. BOX 99344 MOMBASA	QMS/044	Inspection, Cargo survey and laboratory Testing services	10th February 2006	3rd April 2018
Privatization Commission	P O Box 434542-00200 NAIROBI	QMS/114	Provision of Services for the Privatization of Public Assets and Operations, including State Corporations	30th June 2010	14th September 2018
Public Procurement Oversight Authority	P.O. Box 58535-00200, NAIROBI	QMS/273	Regulation of the Public Procurement Systems in Kenya	7th June 2016	14th September 2018
Railway Training Institute	P.O. Box 42226-00100, NAIROBI	QMS/233	Provision of Technical Industrial, Vocational and Entrepreneurship Training at the Main Campus	15th May 2014	14th May 2017
Retirement Benefits Authority	P.O. BOX 57733, NAIROBI	QMS/047	Provision of Retirement benefits regulatory services in Kenya	15th May 2009	21st July 2016
Rift Valley Institute of Science & Technology	P O Box 7182-20100, NAKURU	QMS/171	Provision of Technical and Vocational Education and Training (TVET)	10th January 2013	14th September 2018
Rift Valley Technical Training Institute	P O Box 244-30100, ELDORET	QMS/121	Training services in Technical, Industrial, Vocational & Entrepreneurship Training (T.I.V.E.T)	20th September 2010	13th November 2016
Rift Valley Water Services Board	P.O. Box 2451 - 20100, NAKURU, KENYA	QMS/143	Management of the provision of water and sanitation services in the Rift Valley Region	19th August 2011	18th August 2017
Rural Electrification Authority	P O Box 34585-00100 NAIROBI	QMS/135	Design and construction of electricity lines at Headquarters, Mombasa road, Mariakani, Eldoret, Kisumu and Nyeri	28th June 2011	23rd July 2017
Sangalo Institute of Science & Technology	P O Box 158-50200, BUNGOMA	QMS/223	Provision of Technical, Industrial, Vocational and Entrepreneurship Training (TIVET)	13th Janaury 2014	12th January 2017
Shamberere Technical Training Institute	P.O. Box 1316-50100, KAKAMEGA	QMS/242	Provision of technical, industrial, vocational and entrepreneurship training	30th June 2015	29th June 2018
Sigalagala National Polytechnic	P.O. Box 2966-50100, KAKAMEGA	QMS/259	Provision of technical, vocational and entrepreneurship training	14th September 2015	13th September 2018
Sondhi Trading Company	P.O. BOX 80066-80100, MOMBASA	QMS/046	Import, export and wholesale trade of assorted products	17th October 2009	14th September 2018
South Eatern Kenya University	P.O. Box 170-90200	QMS/260	Provision of teaching, research, extension, innovation and entrepreneurship	25th November 2014	24th November 2017
South Nyanza Sugar Company (SONY SUGAR)	P.O. Box 107, SARE AWENDO	QMS/095	Manufacturing, marketing and supply of Sugar and associated products	17th August 2009	31st August 2018
Southern Engineering Ltd	P.O. Box 84162 MOMBASA	QMS/027	Ship building, ship repairs and general engineering	29th April 2010	1st September 2016
St. John's Teachers Training College	P.O. Box 8-01000, THIKA	QMS/274	Provision of Education and Training of P1 Primary Teachers	19th May 2016	18th May 2019
Steel Structures Limited	P.O. Box 49862-00100, NAIROBI	QMS/284	Design, Fabrication and Erection of Structural Steel	16th July 2016	14th September 2018
Tana Water Services Board	P O Box 1292-10100,NYERI	QMS/073	Provision of affordable, reliable and sustainable water and sanitation services through contracted water service providers within their areas of jurisdiction	6th July 2012	5th July 2018

FIRST | PREVIOUS (Page 8 of 9) NEXT | LAST

Total number of firms: 175

Physical Location:
Certification Body
Kenya Bureau of Standards Headquarters
Popo Road, Off Mombasa Road
South C area, Nairobi

Postal Address:
P.O. Box 54974-00200
Nairobi
Email – General enquiries
cbstaff@kebs.org

Telephone:
Office:(254 20) 6948506

Specific Contacts
Caroline Outa
Head of the KEBS Certification Body
Tel: (254 20) 6948324/263
E-mail: outac@kebs.org

Useful links

- Codex
- PVoC
- Standards Levy
- Bio-Safety
- Non-Destructive Testing
- Banned Products
- Upcoming Training
- Entropy Login

Our services

- Standards Development and Harmonization
- Testing
- Measurments (Calibration)
- Enforcment of Standards
- Product Inspection
- Education and Training
- Management System Certification
- Product Certification
- Training Courses

Industry sectors

- Technical Committees
- Food and Agriculture
- Chemical
- Textile and Leather
- Civil
- Electrotechnical
- Mechanical
- Services
- Trade Affairs

About KEBS

- Corporate Responsibility
- Careers
- News and Events
- Press Release
- Public Notices
- Media Center
- Speeches
- Bids Tenders
- Expression of Interests
- Service Charter
- Complaints Contacts

Other KEBS websites

- ISO Webstore
- Notify Kenya TBT
- Car Inspection Details

Contact us

Landline : (+ 254 20)6948000

Mobile :
+ 254722202137

+ 254734600471

PVoC : + 254724255242

Email : info@kebs.org

Fax : (+254 20) 6948575

| Frequently Asked Questions | Compliments and Complaints | Other KEBS contacts

chss business translation business financeaccounting managementscience economics ids idis awsc arts african-studies arabic confucius french geography history kiswahili languageskills linguistics literature philosophy politicalscience journalism psychology sociology koreanstudies dlis acfrn law-school commerciallaw privatelaw publiclaw psri caselap kisumu mombasa

ISO 9001

GET ISO 9001 CERTIFIED

Certified Firms Lists

- ⇒ISO 9001 QMS
- ⇒ISO 14001 EMS
- ⇒ISO 27001
- ⇒ HACCP
- ⇒ISO 22000 FSMS
- ⇒OHSAS 18001
- ⇒KS 2573
- ⇒FSSC
- ⇒Suspended Firms

Suspended Firms

- ⇒List Firms

Certification Policies

- ⇒ Use Of Marks
- ⇒ Confidentiality
- ⇒ Certification Fees and Terms of Payment
- ⇒ Handling Audit Nonconformities
- ⇒ Handling Enquiries, Complaints and Appeals
- ⇒ Granting, Refusing, Maintaining, Renewing, suspending, Restoring, Withdrawing, Expanding and Reducing of scope of certification
- ⇒ Management of Impartiality

NB: Click on the respective polices above to download.

ISO 9001:2008 Quality Management Systems

Firm Name	Postal address	Cert No	Scope of Certification	Date of Issue	Date of Expiry
Nakumatt Holdings Ltd	P.O. BOX 78355-00507, NAIROBI	QMS/050	Retailing of Household and Consumer goods	17th March 2010	14th September 2018
National AIDS Control Council	P O Box 61307-00200 NAIROBI	QMS/086	Coordination of the National Response to HIV and AIDS in Kenya	3rd June 2010	29th Sept. 2016
National Biosafety Authority	P O Box 28251-00100, NAIROBI	QMS/214	Regulation of the development, transfer, handling and use of Genetically Modified Organisms (GMOs) at the NBA Headquarters	15th May 2013	14th September 2018
National Campaign Against Drug Abuse Authority (NACADA)	P.O. Box 10774-00100, NAIROBI	QMS 192	Campaign against alcohol and drug abuse carried out by the Head Office	30th June 2014	29th June 2017
National Cereals and Produce Board	P.O. Box 30586-00100, NAIROBI	QMS/255	Operational & administrative activities, grain intake, drying, fumigation, weighing services, storage and sale activities	9th July 2015	8th July 2018
National Commission for Science, Technology & Innovation	P O BOX 30623-00100, NAIROBI	QMS/206	Provision of quality advice, coordination and promotion of research, science, technology and innovation in Kenya	10th June 2013	9th June 2016
National Hospital Insurance Fund	P.O. Box 30443-00100, NAIROBI	QMS/062	Provision of Health Insurance in Kenya	22nd July 2008	16th April 2018
National Housing Corporation	P.O. Box 30257-00100, NAIROBI	QMS/081	Design and Supervision of housing development for sale and/or rental, advance of housing loans and manufacture of expanded polystyrene (EPS) building panels	20th September 2010	14th September 2018
National Irrigation Board	P.O. Box 30372-00100	QMS/136	Development, promotion and improvement of irrigation insfrastructure for irrigated agriculture and research in irrigation and irrigated crops	23rd November 2011	30th March 2018
National Social Security Fund - Board of Trustees	P O BOX 30599-00100, NAIROBI	QMS/181	Provision of social security to all Kenyans through payment of the : age, withdrawal surviors, invalidity, emigration and funeral grant	15th January 2013	14th January 2019
National Water Conservation & Pipeline Corporation	P.O. Box 56038-00200, NAIROBI	QMS/059	Provision of hydro engineering services, construction of dams, driling and equipping of bore holes and flood control works in Kenya	8th October 2008	14th September 2018
New Kenya Cooperative Creameries Ltd	P.O. Box 30131 - 00100, NAIROBI	QMS/240	Production, Marketing and sale of fresh milk, fermented milk, long life milk, butter, ghee, cheese and milk powder	9th May 2015	8th May 2018
Nkabune Technical Training Institute	P O Box 330-60200 Meru	QMS/117	Provision of Technical, Industrial, Vocational and Entrepreneurship Training	31st January 2011	30th January 2017
North Eastern Province Technical Treaing Institute	P O Box 329-70100, GARISSA	QMS/226	Provision of Technical, Industrial, Vocational and Entrepreneurship Training (TIVET)	11th December 2013	10th December 2016
Nyandarua Institute of Science and Technology	P O Box 2033-20300,NYAHURURU	QMS/173	Provision of Technical, Industrial, Vocational and Entrepreneurship training	28th February 2013	14th September 2018
Nyayo Tea Zones Development Corporation	P.O. Box 48552-00400, NAIROBI.	QMS/079	Growing and sale of green leaf tea and forest products	16th June 2009	12th August 2015
Nyeri Technical Training Institute	P.O. Box 465-10100, NYERI	QMS/139	Provision of Teaching, Industrial, Vocational and Entrepreneurship Training (TIVET)	30th June 2011	2nd November 2017
Nzoia Sugar Co.		QMS/072	Manufacture of Sugar and its by-products	11th August 2009	15th October 2018

	P.O. BOX 285, BUNGOMA				
Ol'lessos Technical Training Institute	P O Box 210-30302, LESSOS	QMS/168	Provision of Technical, Industrial, Vocational and Entrepreneurship training	18th December 2012	14th September 2018
P.C. Kinyanjui Technical Training Institute	P O Box 21280-00505,NAIROBI	QMS/132	Provision of Technical, Industrial, Vocational and Entrepreneurship Training	20th May 2011	19th May 2017

FIRST | PREVIOUS (Page 7 of 9) NEXT | LAST

Total number of firms: 175

Physical Location:
Certification Body
Kenya Bureau of Standards Headquarters
Popo Road, Off Mombasa Road
South C area, Nairobi

Postal Address:
P.O. Box 54974-00200
Nairobi
Email – General enquiries
cbstaff@kebs.org

Telephone:
Office:(254 20) 6948506

Specific Contacts
Caroline Outa
Head of the KEBS Certification Body
Tel: (254 20) 6948324/263
E-mail: outac@kebs.org

Useful links

- Codex
- PVoC
- Standards Levy
- Bio-Safety
- Non-Destructive Testing
- Banned Products
- Upcoming Training
- Entropy Login

Our services

- Standards Development and Harmonization
- Testing
- Measurments (Calibration)
- Enforcment of Standards
- Product Inspection
- Education and Training
- Management System Certification
- Product Certification
- Training Courses

Industry sectors

- Technical Committees
- Food and Agriculture
- Chemical
- Textile and Leather
- Civil
- Electrotechnical
- Mechanical
- Services
- Trade Affairs

About KEBS

- Corporate Responsibility
- Careers
- News and Events
- Press Release
- Public Notices
- Media Center
- Speeches
- Bids Tenders
- Expression of Interests
- Service Charter
- Complaints Contacts

Other KEBS websites

- ISO Webstore
- Notify Kenya TBT
- Car Inspection Details

Contact us

Landline : (+ 254 20)6948000
Mobile :
+ 254722202137
+ 254734600471
PVoC : + 254724255242
Email : info@kebs.org
Fax : (+254 20) 6948575

ISO 9001

GET ISO 9001 CERTIFIED

Certified Firms Lists

- ⇒ISO 9001 QMS
- ⇒ISO 14001 EMS
- ⇒ISO 27001
- ⇒ HACCP
- ⇒ISO 22000 FSMS
- ⇒OHSAS 18001
- ⇒KS 2573
- ⇒FSSC
- ⇒Suspended Firms

Suspended Firms

- ⇒List Firms

Certification Policies

- ⇒ Use Of Marks
- ⇒ Confidentiality
- ⇒ Certification Fees and Terms of Payment
- ⇒ Handling Audit Nonconformities
- ⇒ Handling Enquiries, Complaints and Appeals
- ⇒ Granting, Refusing, Maintaining, Renewing, suspending, Restoring, Withdrawing, Expanding and Reducing of scope of certification
- ⇒ Management of Impartiality

NB: Click on the respective polices above to download.

ISO 9001:2008 Quality Management Systems

Firm Name	Postal address	Cert No	Scope of Certification	Date of Issue	Date of Expiry
Masinde Muliro University of Science & Technology	P O Box 190-50100, KAKAMEGA	QMS/188	Provision of Higher Education, Research Consultancy and extension at Kakakmega main campus, Bungoma and Webuye Campuses and Nairobi Study Centre	26th September 2013	25th September 2016
Mathenge Technical Training Institute	P O Box 665-10106,OTHAYA	QMS/144	Provision of technical, vocational and entrepreneurship training (TVET)	18th July 2011	17th July 2017
Matili Technical Training Institute	P.O. Box 76 - 50204, KIMILILI	QMS/244	Provision of technical, industrial, vocational and entrepreneurship training	30th June 2015	29th June 2018
Mawego Technical Training Insitute	P.O. Box 289-40222, OYUGIS	QMS/275	Provision of technical, industrial, vocational and entrepreneurship training (TIVET)	17th February 2016	14th September 2018
Mbaraki Port Warehouses (K) Ltd	P.O. BOX 80066-80100, MOMBASA	QMS/043	Collection of rents and maintaining leases, maintenance of company assests, clearing and forwarding services	1st December 2008	14th September 2018
Merchants Technical Services	P.O. Box 40242-80100, MOMBASA	QMS/272	Inspection, cargo survey, fumigation services for import and export goods	16th October 2015	15th October 2018
Meru University of Science & Technology	P O Box 972-60200 ,MERU	QMS/ 217	Provision of University education and research		20th May 2016
Michuki Technical Training Institute	P O Box 4-10202, KANGEMA	QMS/150	Provision of Technical, Industrial , Vocational and Entrepreneurship Training (TIVET)	28th May 2012	24th May 2018
Ministry of Health - Tuberculosis, Leprosy and Lung Disease Unit	P O Box 20781-00202, NAIROBI	QMS/184	Development of policy guidelines, ensuring commodity security and coordination of the implementation of acitivities for leprosy, tuberculosis and lung diseases prevention and control	23rd October 2013	22nd October 2016
Ministry of East AfricanAffairs, Commerce and Tourism, Stae Department of East African Affairs	P.O Box 8846-00200 NAIROBI	QMS/251	Provision of Rgeional Integrtaion	8tH August 2014	7th August 2017
Moi Teaching and Referral Hospital	P.O. BOX 3-30100, ELDORET	QMS/075	Provision of healthcare delivery, Training and health research	27th March 2009	24th June 2018
Moi University	P.O. Box 3900, ELDORET	QMS/099	Provision of higher education	4th December 2009	14th September 2018
Mount Kenya University	P O Box 342-00100, THIKA	QMS/210	Teaching, Research & Consultancy and Community service	19th December 2012	14th September 2018
Muhoroni Sugar Comapny	P.O. Box 2, MUHORONI	QMS/061	Sugarcane production and manufacture and sale of sugar and associated products	14th July 2008	18th January 2018
Multimedia University of Kenya	P.O. Box 15653-00503, NAIROBI	QMS/280	Training, research, technology and innovation at the Main Campus	23rd February 2016	14th September 2018
Murang'a University College	75-10200, MURANG'A	QMS/164	Training, Research and Innovations	5th March 2012	14th September 2018
Mwalimu National SACCO Ltd	P.O. Box 62641-00200, NAIROBI	QMS/084	mobilization of funds from customers and provision of credit services and other financial services	20th July 2009	19th July 2018
Nairobi City Water & Sewerage Company Ltd	P.O. Box 30656-00100, NAIROBI	QMS/063	Water Supply	14th July 2009	12th May 2017
Nairobi Technical Training Institute	P O Box 30039-00100,NAIROBI	QMS/194	Provision of Technical, Industrial, Vocational and Entrepreneurship Training (TIVET)	28th February 2013	14th September 2018

Nakumatt Holdings Ltd	P.O. BOX 78355-00507, NAIROBI	QMS/050	Retailing of Household and Consumer goods	17th March 2010	7th April 2016

FIRST | PREVIOUS (Page 6 of 9) NEXT | LAST

Total number of firms: 175

Physical Location:
Certification Body
Kenya Bureau of Standards Headquarters
Popo Road, Off Mombasa Road
South C area, Nairobi

Postal Address:
P.O. Box 54974-00200
Nairobi
Email – General enquiries
cbstaff@kebs.org

Telephone:
Office:(254 20) 6948506

Specific Contacts
Caroline Outa
Head of the KEBS Certification Body
Tel: (254 20) 6948324/263
E-mail: outac@kebs.org

Useful links

Codex
PVoC
Standards Levy
Bio-Safety
Non-Destructive Testing
Banned Products
Upcoming Training
Entropy Login

Our services

Standards Development and Harmonization
Testing
Measurments (Calibration)
Enforcment of Standards
Product Inspection
Education and Training
Management System Certification
Product Certification
Training Courses

Industry sectors

Technical Committees
Food and Agriculture
Chemical
Textile and Leather
Civil
Electrotechnical
Mechanical
Services
Trade Affairs

About KEBS

Corporate Responsibility
Careers
News and Events
Press Release
Public Notices
Media Center
Speeches
Bids Tenders Expression of Interests
Service Charter
Complaints Contacts

Other KEBS websites

ISO Webstore
Notify Kenya TBT
Car Inspection Details

Contact us

Landline : (+ 254 20)6948000
Mobile :
+ 254722202137
+ 254734600471
PVoC : + 254724255242
Email : info@kebs.org
Fax : (+254 20) 6948575

| Frequently Asked Questions | Compliments and Complaints | Other KEBS contacts

chss business translation business financeaccounting managementscience economics ids idis awsc arts african-studies arabic confucius french geography history kiswahili languageskills linguistics literature philosophy politicalscience journalism psychology sociology koreanstudies dlis acfrn law-school commerciallaw privatelaw publiclaw psri caselap kisumu mombasa

Kenya Bureau of Standards
Standards for Quality life

STAFF EMAIL | TOLL FREE **0800221350**

Sample Test Results Kenya Standards Catalogue

Home About Us Standards Development Metrology Quality Assurance & Inspection Testing Services NQI Training & Membership Certification Body

ISO 9001

GET ISO 9001 CERTIFIED

Certified Firms Lists

- ⇒**ISO 9001 QMS**
- ⇒**ISO 14001 EMS**
- ⇒**ISO 27001**
- ⇒ **HACCP**
- ⇒**ISO 22000 FSMS**
- ⇒**OHSAS 18001**
- ⇒**KS 2573**
- ⇒**FSSC**
- ⇒**Suspended Firms**

Suspended Firms

- ⇒**List Firms**

Certification Policies

- ⇒ **Use Of Marks**
- ⇒ **Confidentiality**
- ⇒ **Certification Fees and Terms of Payment**
- ⇒ **Handling Audit Nonconformities**
- ⇒ **Handling Enquiries, Complaints and Appeals**
- ⇒ **Granting, Refusing, Maintaining, Renewing, suspending, Restoring, Withdrawing, Expanding and Reducing of scope of certification**
- ⇒ **Management of Impartiality**

NB: Click on the respective polices above to download.

ISO 9001:2008 Quality Management Systems

Firm Name	Postal address	Cert No	Scope of Certification	Date of Issue	Date of Expiry
Kenya Urban Roads Authority	P.O. Box 41727-00100, NAIROBI	QMS.236	Construction, maintenance and improvement of urban roads	11th June 2015	10th June 2018
Kenya Utalii College	P.O. Box 31052-00600, NAIROBI	QMS/120	Education, training, research and consultancy in tourism and hospitality	9th October 2014	8th October 2017
Kenya Water Institute	P O Box 60013-00200,NAIROBI	QMS/092	Provision of training, research and consultancy for water and sanitation sector and provision of conference services	31st March 2010	18th June 2016
Kenyatta National Hospital	P O Box 20723-00202,NAIROBI	QMS/148	Provision of Specialized Healthcare Services	2nd April 2012	23rd April 2018
KEPHIS	P O Box 49592-00100, NAIROBI	QMS/083	Agriculture regulatory services : Plant variety protection, seed certification and phytosanitary services and other support services	30th June 2009	25th August 2018
Kiambu Institute of Science & Technology	P O Box 414-00900, KIAMBU	QMS/177	Provision of Technical, Industrial, Vocational and Entrepreneurship training	7th November 2012	14th September 2018
Kibabii Diploma Teachers' Training College	P.O. Box 931-50200, BUNGOMA	QMS/256	Provision of teacher training	30th June 2015	29th June 2018
Kiirua Technical Training Institute		QMS/212	Technical Vocational Education Training (TVET)	25th June 2013	24th June 2016
Kisiwa Technical Training Institute	P.O. Box 657-50200, BUNGOMA	QMS/241	Provision of technical, industrial, vocational and entrepreneurship training	30th June 2015	29th June 2018
Kisumu Polytechnic	P O Box 143-40100, KISUMU	QMS/222	Provision of training in Science, Technology, Innovation, Research and Entrepreneurship	19th August 2013	18th August 2016
Kisumu Water and Sewerage Company	P.O.Box 3210-40100, KISUMU	QMS/157	Provision of potable water services	13thDecember 2011	15th July 2018
Kitale Technical Training Institute	P O Box 2162-30200,KITALE	QMS/153	Provision of Technical, Industrial , Vocational and Entrepreneurship Training	20th June 2012	19th June 2015
Lake Basin Development Authority	P O Box 1516-40100, KISUMU	QMS/195	Sustainable integrated community development and Extension services	14th December 2012	14th September 2018
Lake Basin Development Company	P.O. Box 7037-40100, KISUMU, KENYA	QMS/141	Rice milling and marketing carried out at the Kibos Rice Mill in Kisumu	28th June 2011	7th August 2017
Lake Victoria North Water Services Board	P.O. Box 673-50100, KAKAMEGA	QMS/091	Provision of quality and affordable water sanitation services.	20th July 2009	18th October 2018
Lake Victoria South Water Services Board	P O Box 3325-40100, KISUMU	QMS/176	Development of water and sanitation infrastructure within Lake Victoria South Water Services Board's area	28th June 2013	27th June 2016
Maasai Mara University	P.O. Box 861 - 20500, NAROK	QMS/253	Provision of university education, research, extension and consultancy services at the Main Campus	30th October 2014	29th October 2017
Machakos Teachers' Training College	P O Box 124-90100, MACHAKOS	QMS/225	Provision of Primary Teacher Training	5th September 2013	4th September 2016
Machakos University College	P O Box 136-90100,MACHAKOS	QMS/154	Provision of Higher Education	8th May 2012	3rd August 2018
Maseno University	P.O. Box Private Bag, MASENO	QMS/113	Provision of higher education, research, hotel and conferencing services	1st January 2011	26th January 2018

ISO 9001

GET ISO 9001 CERTIFIED

Certified Firms Lists

- ⇒ISO 9001 QMS
- ⇒ISO 14001 EMS
- ⇒ISO 27001
- ⇒ HACCP
- ⇒ISO 22000 FSMS
- ⇒OHSAS 18001
- ⇒KS 2573
- ⇒FSSC
- ⇒Suspended Firms

Suspended Firms

- ⇒List Firms

Certification Policies

- ⇒ Use Of Marks
- ⇒ Confidentiality
- ⇒ Certification Fees and Terms of Payment
- ⇒ Handling Audit Nonconformities
- ⇒ Handling Enquiries, Complaints and Appeals
- ⇒ Granting, Refusing, Maintaining, Renewing, suspending, Restoring, Withdrawing, Expanding and Reducing of scope of certification
- ⇒ Management of Impartiality

NB: Click on the respective polices above to download.

ISO 9001:2008 Quality Management Systems

Firm Name	Postal address	Cert No	Scope of Certification	Date of Issue	Date of Expiry
Kenya Industrial Estates Ltd	P.O. Box 78029-00507, NAIROBI	QMS/112	Development of Industrial Incubators, provision of credit and provision of business development services in Kenya	7th September 2011	30th March 2018
Kenya Industrial Property Institute	P O Box 51648-00200, NAIROBI	QMS/128	To grant Industrial Property Rights and Promote Innovation for Social and Economic Development	7th August 2013	6th August 2016
Kenya Industrial Research & Development Institute - KIRDI	P O Box 30650-00100, NAIROBI	QMS/190	Provision of Research , Technology and Innovation Services for Government and Clients	2nd October 2013	1st October 2016
Kenya Insitute of Special Education	P.O. Box 48413-00100	QMS/203	Training in Special Needs, Assessment of Children with Special Needs and Disabilities, Production of Specialized Materials and Assistive Devices and Reasearch in Special Needs	2nd April 2014	1st April 2017
Kenya Literature Bureau	P.O. BOX 30022-00100, NAIROBI	QMS/055	Sales, Marketing, Publishing and Printing of books	28th October 2007	15th December 2016
Kenya Medical Training College,	P.O. Box 30195-00100, NAIROBI	QMS/069	Training of Health Professionals	17th June 2009	14th September 2018
Kenya National Highways Authority	P O Box 49712-00100, NAIROBI	QMS/ 224	Design, Construction and Maintenance of National trunk roads (Class A, B and C)	3rd July 2013	2nd July 2016
Kenya Ordnance factories Corporation	6634-30100, ELDORET	QMS/036	Manufacture of military hardware and related products	30th September 2009	14th September 2018
Kenya Ports Authority	P.O. Box 95009, MOMBASA	QMS/087	Facilitation of sea-borne trade by providing marine operation, cargo handling and short- term warehousing services	18th March 2009	4th May 2018
Kenya Railways Corporation	P O Box 30121-00100, NAIROBI	QMS/115	Management of concession(s) and non-conceded assets, promotion, facilitation and development of metropolitan and national railway networks carried out at the KRC headquarters	20th August 2010	7th October 2016
Kenya Roads Board	P O Box 73718-00200 NAIROBI	QMS/089	Management of the Kenya Roads Board Fund and Oversight of the Rehabilitation, Development and Maintenanance of the road network in Kenya	25th June 2010	14th September 2018
Kenya Rural Roads Authority	P.O. Box 48451-00100, NAIROBI	QMS/254	Development, rehabilitation, maintenance and management of rural roads	19th June 2015	18th June 2018
Kenya Rural Roads Authority	P.O. Box 48151-00100, NAIROBI	QMS/254	Development, rehabilitation, maintenance and management of rural roads	19th June 2015	18th June 2018
Kenya School of Government	P.O. Box 23030-00604, NAIROBI	QMS/066	Provision training, research and consultancy	29th June 2012	14th September 2018
Kenya School of Law	P O Box 30369-0010,NAIROBI	QMS/101	Provision of training programme (ATP), Continuing professional development(CPD), Training of Paralegals,Provision of consultancy services and hosting of conferences and social functions	1st February 2009	14th aeptember 2018
Kenya Seed Company Ltd	P.O. BOX 553-30200, KITALE	QMS/052	Research, production, processing and distribution of certified seed	1st July 2007	6th August 2016
Kenya Tea Packers Ltd (KETEPA)	P.O. Box 413-20200, KERICHO	QMS 219	Sourcing, blending and distribution of tea, purification and bottling of drinking water and production of iced tea	8th April 2014	7th April 2017
Kenya Technical Teachers College	P O Box 44600-00100, NAIROBI	QMS/137	Provision of training services in technical teacher education and technology	13th June 2011	12th June 2017
Kenya Union of Savings and Credit Corporation Ltd	P.O. Box 28403-00200, NAIROBI	QMS/279	Provision of SACCOs through advocacy, provision of education, training, research and consultancy and provision of financial services to SACCOs	5th November 2015	4th November 2018
	P.O. Box 28403-00200, NAIROBI	QMS/279		5th November 2015	4th November 2018

Kenya Union of Savings and Credit Corporation Ltd	Provision of SACCOs through advocacy, provision of education, training, research and consultancy and provision of financial services to SACCOs

FIRST | PREVIOUS (Page 4 of 9) NEXT | LAST

Total number of firms: 175

Physical Location:
Certification Body
Kenya Bureau of Standards Headquarters
Popo Road, Off Mombasa Road
South C area, Nairobi

Postal Address:
P.O. Box 54974-00200
Nairobi
Email – General enquiries
cbstaff@kebs.org

Telephone:
Office:(254 20) 6948506

Specific Contacts
Caroline Outa
Head of the KEBS Certification Body
Tel: (254 20) 6948324/263
E-mail: outac@kebs.org

Useful links

- Codex
- PVoC
- Standards Levy
- Bio-Safety
- Non-Destructive Testing
- Banned Products
- Upcoming Training
- Entropy Login

Our services

- Standards Development and Harmonization
- Testing
- Measurments (Calibration)
- Enforcment of Standards
- Product Inspection
- Education and Training
- Management System Certification
- Product Certification
- Training Courses

Industry sectors

- Technical Committees
- Food and Agriculture
- Chemical
- Textile and Leather
- Civil
- Electrotechnical
- Mechanical
- Services
- Trade Affairs

About KEBS

- Corporate Responsibility
- Careers
- News and Events
- Press Release
- Public Notices
- Media Center
- Speeches
- Bids Tenders Expression of Interests
- Service Charter
- Complaints Contacts

Other KEBS websites

- ISO Webstore
- Notify Kenya TBT
- Car Inspection Details

Contact us

Landline : (+ 254 20)6948000
Mobile :
+ 254722202137
+ 254734600471
PVoC : + 254724255242
Email : info@kebs.org
Fax : (+254 20) 6948575

Kenya Bureau of Standards
Standards for Quality life

STAFF EMAIL | TOLL FREE **0800221350**

Sample Test Results Kenya Standards Catalogue

Home About Us Standards Development Metrology Quality Assurance & Inspection Testing Services NQI Training & Membership Certification Body

ISO 9001

GET ISO 9001 CERTIFIED

Certified Firms Lists

- ⇒ISO 9001 QMS
- ⇒ISO 14001 EMS
- ⇒ISO 27001
- ⇒ HACCP
- ⇒ISO 22000 FSMS
- ⇒OHSAS 18001
- ⇒KS 2573
- ⇒FSSC
- ⇒Suspended Firms

Suspended Firms

- ⇒List Firms

Certification Policies

- ⇒ Use Of Marks
- ⇒ Confidentiality
- ⇒ Certification Fees and Terms of Payment
- ⇒ Handling Audit Nonconformities
- ⇒ Handling Enquiries, Complaints and Appeals
- ⇒ Granting, Refusing, Maintaining, Renewing, suspending, Restoring, Withdrawing, Expanding and Reducing of scope of certification
- ⇒ Management of Impartiality

NB: Click on the respective polices above to download.

ISO 9001:2008 Quality Management Systems

Firm Name	Postal address	Cert No	Scope of Certification	Date of Issue	Date of Expiry
Gusii Institute of Technology	P O Box 222,KISII	QMS/205	Provision of traing in research, science, technology, innovation and entrepreneurial training in socio-economic development	15th May 2013	14th May 2016
H.B. Fuller Kenya Limited	P.O. BOX 134548-00800, NAIROBI	QMS/049	Manufacture ofindustrial and construction adhesives, importation and sale of industrial adhesives and provision of toll manufacturing services	19th February 2007	14th September 2018
Hass Petroleum (K) Ltd	P,O, Box 76337-00508, NAIROBI	QMS/231	Marketing of petroleum and petroleum products - LPG and lubricants in Kenya	4th August 2015	3rd August 2018
Higher Education Loans Board (HELB)	P.O. Box 69489-00400, NAIROBI	QMS/093	Provision of loans, bursaries and scholarships to Kenyan Students pursuing higher education	16th June 2009	25th June 2018
Insurance Regulatory Authority	P O Box 43505-00100,NAIROBI	QMS/186	Regulation of the insurance industry in Kenya	29th June 2012	14th September 2018
International Supply Chain Solutions Ltd	P O Box 7041-00200	QMS/100	Management services - training, consultancy, executive search and selection	14th December 2009	14th September 2018
Intertek International Tanzania	77428,DAR ES SALAAM	QMS/211	Inspection and Testing Services for Proleum, Petro-chemicals and Agricultural Products	11th September 2013	10th September 2016
Intertek Testing Services (PTY) E.A. Ltd	P.O. Box 611-80100, MOMBASA	QMS/031	Inspection and testing services for petroleum, petrochemical and agricultural products and provision of environmental services	23rd October 2008	10th November 2017
Jaramogi Oginga Odinga University of Science and Technology	P O Box 210-40601,BONDO	QMS/179	Provision of higher education, research and outreach at the main campus and Kisumu learning centre	20th June 2012	14th September 2018
Jeremiah Nyagah Technical Inst	P.O Box 1264-60100, EMBU	QMS/257	Provision of technical, industrial, vocational and entrepreneurship training	30th June 2015	29th June 2018
Jomo Kenyatta University of Agriculture and Technology	P.O. Box 62000-00200, NAIROBI	QMS/096	Provision of Higher education	29th July 2009	14th September 2018
Kaiboi Technical Training Institute	P O Box 937-30100, ELDORET	QMS/178	Provision of Technical, Industrial, Vocational and Entrepreneurship Training (TIVET)	5th September 2013	4th September 2016
Karatina University	P.O. Box 1957-10101, KARATINA	QMS/270	Provision of training, research and community outreach	30th June 2015	30th June 2018
KEMRI Production Department	P.O. Box 54840-00200, NAIROBI	QMS238	Development and production of medical devices including diagnostic kits	5th November 2014	4th November 2017
Kenya Accountants & Secretaries National Examinations Board (KASNEB)	P O Box 41362-00100, NAIROBI	QMS/187	Development of syllabuses, conduct of professional and technician examinations and certification of candidates in finance, accountancy, governance and management, information technology and related disciplines and accreditation of relevant training institutions	19th July 2013	18th July 2016
Kenya Civil Aviation Authority	P.O. Box 30163-00100, NAIROBI	QMS/107	Air navigation services and air safety security and regulation in Kenya	1st April 2011	20th April 2018
Kenya Education Management Institute	P O Box 62592-00200, NAIROBI	QMS/108	Provision of training in education management	8th November 2011	12th January 2018
Kenya Electricity Transmission Company Limited	P O Box 34942-00100, NAIROBI	QMS/182	Planning, designing, construction, operation and maintenance of electricity transmission infrastructure	10th June 2013	9th June 2016

Kenya Ferry Services Ltd	P.O. Box 96242-80110, MOMBASA	QMS/183	Provision of ferry services at Likoni and Mtongwe channels	11th December 2014	10th December 2017
Kenya Film Commission	P.O. Box 76417-00508, NAIROBI	QMS/127	To promote development of the local film industry and market Kenya as a centre of excellence in film production	13th June 2011	14th September 2018

FIRST | PREVIOUS (Page 3 of 9) NEXT | LAST

Total number of firms: 175

Physical Location:
Certification Body
Kenya Bureau of Standards Headquarters
Popo Road, Off Mombasa Road
South C area, Nairobi

Postal Address:
P.O. Box 54974-00200
Nairobi
Email – General enquiries
cbstaff@kebs.org

Telephone:
Office:(254 20) 6948506

Specific Contacts
Caroline Outa
Head of the KEBS Certification Body
Tel: (254 20) 6948324/263
E-mail: outac@kebs.org

Useful links

- Codex
- PVoC
- Standards Levy
- Bio-Safety
- Non-Destructive Testing
- Banned Products
- Upcoming Training
- Entropy Login

Our services

- Standards Development and Harmonization
- Testing
- Measurments (Calibration)
- Enforcment of Standards
- Product Inspection
- Education and Training
- Management System Certification
- Product Certification
- Training Courses

Industry sectors

- Technical Committees
- Food and Agriculture
- Chemical
- Textile and Leather
- Civil
- Electrotechnical
- Mechanical
- Services
- Trade Affairs

About KEBS

- Corporate Responsibility
- Careers
- News and Events
- Press Release
- Public Notices
- Media Center
- Speeches
- Bids Tenders Expression of Interests
- Service Charter
- Complaints Contacts

Other KEBS websites

- ISO Webstore
- Notify Kenya TBT
- Car Inspection Details

Contact us

Landline : (+ 254 20)6948000
Mobile :
+ 254722202137
+ 254734600471
PVoC : + 254724255242
Email : info@kebs.org
Fax : (+254 20) 6948575

| Frequently Asked Questions | Compliments and Complaints | Other KEBS contacts