INTERNATIONAL JOURNAL OF SOCIAL Sciences and Information Technology
ISSN 2412-0294 www.ijssit.com

http://www.ijssit.com

# A FRAMEWORK FOR EFFECTIVE INFORMATION SECURITY RISK MANAGEMENT IN KENYAN PUBLIC UNIVERSITIES

[1*] **Patrick Macharia Njoroge** *mashnjoro@yahoo.com*
[2**] **James Ogalo** *ogalojames@kisiiuniversity.ac.ke*
[3***] **Cyprian Makiya Ratemo** *makiya@kisiiuniversity.ac.ke*

[1,2,3] *School of Information Science and Technology, Kisii University, Kenya*

***Abstract****: With the universities increasingly depending on information and communication technology to execute their core operations and functionalities, their exposure to growing cyber threats is inevitable and hence unprecedented security risks. With the security risks reportedly growing day by day many universities are reported to be unable to effectively respond to or guard against them. The study objectively sought to determine the security requirements which were important for asset protection in the Kenyan public universities, establish currently implemented security practices, identify vulnerabilities and threats to assets, establish the risk control measures, and develop an effective information security risk management framework for Kenyan public universities. The target population was Kenyan public chartered universities, which were clustered into two, and simple random and purposive sampling techniques were employed for sample selection. The questionnaires were administered to the information and communication technology professionals in the universities. The results indicated that accountability and authenticity were established as strong and important security requirements to incorporate in universities security risk evaluations, with mean values of 4.62 and 4.85 respectively out of the possible value of 5 and they had high factor loading into the extracted component of 0.951 and 0.908 respectively. Further, the universities were aware of the risks they were facing, which should have informed their protection strategies and their risk mitigation plans. However, there was notable deficiency in implementation of controls, which would match the identified risks and therefore, the adoption of the proposed framework would assist universities address the deficiencies identified and reduce if not eliminate the susceptibility to the information security risks.*

***Keywords****: Information Security Risk Management, Threats, Vulnerabilities, Risks*

## 1.0 Introduction

The universities have being integrating information and communication technology (ICT) into their core operations and functionalities, which includes learning and teaching activities, communication and collaborations, research activities, innovations and developments, and information sharing activities .According to Egoeze, Misra, Maskeliunas and Damasevicius (2018), the use of ICT in educational institutions was observed to have tremendous potential to deepen skills, reinforce teaching and learning, improve engagement of students in teaching and learning activities; and provide several avenues of connection between the educational institutions and the world at large.

Moreover, with the universities increased digital reliance to execute their core operations and functionalities, the exposure to cyber threats is equally increasing, exposing the universities to unprecedented security risks (Business/Higher Education Round Table [BHERT], 2016). The security risks are growing day by day due to the increase in terms of ease, sophistication, automation and frequency of the attacks (BHERT, 2016; Wagstaff & Sottile, 2015; Pandey & Mustafa, 2012). Further, Symantec's threat report on internet security, denoted that 10 percent of all the security threats experienced were affecting the education sector (Symantec, 2015). Teng'o (2017), exposed the rise of cyber-attacks targeting to tamper with the students' academic grades, their fee balances and personal records for both students and employees, the universities affected were Kenyatta University and Jomo Kenyatta University of Agriculture and Technology.

Therefore, the security risks to the universities ICT infrastructure and information assets must be mitigated to avoid negative aftermaths such as disruption to the functioning of the universities networks and information systems, loss or damage of valuable data, fraud, and damage to universities reputation, revenue loss and disruption of critical services. The study was motivated by the need to establish effective mechanisms or framework to reduce if not eliminate the susceptibility to information security risks in Kenyan public universities.

### 1.1 Statement of the Problem

The exposure of the universities to information security risks is growing day by day, as they increasingly depend on information and communication technology to execute their core operations and functionalities. The security risks undermine the integrity, availability and confidentiality of the universities ICT systems yet many universities are reported to be unable to effectively respond to or guard against them (Wagstaff & Sottile, 2015; BHERT, 2016). Therefore, the impetus of the study is to reduce if not eliminate the susceptibility to information security risks in Kenyan public universities.

### 1.2 Objectives of the study

The specific objectives of the study were;

1. To examine the security requirements important for the protection of the assets and implemented current security practices in the Kenyan public universities.
2. To examine the vulnerabilities and threats facing the assets in use in Kenyan public universities.
3. To investigate the risk control measures implemented to protect the assets in use in Kenyan public universities.
4. To develop a framework for effective information security risk management in Kenyan public universities.

### 1.3 Conceptual Framework

The conceptual framework for the study as presented in the figure 1 below, is developed from internationally recognized industry security risk framework, namely OCTAVE and customized to the specific requirements of the public universities in Kenya. An effective information security risk evaluation should incorporate main components of risk namely threat, vulnerability and asset and OCTAVE incorporates these components hence chosen as the primary standard framework to inform the research. The framework demonstrates the interaction between the independent variables of the study, intervening variables and the dependent variable. However, due to inadequacy of the C.I.A (Confidentiality, Integrity and Availability) triangle in addressing the evolving threats in the dynamic security environment, other researchers (Cherdantseva & Hilton, 2013; Whitman &

Mattord, 2012; Pandey & Mustafa, 2012) established the need to incorporate additional security requirements for information and related assets. The framework intervening variables namely accountability and authenticity security requirements were introduced to increase the accuracy of the risk assessment. Further, the intervening variables have direct influence on the protection and mitigation strategies for the assets, thus providing the extra capability to address the evolving threats in the universities security environment and hence improved security risk management.

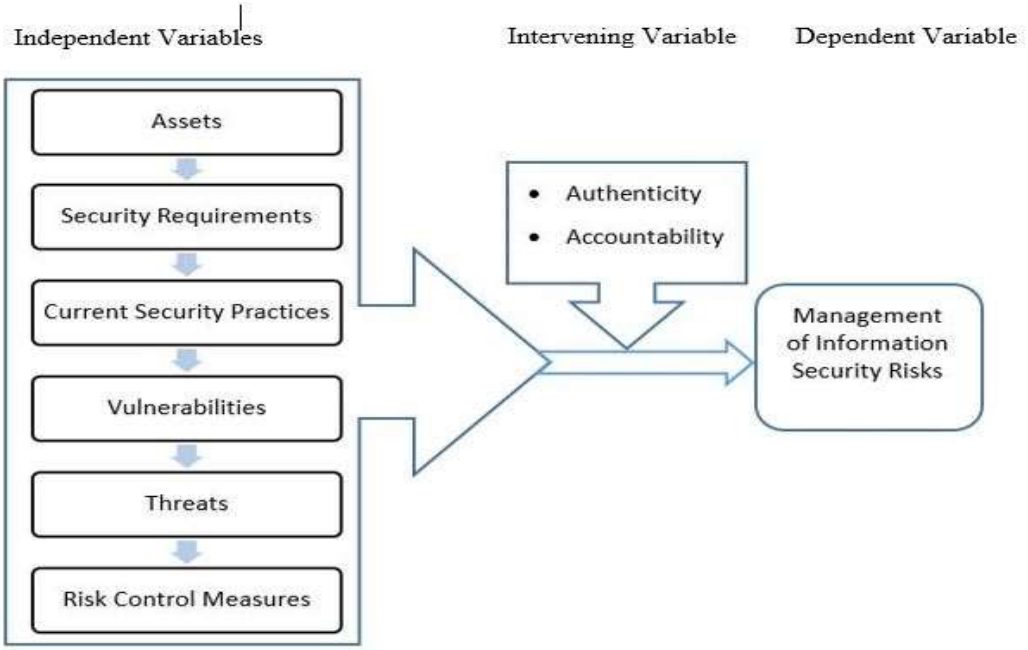


**Figure 1; Conceptual framework for the study based on OCTAVE with additional Security Requirements (Accountability and Authenticity) incorporated. Source; Alberts et al., (2003), and customized to suit the study.**

## 2.0 Review of Related Literature

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is an asset driven, risk-based and self-directed framework for evaluating information security risk within an organization whereby, all the activities and decision making pertaining to the organizational information security risks evaluation are managed and directed by the people working within that organization (Alberts & Dorofee, 2001), thus leveraging on their knowledge about the current organization security practices and processes (Pandey & Mustafa, 2012). The decisions about how to protect the information and the related assets are based on the risks to confidentiality, integrity and availability of the information and related critical assets (Alberts, Dorofee, Stevens & Woody, 2003), and this enables the organizations to match the protection strategies they employ to the security risks they face.

OCTAVE adopts a three-phased approach as discussed below.

**Phase 1:** Building Asset –Based Profiles

The phase focusses on evaluating the organization, whereby the analysis team establishes the information-related assets, which are important to the organization, and determines what the organization is currently doing to protect these important assets. Further, for each of the critical assets, the team describes the necessary

security requirements and identifies the threats to the assets and outlines any weaknesses in the organizational practices and policies (Pandey & Mustafa, 2012; Alberts et al., 2003).

**Phase 2:** Identifying Infrastructure vulnerabilities

This phase is called the technological view, and it involves evaluating the information infrastructure, whereby the key IT operational components for each critical assets are identified and the weaknesses for these components are examined (technical vulnerabilities), (Alberts & Dorofee, 2002; Pandey & Mustafa, 2012).

This phase produces two key outputs namely a list of key components and technological vulnerabilities currently, which apply to the operating systems, applications, network services and architecture.

**Phase 3:** Developing Security Strategies and Plans

In this phase, the risks facing the organization are identified, their impact evaluated, a protection strategy is developed, and necessary mitigation plans to address risks with highest priorities.

**Reasons for selecting OCTAVE to inform our Study**

The framework is well documented and leverages on the knowledge of the people within the organization thus ensuring the risks are well articulated. Further, it contributes to the risk management directly and it's very flexible. Moreover, it incorporates the necessary operational critical threats, vulnerabilities and assets in its evaluation thus increasing its accuracy in assessing the risks (Shevchenko, Chick, O'Riordan, Scanlon & Woody, 2018; Alberts & Dorofee, 2002; Pandey & Mustafa, 2012).

One weakness of the framework is that it only considers the C.I.A –triangle for risk assessment, while the accuracy of the risk assessment can be enhanced by incorporating other attributes such as Auditability, Authenticity, Accountability and Non-repudiation (Cherdantseva & Hilton, 2013; Whitman & Mattord, 2012; Pandey & Mustafa, 2012). Moreover, the methodology considers only critical assets within the risk assessment and leaves out the non-critical assets. The study builds on the strengths of OCTAVE and reinforces the accuracy of the risk assessment through introduction of the intervening variables namely authenticity and accountability security requirements. Further, the study assesses the risks to all assets within the universities.

**3.0 Review of Other frameworks**

Kimwele, Mwangi and Kimani (2011) in their study on information technology security framework for small and medium enterprises (SME) in Kenya, proposed a framework which was specifically tailored for the SMEs in Kenya, with less than 100 employees. However, universities employees exceed the threshold of a 100 employees and their operating environment is very different from the SMEs.

Kitheka (2013), proposed a framework for information security management in Kenyan public universities. The variables of the framework were derived from ISO 27001 standard and NIST special publications. Inherently, the framework put a lot of emphasis on security controls and strategies, which could jeopardize identification of threats, vulnerabilities and risks, which is supposed to inform the security controls and strategies to institute.

Wechuli, Muketha and Matoke (2014), proposed a framework for tackling the cyber security problem in Government Ministries in Kenya. However, the framework did not consider the role of management in combating cyber security threats and availability of skilled security personnel to handle the security functions and the framework did not incorporate a risk assessment methodology.

Joshi and Singh (2016), proposed a quantitative framework for information security risk assessment in universities environment based on the OCTAVE framework. The framework purely considered the C.I.A-triangle security requirements which was identified to be inadequate in handling the evolving threats in the dynamic security environment (Whitman & Mattord, 2012), while other security requirements would be essential if incorporated.

Kiura and Mango (2017), proposed a model for information systems security risk management in private chartered universities in Kenya, which was based on four pillars namely governance, people, operations and physical environment. The model was based on ISO 27001:2013. However, ISO 27001 does not provide a methodology for risk assessment, and it's incumbent upon the implementing organizations to decide on the risk method to utilize, how to assess their risks and security controls to implement, and verify that the options chosen are adequate in meeting its security needs.

Md.Sum and Md.Saad (2017) in their study on risk management in universities identified the need to develop a cost-effective risk management process, methodology or framework which can suit the university setting.

## 4.0 Gaps addressed in the Study

The review of various scholarly sources related to the study identified the following gaps;

(i) Existing security risks frameworks discussed or proposed by the researchers placed inadequate emphasis on threats, vulnerabilities and risks facing the organizations or universities, pointing to a deficiency in management of risks.

(ii) The scholarly sources were mainly concentrating on the confidentiality, integrity and availability security attributes of information and related assets, which were found inadequate in terms of addressing the evolving threats in the security environment (Whitman & Mattord, 2012: Cherdantseva & Hilton, 2013),thus calling for incorporation of other security attributes such as non-repudiation, accountability, authenticity and auditability in the security requirements to address the evolving threats which includes theft, destruction, intentional or accidental damage, unauthorized modification and other abuses from both non-human and human threats.

This study sought to fill the gaps by proposing an effective information security risk management in public universities in Kenya based on OCTAVE, customized to incorporate additional security requirements namely authenticity and accountability to improve on the ability of the universities to address the evolving threats and increase the accuracy of the risk assessment. Such a contribution in literature is highly desirable.

## 5.0 Methodology

The study was carried out in Kenyan public universities, and as per the Commission for University Education (CUE) website, there were 31 fully chartered public universities in operation in Kenya during the time of this study. The researcher employed descriptive survey method to answer the research questions, and the answers to the research questions assisted in testing the proposed framework for effective information security risks management in Kenyan public universities. The public chartered universities were clustered into two based on their actual year of establishment as fully-fledged universities. The first cluster consisted of universities established on or before the year 2001 which were six in number while the second consisted of universities established after the year 2001, which were twenty five in total (Boit & Kipkoech, 2012).

A simple random sample of two universities from each of the clusters was selected to give a total of four universities which formed our sample. The researcher employed purposive sampling to determine the

respondents for the survey from the selected universities. Therefore, the researcher gathered data from the personnel of information and communication technology and computer science departments of the selected public universities who were well versed with the context of our survey since their daily endeavors revolve around the knowledge domain of the survey that is, they deal daily with the administration, management and support of the Universities ICT infrastructure, assets and information and computing processing systems. The target sample was a 100 respondents from the universities, established after contacting the institutions' heads of ICT departments.

The questionnaires were used to collect the primary data of the study. The data was analyzed using frequency, percentages, mean, standard deviation and factor analysis while the results were presented using tables and Likert scale. The instrument of data collection used in the study namely the questionnaire, was developed and subjected to thorough expert review through my supervisors to verify that the instrument measured what it is intended to measure and a pre-test study was carried out. The researcher upheld all the ethical guidelines such as integrity and honesty, and highest levels of confidentiality were maintained throughout the research process from data collection to its presentation. The respondents provided the requested information willingly, which was in line with Kumar (2011) on seeking consent.

## 6.0 Results and Discussion

This presents the results and subsequent discussions.

### 6.1 Security Requirements of Information and related Assets

The findings tabulated in the Table 1.0 below shows that all the security requirements were rated as important with integrity having the highest mean value of 4.90. Authenticity was rated second with a mean value of 4.85 while accountability was rated as fourth with a mean value of 4.62. This implies that authenticity and accountability are desirable security requirements to incorporate into proposed framework to enhance the accuracy of the risk assessment (Cherdantseva & Hilton, 2013; Whitman & Mattord, 2012; Pandey & Mustafa, 2012) and enhance the capability to address the evolving threats in the dynamic security environment and thus address the drawback of C.I.A triangle.

**Table 1.0**

***Importance of Security Requirements***

| | Very Important | Important | Moderately Important | Slightly Important | Not Important | | |
|---|---|---|---|---|---|---|---|
| | 5 | 4 | 3 | 2 | 1 | | |
| **Security Requirement** | **Frequency** | | | | | **Mean** | **Standard Deviation** |
| Integrity | 55 | 6 | 0 | 0 | 0 | 4.9 | 0.3 |
| Authenticity | 55 | 4 | 1 | 1 | 0 | 4.85 | 0.51 |
| Confidentiality | 50 | 4 | 6 | 1 | 0 | 4.69 | 0.72 |
| Accountability | 46 | 10 | 2 | 3 | 0 | 4.62 | 0.78 |
| Availability | 40 | 15 | 6 | 0 | 0 | 4.56 | 0.67 |

### 6.2 Component Matrix

The Table 2.0 below shows the component matrix, where V1=Confidentiality, V2=Integrity, V3=Availability, V4=Accountability and V5 = Authenticity.

**Table 2.0**

***Component Matrix***

**Component Matrix[a]**

| | Component |
|---|---|
| | 1 |
| V1 | 0.947 |
| V2 | 0.939 |
| V3 | 0.888 |
| V4 | 0.951 |
| V5 | 0.908 |

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

As per the Table 2.0, authenticity portrayed a high loading (.908) into the extracted component implying that the security requirement is very strong and important to consider within the universities security risk management systems. This implies that the need to verify identify or provide proof of identity is very critical in improving the security posture of universities as it would help to address evolving threats such as spoofing attacks, where an attacker falsifies information about a target, or impersonates thus gaining unauthorized access, steals data, spreads malwares and attacks the target (Whitman & Mattord, 2012). Further, accountability portrayed a high loading (.951) into the extracted component, implying that the security requirement is very strong and important to consider within the universities security management systems. In an environment where there are increased security attacks both in terms of sophistication and scale, directed at the universities (Wagstaff & Sottile, 2015), holding the users responsible for all their actions becomes paramount. Accountability assists in tracking the happenings, accesses to information and all the resources, and traces all the actions taken and by who (National Research Council, 2014).

### 6.3 Current Security Practices

The study investigated the current security practices implemented by the Kenyan public universities and the results were tabulated as next page.

**Table 3.0**

***Current Security Practices***

| Statements | Strongly Agree | | Somewhat Agree | | Don't Know/ Unfamiliar | | Somewhat Disagree | | Strongly Disagree | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Freq. | (%) | Freq | (%) | Freq. | (%) | Freq. | (%) | Freq. | (%) |
| University Management oversees development and implementation of security policies | 6 | 9.8 | 29 | 48 | 4 | 6.5 | 12 | 20 | 10 | 16 |
| University Management supports security functions through provision of necessary funding | 6 | 9.8 | 35 | 58 | 3 | 5 | 9 | 15 | 8 | 13 |
| University Management participates in security awareness and training | 2 | 3.3 | 32 | 53 | 3 | 5 | 16 | 26 | 8 | 13 |
| University Management spearheads review of security policies | 5 | 8.1 | 22 | 36 | 3 | 5 | 16 | 26 | 15 | 25 |
| University has security policies in place | 11 | 18 | 34 | 56 | 4 | 6.5 | 6 | 9.8 | 6 | 9.8 |
| University has policies governing use of mobile devices within its systems | 8 | 13 | 23 | 38 | 8 | 13 | 12 | 20 | 10 | 17 |
| University collaborates with other government institutions by sharing its intelligence on threats and responses | 8 | 13 | 29 | 48 | 7 | 11.5 | 6 | 9.8 | 11 | 18 |
| University has incidence response plans in place | 3 | 5 | 30 | 49 | 5 | 8.1 | 8 | 13 | 15 | 25 |
| The users of the University systems do understand their roles and responsibilities in matters of cybersecurity consistent with security policies and procedures in place | 4 | 6.5 | 28 | 46 | 2 | 3.3 | 14 | 23 | 13 | 21 |
| The University Management understands their roles and responsibilities | 2 | 3.3 | 29 | 48 | 3 | 5 | 17 | 28 | 10 | 16 |
| User Awareness and Training on cybersecurity within the University is carried out periodically | 3 | 5 | 23 | 37 | 3 | 5 | 15 | 25 | 17 | 28 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 3 | 5 | 27 | 44 | 4 | 6.5 | 14 | 23 | 13 | 22 |
| The University has a training policy aimed at building capacity on cybersecurity for staff handling the security functions | | | | | | | | | | |
| Evaluation of the effectiveness of controls is carried out in the universities | 5 | 8.1 | 27 | 44 | 5 | 8.1 | 12 | 20 | 12 | 20 |
| Necessary updates and improvements on the security policies and other plans are carried out | 5 | 8.1 | 22 | 36 | 3 | 5 | 16 | 26 | 15 | 25 |

Management plays a key role in successful implementation of security risk management program within organizations or universities. 47.6% of the respondents, did somewhat agree that the university management provides support in development and implementation of security policies while a further 9.8% of the respondents did strongly agree. Further, 57.6% of the respondents, did somewhat agree that the university management supports security functions through provision of necessary funding, however 51% of the respondents indicated that the security funding/budget provided was low. Funding is very crucial in establishment of an effective security risk management system in universities as established by Wechuli, Muketha & Matoke (2014). Therefore, in Kenyan public universities more security funding or budget needs to be provided.

Further, majority of the respondents (52.5%), did somewhat agree that the university management participates in security awareness and training which is a good gesture in promoting security in the universities while only 36% of the respondents, did somewhat agree that the university management spearheads the review of the security policies which was below par. The university management should actively be involved in the review of the security policies in conformity with the best practices.

Moreover, majority of respondents, 56% somewhat agreeing while a further 18% strongly agreeing, were in agreement that universities had security policies in place, which was in agreement with research by Ogalo (2012), who found out that majority of enterprises had security policies in place. However, only 37.7% of the respondents somewhat agreed while a further 13% strongly agreed that mobile policies were implemented within the universities. This was in agreement with the findings of IBM Security (2016) that security pertaining to mobile devices in most organizations was inadequate leading to exposure to greater risks, hence the need to implement policies to govern how these mobile devices access and use resources within your network (WaterISAC ,2016).

Furthermore, despite the user awareness and training been very effective at preventing and responding to security incidents (IBM Security, 2016), most organizations were found to lack it. Wechuli et al., (2014), established that lack of user awareness and training can be an impediment to the implementation of an effective information security management system. More effort may be required towards awareness and training in universities and the frequency of the same may need to be increased.

The universities efforts to build capacity for the staff dealing with the information security functions so that they have the right skills and competences was found to be below par with only 44% of the respondents,

somewhat agreeing that the universities do build capacity for staff handling the security functions, while a further 5% of the respondents did strongly agree. In terms of executing the necessary updates and improvements on the security systems and other plans 24.7% of the respondents strongly disagreed while 26.2% somewhat disagreed that the necessary updates and improvements on the security systems and other plans are executed. These points to a weakness in the improvement of the implemented information security risk management systems in the universities, which needs to be addressed.

### 6.5 Vulnerabilities and Threats

Vulnerabilities and threats facing the universities were identified.

**Table 4.0**

***Assessment of Security Vulnerabilities***

| Statements | Strongly Agree | | Somewhat Agree | | Don't Know /Unfamiliar | | Somewhat Disagree | | Strongly Disagree | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Freq. | (%) | Freq. | (%) | Freq. | (%) | Freq. | (%) | Freq. | (%) |
| The University has an up to date assessment of its security vulnerabilities for the assets/controls | 14 | 23 | 31 | 51 | 2 | 3.3 | 9 | 15 | 5 | 8.1 |

Majority of the respondents were in agreement that the universities understood the security vulnerabilities for their assets/controls with 51% somewhat agreeing while 23% of the respondents strongly agreeing.

**Table 5.0**

***Extent of occurrence of the various types of Security Threats***

| | No Extent | Small Extent | Moderate Extent | Large Extent | Very Large Extent | | |
|---|---|---|---|---|---|---|---|
| Security Threats(s) | 1 | 2 | 3 | 4 | 5 | Mean | Standard Deviation |
| | Frequency | | | | | | |
| Viruses | 0 | 4 | 30 | 13 | 14 | 3.61 | 0.92 |
| Spam | 2 | 16 | 15 | 14 | 14 | 3.36 | 1.2 |
| Worms | 2 | 18 | 21 | 12 | 8 | 3.10 | 1.02 |
| Hacking attempts | 6 | 23 | 16 | 11 | 5 | 2.77 | 1.12 |
| Trojan horse | 6 | 23 | 21 | 10 | 1 | 2.62 | 0.93 |
| Phishing | 17 | 15 | 16 | 10 | 3 | 2.46 | 1.21 |
| Denial of Service attacks | 15 | 20 | 13 | 13 | 0 | 2.39 | 1.08 |
| Spoofing attacks | 17 | 23 | 16 | 4 | 1 | 2.16 | 0.97 |
| Ransomware | 21 | 19 | 17 | 2 | 2 | 2.10 | 1.03 |
| SQL Injections | 19 | 27 | 11 | 4 | 0 | 2.00 | 0.88 |
| Man-in-the-middle attacks | 24 | 23 | 11 | 3 | 0 | 1.89 | 0.88 |

The universities had identified the threats facing them, with the top five being viruses, spam, worms , hacking attempts and trojan horse in that order as tabulated in the Table 5.0 above . This was in agreement with Ogalo (2012), who established that virus attacks at 97% were the leading attacks in causing ICT operations disruptions in small and medium enterprises.

### 6.6 Risk Control Measures

Majority of respondents were in agreement that the universities had a risk register, identifying all risks facing their assets in use with 44% somewhat agreeing while a further 30% strongly agreeing. In terms of the risks classification based on likelihood of occurrence and their impact, 42.2% of the respondents did somewhat agree that the universities had such a classification while a further 30% of the respondents did strongly agree. In terms of the risk treatment plans, 47.6% of the respondents did somewhat agree that the universities had a risk treatment plan, while a further 27.9% of the respondents did strongly agree. This strongly indicates that the universities were aware of the risks they were facing, which should have informed their protection strategies and their risk mitigation plans.

**Table 6.0**

***Risks Identification, Classification and Treatment***

| Statements | Strongly Agree | | Somewhat Agree | | Don't Know /Unfamiliar | | Somewhat Disagree | | Strongly Disagree | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Freq. | (%) | Freq. | (%) | Freq. | (%) | Freq. | (%) | Freq. | (%) |
| University has a risk register, identifying all risks facing the universities assets. | 18 | 30 | 27 | 44 | 3 | 5 | 3 | 5 | 10 | 16 |
| Identified risks are classified based on likelihood of occurrence and impact if they occur. | 18 | 30 | 26 | 42 | 4 | 6.5 | 6 | 9.8 | 7 | 11.5 |
| University has a risk treatment plan. | 17 | 28 | 29 | 48 | 4 | 6.5 | 3 | 5 | 8 | 13 |

### 6.7 Mitigation Controls Implementation

Universities had implemented mitigation controls to mitigate the threats they were facing as per Table 7.0 below.

**Table 7.0**

***Extent of Mitigation Controls implementation***

| Mitigation Control(s) | No Extent | Small Extent | Moderate Extent | Large Extent | Very Large Extent | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | | |
| | Frequency | | | | | Mean | Standard Deviation |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Firewalls | 0 | 1 | 7 | 18 | 35 | 4.43 | 0.76 |
| Use of Proxy Servers | 2 | 2 | 7 | 13 | 37 | 4.32 | 1.03 |
| Anti-Virus Software | 0 | 2 | 8 | 20 | 31 | 4.31 | 0.83 |
| Backups | 0 | 0 | 10 | 24 | 27 | 4.28 | 0.73 |
| Application of Software Updates and Patches | 0 | 6 | 13 | 24 | 18 | 3.89 | 0.95 |
| Use of Virtual Private Networks (VPN) | 1 | 8 | 10 | 20 | 22 | 3.89 | 1.1 |
| Monitoring of Logs | 0 | 7 | 18 | 24 | 12 | 3.67 | 0.93 |
| Content Filters | 1 | 11 | 12 | 26 | 11 | 3.6 | 1.04 |
| Intrusion Detection / Intrusion Prevention Systems | 3 | 10 | 15 | 20 | 13 | 3.5 | 1.14 |
| Application Whitelisting | 3 | 12 | 25 | 13 | 8 | 3.18 | 1.06 |

The five topmost controls implemented were the use of firewalls, use of proxy servers, anti-virus software, back-ups, each implemented to a large extent, followed by use of virtual private networks and application of software updates and patches in that order each implemented to a moderate extent. However, based on the threats/attacks identified for the universities, there was notable deficiency in implementation of some controls which would match the identified risks and thus greatly improve the security posture of the universities. This controls included intrusion detection / intrusion prevention Systems (IDS/IPS), software patching and updates, use of content filters, monitoring of logs and application whitelisting which would need to be enforced to a large extent.

### 6.8 Proposed Framework for Effective Information Security Risk Management in Kenyan Public Universities

The proposed framework was developed from internationally recognized industry security risk framework, namely OCTAVE and customized to the specific requirements of the public universities in Kenya with additional security requirements incorporated namely accountability and authenticity to meet the complexities and increase the accuracy of the risk assessment. Other security best practices incorporated on the proposed framework are derived from the ISO 27001:2013 and NIST cybersecurity framework.

However, due to inadequacy of the C.I.A (Confidentiality, Integrity and Availability) triangle in addressing the evolving threats in the dynamic security environment, other researchers (Cherdantseva & Hilton, 2013; Whitman & Mattord, 2012; Pandey & Mustafa, 2012) established the need to incorporate additional security requirements for information and related assets. The framework incorporated the intervening variables namely accountability and authenticity in the security requirements to increase the accuracy of the risk assessment. Authenticity and accountability were observed to have direct influence on the protection and mitigation strategies for the assets, thus providing the extra capability to address the evolving threats in the universities security environment and hence improved security risk management.

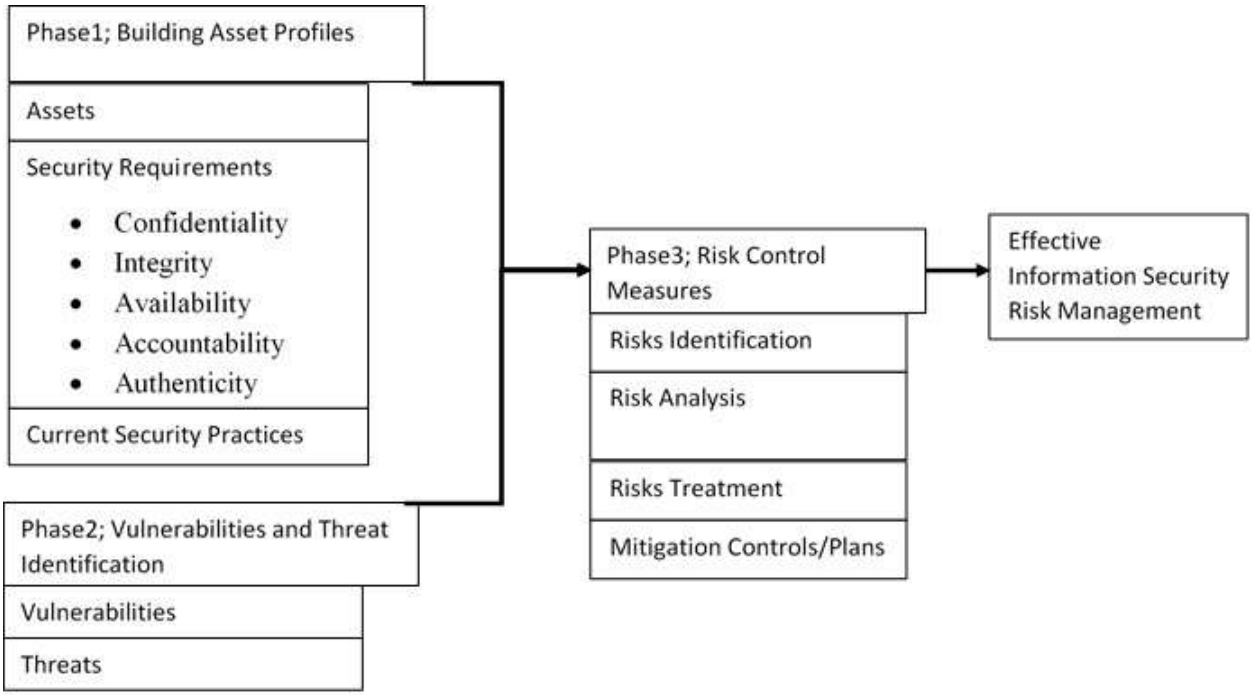


**Figure 2; Proposed Framework based on OCTAVE with additional Security Requirements (Accountability and Authenticity) incorporated.**

**Source; Alberts et al., (2003), and customized to suit the research.**

### 6.9 Variables of the framework

The framework demonstrates the interaction between the independent variables of the study and the dependent variable as shown below in Table 8.0. The variables are derived from OCTAVE risk management framework, while other security practices are incorporated from the ISO 27001:2013 and NIST cybersecurity framework.

**Table 8.0**

***Variables of the Proposed Framework***

| **Phase** | **Independent Variables (Industry Security Best Practices)** | **Information Security Risk Management (ISRM) Objective** |
|---|---|---|
| 1 – Building Asset Profiles | Assets | Effective Information Security Risk Management |
| | Security Requirements ;<br>• Confidentiality<br>• Integrity<br>• Availability<br>• Accountability<br>• Authenticity | |
| | Current Security Practices<br>• Awareness and Training<br>• Frequency of awareness and training | |

| | | |
|---|---|---|
| | • Skills & Competence<br>• Security Policies<br>• Collaboration and Intelligence Sharing<br>• Review of Security Policies<br>• Evaluation of Controls<br>• Updates & Improvements<br>• Provision of security funding<br>• Incidence Management<br>• Mobile Policies | |
| 2-Identification of Vulnerabilities and Threats | Vulnerabilities | |
| | Threats | |
| 3- Risk Control Measures | Identification of Risks | |
| | Risk Analysis | |
| | Risk Treatment | |
| | Mitigation Control/Plans | |

**(a) Building Asset Profiles**

This begins with making an inventory of all the assets, technologies and systems in use, which are utilized in the performance of the core operations and functionalities within the universities. This conforms to the OCTAVE output R01.1 and further in line with ISO 27001:2013 control objectives A.8.1.1, A.8.1.2 and A.8.2.1, and NIST cybersecurity framework category ID.AM. This is very crucial because you cannot protect what you have not identified as valuable and critical in enabling you to meet your goals and objectives.

Secondly, the security requirements of the primary and supporting assets are determined. The security requirements considered by default in most systems are confidentiality, integrity and availability. However, to enhance the capability of our framework to address evolving threats and increase the accuracy of the risk assessment, additional security requirements namely accountability and authenticity are incorporated.

Thirdly, current catalog of security practices implemented by the universities or organizations to protect their assets, need to be established and compared against the set catalog of practices in the industry security standards. By so doing, any gaps or missing interventions can be identified and necessary remedial actions taken. This conforms to the OCTAVE output R01.4. Control Objective A.5 of ISO 27001, requires the management to provide necessary support and direction in the development, approval and implementation of security policies within their organizations. The same control objective requires that the security policies established be reviewed to guarantee their continued suitability and effectiveness. Further, it's incumbent upon the management to provide necessary resources including funding for establishment of an effective security management system as per clause 5.1(c) of ISO 27001. NIST cybersecurity framework subcategory PR.AT-4, requires senior management to participate in awareness and training so that they understand their roles and

responsibilities and be able to set the tone for security in their organizations from the top. Without the Management Support, the information security risk management may not achieve its objective.

NIST cybersecurity framework subcategory PR.AT and ISO 27001:2013 control objective A.7.2.2 recognizes the need to train all the users of the systems so that they understand their roles and responsibilities. This includes normal users, privileged user, third-party stakeholders (such as partners, suppliers and customers) and the senior management who are supposed to set the tone for security in their organizations from the top.

User awareness is critical in addressing the threat of cybersecurity, since it provides the necessary guidance to users on cybersecurity threats prevention and mitigation, which can actually assist reduce the frequency and severity of the threats (Souppaya & Scarfone, 2013). Moreover, ISO 27001:2013 clause 7.2(b) requires that the organization ensures that the persons whose work affects the performance of its security management be of the right competence in terms of education, experience or training. This ignites the need to prioritize formal or structured training for the information security staff within the universities to upgrade or acquire competences necessary to guarantee security in the face of evolving cybersecurity threats.

As per control objective A.5 and A.6.2.1 of ISO 27001:2013, security policies and mobile policies are expected to be developed, approved, implemented and reviewed to meet the universities goals and objectives with the management setting the pace for security from the top. Also, the NIST cybersecurity framework subcategory ID.GV-1 speaks to the establishment of the organizational security policy.

The use of smartphones, laptops, tablets and other mobile gadgets in the universities and other workplaces presents a substantial challenge security wise, since these devices by nature are exposed to malicious actors and compromised applications (WaterISAC, 2016). The mobile devices therefore presents the risk of being an attack entry point into your network, and therefore there is need to craft, implement and enforce policies governing how these mobile devices access and use resources within your network

The security policies developed for implementation are expected to address the following areas amongst others;

i) Physical Security
ii) Asset Identification and Classification
iii) Incident Response
iv) Network Security
v) Change Management
vi) Business Continuity and Disaster Recovery
vii) Password Policies
viii) Cryptography
ix) Access Controls
x) Human Resource Security

Moreover, there is need to review performance of the security management system for effectiveness and efficiency to guarantee that the security requirements of the organizations are being met. This is carried out through assessments or audit and any non-conformities are highlighted, corrective actions taken and lesson learnt incorporated into the improvement of the security management system. ISO 27001:2013 clauses 9 and 10 addresses this aspects as well as NIST cybersecurity framework categories DE.AE, DE.DP and RS.IM.

**(b) Identification of Vulnerabilities and Threats**

Vulnerabilities are weaknesses of a control or an asset which can either be exploited by one or many threats. Both the weakness of an asset (technical vulnerability) and weakness of a control (organizational vulnerability) are examined. This in line with ISO 27001:2013 control objective A.12.6.1, NIST cybersecurity framework subcategory ID.RA-1 and ID.RA-2, and OCTAVE outputs R01.5 and R02.2

Secondly, threats are identified. The security threats always exploit vulnerabilities in the system thus causing loss or harm to an information asset or the organization. This in line with NIST cybersecurity framework subcategory ID.RA-2 and ID.RA-3, and OCTAVE outputs R01.3, which is extended in our case to include threats to both primary and supporting assets.

**(c) Risk Control Measures**

Lastly, a risk register is established. The register identifies the risks facing the universities, describes the risks to create an understanding, examines the impacts of the risks on the assets and the likelihood of their occurrence, prioritizes the risks and defines the treatment plan for the risks. This in line with NIST cybersecurity framework subcategory ID.RA-4, ID.RA-5 and ID.RA-6, and category ID.RM, and OCTAVE outputs R03.1, R03.2, R03.3 and R03.4 which is extended in our case to cover both to primary and supporting assets

**6.10 Justification and Testing of the Proposed Framework**

The proposed framework was tested and validated through the responses received from the respondents in this study. Firstly, majority of the respondents were in agreement that information security risk management was critical to universities continued provision of their critical services and hence availability of their information systems and proper functioning of their networks, prevention of data loss or damage, prevention of damage to universities reputation and fraud. Through the framework, it was established that the universities had identified and analyzed their risks and therefore instituted some protection strategies and mitigation plans. However, based on the threats or attacks identified as facing the universities, there was notable deficiency in implementation of some controls which would match the identified risks and thus greatly improve the security posture of the universities.

The proposed framework further allowed interrogation of the security practices implemented by the universities to protect their assets, and these were benchmarked with the industry best practices and some glaring gaps were identified which were weaknesses within the implemented information security risk management practices. These allowed for identification of practices, which needed to be beefed up if the universities are to reduce or eliminate susceptibility to information security risks. Further, the additional security requirements in the proposed framework were proven beyond doubt as important and strong in information security risk management.

**7.0 Conclusion and Recommendation**

Firstly, the study contributes to the body of knowledge by specifically answering questions, identifying the important security requirements for the protection of assets incorporating particularly authenticity and accountability security requirements, establishing implemented security practices, identifying vulnerabilities and threats; and risks identification, analysis, treatment and control. Further, the study contributes more to the body of knowledge by proposing a framework for effective information security risks management in Kenyan

public universities based on OCTAVE methodology and extended to incorporate additional security requirements namely authenticity and accountability, and customized to the specific requirements of the public universities in Kenya. The proposed framework was instrumental in assisting universities identify their risks, analyze and prioritize the risks, and craft protection strategies and mitigation controls to address the risks and therefore ,the adoption of this framework would assist universities manage the information security risks they face and enable them to effectively reduce if not eliminate their susceptibility to cyber-attacks.

I recommend universities to adopt the proposed framework to enable them effectively reduce if not eliminate the susceptibility to information security risks, which are detrimental to their information systems and assets. Further, the proposed framework provides a viable benchmark for universities to align their security risk practices with to improve on their security posture.

**References**

*Alberts, C. J., & Dorofee, A. J. (2001). OCTAVE Criteria Ver 2.0. CMU-SEI-2001-TR-016*

*Alberts, C. J., & Dorofee, A. J. (2002). Managing Information Security Risks: The OCTAVE Approach. ISBN: 0-321-11886-3*

*Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (August, 2003). Introduction to the OCTAVE Approach. Carnegie Mellon University*

*BHERT. (2016). Cybersecurity Threats and Responses in the Australian Higher Education Sector. Retrieved from https://www.bhert.com/newsletter/issue-36/cybersecurity-threats-and-responses-in-higher-education-sector*

*Boit, J., M., & Kipkoech, L., C. (2012). Liberalization of Higher Education in Kenya: Challenges and Prospects. International Journal of Academic Research in Progressive Education and Development, 1(2). ISSN: 2226-6348*

*Cherdantseva, Y., & Hilton, J. (2013). A Reference Model of Information Assurance & Security. IEEE. Egoeze, F., Misra, S., Maskeliunas, R., & Damasevicius, R. (2018). Impact of ICT on Universities Administrative Services and Management of Students' Records: ICT in University Administration. International Journal of Human Capital and Information Technology Professionals (IJHCITP). 9. 1-15. 10.4018/IJHCITP.2018040101.*

*IBM Security. (2016). Security Threats, Frameworks and Mitigation Efforts: How Can You Lower Your Risk. Retrieved from https://www.rsaconference.com/writable/presentations/file_upload/sop-w05_security_threats_frameworks_and_mitigation_efforts_how_can_you_lower_your_risk_final2.pdf*

*Joshi, C., & Singh, U. K. (2016). Managing Security Risks and Vulnerabilities in University's IT Threats Landscape. International Journal of Computer Applications (0975-8887). Retrieved from https://pdfs.semanticscholar.org/5382/91c27202872495788c26e7ce30824f58cb51.pdf*

*Kimwele, M., Mwangi, W., & Kimani, S. (2011). Information Technology Security Framework for Kenyan Small and Medium Enterprises. International Journal of Computer Science and Security. 5(1)*

*Kitheka, P.M. (2013). Information Security Management Systems in Public Universities in Kenya: A Gap Analysis Between Common Practices and Industry Best Practices. (Masters Dissertation, University of Nairobi). Retrieved from http://erepository.uonbi.ac.ke/bitstream/handle/11295/56607/Kitheka_Information Security Management Systems In Public Universities In Kenya A Gap Analysis Between Common Practices? sequence=3&isAllowed=y*

*Kiura, S. M. & Mango, D. M. (April, 2017). Information Systems Security Risk Management Model in Kenya Private Chartered Universities. European Journal of Computer Science and Information Technology, 5(2), pp. 1-15. ISSN: 2054-0965*

*Kumar, R. (2011). Research Methodology. A Step-by-Step Guide for Beginners. ISBN 978-1-84920-300-5*

*Md.Sum, R., & Md.Saad, Z. (December, 2017). Risk Management in Universities. Retrieved from https://www.researchgate.net/publication/321746840_Risk_Management_in Universities National Research Council. (2014). At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. Washington, DC: National Academies Press. https://doi.org/10.17226/18749*

*Ogalo, J. O. (2012). The Impact of Information System Security Policies and Controls on Firm Operation Enhancement for Kenyan SMES. Prime Journal of Business Administration and Management (BAM). ISSN: 2251-1261, 2(6), 573-581*

*Pandey, S. K., Mustafa, K. (2012). A Comparative Study of Risk Assessment Methodologies*

*For Information Systems. Bulletin of Electrical Engineering and Informatics. ISSN: 2089 – 3191, 1(2), 111 122.*

*Shevchenko, N., Chick, T.A., O'Riordan, P., Scanlon, T.P., & Woody, C. (July 2018).*

*Threat Modelling: A summary of Available Methods. Software Engineering Institute|Carnegie Mellon University*

*Souppaya, M., & Scarfone, K. (2013, July). Guide to Malware Incident Prevention and Handling for Desktops and Laptops. NIST Special Publication 800-83 Revision 1. http://dx.doi.org/10.6028/NIST.SP.800-83r1*

*Symantec. (2015). Internet Security Threat Report. Retrieved 22nd August 2017, from https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf*

*Teng'o, S. (2017, May 11). Cybersecurity: Rise of the Student hacker. Retrieved from https://www.standardmedia.co.ke/ureport/article/2001239325/cyber-security-rise-of-the-student-hacker*

*Wagstaff, K., & Sottile, C. (2015, September 20). Cyberattack 101: Why Hackers Are Going After Universities. NBC NEWS. Retrieved 23rd August 2017, from https://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821*

*WaterISAC. (2016, October). 10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_*

*June2015_S508C.pdf*

*Wechuli, N. A., Muketha, G. M., & Matoke, N. (2014). Cyber Security Assessment*

*Framework: Case of Government Ministries in Kenya. International Journal of Technology in Computer Science and Engineering. ISSN 2349-1582*

*Whitman, M. E, & Mattord, H. J. (2012). Principles of Information Security. Cengage Learning. ISBN-13:978-1-111-13821-9*