European Journal of Computer Science and Information Technology
Vol.5, No.2, pp.1-15, April 2017
Published by European Centre for Research Training and Development UK (www.eajournals.org)

INFORMATION SYSTEMS SECURITY RISK MANAGEMENT (ISSRM) MODEL IN KENYAN PRIVATE CHARTERED UNIVERSITIES

Salesio M. Kiura[1*] Doreen M. Mango[2]

1. *Technical University of Kenya, Nairobi, P.O Box 15991, Nairobi 00100, Kenya*
2. *Catholic University of East Africa, Nairobi Kenya*

* E-mail of the corresponding author: salesio.kiura@gmail.com

ABSTRACT: *This paper proposes a risk management model that can allow universities implement secure information systems. Specifically the paper appraises IS security in the universities and their requirements with a focus on how IS security risks can be managed. The appraisal assisted the researchers to understand the effectiveness of information security management in institutions of higher learning in Kenya. From the survey we carried out, it's clear that the universities face serious IS security challenges. Based on the issues identified as affecting information security management and the role they play to ensure secure systems at the universities, we propose recommendations to improvements in information security management in institutions of higher learning. This paper proposes an encompassing model to organize specific aspects of ISSRM as per the ISO/IEC 27001:2013 standard and structures this model by borrowing from the STOPE (Strategy, Technology, Organization, People, Environment) view of information systems security risk management.*

KEYWORDS: Information systems security, risk management model, private universities, ISO/IEC 27001:2013

INTRODUCTION

The dependence of information technology by organizations consequently elevates information security issues to recognition that it is now playing an important role in our lives (Sipoen, 2001). In a university setting, Criminals, students, employees, visitors (for example in conferences and symposia) pose both technical and non-technical issues that threaten the security of information systems. There have been several reported international incidences of information security breaches in universities (O'Neil (2014), Garrison & Ncube (2011), Beaver (2010)). Here in Kenya there have also been reported breaches that have resulted in negative reporting and a call to action for the information systems security officers in the universities (The Star (2011), SERIANU (2015), Deloitte East Africa (2011)).

Private universities are ran as enterprises, balancing the service to humanity call with the equally important expectation to ensure a return on investment to the sponsoring institutions like churches, trustees and private owners. Just as is the case for purely commercial organizations, information systems risk management is essential for establishing a safe environment for the investments by both the trustees and the sponsoring entities.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

There hasn't been a model proposed for universities to guide on governance, operations, people and physical infrastructure in implementing information systems security measures. In recognition of the need for risk management in the implementation of information systems security, various organizations concerned with standards have published different risk management methods (Saleh and Alfantookh 2011). Whereas these methods have been and are being partially or fully adopted by enterprises with a great emphasis on the technology aspects, this paper looks at the management aspect of IT security. This will be of additional value to the contributions as noted by Saleh and Alfantookh working in different fields for identifying, analysing and minimizing risks for IT activities.

The objective of this paper is to propose a risk management model based on ISO/IEC 27001:2013 combined with our own Kenyan experience by way of a survey that we conducted amongst the private chartered universities. ISO/IEC 27001:2013 provides a comprehensive approach through documenting ten security domains organized into aspects of technical, organizational and physical aspects (Saint-Germain 2005). Further the STOPE (Strategy, Technology, Organization, People and Environment) view provides a structural perspective in the analysis of ISO IEC 217001:2013 standard (Saleh et al., 2007). This paper proceeds from these two to propose a structural model that is precise and targeted for managers with an oversight responsibility in ISSRM. The model is presented analogously to a house structure where the overall roof is successful ISSRM held up by four pillars of governance, operations, people and the physical environment (security infrastructure). The foundation of this successful ISSRM house is proposed here as an organizational culture of pursuing compliance though promotion of supportive attitudes towards information systems security.

Information Systems Security Risk Management (ISSRM) Models

Information Systems Risk Management as a governance issue

Reliance on information systems and the underlying technologies require a responsible approach to both the technical issues involved as well as the management issues of these underlying structures. Success of IS risk management in organizations is enhanced by treating IT security not solely as a technical issue but also approaching the interventions from a governance perspective. Saleh and Bakry (2008) in looking at various IT risk management methods observes that there is profusion of roles, regulations and guidelines. This is an indication of the appreciation that IT security is not solely a technical issue but also relates orthogonally to governance.

We postulate that it is principally the responsibility of top governance organs in an organization (with case example of the private chartered universities in Kenya) to institute and steer programs that will seek to safeguard their information resources. Private universities are faced with a responsibility to protect their own information generated by both internal staff and students as well as information entrusted to them from external stakeholders. Kimwele, Mwangi and Kimani (2011) call this "organizational enlightment". Clearly, such universities have a responsibility to establish information security through a thorough risk management framework.

Several international standards for information security have been published. Notably the ISO 27000 family of standards are very comprehensive. Of particular focus is the International

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

Standard ISO/IEC 27005:2011 which gives managers and staff in IT departments a framework for implementing a risk management approach to assist them in managing their information security management system (ISMS) risks. With this as the point of departure, we aim to contextualize ISSRM from a governance perspective.

Information Systems Risk Management in Context

Other than the general information systems security standards and frameworks, there have been proposals that specifically address particular needs and industries. Smith and Eloff (2002) studied IT risk in healthcare; Jun, Han and Suh (1999) looked at IS risk in eComerce; Esteves and Joseph (2008) looked at eGovernment IS risks; Kimwele, Mwangi and Kimani (2011) studied IS security in SMEs, Niekerk and Labuschagne (2006) in SMMEs. These studies have clearly indicated that for specific application areas and industries, IS risk management presents different objectives, steps, structure and level of application. Moreover, IS security not only includes technical, social and economic aspects but also prevalent security systems are inherently relative and depend on the environment within which they exist. This means that security will be taken or implemented differently in different organizations and universities alike. Overall, each of these studies seek to highlight methods that identify the risk, estimate the risk value prioritize the risks and propose risk mitigation steps.

For the education sector and specifically in the universities, unique ISS issues arise that motivate a study of risk management in universities. These include:

i) Academic freedom – In a typical university setting, there largely exists free ideas exchange and exploration through research by both faculty and the students. Inquisitive minds from the university community means there is liberal investigation of many aspects and especially use of IT tools to carry out research and development. This demands security configuration of access controls in such a way that promotes vast access and sharing of information to satisfy the ever changing demands from the university system users. Moreover, there is an ever changing student and adjunct faculty populations in short spans of each semester as well as temporal users in the form of participants in conferences and symposia held in these institutions. These individuals will have specific demands on the security system in terms of large numbers of user accounts, diverse equipment owned by the students and staff as well as topics and aspects of interest. The adopted IS security measures must be cognizant of the tenets of academic freedom to work in a university setting.

ii) Different perspectives – In a university setting there are various stakeholders represented by management, administration, lecturers, students and oversight organs like the university council. Their different perspectives and consequently priorities lead to potential conflicts of priorities. Given that IS security is a transparent process when it is operating effectively, it is not noticed, can't be quantified (valued) when running well. This can lead to general lack of awareness, prioritization and understanding by administrators, staff, students and generally all the users. Consequently there will be limited support (such as funding) as well as a culture of compliance amongst the users. This state of affairs needs to be arrested before total lack of awareness and responsibility across the entire university community leads to compromised Information systems security.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

iii) Diverse roles - there is a diverse mix of stakeholders within a university that affects applying information systems security controls and procedures. In general terms, there are those who want to provide open access to information while others want to have controlled access to information only by specific audiences. There is also the aspect of having privacy of information (such as grades and fees payment) but the same people also would like easy access to such information (for example not restricted to only accessing the information from within the campus network). A tension therefore exists between the roles in these scenarios. IS Security risk management must therefore seek to strike a balance between transparency and privacy of information.

iv) We add a fourth aspect in this research that for private universities, they are also "businesses" in operation and managing IS security from both the general university perspective and from a "business entity" perspective makes it complex. This "enterprising" culture that would be seen to be counter the academic freedom, service to community and no profits focus introduces a moderating factor in the represented perspectives and priorities of the diverse roles in a private university. An IS security manager in such a private university then has a more specific focus (by the trustees and owners) as compared to other state run/owned universities. Agility and business mind-set becomes a must for such a practitioner.

Information Systems Security at Universities

Our research Design

The objectives of the study we carried out were to:

- Examine the current status of information systems security management in private chartered universities in Kenya.
- Identify the factors that hinder effective information systems security management practices in private chartered universities in Kenya.
- Propose improvements in information systems security risk management in universities.

There are seventeen private chartered universities in Kenya (CUE, 2015). We sampled sixteen of these universities for our survey and the seventeenth one was used to pilot test the questionnaire. In total we worked with respondents from all the sixteen universities. We used a questionnaire that was first sent via email and followed up by an in-person visit by the researchers to select respondents for face to face discussions. The meetings provided opportunities to review university IT policies, standards, security programs and also observations (for example with respect to physical security of the ICT resources premises).

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

There was a strong aspect of qualitative research in the discussions whereby the researchers analysed institutional experiences beyond what is documented. The respondents represented diversity by including those with managerial responsibilities, mid-level management as well as operational staff in the ICT functions in the universities. A similar categorization is used in the ISO/IEC 27001:2013 standard. The table below summarizes the represented roles by the respondents.

Table 1: Summary of respondents' level of authority

Roles	**Tasks / responsibilities**	**Tally**
Top management	ICT Manager	4
	Satellite campus team leaders	7
Middle level management	Programmers	4
	Database Administrators	11
	System administrators	19
	Network administrators	11
	Web site managers	4
Operational staff	User support	11
	Hardware technicians	26
	Software technicians	4
		101

FINDINGS

One of the general observations was that the various private universities had not only a main campus but also satellite campuses in various towns. This came out as affecting ISSM. Specifically 86% had IT departments centralized at the main campus. The other 14% had decentralized to an extent of having data centers at satellite campuses and managing the security and other access details (such as user management) from the campuses

On the status of information systems security management (ISSM) in the universities, we can summarize the findings into eleven aspects. The findings are summarized in the table below:

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

Table 2: Status of ISSM in the universities

Aspect	Finding
Presence of a policy addressing ISSM	90% have a policy 10% do not have
Reporting to management on ISSM	20% don't provide regular reports 80 % report regularly
Management understanding and awareness of the importance of ISSM	15% disagree that management had understanding and appreciation 70% agree that management had a good grasp 15 % are not sure
Management provides support to the IT department	8% no support 92% yes – gets support
Presence of an IT/IS Security officer in the staff establishment	42% had a specific officer responsible 10% - had the role defined but not assigned a specific officer 48% did not have the role specifically defined
Satisfaction with the current arrangements as assuring IS security	13% – not satisfied 9 % not sure 78% - satisfied
Providing security related awareness online for the users	61% Don't provide 39% post related information online
Availing the policy on information security to the end users	53% - No (policy not shared with the users) 47% yes (policy is available to the users) (the most cited being the passwords change policy)
Measuring compliance or effectiveness of information security through Key Performance Indicators (KPIs) or metrics	17% - don't carry out any evaluation 9% did not have the KPIs 74 % carry our regular evaluations / audits
Perception that the general Organizational culture supports information security measures	20% don't agree prevailing culture supports information security 80% agree
Perception that the institution is strategically positioned to detect and defend against security incidents or breaches	13.5% didn't feel well prepared 86.5% felt confident to detect and mitigate the effects

We also sought to identify the prevalence of Information systems security issues that were prevalent in the universities. The following table shows the findings:

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

Table 3: prevalence of IS security breaches

Factor	Percentage of respondents reporting prevalence		Factor	Percentage of respondents reporting prevalence
Viruses	10.7 %		Internal Based Attacks	4.8 %
User Errors	8.9 %		Website Vandalism	4.8 %
Theft of Computers	8.3 %		Unauthorised access to data	4.2 %
Hardware Failures	8.3 %		System Administration Errors	4.2 %
Compromising The system	8.3 %		Botnets	3.6 %
Malicious Software	7.7 %		Phishing	3.0 %
System or Software errors	7.1 %		Having Untrained Staff	1.8 %
Denial of Service Attacks	6.5 %		Lack of Qualified Staff	1.2 %
Cyber Attacks	6.5 %			

Based on the principle of self-assessment and in agreement that each institution had encountered a breach of information security in one way or another, we sought to study the extent to which the following factors were considered to contribute to the breaches. The findings are summarized in the table below

Table 4: Main contributors to IS security breaches

Factor	Finding
lack of (or inadequate) Technology	45% disagree 55% agree
Lack of Qualified Personnel	74 % disagree 26% agree
Little involvement of Top Management	80% disagree 20 % agree
Little incident Detection	70% disagree 30 agree
Poor Organizational capability to respond to security threats	79% disagree 21 agree
Inadequate collegiate support in the university	77% disagree 23 agree
Lack of a culture of compliance (strategic goals and work practices)	29 disagree 71 agree

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

From the respondents we identified the following proposed interventions that they believe would go a long way in improving ISSM in the universities. These include:

- Having a dedicated office dealing with ISSM and recruitment of an ISS practitioner
- Updating management on security updates and management support, involvement in continuous improvement
- Constant regulations and policies on ISSM
- Having the security practitioner in university management
- R&D and learning from other institutions
- Staff training on ISSM on a continuous basis
- Adequate resource allocation to ICT as necessary to upgrade the software and hardware
- Taking feedback from users/customers seriously
- Documenting past problems and learning from them

Having appraised the status of IS security we go ahead and propose a model based on the findings and existing standards. The model can assist in IS security risk management.

Proposed Information Systems Security Management Model

Model Basis

Mwanthi, D. M. (2009) in the study of security in critical information systems in Kenya found low state of readiness in the use ICT to support mission-critical operations of the institutions. The study particularly noted internal and external threats to the university data as a result of inadequacies in technical safeguards, insufficient user training and lack of comprehensive formal information systems security policies. As the trend towards demand for information systems for education institutions grows, there is need to have models for implementing information systems security risk management in the universities. Some of the factors driving up the risks in information systems management are: technology changes at unprecedented rates, continued explosion of the internet and the phenomenon of competing priorities that relegates risk management to a less focus. According to ISO/ISEC 27005:2008 a risk represents a potential that a threat will exploit vulnerabilities of an asset. A key asset is information that a university context must manage.

The ISO/IEC 27005:2011 provides general guidelines for information security risk management. However, the standard is general given the motivation to have it applicable in a wide range of contexts such as governments, commercial and non-profits driven organizations. The domains that are identified in the ISO framework are further categorized to reflect the various levels in organizational management. The table below summarizes the categorization

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

Table 5: Security domains in the ISO/IEC 27000 standard

Management level	Security domain of the ISO/IEC 27000 standard
Operational level	1. Systems development 2. Communications and Operations management 3. Business continuity management 4. Personal security
Mid-Level	5. Physical and Environmental security 6. Compliance 7. Asset classification and control 8. Access control
Top (organizational) level	9. Security policy 10. Organizational security

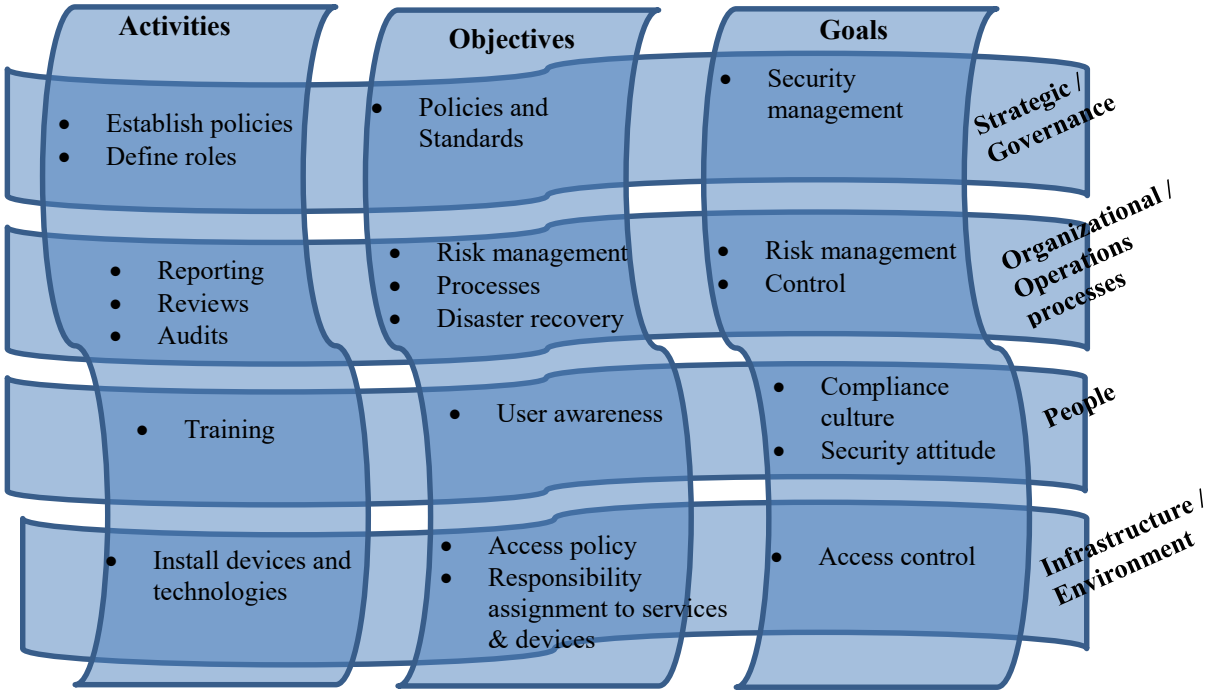
Based on STOPE and ISO/IEC 27000 domains, we mapped our survey findings into the following clusters to bring out the general characterizations of the results of our analysis as in the table below

Table 6: Survey findings mapped to the ISO/IEC 27000 domains

Management level	Domain of the ISO/IEC 27000 standard	Our survey result areas
Operational level	• Systems development • Communications and Operations management • Business continuity management • Personal security	• Reviews and updates to management • Reporting • Technical and Physical environments maintenance • User awareness and training • Activities defined and specific to Universities culture
Mid-Level	• Physical and Environmental security • Compliance • Asset classification and control • Access control	• Disaster recovery and backups • Audits / evaluations and compliance • Definition of roles • Specific processes definition • Objectives aligned to the culture of universities
Top (organizational) level	• Security policy • Organizational security	• Policies • Establishment of security practitioner office • Goals specific to universities practices

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

To come up with the model for the IS risk management based on our survey, we used the STOPE view to structure the results and form a house like representation that has four pillars (governance, operations, people and physical environment aspects). The STOPE view is more structural and therefore provides opportunity to map specific activities, objectives and goals in a given context such as a university information systems management. From the survey results, guided by STOPE we represent in figure 1 the structuarization of the results represented as interweaving fabric representation from both vertical (activities, objectives and goals) and horizontal (strategic, organizational, people, environment) views.



We argue that the technical focus cuts across and at the core of successful ISSRM is to have the non-technical (soft) aspects well managed. Moreover, a cross cutting theme of culture is very important. We especially identify the culture of compliance (to both internal requirements and external requirements like the ISO standards) to be key and therefore is represented as a foundation in the model.

The proposed Model

We represent the model analogously to a house structure (figure 2) where the overall roof is successful ISSRM held up by four pillars of governance, operations, people and the physical environment (security infrastructure). The foundation of this successful ISSRM house is proposed here as an organizational culture of pursuing compliance though promotion of supportive attitudes towards information systems security.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

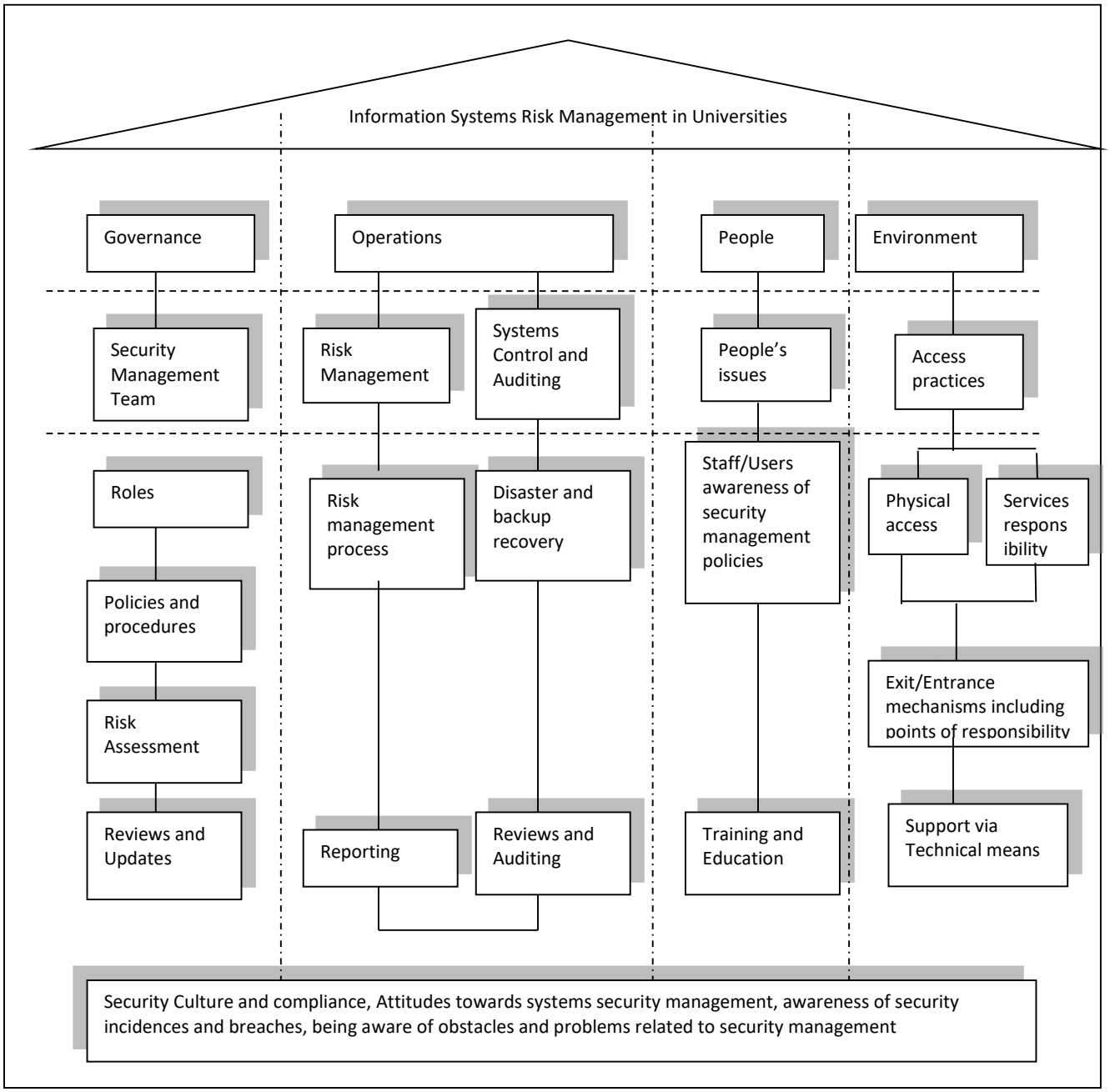


Figure 2: Proposed Information Systems Security Risk Management Model (ISSRM Model)

Governance Pillar

Governance as used in this context refers to the provision for a set of roles, policies and responsibilities and practices by members of a security management team responsible for formulating objectives and policies. The team ensures that objectives and policies are achieved as well as risks being identified are handled appropriately (Allen & Westby 2007). The governance part stresses the importance of considering security management as part of top management

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

responsibility within the university. According to the survey over 80% of the respondents agreed that this will greatly improve security management of the university. This ensures that universities will design their strategy based on the visions and directions pointing towards security management and risk management (Purtell, 2007). The security management team should be chaired by a security practitioner who is ideally a member of the university's management board or top management. Over 90.3% of the respondents agreed that the practitioner should be part of the top most management organ. The team members should constitute members of the university's security department and a representative from every department of the university. The respondents highlighted that involving all the departments of the institution within the security team will greatly improve information systems security management.

Risk assessment is done with a view of identifying risks at different levels within the university so as to prioritize security planning. Asset management is one of the main clauses of the ISO/IEC 27005 standard where two objectives are stated: responsibility of assets and information classification. Regular risk assessment should involve compilation of detailed information about universities assets (in terms of types and values of the assets to the university), identifying various threats, vulnerabilities, possible risks and estimating the cost of security breaches and incidences. Reviews and updates can be identified through meeting, questionnaires, observations, reports, etc. This should be followed by identifying what should be done to reduce risk, systems vulnerability, revising and evaluating the risk process continously.

Governance stresses the need for security practitioners to document, maintain, review and update the uinversity's risk policies and procedures as well as preparation of reports. Further, a good governance policy will also target to share information with the university user community. This can be done via posting information online as well as other security awareness initiatives among employees and users of various systems in the university.

Operational Processes

The operational processes involve putting into practice security programs formulated by the security management team through the involvement of various departments in the university, learning from previous breaches and practices in other institution. Representation and ensuring clear definition of process owners will ensure the critical tasks of auditing, reviewing, reporting, recovery and general systems control are done professionally. The risk management process can be formulated based on the risk assessment of various security breaches documented by the security management team.

People Factors

This relates to the general "people-related-aspects" of information systems security management. It relates closely to balancing academic freedom in the universities to ensuring security of information systems. Specifically in this case it relates to the programs pertaining to users being trained on a continuous basis and making them aware of policies and procedures and what is expected of them in terms of information security. Awareness must also be clear on the consequences of breach as well as avenues for seeking assistance. In a university setting the users will therefore not feel restricted when they are aware of the protocol to be followed allowing them to carry out a potentially dangerous task. An example is when staff request for network ports to be

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

opened to support an exploration for purposes of research. Also, it is possible that a user would like "relaxing" of some security measures in a controlled experiment like testing an application under development. The security policy should cover the security management team's roles and responsibilities as well as continous monitoring of staff who are entrusted to manage information systems in the university. Security awareness should be made part of the organization's policy, well documented and communicated with an effort to address people factors that can lead to breach. Training and awareness programs will encourage staff's or employees to be aware of security incidences as well as prepare useful and timely reports based on security breaches.

Environment

Infrastructure and environment plays a critical role in securing systems. As ISO/IEC 27005:2011 notes, information assets include the tangible and intangible items. These include services, equipment as well as physical access set ups to the facilities, like computer laboratories, server rooms and other premises with installed IT equipment. It is the responsibility of the IS security management team to define access practices that are applicable for both the physical assets as well as for the service. The physical measures should include but not limited to how the premises are accessed in the university; how students, staff, employees and visitors access different areas of the university. Various technical options are at the heart of the environment aspects in ISSM and should be exploited with clear responsibilities defined at all levels.

Security Culture and Compliance

Security culture and compliance is about users' or employees' attitudes and awareness of the importance of information systems security management in the university. Awareness contributes to staff's attitudes towards security policies and procedures, their level of awareness of security, security breaches and limitations of implementing security management in the university. Lowry and Goetsch (2001) refer to awareness as shared culture of mutual responsibility towards attaining some level of security. Employees should be provided with information and the necessary tools to respond to various situations and be able to take action when called upon to do so. The attitude of security compliance brings out the effectiveness of information systems security management and the procedures to ensure continuous improvements.

The users of the systems in place are very important especially when implementing security policies. Security should be a way of life in the university. Security culture forms the foundation for the four pillars of the model thus gearing towards achieving effective systems security management within the university. If handled well it could go a long way towards achieving or making everyone in the institution aware of IT security.

CONCLUSION

The results of the survey we carried out indicated that Kenyan private chartered universities have made tremendous progress in implementing information systems security. However, these universities are facing numerous challenges especially where implementation of security is concerned because of the diverse roles evidenced in university environments. A risk management model goes a long way to ensure protection of the information resources – something that is crucial given the nature of universities' work. Whereas technology is vital, it is important to consider the non-technical aspects of governance, processes, people issues, environments and cultural factors

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

of universities. By relating our findings to the international standards (ISO/IEC) and also the STOPE view of ISSRM, we have proposed a risk management model that we believe adds value to the domain of ensuring information systems security. The model provides universities management with a working strategy to assess and implement a more holistic approach to information systems security management. Further, by using the model, we believe the model provides a platform for securing of university systems by combining aspects of governance, processes, people, infrastructure and cultural factors to ensure that an effective information systems security management is in place, thereby minimizing risks to university's main asset of information capital.

REFERENCES

Allen, J., & Westby, J.R. (2007). Characteristics of effective security governance. Governing for Enterprise Security (GES) Implementation Guide (CMU/SEI- 2007-TN-020).Software Engineering.

Beaver, K. (2010) ,Information Security in Higher Education. Sophos. USA

CUE Commission of Higher Education (2015). Status of Universities in Kenya [online]. Available at: http://www.cue.or.ke/index.php/accredited-campuses-of-universities-in-kenya. [Accessed 07 March 2017]

Deloitte East Africa (2011). 2011 East Africa Application Security Survey, safeguarding the future [online]

Esteves, J., Joseph, R.C., 2008. A comprehensive framework for the assessment of e-Government projects. Government Information Quarterly 25, 118–132.

Garrison, C.P. & Ncube, M. (2011) 'A Longitudinal Analysis of Data Breaches', Information Management and Computer Security, Vol. 19, No. 4. pp. 216-230.

ISO/IEC 27001: 2013 (en). Information Technology – Security Techniques – Information security management systems – Requirements. International Standards Organization, www.ISO.org, Geneva, Switzerland.

ISO/IEC 27005:2011. Information technology -- Security techniques -- Information security risk management. International Standards Organization, www.ISO.org, Geneva, Switzerland.

ISO/ISEC 27005:2008. Information technology -- Security techniques -- Information security risk management. International Standards Organization, www.ISO.org, Geneva, Switzerland.

Jung, C., Han, I., Suh, B., 1999. Risk analysis for electronic commerce using case-based reasoning. International Journal of Intelligent Systems in Accounting, Finance and Management 8 (1), 61–73.

Kimwele, M., Mwangi, W. and Kimani, S. (2011). Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs). International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (1): 2011

Lowry, C.B. and Goetsch, L. (2001). "Creating a culture of security in the university of Maryland libraries". Portal: Libraries and Academy, Vol.1, no.4: pp. 455-464.

Mwanthi, D. M. (2009). An assessment of security in critical information systems used by universities in Kenya. Unpublished master's thesis

Niekerk, L., Labuschagne, L., 2006. The PECULIUM model: information security risk management for the south african SMME. In: Proceedings of the ISSA from Insight to

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

Foresight Conference, 5–7th July 2006, Sandton, South Africa.

O'Neil, M. (2014) Data breaches dent universities' finances, reputations. The Chronicle of Higher Education21 March 2014 Issue No:312. Available at: http://www.universityworldnews.com/article.php?story=20140321161842666 (Accessed 07 March 2017)

Purtell, T. (2007). A new view on IT risk. Risk Management, 54(10), 28.

Saint-Germain, R. (2005) Information Security Management Best Practice Based on ISO/IEC 17799. The Information Management Jour n a l. July /August 2005

Saleh, M.S., Alfantookh, A., 2011. A new comprehensive framework for enterprise information security risk management. Applied Computing and Informatics (2011) 9, 107 – 118

Saleh, M.S., Alrabiah, A., Bakry, S.H., 2007. A STOPE model for the investigation of compliance with ISO 17799:2005. Journal of Information Management & Computer Security, Emerald 15 (4), 283–294.

Saleh, M.S., Bakry, S.H., 2008. An overview of key IT risk management methods. Saudi Computer Journal 6 (2).

SERIANU (2015). Kenya Cyber Security Report 2015. Available at: www.serianu.com/downloads/KenyaCyberSecurityReport2015.pdf (Accessed 07 March 2017)

Siponen, M. T. (2001). A Conceptual Foundation for Organizational Information Security Awareness. Information Management & Computer Security, Vol.8, No. 1, pp.31-41.

Smith, E., Eloff, J.H.P., 2002. A prototype for assessing information technology risks in health care. Computer & Security 21 (3), 266–284.

The Star (2011). Student fails to stop KU graduation date [online] Available at: http://www.the-star.co.ke/national/national/52785-student-fails-to-stop-ku-graduation-date (Accessed: 13 February 2017)

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)