University of Nairobi

School of Computing and Informatics

A Framework for Assessing the Insider Threat in Parastatals in Kenya.

Michael Juma Abuli

P54/79377/2015

Supervisor

Dr. Evans Anderson Kirimi Miriti

November, 2016

A Research Project Submitted in Partial Fulfillment of the Requirements of the Master of Science in Information Technology Management degree, School of Computing and Informatics, University of Nairobi

DECLARATION

I hereby declare that this research project is my original work and has not been presented or is due for presentation for any award at any learning Institution.

…………………. …………………

Signature Date

Michael Abuli Juma.

P54/79377/2015

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

……………… ……………….

Signature Date

Dr. Evans Anderson Kirimi Miriti,

School of Computing and Informatics,

University of Nairobi.

DEDICATION

I dedicate this report to the continuous awareness of insider threats and evolution of countermeasures to tackle insider threats in Kenyan Public institutions.

ACKNOWLEDGEMENTS

This project would not have been possible without the backing of many individuals and God. Firstly, I thank The Almighty for the good fortune granted to see me through this course. Sincere appreciation to my project supervisor, Dr. Evans Anderson Kirimi Miriti, for the direction and who read several alterations of this report and helped make sense of the entire study. In equal measure, I would as well like to thank all the respondents who took time to fill the questionnaires. It's through their efforts that data was collected for analysis.

Finally, many thanks to my family and numerous friends who put up with the time away from them to work on this study, always offering support and love.

ABBREVIATION AND ACRONYMS

AAA - Authentication, authorization, and accounting

BFID - Banking Fraud Investigations Department

CDSA - Common Data Security Architecture

CERT - Cybersecurity Emergency Response Team

CIA - Central Intelligence Agency

CPNI - Britain's Centre for the Protection of National Infrastructure

DLP - Data Loss Prevention

HTTP - Hypertext Transfer Protocol

HTTPS - HTTP over TLS or HTTP over SSL or HTTP Secure

IDS - Intrusion Detection System

INSA - Intelligence and National Security Alliance

IPS - Intrusion Prevention System

ITSRA - Insider Threat Security Reference Architecture

MAC address - media access control address

NIST - National Institute of Standards and Technology

NSA - National Security Agency

PwC - PricewaterhouseCoopers

SABSA - Sherwood Applied Business Security Architecture

SEM - Security Event Management

SIEM - Security Information and Event Management

SIM - Security Information Management

SME Subject-Matter Expert

ABSTRACT

Kenyan parastatals have been slow to address the insider threat problem. Nationally, recent industry surveys provide evidence that the Kenyan Banking sector followed by Kenyan Public institutions have been the hardest hit by insider attacks. Billions of shillings have been lost through insider attacks whether malicious or accidental.

The main objective of the study was to select and test an appropriate framework for dealing with the insider threat problem in Kenyan public institutions. In addition, the study was expected to advantage the Government of Kenya and its parastatals to help them mount a substantive proactive defense program against insider threats.

The study utilized a case study strategy since it investigated phenomena within its real-life context. This method also provided comprehensive grounds for generalization of data for illustrating statistical findings. Data was gathered through structured questionnaires which contained closed-ended questions. Data was then coded and tabulated to facilitate data analysis and subjected to various analyses to test hypotheses.

The main finding in this study was that controls and countermeasures of well over half of Kenyan parastatals interviewed do not have viable mitigation strategies against the insider threat problem because there were no corporate plans to counter insider threats. Consequently, sequential layers of Application, Data and Information which rely on corporate policies, have standalone controls that do not refer to the organizational policies and procedures therefore, there was no pointer to the extent of security and controls needed to be implemented at these layers.

The study recommends that Kenyan Parastatals should customize their mitigation strategies according to their organizations' goals which will enable a multi-tiered insider threat plan of action so as to tailor individual organizations' countermeasures and policies to meet its unique needs by continuous monitoring, analyzing and auditing all network, user, system activity and policy enforcements to identify abnormal behavior and usage patterns.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE INTRODUCTION

1.1 Background to Research Problem

Kitusta (2012) observed that there were few statistics on insider attacks in Kenya in 2012 because they were rarely reported to the authorities. This occurred when management of most Kenyan organizations felt that the harm from reporting insider attacks outweighs the benefit of public prosecution of the perpetrators. In 2013, insider attacks were the biggest security threats facing Kenyan organizations (Kigen et al., 2013). Not only did the scope of insider threats become heightened, the attacks developed in complexity, were much more constant and utilized witty tactics than the previous year. In the same year, Akelola (2015) says that the Banking Fraud Investigations Department (BFID) in Kenya made public the illegal entry into bank accounts between April 2012 and April 2013 that caused misplacement of 1.49 billion Kenyan Shillings belonging to bank clients. The plans were devised by bank insiders. Additionally, the report mentions that insider threat damages were elegant, taking notably a minimum of one hundred and twenty days to be discovered. A subsequent study by Kigen et al. (2015) equally recognized that at least five billion Kenyan Shillings of public funds vanished because of insider attacks, followed by the private sector with a loss of four billion Kenyan Shillings in the year 2014.

Stewart (2014) in the same manner observed that most threats came from internal sources, but too many organizations spotlighted external threat sources and diminished the internal sources. Cole (2011) notes that similarly, insider threats do not solely apply to vengeful actions, user blunders and unawareness played a major role in credible staff putting organizations at risk to external threats. Consequently, Nurse et al. (2014) points out that the increase in the insider threat scourge has brought about different frameworks for mitigating the insider threat, each with its specific view on the problem and the particular area which it desires to pacify.

1.2 Problem Statement

Insider threats continue to be an under-addressed problem. This was supported by the PwC (2014) study which stated that less than half (49%) of organizations surveyed demonstrated that they have actualized blueprints to tackle insider threats. Additionally, not more than 44 percent of respondents to the same study reported they had procedures for appraising third parties prior to involvement in business functions with them, and only 31 percent incorporate information security requirements in contract deliberations with the said external parties. Kigen et al. (2015) further elaborated that more and more insider threat frameworks have emerged through the years, however, the uptake of these frameworks in Kenyan parastatals was still a challenge.

1.3 Main Objective

The key goal of this research was to select an appropriate internal threat framework suited for the Kenyan Parastatals and to examine how parastatals in Kenya approach insider threat mitigation.

1.4 Specific Objectives

The specific goals for this research study was

1. To analyze existing insider threat frameworks.
2. To select an appropriate insider threat framework for Kenyan parastatals.
3. To examine how parastatals in Kenya approach insider threat mitigation using the selected insider threat framework.

1.5 Significance

This study was expected to benefit the Government of Kenya and its parastatals by creating awareness and building skills on insider threats to help protect vital information technology systems against the insider threat risk. The parastatals in Kenya will use this study as a reference to secure the enterprise from the insider threat problem, data loss and potential fraud.

In addition, this study has revealed that there are gaps in Kenyan legislation on insider threats, therefore there is no national guidance on the mitigation measures expected in Kenyan parastatals. Consequently, future studies should detail Kenyan legislation gaps on insider threats.

In conclusion, this study details billions of Kenyans taxpayers’ money lost through insider attacks. Highlighting insider threat mitigation techniques will lead to improved countermeasures and controls against insider threats which translates to the Kenyan citizens restoring confidence in Public institutions.

1.6 Scope

The study due to time and budget constraints will only cover Kenyan public institutions also known as parastatals. The private sector organizations have been left out. In addition, this study referred to insider threats legislation from USA and UK because there is absence of Kenyan legislation on insider threats.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

Akelola (2015) says that in 2010, Kenyan banks incurred losses of 2.5 billion shillings and the majority, 80 percent, of these activities, were committed by employees. In addition, the report mentions that recently, technologically advanced organizations were unable to discover an insider was unlawfully retrieving an unspecified large number of documents. According to Basani (2013), between 2006 and 2013, Edward Snowden was able to get unauthorized access and download sensitive data from the National Security Agency (NSA), the Central Intelligence Agency (CIA) and Dell. The author further states that the Snowden tragedy should be a forewarning to public and private enterprises to take up mitigation techniques that provide complete and continuous knowledge, programmed monitoring of vital security countermeasures to reduce insider threat risk to their enterprises. There was need for iterative monitoring, scrutiny and investigation of the entire network infrastructure, user activity, information system and policy administration to pinpoint unusual behavior and utility trends. In the recent past, Kenyan Parastatals have been worst hit by insider perpetrated attacks says Kigen (2012). 73 percent of these attacks were carried out by insiders with aid of loopholes in the ICT systems of the affected parastatals. This has led to lose of billions of shillings through insider attacks the study further states.

2.2 Insider Threat Frameworks

Ryan et al. (2013) defines an insider threat framework as some form of logical structure or model to guide an enterprise to organize information or activities to mitigate against an insider attack. An equally important definition was by the Intelligence and National Security Alliance (INSA) (2013) which explains an insider threat framework as a vigorous plan that harmonizes and interprets technical and nontechnical pointers to bring about a comprehensive view of an enterprise' insider threat risk from employees pinpointed as likely threats. Similarly, Balakrishnan (2015) characterizes an insider threat framework as a mitigation approach that contains a meticulous plan with top organizational authority support directed by policies, procedures, and controls with the main aim of reducing the risk related to insider threats to an acceptable level. The most significant aspects of the definitions to note were that the insider threat framework were structured, integrates and analyses technical and non-technical aspects and importantly the program must have senior management and all staff buy in to enable a unified glimpse of an organization's insider threat risk.

Schultz (2002) observes that programs for comprehending and anticipating insider threats would be an important step to counter insider attacks. The author argues that an approach to prediction was to identify corresponding attack affiliated symptoms from which hints can be compiled to expect and discover attacks. In contrast, Kramer et al. (2005) notes insider attacks were difficult to predict because research aimed at prediction was still at its infancy. However, Shaw et al. (2005) noted that a common factor in insider attacks was that in most cases, damage could have been prohibited by well-timed effective plans in advance of the attack. Similarly, Dark (2011), noted that it was possible to combine employee workstation and internet activity with alternate enterprise and social measurements to deduce the impulse of the potential would be insider threat and anticipate the dealings that they would perform, which may enable early classification of high risk employees. Montelibano et al. (2012) contemplates that from the time an insider makes a choice to devastate an enterprise culminating to the point at which harm is done to the same enterprise, there prevails chances for the prevention, detection, and response to the adversity.

The authors state that an enterprise should have adequate capacity to anticipate insider attacks. In absence of this, the enterprise should have competent countermeasures to discover insider threat activity. In conclusion, the enterprise should have legitimate incident response procedures to subdue the adversity arising from the perpetrator’s actions.

Additionally, according to Hancock (2016), Britain was one of the biggest targets of cyber-attack worldwide. One of the objectives of the United Kingdom's (UK) Cabinet Office in charge of Cyber Security Strategy 2011-2016 was making the UK one of the most protected technological spaces in the world to conduct business, fortify the UK to against electronic/digital attacks, help shape a clear, thriving and reliable cyberspace and to frame the UK’s cyber security capacity. Through CPNI’s work program with the University of Oxford, Britain aims to develop advice and guidance on how to aid in reduction of the risk of insider attacks. CPNI research forms part of an on-going analysis into the insider threat. It includes exploration of past insider transgresses, identifies patterns among the perpetrators and organizations involved, and suggests countermeasures to the threat. Britain's CPNI on the matter of Managing Insider Risks to Information Technology, states the key themes an insider threat program should contain namely, response plan, user data logging, understand workplace behavior, set expected behavior, create holistic processes, deter attacks, use analytical capabilities, conduct risk assessments that include insider risks, establish governance, develop effective information management, prevent by design. In contrast the Cybersecurity Emergency Response Team (CERT) Insider Threat Plan cites elements that can be utilized to fortify the insider threat mitigation procedures to include organization-wide participation, formalized and defined program, integration with enterprise risk management, insider threat practices related to trusted business partners, prevention, detection and response infrastructure, insider threat training and awareness, data collection and analysis tool, policies and procedures, protection of employee liberties and privacy rights, communication of insider threat events, insider threat incident response plan, confidential reporting procedures and mechanisms and oversight of program compliance and effectiveness.

Additionally, the primary concern in insider threat frameworks according to the Insider Threat Task Force Report (2013), was that there was no existing point of references for insider threat plans in private organizations, therefore, it was a challenge for firms to measure where they position themselves relative to their fellow sector firms in order to make preferred choices on their insider threat plan of action.

In contrast, according to United States of America's National Institute of Standards and Technology (NIST) Voluntary Framework for Improving Critical Infrastructure Cybersecurity, an insider threat framework should contain a multilayered enterprise risk administration procedures executed by the risk role. In addition, the framework should be tightly connected to enterprise structure and information security design. Furthermore, the program should spotlight application development life cycle, ordered process as well as formative and rapid implementation. With the layered risk mitigation approach, the first tier addresses risk from an organizational view with the establishment of a governance structure and enterprise risk management plan of action. The second layer involves risk from a business process angle shepherded by the risk advise from the governance layer. The third layer addresses risk from an information network infrastructure point of view and is guided by the risk decisions at layer one and layer two. Risk appetite at layer one and layer two impact the ultimate choice of and deployment of needed safeguards at the information network infrastructure. Executing the risk management framework tasks involves classification of information and systems and capturing the results in the security plan. The subsequent procedures involve selecting the security countermeasures based on the security plan. Thirdly, security controls specified in the security plan are implemented. Finally, continuous assessment of security controls involves repeated assessment of safeguards and organizational surroundings to determine the security effects of suggested and or agreed changes to the network infrastructure, applications and the organizational backdrop of operation.

According to Fischer et al. (2014), after repeated cyber intrusions into critical infrastructure by trusted insiders in the year 2013, the United States President, Barack Obama, issued an Executive Order 13636 titled “Improving Critical Infrastructure Cybersecurity”, in order to demonstrate the need for improved security of the technological space. The term critical infrastructure was used to define information assets, pivotal to a country that their corruption would have a negative impact on national safety, national welfare, a country’s information security, the economy or health, or a permutation of any the factors. The command consented various stakeholders with interagency policy coordination, periodic in-progress reviews, information sharing, civil rights protections, optional cybersecurity plans, recognition of vital information assets, forums to enable improvements, and encouragement of take up of baseline procedures to help protect vital assets. This process gave birth to the National Institute of Standards and Technology (NIST) voluntary framework for improving critical infrastructure cybersecurity.

The following discussion compared similarities and distinctions of the frameworks based on the NIST framework. The frameworks were; Framework for understanding and predicting insider attacks by Schultz (2002), Predictive Modeling for Insider Threat Mitigation Greitzer et al. (2009), Insider Threat Security Reference Architecture (ITSRA) Montelibano et al (2012) and Framework for Characterizing Attacks, Nurse et al (2014).

2.2.1 Framework for understanding and predicting insider attacks by Schultz (2002)

The framework by Schultz (2002) states that there are various possible pointers of insider threats which exist and that no one pointer can administer a satisfactory warning of an impending insider attack. The prospective pointers include; deliberate labels, significant errors, preliminary demeanor, mutual usage styles, verbal demeanor and personal qualities see figure 1. In support of the framework, an assumption was that it was feasible to express each of the possible pointers as a numerical calculation that is made up of a number of factors each with its own adjustment or emphasis. For example,

$$Ke = 1.078K1i - 0.944K2i + 0.626K3i + 0.098K4i \ldots - 1.92$$

Where

1. *K*e = is the anticipatory value. The greater its worth the greater the possibility of an insider attack.
2. *K1i, K2i, K3i, K4i* were any four chosen indicators (e.g. deliberate labels, significant errors, preliminary demeanor, mutual usage styles, verbal demeanor and personal qualities)
3. *1.078, 0.944, 0.626* and *0.098* the numbers in front of each would be their weighting in the equation.
4. –1.92 is the constant.

Although the figures here were imaginary, exact figures can be obtained by precisely scrutinizing a substantial quantity of documented insider attacks that have materialized in the existence of possible pointers, the adjusting for every pointer can be deduced.

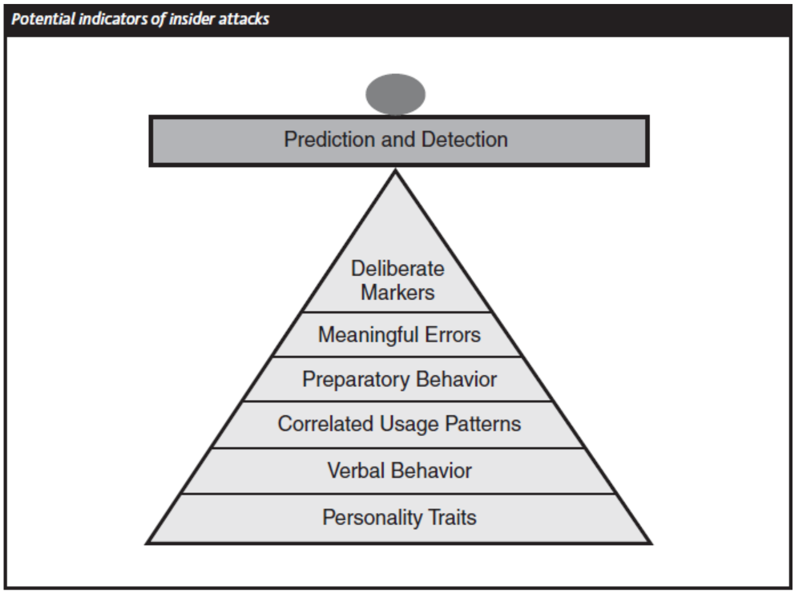


Fig 1: Framework for understanding and predicting insider attacks. Source Schultz (2002)

The framework incorporates several indicators and a mathematical portrayal of each indicator's presence, to make it conceivable to predict and detect insider attacks. The premise of the framework being no single clue was enough for envision and uncover insider attacks. Equally important, the framework can be highly personalized to fit any organization's risk appetite because the weightings against each of the indicators can be regulated accordingly.

In contrast, the framework is unproven because validation testing had not been performed on the model by its authors. There is no multi-tier organization wide risk management process associated with this framework therefore the information security architecture was standalone and did not addresses risks from an organizational perspective. There was no focus on system development life cycle. This will contravene the ultimate choosing and implementation of required countermeasures and controls at the information network infrastructure layer. The framework seems suitable for small organizations because the indicators and the mathematical equation applied to large organizations with more than 100 staff will be tedious, complex and difficult to implement and frequently update on a per staff member basis. A mistake in calculating some of the indicators and their weightings e.g. verbal behavior and personality traits could potentially cause a wrong judgement to be passed and cause resentment from an affected member of staff.

2.2.2 Predictive Modeling for Insider Threat Mitigation Greitzer et al. (2009)

The approach by this framework arises that in cases of insider threat, anticipatory capacities were utilized by uniting an insider's psychosocial information, with the traditional information security audit data. This hybrid approach creates a baseline from normal employee activities while identifying deviations from "normal" behavior as irregularity. This in turn was used as input for threat analysis. An enormous quantity of inapplicable data was examined in the conversion from data to inferences to pointers to demeanors (See Figure 2) The data were impertinent in that majority of the monitored occasions were hard to differentiate from normal chores. The Reasoner extracts and shows deviations from norms. In most cases, the priority of occurrences is important, as well as the period between occurrences. Next, it matches up prevailing pointers in summation with previously discovered pointers and demeanors to establish the probability of demeanors that are likely to manifest insider threats. The probability used by it were obtained from the investigators' knowhow of threat events. The architecture was ascertained by contrasting the yield of the reasoner to the choice of the observer describing the insider risk events.

The major gain with Predictive Modeling for Insider Threat Mitigation Greitzer et al (2009) was that it tended to be proactive as it focused on discovering harmful actions before they happen. The monitoring and analysis campaign was timely and effective as compared to A Framework for Characterizing Attacks, Nurse et al. (2014). The model was able to observe finite changes in demeanor over time to show patterns that were visible above noticeable backdrop activity which was useful in detecting the most discreet insiders hiding demeanors amongst “background noise” to escape capture.

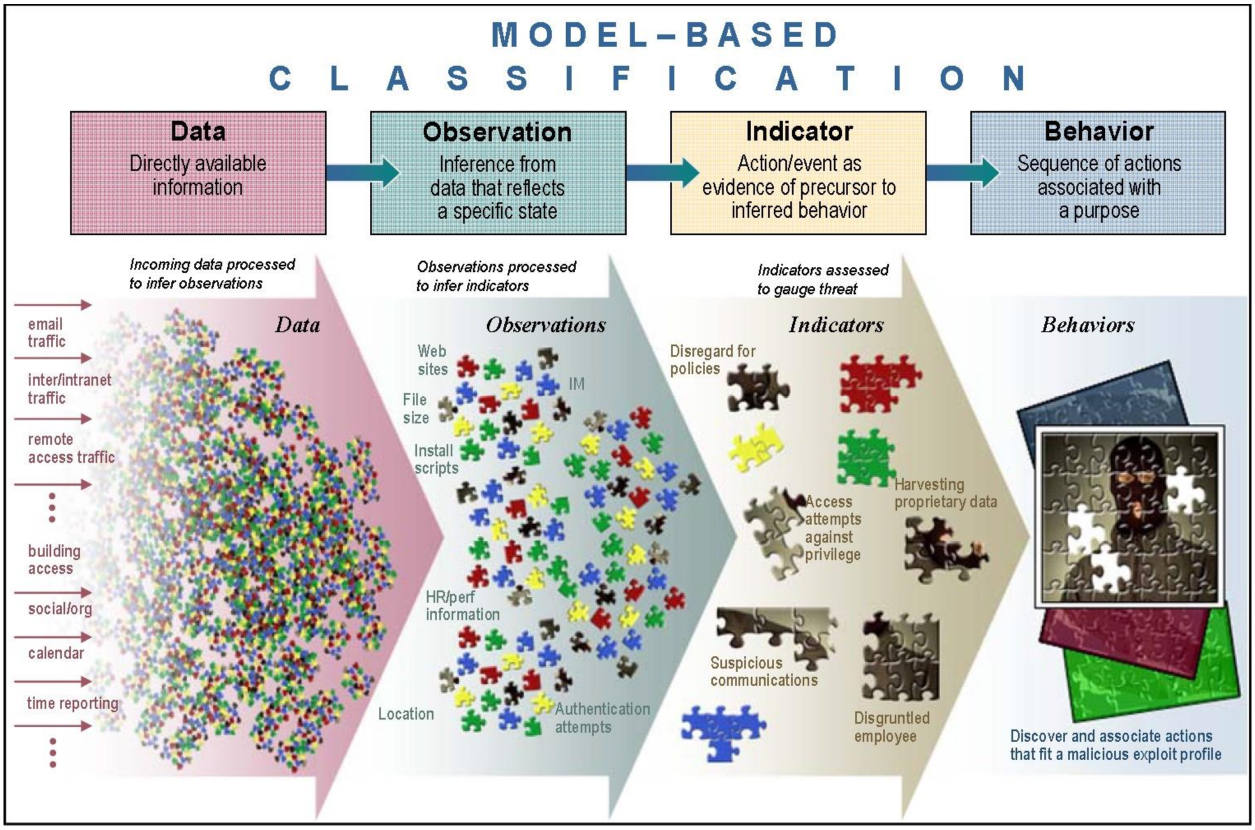

MODEL–BASED
CLASSIFICATION
Data
Directly available information
Observation
Inference from data that reflects a specific state
Indicator
Action/event as evidence of precursor to inferred behavior
Behavior
Sequence of actions associated with a purpose
Incoming data processed to infer observations
Observations processed to infer indicators
Indicators assessed to gauge threat
Data
Observations
Indicators
Behaviors
email traffic
inter/intranet traffic
remote access traffic
building access
social/org
calendar
time reporting
Web sites
IM
File size
Install scripts
HR/perf information
Location
Authentication attempts
Disregard for policies
Harvesting proprietary data
Access attempts against privilege
Suspicious communications
Disgruntled employee
Discover and associate actions that fit a malicious exploit profile

Fig 2: Model-Based Predictive Classification Concept: Source: Greitzer et al (2009)

The demerit of this framework is that the multi-tier organization wide risk management process was absent therefore risk from an organizational perspective was not incorporated within the framework. A complete corporate structure encompassing enterprise risk management plans was required in order to guide the choice of security countermeasures at the lower security levels i.e. information system level, data level and application level. In addition, another major drawback with the predictive model was that employment was established upon confidence, which is dependent upon freedom and legal rights. Although the enterprise maintains the right to conduct workstation surveillance for security decisions, there was the likelihood for lower confidence. Consequently, the procedures need to be revealed and explained through awareness across all employees. The complexity of the model increases with the number of employees of a particular organization which may lead to a large consumption amount of data for a particular predictive process. Additionally, the devastating effect of a false accusation (false positives) on an employee was a high likelihood in case the patterns were misinterpreted. There was potential for a coincidence between observable demeanor of regular versus illegal workstation conduct which may make pattern recognition a problem. Finally, data sensitivity in different legal jurisdictions in the world makes progress in this area difficult.

2.2.3 Insider Threat Security Reference Architecture (ITSRA) Montelibano et al (2012)

The framework, has a multi-tiered approach consisting of four security layers: Business, Information, Data, and Application provides a holistic solution to insider threat. At the Layer 1, Business, contains corporate business needs, such as an enterprise's strategy and also entails the formulation of policies, regulation and procedures that determines the risk appetite and eventually countermeasures to be deployed in other levels. The next layer, describes the enterprise's network infrastructure and associated components and devices. This layer also known as the information layer in addition combines the OS and software needed to administer the organization's infrastructure. Further downward, a subsequent Layer is Data which contains the organization's information assets. Finally, at the bottom layer, Application, deals with the development life cycle of software to addresses both the purchase and creation of software that contribute to the organization's strategy by ensuring that policies formulated at the corporate layer were enforced.

At each of the layer adequate controls were required in the of three security fundamentals of authorized access, acceptable use, and continuous monitoring. Implementing organizations were required to implement countermeasures at every level to tackle insider threats. The four levels were interdependent and none can function as a standalone layer because of the association of pointers and application of controls cuts across all four layers and forms the most important point of this approach see Figure 3 for Insider Threat Security Reference Architecture, Table 1 for a sample subset controls in the ITSRA framework while Figure 4 shows how the ITSRA can combine with insider attack designs to form a modified organization security plan.

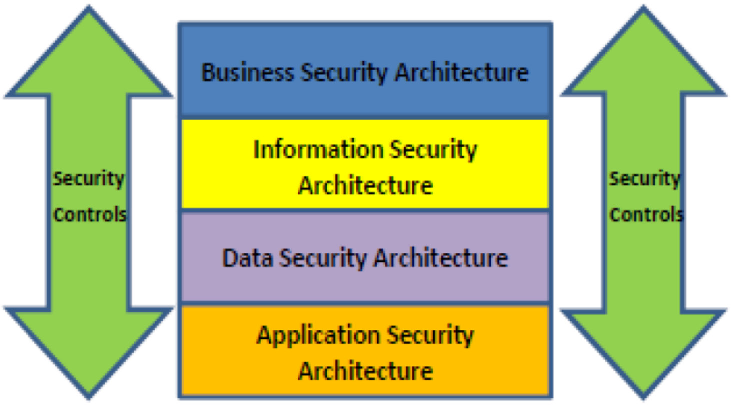
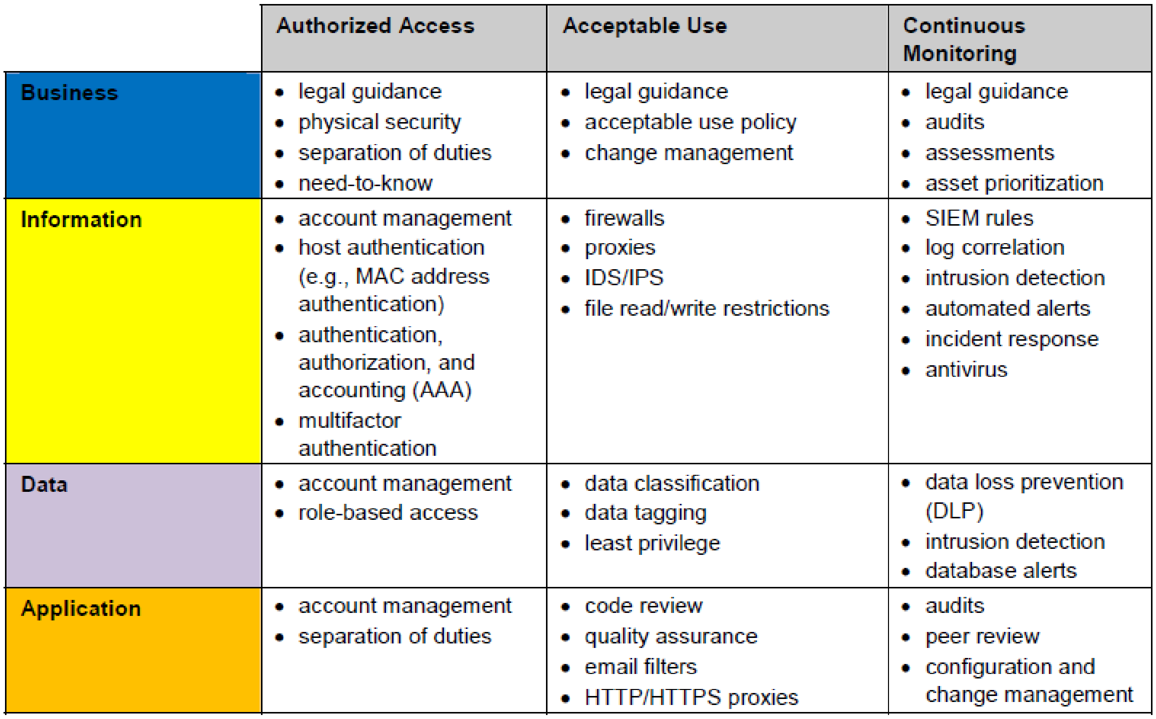

Security Controls
Business Security Architecture
Information Security Architecture
Data Security Architecture
Application Security Architecture
Security Controls

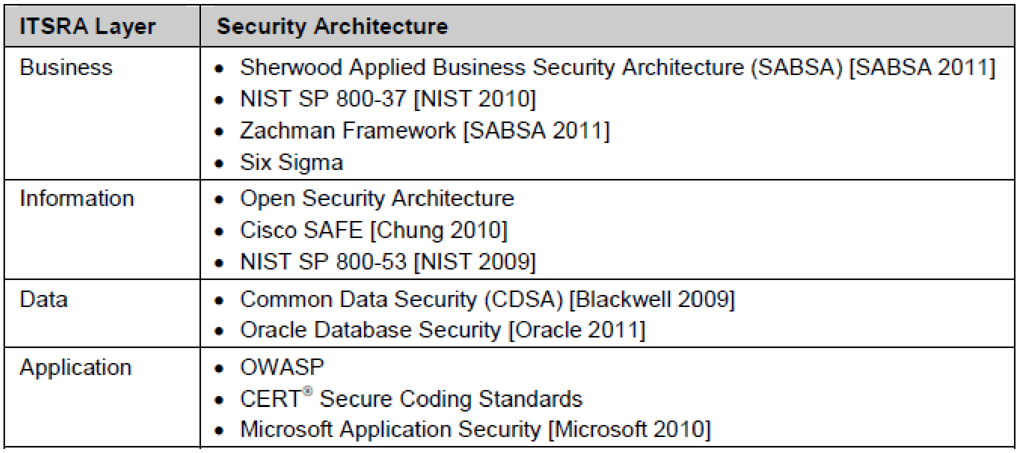
Fig 3: Insider Threat Security Reference Architecture (Montelibano & Moore, 2012).



	Authorized Access	Acceptable Use	Continuous Monitoring
Business	- legal guidance - physical security - separation of duties - need-to-know	- legal guidance - acceptable use policy - change management	- legal guidance - audits - assessments - asset prioritization
Information	- account management - host authentication (e.g., MAC address authentication) - authentication, authorization, and accounting (AAA) - multifactor authentication	- firewalls - proxies - IDS/IPS - file read/write restrictions	- SIEM rules - log correlation - intrusion detection - automated alerts - incident response - antivirus
Data	- account management - role-based access	- data classification - data tagging - least privilege	- data loss prevention (DLP) - intrusion detection - database alerts
Application	- account management - separation of duties	- code review - quality assurance - email filters - HTTP/HTTPS proxies	- audits - peer review - configuration and change management

Table 1: The ITSRA Matrix – Subset of Controls per Layer. Source: Montelibano (2012)

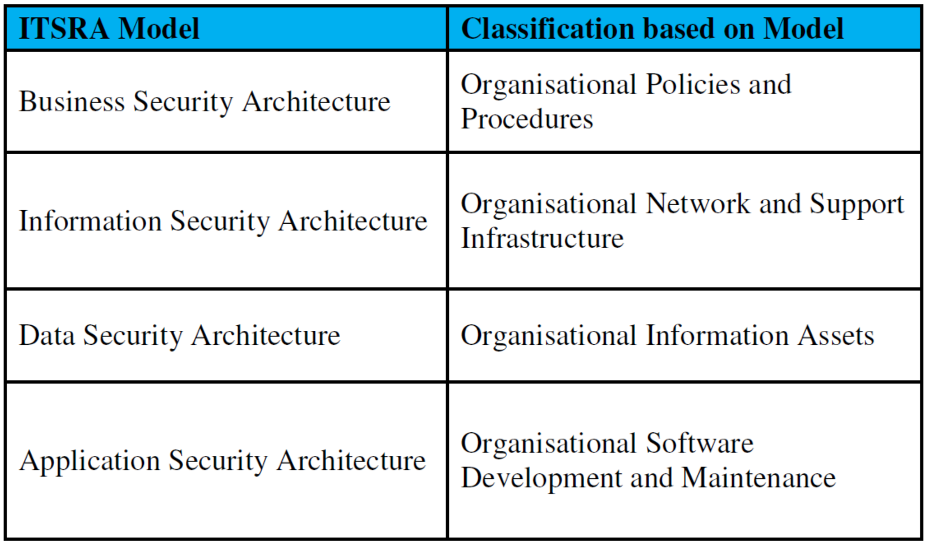
The ITSRA also describes how generally accepted practices according to security standards today that can be incorporated to generate an organization oriented insider threat plan, see Table 2.



ITSRA Layer	Security Architecture
Business	• Sherwood Applied Business Security Architecture (SABSA) [SABSA 2011] • NIST SP 800-37 [NIST 2010] • Zachman Framework [SABSA 2011] • Six Sigma
Information	• Open Security Architecture • Cisco SAFE [Chung 2010] • NIST SP 800-53 [NIST 2009]
Data	• Common Data Security (CDSA) [Blackwell 2009] • Oracle Database Security [Oracle 2011]
Application	• OWASP • CERT® Secure Coding Standards • Microsoft Application Security [Microsoft 2010]

Table 2: Security Practices. Source: Montelibano (2012)

The ITSRA framework was developed by the Software Engineering Institute under the CERT Program drawing from existing best practices and standards. In summary, ITSRA focus was on best practices and standards while the other three frameworks focus on an individual's mind set to create an insider threat program.



ITSRA Model	Classification based on Model
Business Security Architecture	Organisational Policies and Procedures
Information Security Architecture	Organisational Network and Support Infrastructure
Data Security Architecture	Organisational Information Assets
Application Security Architecture	Organisational Software Development and Maintenance

Fig 4: ITSRA Model and Classifications derived. Source Allison (2013)

The origin of ITSRA can be deduced from both the NIST [EOPUS 2007, NIST 2009] and the Federal Enterprise Architecture [CIOC 2001, EOPUS 2007] outlines Montelibano et al (2012). ITSRA uses best practices and standards where human rights, privacy and legal issues pertaining to a jurisdiction were observed during implementation of the framework. The holistic approach by

ITSRA ensures the framework covers the enterprise end to end from the multi-tier levels of Business, Information, Data and Application. Using this framework, there was a multi-tier organization wide risk management process therefore the subsequent information, data and application layers benefit from the choosing and implementation of remedies based on business goals. Focus at the Application layer was on application development life cycle as well as malleable and rapid implementation. With the layered risk mitigation method, the first level takes care of risk from an enterprise view with the formulation of holistic corporate plans and long term risk mitigation strategy while the second layer addresses risk from procedures a mission and business process and refers to the corporate layer. In conclusion the third layer addresses risk from an information infrastructure view borrowing from layer one and layer two. Furthermore, the framework can be refined and was highly modifiable at every stratum to make the corresponding safeguards fit to any enterprise willing to adopt it. At the same time an enterprise intending to implement the framework can incorporate insider threat library patterns that manifest the highest likelihood to occur against its operations and feed it to the architecture of ITSRA, the framework then offers fine suggestions at each security stratum to encompass that particular insider attack vector. Also, of great importance, the framework progresses from a broad reference plan to an instantiated organization plan with the ability to be customized to fit a specific establishment's needs. Additionally, the framework advocates intricate details by combining both routine and strategy based counsel from the insider attack library and existing generally accepted procedures to provide recommended countermeasures such as HR procedures, physical security practices, intrusion prevention system signatures, security information and event management (SIEM) rules. Last but not least, it was unquestionable that the three principles of security namely; authorized access, acceptable use, and continuous monitoring span all four layers of the framework end to end. In conclusion, the framework was a holistic approach developed by experts in a public private partnership for a unified consensus.

The framework, however, did not have an arrangement for detecting the social actions of users. The no show of the psychological status monitoring means that the framework was limited in anticipating potential threat employees in any organization.

2.2.4 A Framework for Characterizing Attacks by Nurse et al (2014)

Nurse et al (2014) came up with a framework for characterizing insider attacks based on the need to identify the elements of the insider threat problem. The diagrammatic representation resulted from constructing patterns and affiliations relating to insider threat. The framework showed in Figure 3 consisted of elements represented in four sections; insider attack catalyst, actor characteristics, attack characteristics and enterprise characteristics. In the figure, enclosed boxes were used to show the elements, continuous solid arrows define relationships between the elements however the dashed lines refer to potential relationships.

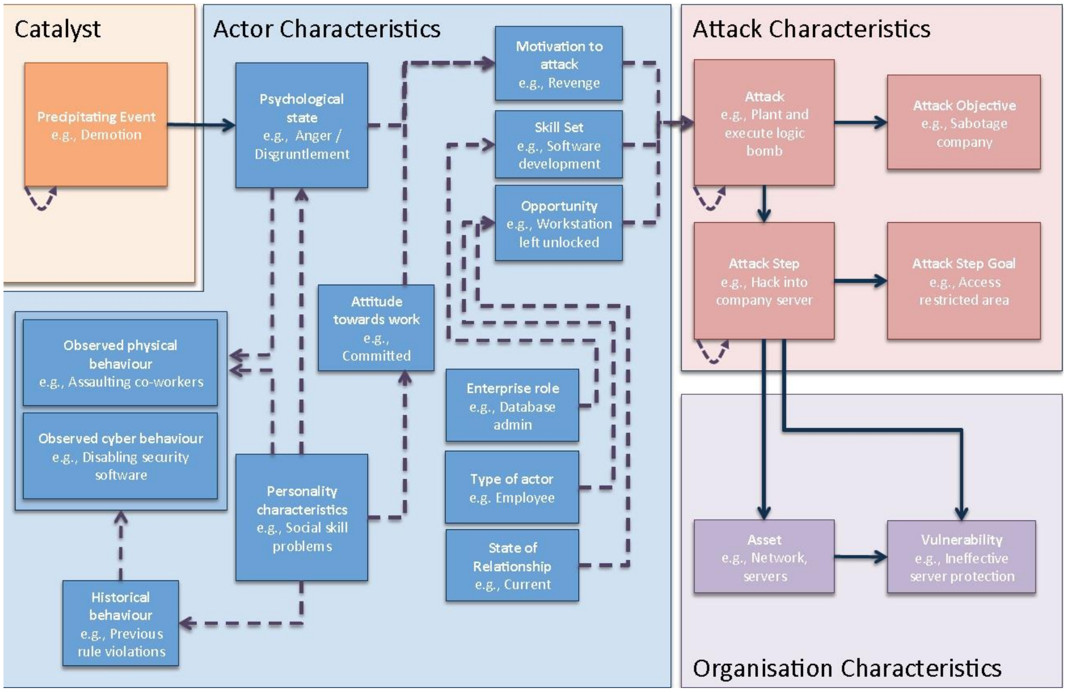


Fig 5: A Framework for Characterizing Attacks. Source: Nurse et al. (2014)

Merits for A Framework for Characterizing Attacks, Nurse et al. (2014) was that it provided a comprehensive approach of the insider threat because of its insider centric approach. In addition, the framework grants a variety of attacks to be encompasses since the actor (individual) elements were as disparate as they come. In conclusion, the framework conceded organizations to delve deeper in gaining an understanding of the environment (catalyst), the attack (system) and the organization.

The major drawback with Framework for Characterizing Attacks, Nurse et al. (2014) was that there were no multi-tier organization wide risk management process therefore subsequent layers e.g. the information security architecture was standalone and did not refer to the organizational goals. The program ignored focus on areas such as application development process, disciplined and structured process as well as flexible and agile implementation. With absence of the tiered risk management approach, risks from an enterprise view with the establishment of a holistic corporate risk management strategy were also overlooked. Ultimately, the choice of controls at the information, data and application layer were not guided by organizational risk appetite. In addition, in order for the framework to be utilized, detailed information on employees must be collected and analyzed as well as frequently updated to capture evolving threats. The gathering of such detailed information may raise privacy issues and even raise resentment from employees. A subsequent drawback was that the framework was too complex in terms of collection of employee patterns and analysis of insider threat alterations. There were several possible attack occurrences because of the links between the elements and the dashed lines to indicate future associations. Another argument was that because of its insider centric approach the framework focused too much on the actor and discounted the disclosure of the insider threat. It tended to be reactive as it focused on exposing insider attacks acts after their occurrence rather than being proactive. It consolidated on the mental make-up of an individual because focus was on the human actor as can be seen by the plenty actor characteristics. Moreover, there were several actors and did not fixate on a lone threat by the actor. This generic perspective could perhaps neglect fine particulars of an attack. Thus a change to one form of attack may not be portrayed by the framework. Finally, the framework was confusing and meant for Information Technology Security pundits to understand and implement.

2.3 Summary

In comparison the Framework by Montelibano et al (2012) drew its components from the (NIST) Voluntary Framework for Improving Critical Infrastructure in order to align insider threat practices based on business needs to integration with enterprise risk management. The reasons were detailed in the following summary.

		Schultz (2002)	**Greitzer et al. (2009)**	**Montelibano et al. (2012)**	**Nurse et al. (2014)**
1.	Framework Core details activities, references and	Has Framework Core	Has Framework Core	Has Framework Core	Has Framework Core

	outcomes in insider threat mitigation				
2.	Framework Profile (Current Organization Profile vis a vis Target Profile)	Has Framework Profile	Has Framework Profile	Has Framework Profile	Has Framework Profile
3.	Implementation levels corresponding to an organization layers (Business, Information, Data and Application)	No implementation levels	No implementation levels	Implementation levels	No implementation levels
4.	Interdependent and Coordination of Framework among organization's levels	Standalone levels	Standalone levels	Interdependent	Standalone levels
5.	Reiterative Process	Reiterative	Reiterative	Reiterative	Reiterative
6.	Profile Component to align insider threat practices based on business needs and Integration with enterprise risk management	Unaligned to business needs	Unaligned to business needs	Aligns insider threat practices based on business needs	Unaligned to business needs

Table 3: Comparison of Insider Threat Frameworks Using the NIST Voluntary Framework

Undoubtedly, all the frameworks namely Schultz (2002), Greitzer et al. (2009), Montelibano et al. (2012) and Nurse et al. (2014) had a framework core that detailed activities, references and outcomes in the respective insider threat mitigation program. However only the Framework by Montelibano et. al (2012) had a Framework Profile which specified current cybersecurity activities and the strategy to be used by the Organization in question in order to achieve the Target Profile. In addition, Montelibano et al (2012) specified implementation levels corresponding to an organization stratum (Business, Information Infrastructure, Data and Application).

At each implementation level, adequate controls were required on authorized access, acceptable use, and continuous monitoring. Implementing organizations were required to implement countermeasures at each tier to address insider attacks. In contrast, the frameworks by Schultz (2002), Greitzer et al. (2009) and Nurse et al (2014) did not have a Framework Profile therefore the implementing organization had no way to specify the Current Organization Profile and the desirable Target Profile in readiness to counter insider threats.

Furthermore, the three frameworks did not have Implementation levels corresponding to an organization's layers (Business, Information, Data and Application). There was Interdependence and Coordination of controls in the Montelibano et al (2012) Framework among organization’s levels. The Business, Information, Data and Application have controls implemented at each layer and these controls cannot work without referencing each other.

The Montelibano et. al (2012) framework specified the internal threat program as a reiterative Process that was continuous in nature. However, the implementation of the other three frameworks Schultz (2002), Greitzer et al. (2009), and Nurse et al (2014) was a one off endeavor. The reiterative process accounts for new and emerging insider threats as well as existing threats to make it a holistic framework in encompassing internal threats. Another advantage of Montelibano et al (2012) framework over Schultz (2002), Greitzer et al. (2009), and Nurse et al (2014) was that the Profile Component tended to align insider threat practices based on business needs in order to integrate insider threat mitigation with enterprise risk management.

Figure 6 shows the Conceptual Framework

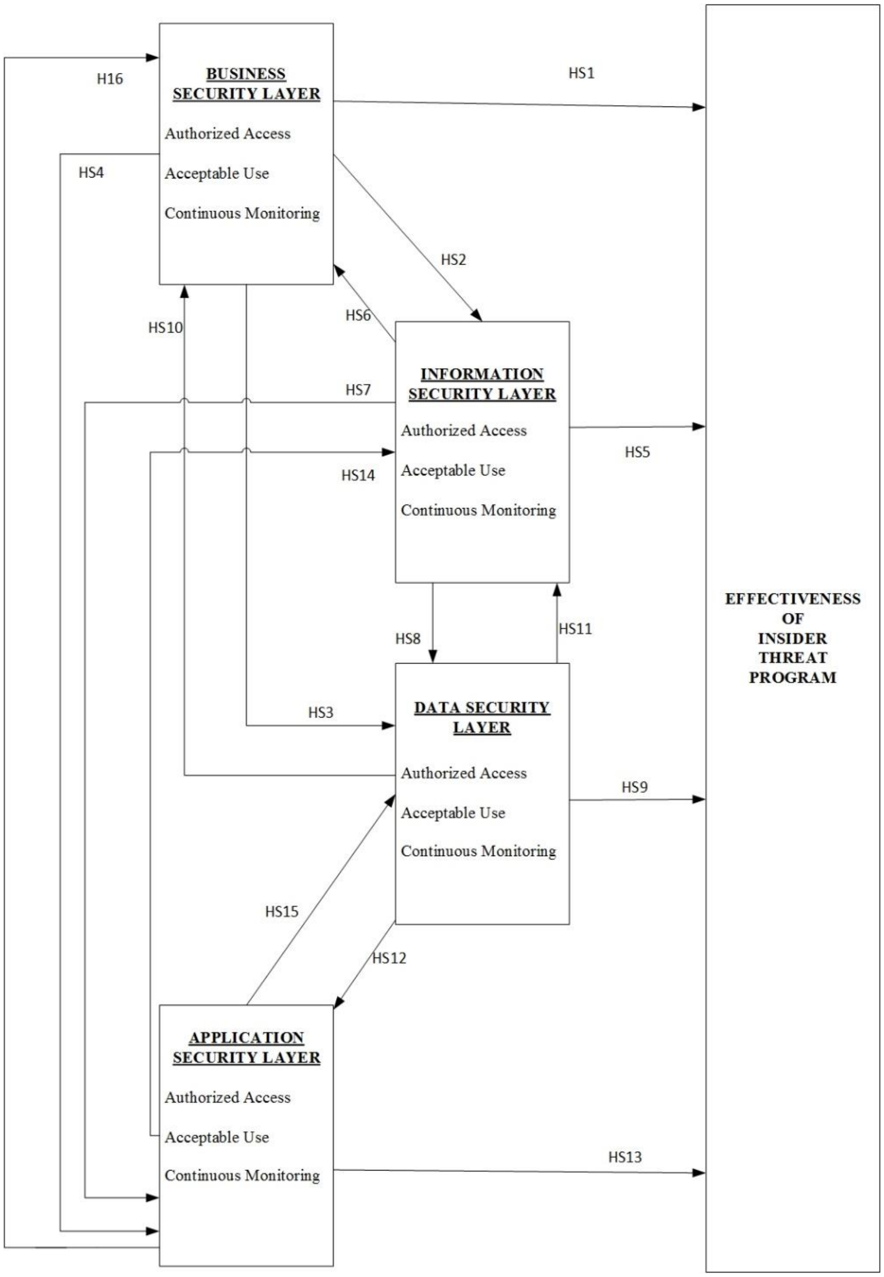


Fig 6: Conceptual Framework: Effectiveness of Insider Threat Program

2.4 Study Hypotheses

1 An appropriately structured business security layer leads to more effective insider threat program (**HS1**)

2 There is a relationship between the business security layer and the information infrastructure security layer (**HS2**)

3 There is a relationship between the business security layer and the data security layer (**HS3**)

4 There is a relationship between the business security layer and the application security layer (**HS4)**

5 An appropriately structured information security layer leads to more effective insider threat program (**HS5**)

6 For effectiveness of Insider Threat Program, the information layer refers to the Business Layer (**HS6**)

7 For effectiveness of Insider Threat Program, the application layer refers to the information layer (**HS7**)

8 For effectiveness of Insider Threat Program, the information layer refers to the data layer (**HS8**)

9 An appropriately structured data security layer leads to more effective insider threat program (**HS9**)

10 For effectiveness of Insider Threat Program, the data layer refers to the Business Layer (**HS10**)

11 For effectiveness of Insider Threat Program, the data layer refers to the information layer (**HS11**)

12 For effectiveness of Insider Threat Program, the data layer refers to the application layer (**HS12**)

13 An appropriately structured application security layer leads to more effective insider threat program (**HS13**)

14 For effectiveness of Insider Threat Program, the application layer refers to the information layer (**HS14**)

15 For effectiveness of Insider Threat Program, the application layer refers to the data layer (**HS15**)

16 For effectiveness of Insider Threat Program, the application layer refers to the business layer (**HS16**)

2.8 Operationalization

McLeod (2008) defines operationalization as the process of strictly defining variables into measurable factors. The process defines concepts and allows them to be measured, empirically and quantitatively. Operationalization defines the exact measuring method used, and allows other scientists to follow exactly the same methodology.

	Concept	Variable	Indicator	Type	Measurement
1.	Business Layer Policies	Authorized Access	• Legal advice • Physical security • Separation of duties • Need-to-know	Ordinal	Likert Scale
		Acceptable Use	• Legal advice • Acceptable use policy • Change management	Ordinal	Likert Scale
		Continuous Monitoring	• Legal guidance • Audits • Assessments • Asset prioritization	Ordinal	Likert Scale
2.	Information Layer Controls	Authorized Access	• account management • host authentication • AAA • Multifactor authentication	Ordinal	Likert Scale
		Acceptable Use	• Firewalls • Proxies • IDS/IPS • File Read/Write restrictions	Ordinal	Likert Scale
		Continuous Monitoring	• SIEM • Log correlation • Intrusion detection • Automated alerts • Incident response	Ordinal	Likert Scale

	Concept	Variable	Indicator	Type	Measurement
			• antivirus		
3.	Data Layer Controls	Authorized Access	• account management • role based access	Ordinal	Likert Scale
		Acceptable Use	• Data classification • Data tagging • Least privilege	Ordinal	Likert Scale
		Continuous Monitoring	• DLP • Intrusion detection • Database alerts	Ordinal	Likert Scale
4.	Application Layer Controls	Authorized Access	• account management • separation of duties	Ordinal	Likert Scale
		Acceptable Use	• Code review • Quality assurance • Email filters • HTTP/HTTPS proxies	Ordinal	Likert Scale
		Continuous Monitoring	• Audits • Peer review • Configuration and change management	Ordinal	Likert Scale

Table 4: Concept, Variables and Measurement of Variables

CHAPTER THREE: RESEARCH METHOD

This section comprises the research design that was employed on the study, the population and its description, data collection, analysis and the procedures.

3.1 Research Design

A combination of descriptive research and explanatory research was utilized in the study.

Saunders et al (2009), defines explanatory as a type of research where the researcher begins with developing hypotheses before collecting any data. On the other hand, the authors define descriptive research as a statistical research used to describe characteristics of the population in frequencies, averages, mean and median with the main aim of describing the data and characteristics about what is being studied.

The study implemented the survey research design model. Surveys were extensible because large data was collected from Kenyan parastatals and it described the behavior of the population as a whole and not the behavior of each parastatal in the population (Saunders, 2009). They provided information that was useful for drawing comparisons and generalizations. Primary data was collected through the use of structured questionnaires. Chief Security Officers were requested to fill in the questionnaires and in their absence Chief Information Officers executed the task. The survey contained closed ended questions to extract accurate information from the respondents. Questionnaires were preferred because they were an efficient way of gathering information from Kenyan parastatals, (Saunders, 2009). At first, the questionnaire was designed and rolled out to few members of the population for testing. This was done in order to strengthen the accuracy of data to be collected for the study. The researcher eventually rolled out the verified questionnaire using the Survey Monkey tool that collected responses online and automatically populates the responses on an online spreadsheet. See Appendix B for the survey questions that were used for the purposes aforementioned.

3.2 Population and Sampling

The participants were Kenyan government public institutions also known as state corporations or parastatals. Kenya has 262 parastatals as detailed in the Report of the Presidential Taskforce on Parastatal Reforms (2013). A sample consists of one or more elements from the population. Saunders et al (2009), describes a sample as an instance of the population of the study. Sample size was an excerpt of the population. In this study, the sample size was 32 parastatals. To calculate the proportion of parastatals that we were to be interviewed, we divided the sample size by the population size to get our sampling fraction: 32/262 = 0.12, and this meant that we were going to sample approximately 12% of the population. We also calculated the elevation factor which was 262/32 = 8, which meant that each of the parastatals interviewed represented 8 parastatals of Kenya. Therefore, the study was conducted on 32 parastatals in Kenya and the questionnaires were distributed to Chief Security Officers or their equivalent representatives in the respective parastatals.

3.3 Data Analysis

The completed questionnaires were edited for integrity and evenness. It was made ready for analysis by coding the responses. The responses were coded from strongly disagree which had a value of one to strongly agree which had a five. Since the questions on the questionnaire were based on the Likert scale, the measure used was mode, or the tall of the most frequent response for descriptive statistics. This made the survey results much easier for the researcher to interpret. Quantitative data collected were automatically analyzed by the use of frequencies and percentages utilizing the survey monkey tool. The information collected was presented using bar charts. Hypothesis were tested based on the average of the responses and to check the relationship between the variables.

3.4 Ethical Considerations

An introductory letter was composed to notify the population sample of the purpose of the research study and assured confidentiality of the responses. The questionnaire was made anonymous and as such respondents were not allowed to put down their names or those of their organizations. Personal data was not asked for this study. The filled online questionnaires were destroyed after data collection and analysis. Participation in this study was on a voluntary basis as was stated on the introductory letter, and if a respondent declined participation, another participant was chosen randomly to fill the questionnaire.

CHAPTER FOUR RESULTS AND DISCUSSION

4.1 Descriptive Statistics

The response rate was 100% since 32 respondents completed the survey which was administered in the month of August 2016 between the dates 18/08/2016 – 23/08/2016.

4.1.1 Insider Threat Controls, Policies and Procedures at the Business Layer of Kenyan Parastatals

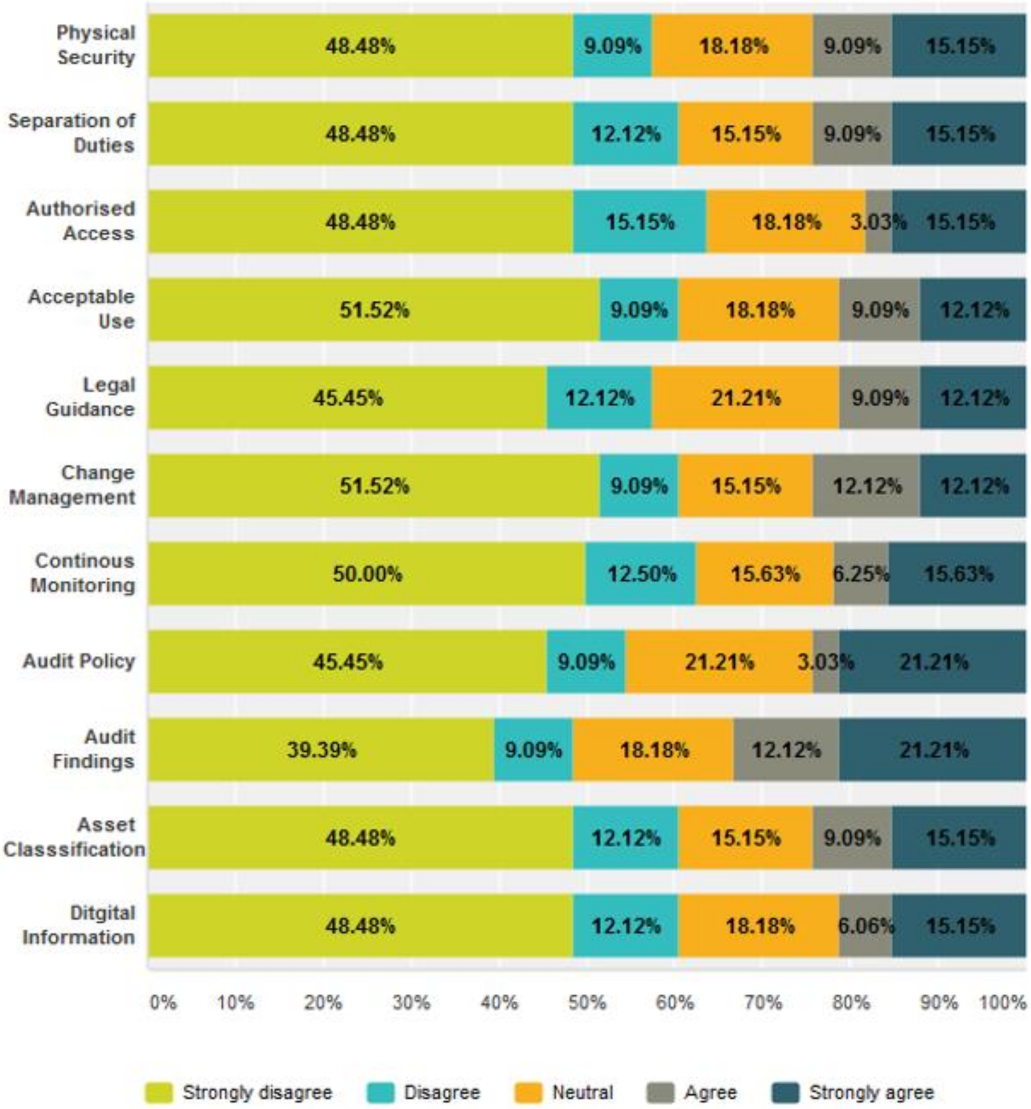


Fig 7: Findings on Insider Threat Controls, Policies and Procedure, at the Business Layer

As can be show in Figure 7, at the business application layer, 15.15 percent of the respondents felt satisfied with their organization's implementation of physical security policy, separation of duties policy and authorized access policy. In contrast, 48.48 percent which was a majority of the respondents, reported that their organizations did not have a documented, approved and implemented physical security policy, separation of duties policy and authorized access policy in their organization’s mission and objectives.

On the other hand, of the respondents interviewed, more than half (51.52 percent) depicted that they did not have a functional acceptable use policy. Legal guidance did not form a basis of drafting the policies at the business layer as shown by 45.45 percent of the respondents. An estimated 51.52 percent of respondents said that there were no change management policies at the business layer in their organization. In addition, about half of respondents indicated that a continuous monitoring policy was in not in place. 45.45 percent of respondents felt that an organizational audit policy had not been realized. In the same way, 39.39 percent of those who responded felt that results of audit findings were never looked into. In a like manner, about 48.48 percent of respondents say they had no asset classification program in place. Last but not least, an estimated 48.48 percent had an organizational policy governing generation, storage, transmission and retention periods for digital information.

The mean ranges from 2.21 the lowest which was closer to 2 for disagree to the greatest mean of 2.67 which was closer to the value of 3 for neutral. The standard deviation detailed how the responses were distributed about the mean. A smaller value indicated that more of the data was concentrated about the mean while a larger value one portrays the data were more spread out. The standard deviation in figure 8 ranges from 1.42 which was the lowest to 1.59 which was the highest. The standard deviations were less than 1.59 which indicates the responses distribution was spread very closely around the mean response allowing for accurate conclusions and inferences.

4.1.2 Insider Threat Controls, Policies and Procedures at Information Layer of Kenyan Parastatals

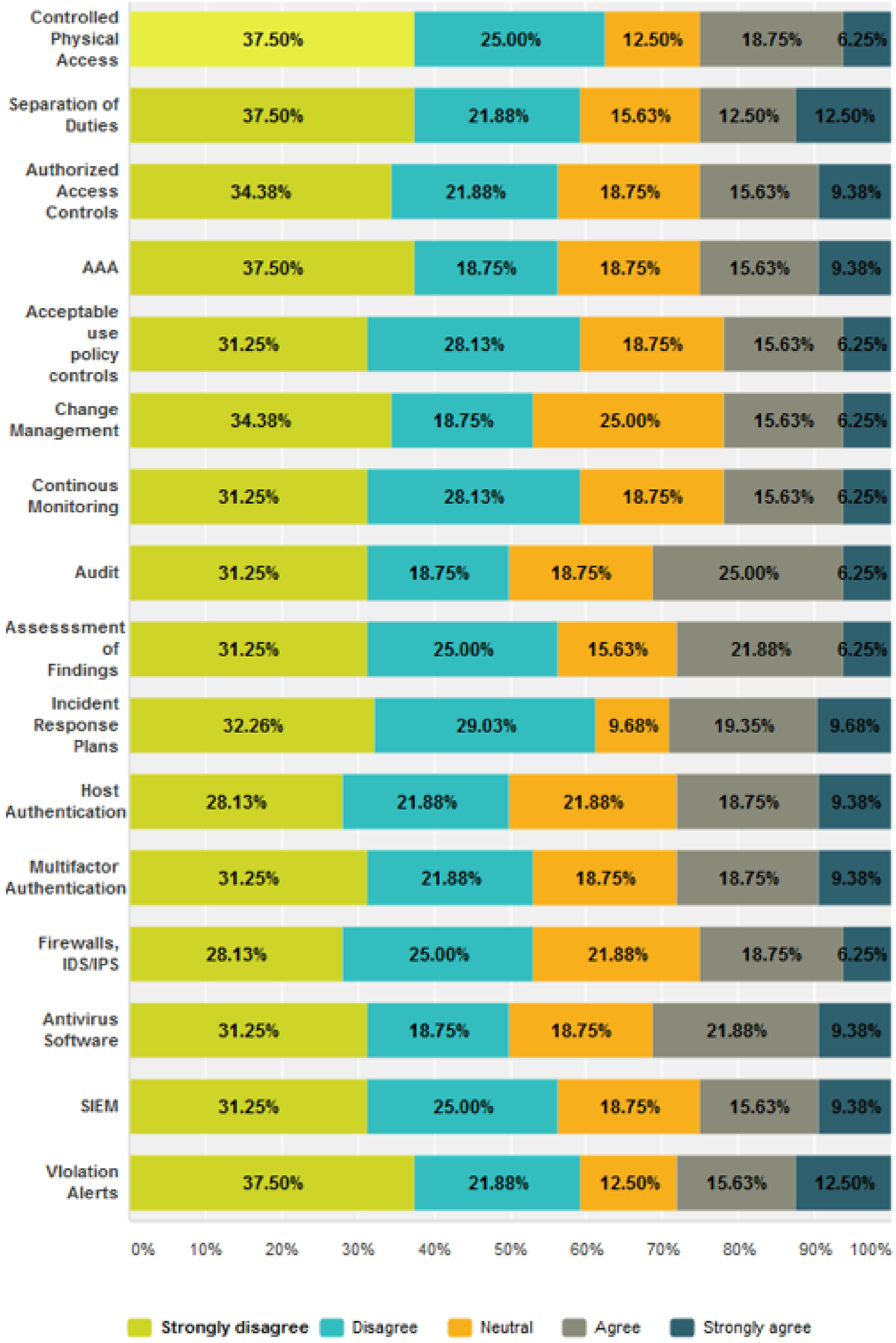


Fig 8: Findings on Insider Threat Controls, Policies and Procedures at the Information Layer

As depicted in Figure 8, respondents were asked to comment on the controls in place at the Information Infrastructure Layer and 6.25 percent strongly agreed that there were physical access controls in place in their organizations. However, 37.5 percent disapproved that the said controls were documented, approved and implemented. 12.50 percent of the respondents' organization had actualized separation of duties at the information infrastructure layer. In regards to authorized access controls and authentication, authorization, and accounting (AAA), 9.38% of respondents felt that there was execution of the controls in their organization. Furthermore, at 6.25 percent each, the minority of those who were surveyed stated that acceptable use policy, change management, continuous monitoring, audit, assessment of audit findings was part of the information infrastructure controls in their organization. Likewise, 9.38 percent of those interviewed maintained that incident response plans, host authentication, multifactor authentication, antivirus software and security information and event management (SIEM) controls had been put into effect in their respective organizations. Again, a small number (6.25 percent) of those surveyed were of the opinion that firewalls and IDS/IPS were put into practice in their organizations. Finally, 12.50 percent of respondents claimed that they had enacted automated alerts when the above controls had been violated at the information infrastructure layer.

The mean ranges from 2.31 the lowest which was closer to 2 for disagree to the greatest mean of 2.51 which was closer to the value of 3 for neutral. The standard deviation in figure 10 ranges from 1.25 which was the lowest to 1.43 which was the highest. The standard deviations were less than 1.43 which indicated the responses distribution was spread very closely around the mean response.

4.1.3 Insider Threat Controls, Policies and Procedures at the Data Layer of Kenyan Parastatals

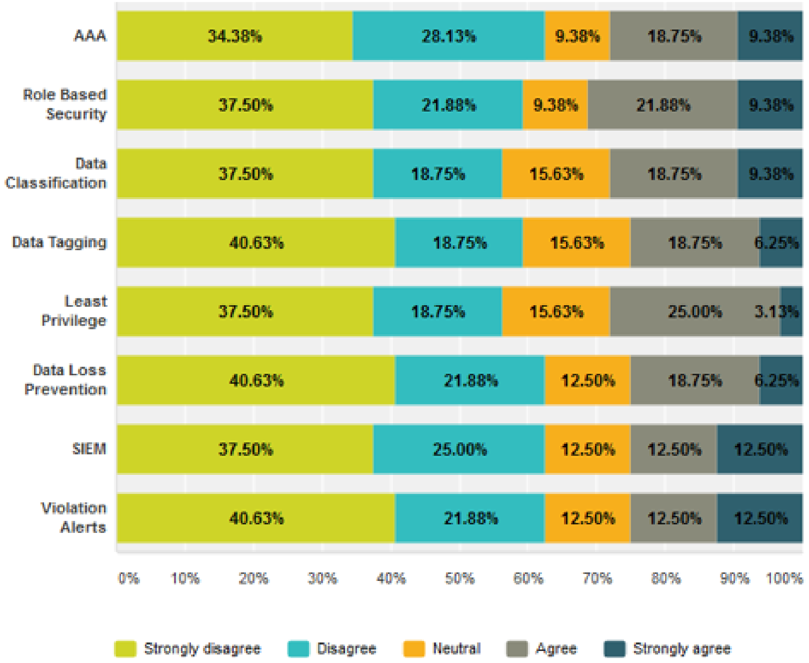


Fig 9: Findings on Insider Threat Controls, Policies and Procedures at the Data Layer

The minority (9.38 percent) of those interviewed reported that authentication, authorization, and accounting (AAA), role based security and data classification had been accomplished at the data layer of their organization. Equally important, 6.25 percent of those who responded reported that data tagging and data loss prevention was achieved by their organization. Correspondingly, 3.13 per cent of those surveyed were of the opinion that principle of least privilege was fulfilled in their organizations. Furthermore, 12.50 percent of respondents expressed that SIEM and alerts on controls violation had been applied in their respective organizations. In conclusion, this translated to weak or no policies, controls and tools to implement Authorized Access, Acceptable Use and Continuous Monitoring at the data security layer. The mean ranges from 2.31 the lowest which was closer to 2 for disagree to the greatest mean of 2.44. The standard deviation in figure 12 ranges from 1.29 which was the lowest to 1.43 which was the highest. The standard deviations were less than 1.43 which indicates the responses distribution were spread very closely around the mean response.

4.1.4 Insider Threat Controls, Policies and Procedures at the Application Layer of Kenyan Parastatals

As depicted in Figure 11, 15.63 percent of respondents' organization applied AAA at the Application Layer. Furthermore, 12.50 percent of those who were surveyed maintained that Separation of duties, Quality Assurance, Configuration management, change management controls were put into action in their organizations.

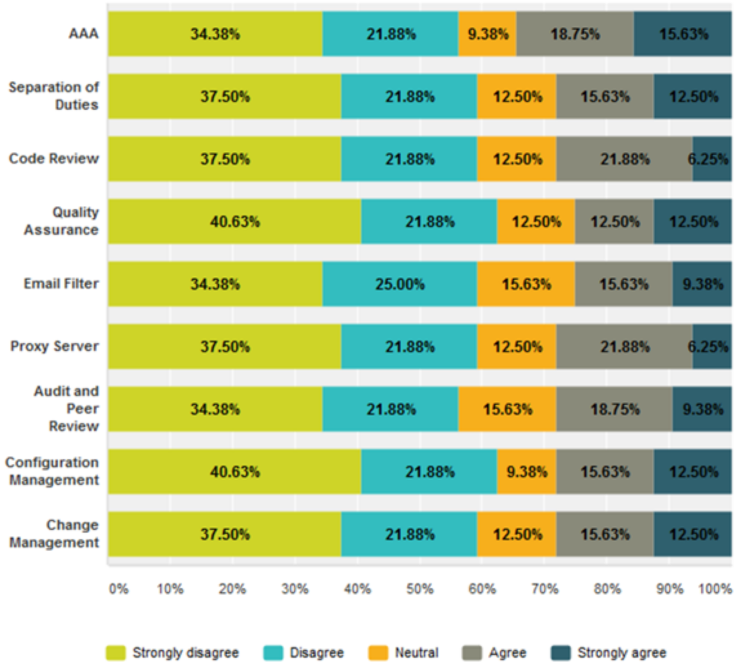


Fig 10: Findings on Insider Threat Controls, Policies and Procedures at the Application Layer

In addition, 9.38 percent claim that controls on Email Filter, Audit and Peer Review were in place. Lastly 6.25 per cent of those surveyed were of the opinion that Code review and proxy servers had been executed in their organization. In summary, this translated to weak or no policies, controls and tools to implement the three security principles of Authorized Access, Acceptable Use and Continuous Monitoring at the application security layer. The mean ranges from 2.34 the lowest which was closer to 2 for disagree to the greatest mean of 2.59 which was closer to 3 for neutral. The standard deviation in figure 14 ranges from 1.34 which is the lowest to 1.50 which was the highest. The standard deviations were less than 1.50 which indicated that the responses distribution was spread very closely around the mean response.

4.2 Hypothesis Testing

Sample size was denoted by N. The mean (µ)was calculated from sample data by finding the average value of the responses. Table 5 presents the mean, standard error of the mean and standard deviations of all the measures of the sixteen hypotheses. A mean of 3.5 was taken as the critical value where any value equal or greater than 3.5 would lead to acceptance of the hypothesis indicating that the respondents agreed or strongly agreed to the statements used in testing that hypothesis. Any value that was less than 3.5 would mean that respondents were neutral, disagreed or strongly disagreed. The critical t value was -2.132 in the one tail test. Any value below that indicated that the null hypothesis was rejected and the alternate was hence accepted

	Sample Size (N)	Mean (µ)	Standard Deviation	Standard Error Mean
HS1	32	2.2020	1.46472	.25498
HS2	32	2.4688	1.34367	.23753
HS3	32	2.4375	1.43544	.25375
HS4	32	2.4375	1.45774	.25769
HS5	32	2.3958	1.27124	.22472
HS6	32	2.4688	1.34367	.23753
HS7	32	2.4688	1.39085	.24587
HS8	32	2.4375	1.43544	.25375
HS9	32	2.3854	1.37074	.24231
HS10	32	2.4063	1.38795	.24536
HS11	32	2.4375	1.43544	.25375
HS12	32	2.3438	1.45046	.25641
HS13	32	2.3854	1.40687	.24870
HS14	32	2.3750	1.36192	.24076
HS15	32	2.4688	1.39085	.24587
HS16	32	2.3750	1.47561	.26085

Table 5: Mean, Standard deviation and standard mean error of the hypothesis

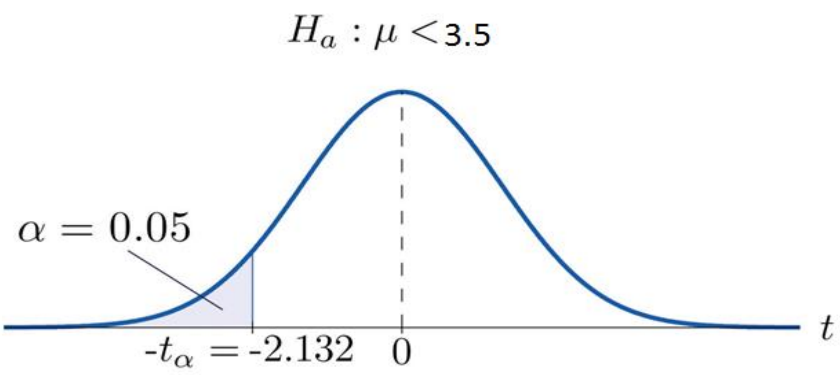


Fig 11: Hypothesis test criteria

One student t test was applied to assess all the 16 hypotheses. Results in Table 5 indicate that all the t statistics were below the critical t value of -2.132 and the differences were significant ($p < 0.05$). This hence implied that the entire sixteen hypotheses were rejected.

	Test Value = >3.5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
H1	-5.091	31	.000	-1.29798	-1.8173	-.7786
H2	-4.342	31	.000	-1.03125	-1.5157	-.5468
H3	-4.187	31	.000	-1.06250	-1.5800	-.5450
H4	-4.123	31	.000	-1.06250	-1.5881	-.5369
H5	-4.913	31	.000	-1.10417	-1.5625	-.6458
H6	-4.342	31	.000	-1.03125	-1.5157	-.5468
H7	-4.194	31	.000	-1.03125	-1.5327	-.5298
H8	-4.187	31	.000	-1.06250	-1.5800	-.5450
H9	-4.600	31	.000	-1.11458	-1.6088	-.6204
H10	-4.458	31	.000	-1.09375	-1.5942	-.5933
H11	-4.187	31	.000	-1.06250	-1.5800	-.5450
H12	-4.509	31	.000	-1.15625	-1.6792	-.6333
H13	-4.482	31	.000	-1.11458	-1.6218	-.6074
H14	-4.673	31	.000	-1.12500	-1.6160	-.6340
H15	-4.194	31	.000	-1.03125	-1.5327	-.5298
H16	-4.313	31	.000	-1.12500	-1.6570	-.5930

Table 6: One-Sample Test

The following section tested and discussed results of each hypothesis individually.

Hypothesis 1 (HS1) claimed that an appropriately structured business security layer leads to a more effective insider threat program. The mean response was 2.2020 which is less than the critical value of 3.5. Additionally, the t value is -5.091 for the hypothesis which is below the critical t value of -2.132 hence reject the hypothesis. The business layer contains policies, procedures and controls on Authorized Access, Acceptable Use and Continuous Monitoring. The significant finding is that a majority of Kenyan parastatals do not have the business layer structured with appropriate controls policies and procedures to counter insider threats. And as a consequence, the insider threat program is ineffective.

Hypothesis 2 (HS2) stated that there is a relationship between the business security layer and the information infrastructure security layer. The mean response was 2.4688 which is less than the critical value of 3.5. Additionally, the t value is -4.342 for the hypothesis which is below the critical t value of -2.132 hence rejection of the hypothesis. With this consideration, the deduction denotes that in Kenyan parastatals there is no relationship between policies, procedures and controls at the Information layer, with those at the business layer. Business layer contains enterprise wide corporate policies. This is a significant finding since controls, policies and procedures are stand alone at the information layer and do not refer to business layer. The information layer controls, policies and procedures do not have the enterprise view of risk on insiders which in turn signifies that insider threat program is ineffective amongst Kenyan parastatals.

Hypothesis 3 (HS3) detailed that there is a relationship between the business security layer and the data security layer. The mean response was 2.4375 which is less than the critical value of 3.5. Furthermore, the t value is -4.187 for the hypothesis which is below the critical t value of -2.132 and as a ramification the hypothesis is rejected. The business layer policies and controls have a comprehensive view of organization wide risk and hence data layer policies controls and procedures should be derived from the business layer in order to have an effective insider threat program. The vital finding here is that Kenyan parastatals data layer policies, procedures and controls have no relationship with those at the business layer. Business layer contains enterprise wide corporate policies and as such should be used to derive lower layer policies. With the absence of a relationship between the business security layer and the data security layer leads to an ineffective insider threat program.

Hypothesis 4 (HS4) claims that there is an association between the business security layer and the application security layer. The mean response was 2.2020 which is less than the critical value of 3.5. Additionally, the t value is -4.123 for the hypothesis which is below the critical t value of -2.132 as a result, the claim is rejected. The business layer has an overarching organization wide view of insider threat risk and as such application layer policies, controls and procedures should be derived from the business layer so that the outcome is an effective insider threat program. The critical finding here is that Kenyan parastatals' information layer has no relationship with the business layer. With absence of this relationship between the business security layer and the application layer leads to an ineffective insider threat program.

Hypothesis 5 (HS5) assertion is that an appropriately structured information security layer leads to more effective insider threat program. The mean response was 2.3958 which is less than the critical value of 3.5. Additionally, the t value is -4.913 for the hypothesis which is below the critical t value of -2.132 and as a result the hypothesis is dismissed. An appropriately structured information security layer contains policies, procedures and controls on Authorized Access, Acceptable Use and Continuous Monitoring. The important finding is that Kenyan parastatals do not have these policies, procedures and controls at the information security layer and as such chances of an effective insider threat program are reduced.

Hypothesis 6 (HS6) petitions that for effectiveness of Insider Threat Program, the information layer refers to the Business Layer The mean response was 2.4688 which is less than the critical value of 3.5. Moreover, the t value is -4.342 for the hypothesis which is below the critical t value of -2.132 effectively leading to rejection of the hypothesis. The business layer should contain overall corporate insider threat policies, controls and procedures hence information layer should derive its controls policies and procedures from the business layer in order for an effective insider threat program without which the effectiveness of the insider threat program is decreased.

Hypothesis 7 (HS7) claims that for effectiveness of Insider Threat Program, the application layer refers to the information layer The mean response was 2.4688 which is less than the critical value of 3.5. Additionally, the t value is -4.194 for the hypothesis which is below the critical t value of -2.132 hence reject the hypothesis. The finding here is that amongst Kenyan parastatals there is no relationship between the application layer and the information infrastructure layer. In essence, there is a mutually beneficial relationship between the application layer and the information infrastructure layer. The type of applications controls, procedures and policies installed at the application layer determine the type of information infrastructure layer controls, procedures and policies since the application in any organization determines the infrastructure to be installed and its respective controls, policies and procedures which leads to an effective insider threat program.

Hypothesis 8 (HS8) demands that for effectiveness of Insider Threat Program, the information layer refers to the data layer. The mean response was 2.4375 which is less than the critical value of 3.5. Additionally, the t value is -4.187 for the hypothesis which is below the critical t value of -2.132 hence rejection of the hypothesis. Based on the ITSRA framework by Montelibano (2012) the corporate network and support infrastructure controls, procedures and policies should refer to the organizational information assets policies, controls and procedures in order to streamline countermeasures against the insider threat so as to mount an effective insider threat program. However, the results show that Kenyan parastatals at the information layer, policies, controls and procedures do not refer to policies, controls and procedures at the data layer hence an ineffective insider threat program.

Hypothesis 9 (HS9) explains that an appropriately structured data security layer leads to a more effective insider threat program. The mean response was 2.3854 which is less than the critical value of 3.5. Besides, the t value is -4.600 for the hypothesis which is below the critical t value of -2.132 and as a consequence the hypothesis is rejected. The data layer should be structured with policies, controls and procedures on Authorized Access (account management, role based access) Acceptable Use (Data classification, Data tagging, Least privilege), Continuous Monitoring (DLP, Intrusion detection, Database alerts) which leads to an effective insider threat program. The major finding here is that Kenyan parastatals at the data security layer have not appropriately structured their policies, controls and procedures to lead towards an effective insider threat program.

Hypothesis 10 (HS10) For effectiveness of Insider Threat Program, the data layer refers to the Business Layer The mean response was 2.4063 which is less than the critical value of 3.5. Additionally, the t value is -4.458 for the hypothesis which is below the critical t value of -2.132 hence the results refutes the hypothesis. The significant finding is that amongst Kenyan parastatals the data layer does not refer to the business layer. The business layer should contain overall corporate insider threat policies, controls, procedures and insider threat risk appetite hence data layer should derive its controls policies and procedures from the business layer in order for an effective insider threat program without which the effectiveness of the insider threat program is diminished.

Hypothesis 11 (HS11) says that for effectiveness of Insider Threat Program, the data layer refers to the information layer. The mean response was 2.4375 which is less than the critical value of 3.5. Additionally, the t value is -4.187 for the hypothesis which is below the critical t value of -2.132 hence reject the hypothesis. The results show that Kenyan parastatals at the data layer, do not refer to information layer hence an ineffective insider threat program. Based on the ITSRA framework by Montelibano (2012) the organizational information assets controls, procedures and policies should refer to the corporate network and support infrastructure controls, procedures and policies in order to streamline countermeasures against the insider threat so as to mount an effective insider threat program.

Hypothesis 12 (HS12) claims that for effectiveness of an Insider Threat Program, the data layer refers to the application layer (HS12) The mean response was 2.3438 which is less than the critical value of 3.5. Additionally, the t value is -4.509 for the hypothesis which is below the critical t value of -2.132 hence rejection of the hypothesis. The significant finding here is that Kenyan parastatals' policies, procedures and controls on organizational information assets do not refer to organizational software development and maintenance policies, procedures and controls which according to the ITSRA by Montelibano (2012) leads to an ineffective insider threat program. This is because policies, procedures and controls need to be streamlined between the data and application layer for an organization to mount a substantive insider threat program.

The hypothesis 13 (HS13) states that an appropriately structured application security layer leads to a more effective insider threat program. The mean response was 2.3854 which is less than the critical value of 3.5. On the other hand, the t value is -4.482 for the hypothesis which is below the critical t value of -2.132 as a consequence the hypothesis is rejected. The finding presents that Kenyan Parastatals do not have controls, policies and procedures at the application layer to mount an effective insider threat program. An appropriately structured application security layer should contain policies on Authorized Access, Acceptable Use and Continuous Monitoring without which the effectiveness of the insider threat program is diminished in Kenyan parastatals.

Hypothesis 14 (HS14) For effectiveness of Insider Threat Program, the application layer refers to the information layer. The mean response was 2.3750 which is less than the critical value of 3.5. Furthermore, the t value is -4.673 for the hypothesis which is below the critical t value of -2.132 hence rejection of the hypothesis. The key finding here is that Kenyan parastatals' organizational software development and maintenance policies, controls and procedures do not refer to organizational network and support infrastructure policies, controls and procedures hence leads to an ineffective insider threat program. The application layer should refer to the information layer in order to streamline policies, controls and procedures at both layers to increase the chances of an effective insider threat program in Kenyan parastatals.

Hypothesis 15 (HS 15) state's that for effectiveness of Insider Threat Program, the application layer refers to the data layer. The mean response was 2.4688 which is less than the critical value of 3.5. Moreover, the t value is -4.194 for the hypothesis which is below the critical t value of -2.132 hence rejection of the hypothesis. The evidence suggests that Kenyan parastatals' organizational software development and maintenance policies, controls and procedures do not refer to organizational information assets policies, controls and procedures. When application layer policies, controls and procedures are not streamlined with data layer policies, controls and procedures this leads to ineffective insider threat program by the parastatal.

Hypothesis 16 (HS16) says that for effectiveness of Insider Threat Program, the application layer refers to the business layer. The mean response was 2.3750 which is less than the critical value of 3.5. Additionally, the t value is -4.313 for the hypothesis which is below the critical t value of -2.132 hence reject the hypothesis. Thusly, the results exhibit that in Kenyan parastatals the application layer controls, policies and procedures do not refer to the business layer controls, policies and procedures. This means that standalone controls, policies and procedures are implemented at the application layer that do not refer to corporate polies on insider threat mitigation. To lay emphasis on this finding, the application layer controls, policies and procedures are implemented without a view of the parastatal's organization wide risk appetite which may lead to ineffective lower lever insider threat controls, policies and procedures.

4.3 Implications of Results on Framework

The findings thus imply that Kenyan parastatals do not mount substantive insider threat mitigation endeavors based on the ITSRA framework by Montelibano (2012). This explains the high insider perpetrated attacks on Kenyan parastatals over the years. The framework does not need modification and remains the same. Kenyan parastatals need to adopt considerable mitigations efforts based on the ITSRA framework by Montelibano (2012) in order to fully characterize the insider threats problem.

4.4 Achievements

The study, based on the NIST Voluntary Framework for Improving Critical Infrastructure Cybersecurity, has analyzed existing insider threat framework namely Framework for understanding and predicting insider attacks by Schultz (2002), Predictive Modeling for Insider Threat Mitigation Greitzer et al. (2009), Insider Threat Security Reference Architecture (ITSRA) Montelibano et al (2012) and Framework for Characterizing Attacks, Nurse et al (2014). After which an appropriate insider threat framework, the Insider Threat Security Reference Architecture (ITSRA) by Montelibano et al (2012 was selected and tested how parastatals in Kenya approach insider threat mitigation using the selected insider threat framework. The research objectives have been met.

4.5 Recommendations for Practice

After testing the hypotheses, it confirms that Kenyan Parastatals at their business layer, the information layer, the data layer and the application layer do not implement the three security principles of Authorized Access, Acceptable Use and Continuous Monitoring. Furthermore, the four layers which were interdependent, since controls and policies cut across all the four layers, were implemented as standalone policies amongst Kenyan parastatals and did not refer to one another for streamlining of controls, policies and procedures between the layers.

Kenyan parastatals need to adopt a multi-tiered risk mitigation technique to develop an effective organization-wide insider threat risk management strategy. This takes care of the high level risk decisions at the business layer. Consequently, the subsequent layers of information, data and application layer should be guided by these business layer risk decisions and impact the choice of needed lower layer controls and activities which were closely associated with the enterprise architecture. In addition, there were dependencies at each layer (business, information, data and application) which allows for controls to be put in place and for a breach to be detected and fixed at any one of the layers before damage can be done. As such any security plan used by the Kenyan Parastatals must deploy countermeasures to be in place to address the insider threat vulnerability in any layer where the breach could occur. Additionally, the organization also needs a formal endeavor to ensure controls, whether they prohibit, capture, or retort, should cut across vertically through the security tiers to provide the information security. In other words, defining information security needs at the corporate level and implementing relevant controls through the other layers will positively focus the organization to counter any insider threats perfectly.

4.6 Recommendations for Further Research

Because of time and budget constraints, the study was limited to mitigation efforts by Kenyan parastatals. Future research should focus on both private and public Kenyan institutions. In addition, Kenyan legislation on insider threats is absent therefore leaves room for future investigation on measures the Government of Kenya is conducting or is planning to remedy the insider threat problem.

REFERENCES

Akelola, S. (2015). *Prosecuting Bank Fraud in Kenya: Challenges faced by the Banking Sector* Retrieved from http://www.cipfa.org/-/media/files/policy%20and%20guidance/the%20journal%20of%20finance%20and%20management%20in%20public%20services/vol%2014%20no%201/jfmps---march-2015---akelola.pdf?la=en.

Allison, D. (2013). *The insider threat problem: The case of a Jamaican government Organization*. Retrieved from http://pure.ltu.se/portal/sv/studentthesis/the-insider-threat-problem(dd596b2e-3bf8-4b8e-b0d8-a06ed81664f6).html

Balakrishnan, B. (2015). *Insider threat mitigation guidance*. Retrieved from: https://www.sans.org/reading-room/whitepapers/monitoring/insider-threat-mitigation-guidance-36307.

Basani, V. (2013). *Edward snowden and the nsa: A lesson about insider threats*. Retrieved from: http://www.bloomberg.com/news/articles/2013-07-03/edward-snowden-and-the-nsa-a-lesson-about-insider-threats.

Cole, E. (2009). *Network security bible*. John Wiley & Sons.

Dark, M., J. (2011). *Information assurance and security ethics in complex systems: Interdisciplinary perspectives*. IGI Global.

Greitzer, F. L., Paulson, P., R, Kangas, L. J., Franklin, R. L., Edgar, W. T., & Frincke, A. D. (2009) *Predictive modeling for insider threat mitigation*. Retrieved from http://www.pnl.gov/coginformatics/media/pdf/tr-pacman-65204.pdf.

Guide for applying the risk management framework to federal information systems : A security life cycle approach (2010) Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

Intelligence and national security alliance (2013): A preliminary examination of insider threat

programs in the U.S. private sector. Retrieved from http://csrc.nist.gov/cyberframework/framework_comments/20131213_charles_alsup_insa_part4.pdf

Kisutsa, C., & Shiyayo, B. *The kenya cyber security report (2012)* Retreived from

http://www.serianu.com/downloads/KenyaCyberSecurityReport2012.pdf.

Kigen, P., Kisutsa, C., Muchai, C., Kimani, K., Mwangi, M., & Shiyayo, B. *The kenya cyber security report (2014)* Retreived from http://www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf.

Kigen, P., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., Kaimba, B., Mueni,

F. & Shitanda, S. *The kenya cyber security report (2015)*. Retreived from http://www.serianu.com/downloads/KenyaCyberSecurityReport2015.pdf

Kramer, L. A., Heuer Jr, R. J., & Crawford, K. S. (2005). *Technological, social, and economic trends that are increasing US vulnerability to insider espionage*. [DTIC document]. Monterey, CA: Defense Personnel Security Research Center

Centre for the protection of national infrastructure, managing insider risks to it: Key principles. Retrieved From http://www.cpni.gov.uk/documents/publications/2016/25-april-2016-160224_cpni_insider_threat-2.pdf?epslanguage=en-gb

McLeod, S. A. (2008). *Independent, dependent and extraneous variables*. Retrieved from

www.simplypsychology.org/variables.html.

Montelibano, J., & Moore, A. (2012) *Insider threat security reference architecture* (itsra).

Retrieved from: www.sei.cmu.edu/reports/12tr007.pdf

Nurse, J. R. C., Buckley, O., Legg, P., Goldsmith, M., Creese, S., Wright G. & Whitty, M.

(2014) *Understanding insider threat: A framework for characterizing attacks*. Retrieved from https://www.cs.ox.ac.uk/files/6576/writ2014_nurse_et_al.PDF.

PwC's 2014 US state of cybercrime survey. Retrieved from: http://www.pwc.com/us/en/increasing-it-effectiveness/publications/2014-us-state-of-cybercrime.html.

Ryan M., M., Martin, T., & Martin, J., L. (2013). *Information security risk assessment toolkit:*

practical assessments through data collection and data analysis. Syngress Publishing.

Schultz, E., E.(2002) *A framework for understanding and predicting insider attacks*. Retrieved

from: www.sciencedirect.com/science/article/pii/S016740480201009X.

Shaw, E., & Sellers, L. (2005). *Application of the critical-path method to evaluate insider risks.*

Saunders, M., Lewis, P. & Thornhill, A. (2009). *Research methods for business.* Pearson.

The Kenyan constitution of 2010. Retrieved from: http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=const2010

The presidential taskforce on parastatal reforms. (2013). Retrieved from: http://www.scac.go.ke/index.php/2015-02-16-09-34-58/implementation-commitee.

APPENDIX A

LETTER OF INTRODUCTION

Dear Respondent,

I am a graduate student undertaking a Master’s degree in Information Technology Management at the University of Nairobi. I am currently carrying out a study on Framework for Countering Insider Threat to Information Systems: Case Study of Parastatals in Kenya. The information required is purely for academic research purposes and therefore the data collected is confidential. The questionnaire to be used in the study will be anonymous and as such respondents will not be allowed to put down their names. Personal data will not be asked for in this study. The filled online questionnaires will be destroyed after data collection and analysis. Participation in this study is on a voluntary basis and if a respondent declines participation, another participant will be chosen randomly to fill the questionnaire.

APPENDIX B

QUESTIONNAIRE

Section A: Business Security Layer

Please indicate your level of agreement to the statements on the table below about your organization. The rating is as follows:

1- Strongly disagree 2 – Disagree 3 – Neutral 4 – Agree 5 - Strongly agree

Statement	**1**	**2**	**3**	**4**	**5**
a. In my organization's business objectives there is a Physical Security Policy that has been documented, approved and implemented.					
b. Separation of duties Policy is in my organization's business objectives and has been documented, approved and implemented					
c. There is Legal guidance on authorized access in my organization's business objectives and has been documented, approved and implemented					
d. There is Legal guidance on acceptable use in my organization's business objectives and has been documented, approved and implemented					
e. Acceptable use policy is part of my organization's business objectives and has been documented, approved and implemented					
f. Change management Policy is part of my organization's business objectives and has been documented, approved and implemented					
g. There exists a Policy on Continuous monitoring of Information Systems and Data in my organization and has been documented, approved and implemented					

Statement	1	2	3	4	5
h. There exists an Audit Policy and is part of my organization's business objectives and has been documented, approved and implemented					
i. My organization has an Assessment of Audit Findings Policy and is part of my organization's business objectives and has been documented, approved and implemented					
j. My organization conducts Asset classification and prioritization Procedures and is part of my organization's business objectives and documented and approved					
k. There were documented, approved and implemented guidelines for ensuring the proper management of my organization's digital information.					

Section B Information Infrastructure Security layer

At the Information Infrastructure Security layer, my organization has documented, approved and implemented the below controls and procedures

Statement	1	2	3	4	5
a. Controlled Physical Access to the Information Infrastructure					
b. Implementation of Separation of duties					
c. Authorized Access Controls					
d. Account management through authentication, authorization, and accounting (AAA), file read/write restrictions					
e. Acceptable use policy controls					
f. Change management procedures					

Statement	**1**	**2**	**3**	**4**	**5**
g. Continuous monitoring policy					
h. Information Infrastructure Audit					
i. Assessment of Information Infrastructure Audit Findings					
j. Incident response plans and Disaster Recovery plans based upon Criticality and Asset Classification					
k. Host authentication (e.g., mac address authentication)					
l. Multifactor authentication (knowledge (something you know); possession (something you have), and inherence (something you are))					
m. Implementation of perimeter firewalls, proxies, IDS/IPS, intrusion detection					
n. Desktop antivirus software					
o. Real-time analysis of security alerts generated by network hardware and applications through SIEM rules, log correlation					
p. Automated alerts on violation of controls					

Section C Data Security Layer

At the Data Security layer, my organization has documented, approved and implemented the below controls and procedures

Statement	1	2	3	4	5
a. Controlled Physical Access to data storage facilities					
b. My organization has implemented account management through authentication, authorization, and accounting (AAA) in regards to access of data					
c. My organization implements role-based security by restricting data access only to authorized users (e.g. mandatory access control (MAC) and discretionary access control (DAC)).					
d. Data in our organization is categorized based on types, location, access levels implementation and protection levels in adherence to compliance regulations.					
e. Data in our organization is tagged based on sensitivity (e.g. confidential, Non-confidential, Sensitive, Very sensitive)					
f. Processes, users and programs access only the data and resources necessary for their legitimate purpose (Least privilege)					
g. My organization monitors, detects and blocks potential data breaches / data ex-filtration of sensitive data while in-use, in-motion, and in storage to ensure sensitive data is undisclosed to unauthorized personnel					
h. My organization has a security information and event management (SIEM) system that monitors the organization data traffic for malicious activity or policy violations about data (e.g. intrusion detection system (IDS), network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS))					

Statement	1	2	3	4	5
i. In my organization, there exists automated alerts that continuously monitor, analyze, record and raise alarms when the data governance policy is violated					

Section D Application Security Layer

At the Application Security layer, my organization has documented, approved and implemented the below controls and procedures

Statement	1	2	3	4	5
a. My organization has implemented disaster recovery plans for business applications					
b. My organization has implemented account management through authentication, authorization, and accounting (AAA) in regards to access of business applications					
c. My organization has implemented separation of duties in business applications					
d. My organization carries out systematic examination of business applications source code to detect and correct defects overlooked in the initial development phase, improving the overall quality of software					
e. My organization continuously checks and ensures that developed applications complies with standardized quality specifications.					
f. My organization uses software to automatically inspect incoming email for spam and computer viruses and outgoing email to ensure messages comply with appropriate laws.					
g. My organization uses a proxy server to act as an intermediary that evaluates requests, facilitates access and provides anonymity from clients seeking resources from servers.					
h. My organization carries out IT audits to examine and evaluate the organization's applications to determine whether IT controls protect corporate assets, ensure data integrity and were aligned with the business's overall goals.					

Statement	**1**	**2**	**3**	**4**	**5**
i. My organization carries out identification, maintenance, status reporting, and verification of configurable items in all business applications.					
j. My organization implements identification, impact analysis, documentation, and approval or rejecting of change requests.					

APPENDIX C
PROJECT SCHEDULE AND COST

The research period was seven months from May - November 2016. The cost elements of the research were projected to be Kshs. 110,000 to cover operational/administrative, technical and functional requirements and roles. The study was expected to take three phases.

MILESTONE	**ACTIVITIES**	**DURATION**	**ESTIMATED COST**
Phase I: Planning the research –Milestone One	Approval of research proposal	3 weeks	Ksh. 10,000
	Identify research organizational needs and requirements		
	Establish a working supervisory team/implementation committee	2 weeks	Ksh. 1,000
	Prepare written requests to participating stakeholders/ seek authority from all entities	1 week	Ksh. 10,000
Phase II: Implementation – Milestone Two	Develop procedural documents for stakeholders	1 week	Ksh.1,000
	Data collection: present questionnaires	4 weeks	Ksh. 40,000
	Tools and techniques analysis	2 weeks	Ksh. 6,000
	Development of test model	3 weeks	Ksh. 1,000
	Testing	2 weeks	Ksh. 5,000
Stage III: Monitoring, Reporting and Closure – Milestone Three	Make program adjustments where necessary	2 weeks	Ksh. 1,000
	Data analysis	3 weeks	Ksh. 30,000
	Document final report	3 weeks	Ksh. 1,000
	Evaluate research outcome	3 weeks	Ksh. 4,000
TOTAL		**24 WEEKS**	**KSH. 110,000.00**