Determining Information Security Maturity Level of an organization based on ISO 27001

Daniel Makupi[1], Nelson Masese[2]
[1]*Ph.D student, School of Computer Science and Bioinformatics, Department of Information Technology Security, Kabarak University, Private Bag 20157, Kabarak, Kenya*
[2]*Senior Lecturer, School of Computer Science and Bioinformatics, Department of Information Technology Security, Kabarak University, Private Bag 20157, Kabarak, Kenya*
[1]dmakupi@kabarak.ac.ke
[2]nmasese@kabarak.ac.ke

Abstract
Technology adoption is key critical component for organization success. With continued and rapid advancement in technology especially brought by the need for employees to use their personal devices, it presents a major opportunity and challenge for enterprises, it poses a challenge as adversaries have taken advantage of widening cyber space to attack information and information systems. Our study provides a solution by designing a model to compute information security maturity of universities. The research is based on ISO 27001 by involving specific clauses relevant to universities because of its unique organizational ecocentric nature having varied categories of user's and extensive research allowing it to serve as a plausible area for study compared to other organizations. The cumulative factors having being considered statistically varied towards contribution towards the maturity model. The model is then designed considering the different information security levels of compliance suggested by ISO 27001. The study adopted design research approach to come with the model design.
Keywords: *Model, design, Maturity, ISO 27001*

I. INTRODUCTION

Information Security Management is the process of managing day to day security work, training and awareness of security programs and how compliance to security policies are handled [1]. Information Security Maturity level is the measurement of the organization's capability to remain secure [2]. Information security management is a very important requirement for all enterprise today because it has proved to help in improving the effectiveness and efficiency of enterprise business processes [3].

Because of the benefits accrued in adoption and use of technology and the need to gain competitive advantage Organizations have begun to realize and start doing information security performance evaluation. In not more than two decades ago organizations have begun Identifying, planning, scheduling and implementing information security management as an organizational framework [4]. In evaluation of information technology, there have been several frameworks that have been widely accepted and proven such as The British Standard for information security management (BS7799) later, International Standards Organization (ISO 27001 & ISO 17799), IETF security architecture (Internet Engineering Task Force), the National Institute of Standards and Technology (NIST 800 series special publications), Control Objectives for Information and related Technologies (COBIT), and Committee of Sponsoring Organizations (COSO) are some of the most prominent initiatives in management of information security and risk management systems [5].

The information security maturity model (ISMM) is a model to evaluate the ability of organizations to meet the objectives of security, namely, confidentiality, integrity, and availability while preventing attacks and achieving the organization's mission despite attacks and accidents [6]. The model defines a process that manages, measures, and controls all aspect of security. It relies on four core indicators comprising of different compliance states for benchmarking and as an aid to understanding the security needs in the organization. These indicators are goal-driven to achieve the security needs [7]. Therefore, the core objective of the study is to develop a model that would to aid universities in determining the level of maturity in regard to information security. The model cumulatively consider IS security factors and

how it impacts on maturity level based on the different levels of compliance levels available in ISO 27001.

The design of the model would be guided by the following objectives:-

i. To determine the critical information security risk factors that impact on security of universities based on ISO 27001.
ii. To design a model for cumulatively computing information security maturity of an organization based on ISO 27001 compliance levels.

1.2 Statement of the research Problem

With the ever growing cyber space, information security preparedness and countermeasure becomes the only available remediation that universities should focus to reduce the devastating nature of attacks and to provision assurance of information within their custody. This vast trend may be due, in part, to the sheer number of personal records kept by these institutions, considering their ever-changing student bodies, as well as the valued open, collaborative environment of most colleges and universities. Therefore without continual and timely awareness on their information technology infrastructure vulnerabilities, universities are exposed to attacks which brings down there information infrastructure.

II. LITERATURE REVIEW

2.1 Information Security Maturity Factors Relevant to Universities.

The critical information security risks that target universities originate from human behaviour. People are regarded as the greatest weakness of Information Security according to [8] and [9]. For this reason, information protection should not be only a technical issue, but also social, for which there is no purely technological solution known. Therefore, measures towards information security should not only address technological and physical issues but also administrative, to change human behaviour in the organization. [10] Proposes to classify Information Security measures as they aim to affect educational institutions and industry.

i. Administrative measures: aim to change people's behaviour; affect the organization and its members. They may be formal rules present in an Information Security Policy or informal training and education to promote knowledge on Information Security [11]. They are related to standards, organizational structure and Information Security processes.
ii. Technical measures: Aim to affect the technology used to process and store information, ensuring access only to those who are legitimately authorized [12]. They operate in computer systems and may reinforce administrative measures.
iii. Physical measures: Designed to protect information and its assets by physical mechanisms that affect the physical environment [13]. They are related to security of property, such as doors, locks and perimeters, and measures against environmental events such as floods and fire.

According to, [14], [15] suggest various administrative, technical and physical measures. Although some of them are widely adopted, such as the use of firewall, antivirus, anti-spam, logical access control, proxy, the existence of Information Security Policy, incident treatment team, backup routines, the use of uninterruptible power supply (UPS) and a safe box to store media, [16] agrees and adds that the simple adoption of measures proposed by standards and models does not guarantee the mitigation of risks.

Likewise, [17] explains that the organization should select in the standard the most appropriate measures, considering its own requirements. In order to avoid the adoption of inappropriate measures to the needs and characteristics of the organization, decisions about adoption should be guided by the risks identified in an analysis and risk assessment process aligned to organizational plans, strategies and objectives. The next section discusses the specific risk factors relevant to universities according to ISO 27001 standard.

2.2 Mathematical Modelling

Mathematical models are designed to describe physical systems by equations or, more in general, by logical and computational structures [18]. All real systems can be observed and represented at different scales by mathematical equations. The selection of a scale with respect to others belong, on one side, to the strategy of the scientists in charge of deriving mathematical models, and on the other hand to the specific application of the model [18].

Systems of the real world are generally nonlinear. Linearity has to be regarded either as a very special case, or as an approximation of physical reality. Then methods of nonlinear analysis need to be developed to deal with the application of models. Computational methods are necessary to solve mathematical problems generated by the application

of models to the analysis and interpretation of systems of real world.

Computational methods can be developed only after a deep analysis of the qualitative properties of a model and of the related mathematical problems. Different methods may correspond to different models. In the previous section statistical results have generated the relevant regression model that gives the weighted relative impact of independent variables on the independent variable that will be used for the model design and logic programming. The next section outlines the process of model derivation.

2.3 Conceptual Framework

A conceptual framework is a research tool intended to assist a researcher to develop awareness and understanding of the situation under scrutiny and to communicate [19]. The concept used in this study is based on ISO/IEC 27001 standard. Stage one shows the formula derivation Conceptual framework for computing University information Security Maturity, and Stage two can entail a prototype Implementation Conceptual framework.

The diagram below shows the conceptual framework with its components that was utilized in the study.

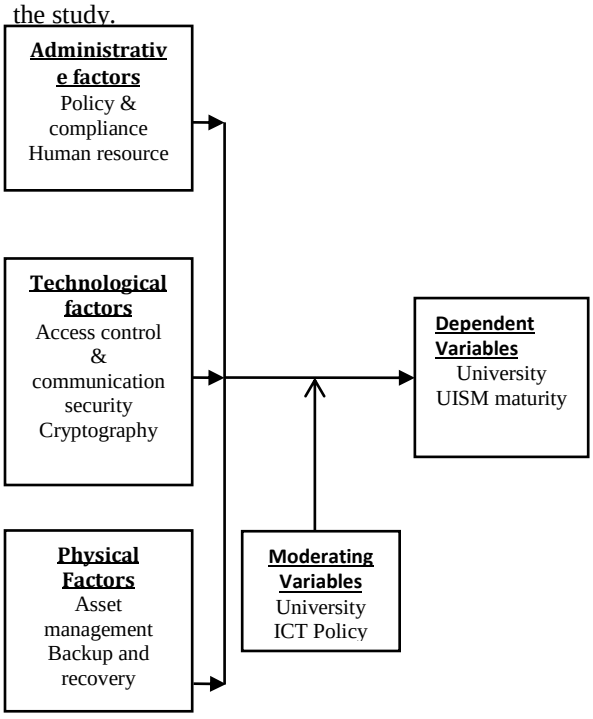

Figure 1: Formula derivation Conceptual framework (Author, 2018)

The proposed conceptual framework above has three key areas of concerns. The independent variables drawn from ISO/IEC 27001 standard which acts has the benchmark controls that are to be considered. Also, the university ICT policy has the intervening variable that determines the impact of independent variables on the dependent factor information security (UISM) maturity in universities. Overall upon consideration of the different factors in the independent variable the maturity will be computed based on the weighted emphasis of each particular factor and therefore will serve to inform the university information security maturity.

2.4 Coefficients/weights for university information security

The weights considered for the model are based on statistical data obtained from statistical analysis shown below in Table 1

Table 1 Coefficients (Research, 2018)

Model	Unstandardized Coefficients		t	Sig.
	B	Std. Error		
(Constant)	-.305	.159	-1.916	.058
Administrative Factors	0.596	.102	5.861	.000
Technological Factors	0.278	.104	2.671	.009
Physical Factors	0.301	.094	3.194	.002

a. Dependent Variable: University Information Security Maturity

The regression Equation

$$Y = c + \beta 1x1 + \beta 2x2 + \beta 3x3 + e$$

Where:

Y =University Information Security Maturity

C =Constant

β1, β2 and β3 = Weights

X1= Administrative Factors

X2= Technological Factors

X3= Physical Factors

e =Standard Error

The Model Equation will be given as:

$$U.I.S.M = -0.305 + \{0.596 * \text{administrative factors}\} + \{0.278 * \text{technological factors}\} + \{0.301 * \text{physical factors} + 0.59$$

The weighted value for each factor was then considered for model development by incorporating into a web based computational logic.

III. DERIVATION OF WEIGHTS FOR UISMM MATHEMATICAL MODEL

For computation of information security maturity of an organization predetermined questions

are used to denote maturity when satisfied by presenting to respondents on a web based interface. Maturity assessment questions were asked where respondents answered in a scale of 0 to 5 whereby 0 meant that the respondent agreed that their process are performed informally while 5 being the highest meant that the organization process were continuously improving which is a desired characteristic in information security maturity (ISM). The other indicators progressively reflected a positive projection in continuous process perfection respectively. The scores of the respondent per assessment question denoted the level of compliance to ISO 27001 standard by the respondent and associated organization which in this case was referred to as Security maturity level of the organization. The following linear regression modelling equation obtained from statistical analysis was actualized by having weighted coefficients obtained from regression model being used to determine university information Security maturity.

Equation 2 proposed university information Security maturity (Author, 2018)

USIM $\sum_{i=1}^{n}(W_i R_i)$

Where; $\mathbf{W_1}$, $\mathbf{W_2}$, $\mathbf{W_3}$..... $\mathbf{W_n}$, respectively are the weights determined through focusing group discussion by this study.

While; $\mathbf{R_1}$, $\mathbf{R_2}$, $\mathbf{R_3}$..... $\mathbf{R_n}$ respectively are the weighted indicators that determines the state of a particular risk security factor.

4.1 Model Design Scenarios

Suppose all the assessment questions have constant coefficients, such that $W=W_1=W_2=\ldots W$, Then, the weight will be W, whereby;

Equation 3 Mathematical Maturity Model (Author, 2018)

$$\mathbf{UISM = W R_1+WR_2+WR_3+\ldots WR_n.}$$

Since W is common,

$$\mathbf{UISM= W (R_1+R_2+R_3+ \ldots Rn)}$$

4.2 Model development process

In the case of the study, there were 36 questions that were used for information security maturity assessment, in which case, n=36 and the maximum score that the user could have in a scale of 0 to 5 was; 6*36 = 216.

If we put back this to maturity equation obtained in model design process in the previous section above, then;

Equation 1 Percentage Maturity Factor (Author, 2018)

$$UISM = \frac{R1}{216} + \frac{R2}{216} + \frac{R3}{216} + \cdots \frac{R36}{216}$$

Therefore;

$$UISM = \frac{1}{216}(R1 + R2 + R3 + \cdots R36)$$

Hence;

$$Weight = \frac{1}{216} = 0.005(\text{Rounded off})$$

In the view of the above, the relevant weight for the UISMM model based on 36 Assessment questions was **0.005**; the value of maturity factor of UISM could be represented as a percentage factor (UISM %) as shown in equation below;

$$UISM = 0.005(R1 + R2 + R3 + \cdots R36) * 100$$

Hence

$$\boldsymbol{Y = 0.5(R1 + R2 + R3 + \cdots R36)\%}$$

4.3 UISMM Maturity

By achieving the weight and the maturity level of the organization, which denotes the level of compliance to the ISO 27001 standard, as shown in equation above, UISM was computed as a level of immaturity or non-compliance to ISO 27001 standard. UISM basically represented the gap between full compliance to ISO 27001 standard and the actual security position of the organization represented by the maturity score.

The compliance level that organizations achieves is deduced according to ISO 27001 requirement which includes; state of non-compliance, initial compliance, and basic compliance, acceptable and full compliance respectively [20].

4.4 UISMM Model metrics

Information security maturity of an organization was determined as shown in equation in the previous section which represented the compliance level of the organization to ISO 27001 standard, and secondly computing UISM as shown in equation 6 which represents the organizations deficit score or gap for it to attain full compliance to ISO 27001 standard. There are therefore five model scenarios which are illustrated in figure 1 below, namely; non-compliance, initial compliance, and basic compliance, acceptable and full compliance.

IV. COMPLIANCE STATES

5.1 State of Full compliance

For organization to have full compliance security is managed by identifying the security concerns and security incidents are tracked in a systematic way. The organization must have proper

policies for security in a formal sense and business plans would have items for security. The use of specific technologies throughout the organization is in a uniform manner and the implementation came to existence out of a business plan. The desired full compliance state were the process are cautiously improving according to ISO 27001 compliance will be determined by the model taking into consideration sum of organization scores for the 36 information security assessment questions is equal to 216.

Equation 4 Desired state of full compliance and continuous improvement in process (Author, 2018)

That is; $R1 + R2 + R3 + \cdots R36 = 216$

By substituting back to equation in equation 1,

$\boldsymbol{UISM = 0.0046(216) = 100\%}$;

Equations 4 above depicts that the user and their organizations are fully compliant to the specific requirements of ISO 27001 standard at UISM=100% and that it is fully compliant and process are continuously improving.

5.2 State of Acceptable compliance

This state is characterized by central management of all security related issues and policies. Users are trusted but their interactions with the systems are viewed as vulnerability. No ad hoc changes and central configuration models, from which all configurations are derived, are implemented. Security policies and procedures are now in place together with adequate delivery mechanisms to aid awareness and compliance. Access controls are mandatory and are closely monitored. Security measures are introduced on a cost/benefit basis and ownership concept is in place. By substituting back to equation in equation 5,

Equation 5 Acceptable state of compliance were organizations are conscious about their security needs (author, 2018).

$\mathbf{UISM = 3/4(0.0046(216) = 75\%}$;

Equations 5 above explained that the security measures are introduced on a cost/benefit basis and ownership concept is in place illustrating that the user and their organizations have acceptable level of compliance to the specific requirements of ISO 27001 standard at UISM=75% .

5.3 State of basic compliance

This state is the starting point for any organization that wants to protect its investment and ensure continuity. Application and network security is implemented but changes are not centrally managed and ad hoc security requests are common. In this state, organizations trust the interaction between the user and the systems. Security awareness programs are being considered for key resources only. IT security procedures are informally defined and some risk assessments taking place. In addition, responsibilities for IT security have been assigned but enforcement is inconsistent. Some intrusion and detection testing can also be performed.
By substituting back to equation in equation 1,

Equation 6 Basic compliance state usually centered on the business activities of the organization and the protection of core systems (author, 2018)

$\mathbf{UISM = \frac{1}{2}(0.0046(216) = 50\%}$;
Equations 6 from the basic compliance state it depicts two restrictions that are faced at this stage: First, financial restriction and spending on systems that don't add value to the income of the business. Second, organizations classify their initial investments in security as completed. The user and their organizations have basic level of compliance to the specific requirements of ISO 27001 standard at UISM=50%. Organization will have a perception that their systems are protected and they become unaware of the threats and vulnerabilities.

5.4 State of Initial Compliance

As long as an organization is conscious about the threats that their information systems face then that organization is considered in the initial state of compliance. This state is characterized by being chaotic, inconsistent, ad hoc, and in response to attacks and possibly because of losing resources due to an attack.
By substituting back to equation in equation 1,

Equation 7 Initial starting point for any organization (author, 2018)

$\mathbf{UISM = 1/4(0.0046(216) = 25\%}$;

The goals at the initial state are usually centred on the business activities of the organization and little attention is focused on securing the organization. Equations 7 above explains that goals will change in response to attacks by implementing some kind of protection but it will not be continuous. The user and their organizations have

initial level of compliance to the specific requirements of ISO 27001 standard at UISM=25%. The organization has little practical implementation in security systems.

5.5 None Compliance state

During the none-compliance state the management does not consider investing in security related systems necessary for the overall business strategies. In addition, the organization does not assess the business impact of its vulnerabilities and it does not understand the risks involved due to these vulnerabilities.

By substituting back to equation in equation 1,

Equation 8 Non-compliance state is characterized by none existence of policies and procedures (author, 2018)

$$\mathbf{UISM} = (\mathbf{1/4(0.0046(216))} - \mathbf{0}\ (\mathbf{0.0046(216)} = \mathbf{25\%\ all\ below})\ ;$$

From Equations 8 above the state of non-compliance occurs when activities are done informally and no guided procedures are followed by the organization. It shows that the user and their organizations have non-compliant to the specific requirements of ISO 27001 standard at is UISM is below 25 %.

5.6 Maturity Threshold Scores

The working of the maturity model assessment threshold scale is such that the threshold scores which are in a scale of 0 to 5 were pegged at 4. This score denotes that the organization agree to be compliant to the requirements of ISO 27001 standard. Score 5, which denote that the organization process are in desired state and continuously improving in line with ISO 27001 compliance standard requirements. This meant that the organizations average score per assessment question was at a mature 5 and therefore desired level of maturity.

However, average scores of 0, 1, 2 and 3 which are below the threshold score (4) means that the organizations maturity index is increasingly tending towards 0% which is considered to be highly risky for the organization. These scenarios therefore call for action by the organization to minimize the information security risk. Recommendations for best practices are therefore associated on the threshold scores.

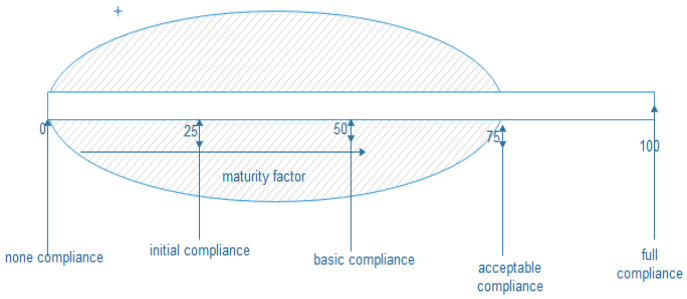

Figure 1 Assessment Scale Source: (Author, 2018)

As presented above, the state of non-compliance is represented by a score between 0% - 24% maturity, initial compliance at 25%-49%, basic compliance 50%-74%, acceptable compliance 75%-99% and full compliance at 100% maturity level. The 0% and 100% maturity are atomic values which are pegged on a scale of 0 to 5 and is unrealistically achievable in any information security situation.

The entirety of information security maturity levels discussed above seeks to show the level of compliance that a particular organization can be accordingly with its information security process. Based on the specific level an information security index computation logic is provided and a guiding recommendation report is determined based on associated risks.

V. RECOMMENDATION

The research provides an invaluable input into provisioning a model to determine information security maturity. The studies empirical contribution strengthens social and technical approaches to IS security. The research viable output on different levels of computation can be extended to other organizations. There's unlimited potential for a model that is readily accessible and provides a prediction through auditing of information security maturity levels of compliance for organisations. The depiction of official information security maturity would offer a feasible mechanism for universities to improve their information security.

ACKNOWLEDGMENT

I wish to thank the head of the school of Computer Science and Bioinformatics as well as the Department of Information Technology, Kabarak University for the support accorded to me during the development of the model.

REFERENCES

[1.] Yang, Yaping. "Literature review of information security practice survey reports." (2018).

[2.] Dzazali, Suhazimah, "Social Factors Influencing the Information Security Maturity of Malaysian Public Service Organization: An Empirical Analysis" (2006). *ACIS 2006 Proceedings. Paper 103*.Electronic version found at http://aisel.aisnet.org/acis2006/103.

[3.] Surni Erniwati and Nina Kurnia Hikmawati. An Analysis of Information Technology on Data Processing by using Cobit Framework, (IJACSA) Intermasional Journal of Advanced Computer Science and Application, Vol. 6 No. 9 2015, pp 151 – 157.

[4.] Kerzner, H., & Kerzner, H. R. (2017). *Project management: a systems approach to planning, scheduling, and controlling*. John Wiley & Sons.

[5.] Almutiq, Mutiq Mohammed. "An evaluation model for information security strategies in healthcare data systems." PhD diss., Keele University, 2018.

[6.] Suwito, M. H., Matsumoto, S., Kawamoto, J., Gollmann, D., & Sakurai, K. (2016). An Analysis of IT Assessment Security Maturity in Higher Education Institution. In *Information Science and Applications (ICISA) 2016* (pp. 701-713). Springer, Singapore.

[7.] Malik F. Saleh Management Information Systems, Chair Prince Mohammad Bin Fahd University Al Khobar, 31952, Saudi Arabia, 2011

[8.] Da Silva, Denise Ranghetti Pilar, and Lilian Milnitsky Stein. "Information Security: A Reflection on the Human Component." *Science & Cognition* 10 (2011).

[9.] Curry, M., Marshall, B., Crossler, R. E., & Correia, J. (2018). InfoSec Process Action Model (IPAM): Systematically Addressing Individual Security Behavior. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *49*(1), 49-66.

[10.] Bourgeois, Dave, and David T. Bourgeois. "Information Systems Security." *Information Systems for Business and Beyond* (2014).

[11.] Siponen, Mikko T. "A conceptual foundation for organizational information security awareness." *Information Management & Computer Security* 8, no. 1 (2000): 31-41.

[12.] Albuquerque Junior, Antonio Eduardo de, and Ernani Marques dos Santos. "Adoption of Information Security measures in public research institutes." *JISTEM-Journal of Information Systems and Technology Management* 12, no. 2 (2015): 289-315.

[13.] Garcia, Mary Lynn. *Design and evaluation of physical protection systems*. Elsevier, 2007.

[14.] Björck, Fredrik. *Discovering information security management*. Department of Computer and Systems Sciences, Stockholm University, 2005.

[15.] Belasco, K., and S. P. Wan. "Online retail banking: security concerns, breaches, and controls." Handbook of Information Security: threats, vulnerabilities, prevention, detection, and management 1 (2006).

[16.] Dresner, Daniel Gideon. "A study of standards and the mitigation of risk in information systems." PhD diss., The University of Manchester (United Kingdom), 2011.

[17.] ABNT, AB de NT. "NBR ISO/IEC 17799–Tecnologia da Informação–Código de prática para gestão da segurança da informação." Rio do Janeiro: ABNT (2005).

[18.] Makupi, D., Karume, S.M., Rabah, K. (2016). The Impact of Driver Behaviour on Road Accidents and the Need for a Driver Road Safety Index (DRSI) in Kenya. Mara Res. J. inf. Sci. Technol. Vol. 1, No. 1, pp. 66 - 77. ISSN 2518-8844.

[19.] Kombo, Donald Kisilu, and Delno LA Tromp. "Proposal and thesis writing: An introduction." Nairobi: Paulines Publications Africa 5 (2006): 814-30.

[20.] Siponen, Mikko, and Robert Willison. "Information security management standards: Problems and solutions." Information & Management 46, no. 5 (2009): 267-270.