AN ISO 27001 BASED MODEL TO DETERMINE UNIVERSITY INFORMATION SECURITY MATURITY UNDER UNCERTAINTY

MAKUPI DANIEL

A Thesis Submitted to the Institute of Postgraduate Studies and Research for Partial Fulfilment of the Requirements for Doctor of Philosophy in Information Technology Security and Audit of Kabarak University.

JANUARY, 2021

DECLARATION

1. I do by declare that:

(i) This thesis is my original work prepared with no other than the indicated sources and to the best of my knowledge; it has not been presented for the award of a degree in any university or college.

(ii) The work has not in-cooperated material from other works or a paraphrase of such material without due and appropriate acknowledgement.

(iii)The work has been subjected to processes of anti-plagiarism and has met Kabarak University 15 per cent similarity index threshold.

2. I do understand that issues of academic integrity are paramount and therefore I may be suspended or expelled from the University or my degree may be recalled for academic dishonesty or any other related academic malpractices.

Signed: ______________________________Date:__________________________

Name of Student: **MAKUPI DANIEL** Admission Number: **GDS/M/0484/05/17**

RECOMMENDATION

This Thesis entitled **“An ISO 27001 Based Model to Determine University Information Security Maturity under Uncertainty”** and written by Makupi Daniel is presented to the Institute of postgraduate studies and research of Kabarak University. We have reviewed his thesis and recommended it be accepted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Information Technology Security and Audit of Kabarak University.

Signed …………………….. **Date** ………………..…………

Dr. Nelson Masese

Department of Computer Science

Kabarak University.

Signed …………………….. **Date** ………………..…………

Prof. Simon Maina Karume

Department of Computer Science

Kabarak University.

COPYRIGHT

ACKNOWLEDGMENTS

I express my special thanks and gratitude to my supervisors Dr. Nelson Masese and Prof. Simon Maina Karume who has immensely contributed to this work. I also express my appreciation to the University staff, members of the Computer Science Department, librarians and my classmates for their valued ideas.

DEDICATION

This work is dedicated to my parents David and Nelly Chemaoi who have been the source of my inspiration.

ABSTRACT

The use of information technology and related process has permeated into organizations of all sizes. Moreover, in recent years, almost all organizations, if not all are involved in protecting their technology investment, if not for protecting cooperate image, then for ensuring provision of confidentiality, Integrity and availability of Information security ensures availability of services to stakeholders. Information security managers must be aware of their information security posture to better prepare in advance and minimise the risk of attacks. The study came up with a model based on ISO 27001 to aid universities in determining their level of maturity in information security. The study adopted specific clauses relevant to universities because of its unique organizational egocentric nature having varied categories of users and extensive research allowing it to serve as a plausible area of study compared to other organizations. The study adopted scientific approach to obtain data using simple random sampling with an online questionnaire distributed to respondents and analysed with SPSS. Secondly, design science approach was then adopted for realization of the web based model. From the output, foremost Reliability and validity of data collection for analysis was carried out which revealed a Cronbach Alpha of 0.917. The impact of Individual variable weights to university information security was then established, followed by inferential analysis showing how individually the different variables impact on the maturity model. From the regression, administrative factors impacted on overall security at .436, technological factors at -.157and physical factors .590respectively with statistic overall regression model significant at r^2= .610, F (3, 116)=60.517; p <0.05. All the three factors were found to correlate significantly with the risk management mechanism and therefore taken into consideration for model design and development. Using Goal Question Metrics approach (GQM), individual variable weights were mapped to the model. To implement the model, design science approach was followed realizing a prototype of a web-based implementation available at www.matricuda.com/makupi. The functional model determined maturity in information security and produced relevant organizational specific report.

Keywords: *Information, maturity, model, metrics, university, ISO 27001*

TABLE OF CONTENTS

LIST OF EQUATIONS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ISMS	Information Security Maturity System
ISO	International Organization for Standardization
IEC	International Electro-technical Commission
ISMM	Information Security Maturity Model
MVC	Model View Controller pattern
BC	Business Continuity
DC	Disaster Recovery
BCM	Business Continuity Management
PDCA	plan-do-check-act
DRP	Disaster recovery plan
RTO	Recovery time objective
ICT	Information Communication Technology
NIST	National Institute for Standards and Technology
US	United States
HIPAA	Health Insurance Portability and Accountability Act
UK	United Kingdom
ISACA	Information Systems Audit and Control Association
BAI	Build, Acquire, And Implement
HIPPA	Health Insurance Portability and Accountability Act
ISC	Information System Security Certification Consortium
CISSP	Certified Information Systems Security Professional
IBM	International Business Machines
CEO	Chief Executive Officer
LSC	Local Security Committees
IAO	Information Asset Owners
ISSP	Issue-Specific Security Policy
PDA	Personal Digital Adapters
ITAM	IT Asset Management
HR	Human Resource
KPA	Key Process Areas
CMM	Capability Maturity Model
ANOVA	Analysis of Variance

SSE	System Security Engineering
HLI	Higher Learning Institution
EAMMF	EA Management Maturity Framework
KMO	Kaiser Meyer Olkin
POC	Proof of Concept Approach
GQM	Goal Question Metrics Approach
UISM	University Information Security Maturity
IT	Information Technology
IS	Information System
COBIT	Control Objective for Information and related Technologies
MLoSC	Maritime Logistics and Supply Chain
AHP	Analytic Hierarchical Process
MITIGATE	Multidimensional, Integrated, Risk Assessment Framework and Dynamic, Collaborative Risk Management Tools for Critical Information Infrastructures
ES-C2M2	Electricity Subsector Cyber Security Capability Maturity Model

OPERATIONAL DEFINITION OF TERMS

Information Security Maturity Model: Information Security Maturity Model (ISMM) is a tool 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 (Saleh, 2011).

Metric: The standard of measure of a degree to which a software system or process possesses some property. (Mari & Maul, 2020).

University: An institution of higher education and research which awards academic degrees in various academic disciplines (Louw & Von Solms, 2018).

ISO 27001: ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an Information Security Management System (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes (Haqaf & Koyuncu, 2018)

CHAPTER ONE

INTRODUCTION

This section discusses the background of the concepts and problems to be addressed towards information security maturity. It further proceeds to state the research problem, outlining the research objectives, lists the research questions, and defines the scope, assumptions, significance and the expected outcomes of the study.

1.1Background to the Study

Determination of maturity in information security is key to every organization seeking to gain competitive advantage. In not more than two decades ago, organizations have begun Identifying, planning, scheduling and implementing information security management as an organizational framework (Edwards, 2018). "Maturity" in this case, relates to how formal and optimized processes are for any given program. Higher level of maturity signifies few number or chances of avoidable errors occurring. This is a reflection of quality in the use of resources.

In evaluation of information security, they 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 (Rhodes-Ousley, 2013; Whitman & Mattord, 2012; Information Systems Audit and Control Association (ISACA), 2012; The ISO 27000 directory, 2007; Yost, 2007; Bowen *et al*., 2006).

The different standards and information security frameworks that already exist have been helpful to organizations for efficiency in information security risk management (Khouja *et al*., 2018). However, because of proliferation of the cyberspace and more continued reliance on information and related technologies in operations of organizations, it has led to elevated levels of information security requirements (

Moulton & Coles, 2003; Posthumus &Solms, 2004; Kooper, Maes, & Lindgreen, 2011; Bahl & Wali, 2014; Edwards, 2018) in view of continued information security needs and ever-changing information security landscape, the existing processes and governance structures still appear to be unfit, unstructured, and unreliable.

Moreover, there exist a gap in modelling information security maturity models given that there is inadequate attention to what should be treated as adequate security and how information security controls can be considered as effective. It's therefore difficult for organizations to optimize their security requirements and inhibits realization on threats facing them including the likelihood and possible impact. Without a requisite model that fits the organization process, it proves difficult for organizations to measure performances, ensure compliance to regulations, validate sufficiency in safety, and identify improvements in information security.

Given the ever-widening cyberspace and the challenges of proliferation of technology, organizations especially universities in this case study, need to clearly comprehend and determine their information security maturity levels, resulting priorities, what is important, and what is relevant to them, what approaches will work, the direction they need to take, and most importantly which correct defence in depth strategy to alleviate the situation.

There are two approaches in implementing maturity models. The top-down approach, entailing a fixed number of maturity stages specified in the beginning with each stage having its own characteristics, supporting how maturity evolves (Becker et al, 2009). On the other hand, bottom-up approach according to Lahrmann, *et al.,* (2011), proposes that first distinct assessment characteristics are determined then clustered into maturity levels to denote more general view of maturity evolution.

This research work, designs and develops an information security maturity model to assess the level of maturity based on specified rules in ISO 27001. The model divides organization into five levels of attainment. The levels depend on controls in place and automation. The levels are nonexistence, *ad hoc*, *repeatable*, *defined*, *managed*, or *optimized*. In practice auditors consider technology, tools, techniques, resources and the overall infrastructure to ascertain the level of maturity in information security.

The model was therefore, adapted from ISO 27001 and applied in two scenarios. First, the model considers input weights from individual organization and process weighted agreements according to the different information security factors derived from ISO 27001. It then, generates a report documentation on the indicated areas of concern. Then, it determines whether the organization is at a suitable security level or need to develop the security procedures. However, the model takes into consideration the ISO 27001 areas that are closely applicable to university subsector. After successful assessment of maturity, defence in-depth strategies such as has reconnaissance, foot-printing, enumeration, scanning can be undertaken.

1.2 Statement of the Problem

In the 21st century, universities like any other organizations face unique information security challenges amid the ever widening cyber space. They must respond to the demands for ensuring protection of stakeholder's data while minimising information risks coupled with the BYOD reality within its ecosystem. At the same time, they are constrained on which approach to use in order to prior prepare against information security attacks. Their strategies, are, therefore in-house audits and some depend on compliance to existing guidelines and frameworks. However, Susanto & Almunawar (2018), in their research work, noted that despite such many certification standards and information security frameworks in place, concerns have been raised on the "effectiveness of such alignment and information security audit and governance being viewed as an unmanageable mechanism" which makes it difficult for organizations to appropriately counter attacks. If universities are to ensure information security and prepare for attacks while ensuring they gain maturity in information security, at minimum, they need at least a dedicated model taking into consideration specific concerns facing its strategic assets. It is only when universities are conscious of their information security that they can succeed in addressing their information security concerns.

1.3 Objective of the Study

The main objective of the study was to develop a model to aid universities in determining the level of maturity in regard to information security based on ISO 27001 standards. The specific objectives being:-

i. To determine the critical information security risk factors that impact on the security of universities based on ISO 27001.

ii. To explore the existing models used in assessing information security maturity.

iii. To design a model to determine university information security maturity.

iv. To implement the model to determine university information security maturity level.

v. To verify the prototype for computing information security maturity in universities

1.4 Research Questions

The research seeks to answer the following questions;-

i. What are the critical security risk factors that impact on the security of universities based on ISO27001?

ii. What are the existing models used in assessing information security maturity?

iii. How can a model determine the maturity level of information security in universities be designed?

iv. How can the model determine university information security maturity level be implemented?

v. Can the model compute university information security maturity?

1.5 Research Contributions

The output of this research is to come up with the following deliverables;

i. A report on critical security risk factors that impact on the security of higher learning institutions based on ISO27001.

ii. A report on existing models used to determine information security maturity.

iii. A prototype of a web-based implementation model to assist universities to determine information security maturity based on ISO 27001.

iv. A verification report on the functionality of the prototype to determine university information security maturity.

1.6 Justification of the Study

This study contributes in reducing information security attacks within the dynamic cyber space ecosystem of Universities. The complex nature of combination of student and employee personal and confidential data such as medical records, commercially desirable research and financial information makes universities prime targets. In contrast the open collaborative learning environment brought about by cultural openness of universities has made them face unique challenges compared to other organizations because of its wide attack surfaces necessitated by networks that must allow for more open access to different stakeholders. For information security managers, the model provides a facility to aid in quantitative evaluation of investments against returns. Given that universities play a key role in economic growth by providing necessary knowledge and skills through research, then the enhanced protection of its information technology infrastructure is beneficial to university stakeholders directly and indirectly.

1.7 Scope of the Study

This study primarily focused on developing an Information Security Maturity Model specifically, to Compute Information Security Maturity level of universities. Data was obtained from 120 respondents directly involved in information technology operations in both public and private universities in Kenya. Case study organizations were involved in the evaluation to determine their positions on the developed five-layer maturity model. By universities being able to determine their maturity, then their investment in information infrastructure can be justified. It is worth highlighting, however, that the maturity model developed is not a substitute for an information security improvement program existing. It can only be used to appraise an organization by determining its maturity in information security and giving a relevant recommendation report; it is not meant to prescribe a solution to raise the organization’s information security.

1.8 Limitations of the Study

Despite the overall realization by developing an information security maturity model for organizations achieved in this study there were, some limitations which included:

i. Large Organizational Bias: Samples were drawn from 74 universities in Kenya involving 120 key personnel directly involved in organizational information technology operations. This hampers transferability of results since the economic outcomes of this research might differ with non-academic institutions and also small-size organizations whose economic realities& situational operation setting differ on security investments.

ii. Focus Area of Study: The environment context of data collection happened in universities because of its significant number of the population coming together in one setup and complex nature of BYOD policy coupled with the different types of clients ranging from students doing research and experiments and faculty. This multifaceted structure of university setting makes the results more applicable for universities than other types of organizations.

iii. Also, there is a possibility that respondents were dishonest as to provide inaccurate data on the nature of risks and security defence-in-depth strategy. Although giving dishonest results was minimized by strongly advising that the data being collected were strictly for educational purpose and will not be used for other purposes outside what is outlined in the research permit.

1.9 Assumptions of the Study

The study assumed that all the respondents were knowledgeable in information security concerns of their respective organizations and intelligent enough to answer all the questions appropriately. There was no training undertaken and questions were answered with required honest &integrity.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter discusses information security (ISMS) maturity, information security maturity factors based on ISO 27001 that are relevant to universities and finally the existing information security maturity models.

2.1.1Maturity

Maturity is a mosaic of several notations (COED, 2011). The economic, industry or organizations perspective point of view is growing to the point where substantial growth cannot further expand. Maturity in this case, relates to how formal and optimized information security processes are for university sub- sector.

Information Security Management is the process of managing the day to day security work, training and awareness of security programs & how compliance to security policies are handled (Humphreys, 2008). Information Security Maturity level is the measurement of the organization’s capability to remain secure (Dzazali, 2006). It is important for organizations today, in order to improve effectiveness and efficiency of enterprise business processes (Surni & Nina, 2015).

2.1.3 Information Security Maturity Model (ISMM)

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 (Suwito, *et al*, 2016). 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 security needs **(**Malik, 2011).

2.2 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 (Mitnick & Simon, 2003; Silva & Stein, 2007; Sêmola, 2014). 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.

Curry*et al* (2005) proposes to classify Information Security measures as they aim to affect educational institutions and industry. Similarly, Alisom Anderson and Dennis Langley developed a security management system based on security studies of different organizations and proposed three groupings for monitoring internal security controls and introduced the Management, Technical and Operational (MTO) approach. Therefore accordingly below are factors that are relevant to an educational entity.

i. Administrative measures: these are formal rules present in an Information Security Policy or informal training and education to promote knowledge on Information Security (Siponen, 2000). 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 (Albuquerque & Santos, 2015). 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 (Garcia, 2007). They are related to the security of property, such as doors, locks and perimeters, and measures against environmental events such as floods and fire.

According to, (Björck, 2005), Belasco and Wan (2006) and ABNT (2005) 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, Sêmola (2014) warns that each organization has its own characteristics, and that this leads to particular needs of Information Security. Dresner (2011) agrees and adds that the simple adoption of measures proposed by standards and models does not guarantee the mitigation of risks.

Likewise, ABNT (2005) 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 the ISO 27001 standard.

2.2.1 Human Resource Security

Employees, contractors, and people within an organization are the greatest assets to that organization because of the value they bring in. however, they are considered to be the weakest link in information security (Bulgurcu *et al.,* 2010). According to ISO 27001's control 8; human resource security is most important because the security of information in any organization is the responsibility of the employees and other people within that organization. Although some security threats and breaches are as a result of non-human factors, most of these threats and breaches are widely propagated by humans either accidentally or maliciously (Brauch, 2011).

The management of Information Security focuses on technology, processes, and people although many educational institutions put a lot of emphasis on securing processes and technologies. Information security, therefore, has it's on the human challenge and that means that it is the people that develop the culture of the organization and therefore custodians of security (Ashenden, 2008).

Recent research indicates that over 80% of system-related theft and fraud in Kenya were perpetrated by insiders who include employees of organizations. The report continues to portray that in 2016 alone, 50% of the direct costs of cybercrime was attributed to insider threats (Serianu, 2016). In as much as the people are seen to be the main perpetrators of security breaches, employees and other people within organizations can be targeted in the event, for instance, KPMG Cyber Crime Survey of 2015 indicates that 64 percent of security breaches in many organizations target senior management and directors.

The main objective of ISO 27001's control 8 is to set rules and baseline requirements that organizations can apply prior to, during, and after termination or change of employment for all the employees hired or contracted by that organization.

i. Prior to Employment

Pre-employment security issues captured in Control A.8.1 of the standard aims at ensuring that the most suitable candidates are hired for the job and that they understand their responsibilities in respect of the ISMS and information security within the organization (Calder & Watkins, 2008). In this case, the organizations are required to do a thorough screening of the candidates being considered for the position by verifying their background in accordance with relevant laws, ethics, and other regulations, the perceived risks, proportional to the business requirements, and the classification of the information to be accessed. In addition, the control requires that the candidates being considered must agree to the terms and conditions of employment by signing non-disclosure agreements where they will be working with sensitive organizational information.

ii. During Employment

Control A.8.2 of ISO standard applies to employees, contractors and other users who work to bring value to the organization and the period during which they serve in those organizations. This is to basically ensure that the hired employees and contractors are aware of their security responsibilities and execute them. The main objective of this control is to ensure that all the employees, contractors and other third-party users are aware of information security threats and are fully equipped to support the organizational security policy in their normal operation by reducing the risk of human error. In the event, all the concerned must strictly comply with the organizational laid down policies and procedures (Annane *et al,* 2019).

The organization should focus on security awareness and training on the entire user population with the management setting precedence for suitable IT security behaviour within an organization. Effective information security awareness, education, and training programs should be established in all levels of the university and should act as a basis for a formal disciplinary process for employees, contractors, and other third-party users who commit security breaches (Wilson & Hash, 2003).

iii. **Termination or change of employment**

The objective of this control is to ensure that employees, contractors, and other third-party users change employment or exit the organization in an organized fashion. In this case, the responsibilities for performing termination or change of employment for the concerned employees or contractors are well defined and assigned. Upon termination of employment, agreement or contract, the affected employees, contractors, or other third party users are required to return the organization's assets which they possess. In addition, the access rights and permissions for which the employees or contractors were assigned needs to be revoked upon termination or changed appropriately if the affected persons are changing employment terms (ISO 27001, 2013).

2.2.2 Information Security Policy

A policy is a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters. The Code of Practice was adopted as an international standard by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) as ISO/IEC 17799 in 2000 as a framework for information security.

Management from all communities of interest must consider policies as the basis for all information security efforts. Policies direct how issues should be addressed and technologies used. Security policies are the least expensive control to execute, but the most difficult to implement (Jennex & Durcikova, 2019).

The management of universities included should have a security policy in place; policy is classified into issue or system specific. The issue specific policy (ISSP); addresses specific areas of technology, requires frequent updates and contains an issue statement on the organization's position on an issue. On the other hand, while the issue-specific policies are formalized as written documents, distributed to users, and agreed to in writing, System specific is frequently codified as standards and procedures used when configuring or maintaining systems. The policy needs to be managed and classified to be effective in an organization (Zeegers, 2018).

Policies in an organization are the living documents that must be managed and nurtured has they constantly change and grow. Special considerations should be made for organizations undergoing mergers, takeovers, and partnership. In order to remain viable, policies must have an individual responsible for reviews, a schedule of reviews, a method for making recommendations for reviews and an indication of effective and revision date.

Automated policy management has also emerged as a new category of software for managing information security policies. In recent years, this category has emerged in response to needs articulated by information security practitioners (Ganek, & Corbi, 2003). While there have been many software products that meet specific technical control needs, there is now a need for software to automate some of the administration of policy

Secondly, the classification of information is an important aspect of policy. The same protection scheme created to prevent production data from accidental release to the wrong party should be applied to policies in order to keep them freely available, but only within the organization. In today's open office environments, it may be beneficial to implement a clean desk policy (Elsbach, & Bechky, 2007). A clean desk policy stipulates that at the end of the business day, all classified information must be properly stored and secured.

2.2.3 Information Security Compliance

The state of compliance is the act of being in conformity to fulfil the official requirements whereas security compliance is the state of conforming with functional security requirements that are imposed externally and of giving assurance thereof (Julisch, 2009). Compliance management, on the other hand, is the procedure through which educational institutions universities included deals with the entire compliance process from the onset (Chatzipoulidis & Mavridis, 2009). The ISO27001 A.15.1 standard deals with the requirement that the organizations should avoid breaching any law, statutory, regulatory or contractual obligations, and of any security requirements.

Information security compliance therefore, is imperative for organizational risk management. However, top management in this context, are required to know what level of protection they are getting from their investments in security. It is even harder to estimate how well these investments can be expected to protect their organizations in the future as security policies, regulations and the threat environment are constantly changing (Beres, *et al.*, 2009). An information system would transition between several distinct vulnerability states. The first state is hardened and it occurs when all security-related corrections, usually patches, have been installed.

The second is vulnerable and it occurs when at least one security-related correction has not been installed. The final state is compromised and it occurs when it has been successfully exploited (Arbaugh, 2000). Within these states, metrics need to indicate how secure the university is so that the window of exposure can be minimized by the security operations teams in an organization by following a standard patching process to eliminate vulnerability and any associated risks. The security team either deploys patches after the vulnerability was first disclosed or updates signatures that are associated with attacks.

The longer the window of exposure, the more the organization is exposed to attacks and exploits. The magnitude of risks is minimized if organizations are conscious of their security needs. Therefore the proposed ISMM closely considers five levels of compliance. Security is believed to improve as the organization moves up these five levels (Saleh, 2011). The levels of compliance are shown below in figure 1.

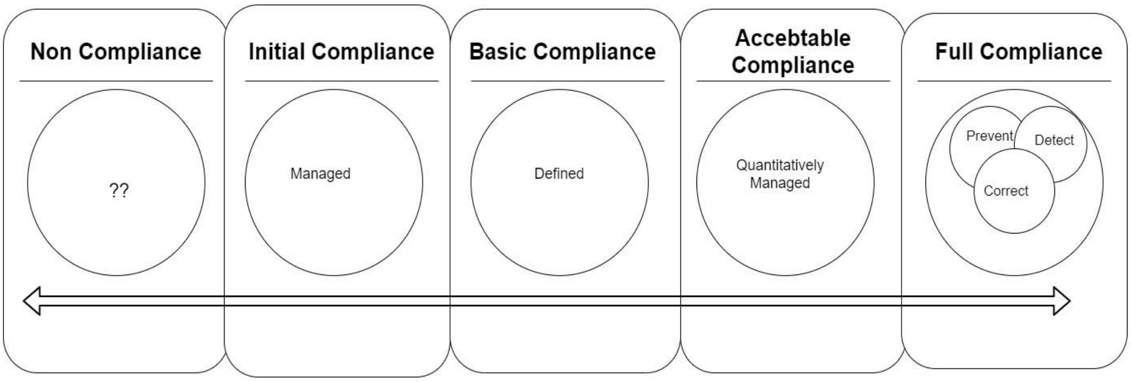


Figure 1: Levels of Compliance (source: Hwang & Cha, 2018)

On the other perspective, none compliance is characterized by none existence of policies and procedures to secure the business. Management does not consider investing in security-related systems necessary for 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 (Schneider, 2000).

The initial compliance state is the starting point for any organization (Checkel, 2001). As long the university is conscious about the threats that their information systems face then the institution is considered to be 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 (Stoneburner, 2000). Organizations recognize the business risks due to vulnerabilities but have no defined policies or procedures to protect the organization.

2.2.4 Access Controls

According to Cruz (2013), lack of appropriate access controls leads to exposure of university assets to potential threats. Exposures are system configuration issues or mistakes in software which allow access to information or act as a springboard for hackers to gain access to a network or a system. Cruz further outlines the attributes of exposure to systems or organizations as; able to allow attackers to collect system information, able to allow attackers to hide traces of their activities, able to include capabilities that can be easily compromised even though their behaviour was expected, the primary entry point for attackers to gain access to systems or organizations, and that exposure is a big problem according to reasonable security policies.

Accordingly, universities need to implement a robust internal control system to ensure that it is not unduly compromised to threats. These internal controls are necessary to guarantee that; The Universities organizational framework sets up comprehensible outlines of authority, The University systems and arrangements should offer business continuity planning, and the process of introduction and assessment strategic plans is all-inclusive and is held on to.

According to Thomson, (2017), the definition for Security access controls is; administrative or technical countermeasures or safeguards to avoid, counter, or decrease loss or inaccessibility due to threats acting on their corresponding vulnerability. These security access controls are categorized into three; physical controls, technical controls and administrative or process controls. Physical controls refer to all physical deterrents and barricades that control access, for instance, lock and keys, and video surveillance systems. Technical controls refer to systems and software used to control access, for example, antivirus software and firewalls. Administrative controls, on the other hand, refer to established policies, procedures, laws, guidelines, and practices that regulate access to information and information systems (Tipton & Nozaki, 2012).

Further, Thomson, (2017) argues that security controls can be classified based on the phase of activities involved in implementing them and the purposes for which they are implemented. The classification includes; preventive controls, detective controls, and corrective controls. Preventative controls are implemented to thwart threats from exploiting vulnerabilities. Detective controls are implemented to identify the threat that land in organizations' information systems. Corrective controls, on the other hand, are implemented to tone down or reduce the outcomes of the threat being manifested. When the environment limits the implementation of activity phase controls or that the activity phase controls fail to operate or are unavailable for use, Thomson, (2017) suggest an alternative set of controls which organizations can implement. He terms these set of controls as compensatory controls and they include; implementation of backup generators, hot sites, and server isolation. Table 1 illustrates the activity phase of the controls (Rodal, 2016).

Table 1: Illustration of Activity Phase Control

PREVENTIVE	DETECTIVE	CORRECTIVE	COMPENSATORY
Security Awareness Training	System Monitoring	OS Upgrade	Backup Generator
Firewall	IDS	Backup Data Restoral	Hot Site
Anti-virus	Anti-Virus	Anti-Virus	Server Isolation
Security Guard	Motion Detector	Vulnerability Mitigation	
IPS	IPS		

According to ISO 27001 (2013), access controls as the name suggests are mechanisms that protect information and information systems from being accessed by unauthorized persons. It is captured in control A.11 of the standard and its main objective is to control access to information. It is broken down into seven sub-clauses denoted as A.11.1 to A.11.7 namely; Business requirements for access control, user access management, user responsibilities, network access control, operating system access control, application, and information access control, and mobile computing and teleworking.

2.2.5 Cryptography

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries (Becket, 1988). More generally, cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages (James, 2011). Also, various aspects of information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, and communication science, none the less becoming specifically critical in universities. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications (Oded, 2004).

Cryptographic controls should be used whenever it is necessary to protect confidential information against unauthorized access (Tuna, *et al,* 2017). Cryptography is the science of writing in secret code, while the encryption is the specific mechanism to convert the information in a different code that is understandable to those who know the mechanism of encryption/decryption (Waschke, 2017).

Therefore, some examples were cryptographic controls are applied include: when you have a device with confidential information such as; external hard drive, flash drive, laptop, etc. and it goes outside the organization. Also you want to send an email with confidential information, file server with a folder to which all employees have access but one (or more) of the files contain confidential information, a public website that users can access by entering username or password (in this case, the password is sensitive information which, if not traveling on a secure channel, could be disclosed), you have a website from which you offer e-commerce and have a payment gateway and when employees connect to the corporate network from home to access corporate resources (Turban, *et al*,2017).

2.2.6 Physical and Environmental Security

Control 9 of ISO 27001 deals with physical and environmental security and its main objective is to prevent unauthorized physical access, damage and interference to the organization’s premises and information (ISO 27001:2013). According to Henage & Henage (2013), physical security is achieved through the installation of physical access barriers whereby a physical access barrier hinders or limits access to valuable assets to those who have authority to gain access. In its simplest form, it would include locks on doors to restricted areas. However, as the value of the asset and the risk of loss increases, the sophistication of the physical access controls should also increase. According to ISO 27001 (2013), physical and environmental security is broadly classified into two classes, namely; secure areas that are addressed in control A.9.1, and equipment security that is addressed in control A.9.2.

i. **Secure Areas**

The main objective of this control A.9.1 of ISO 27001 is to protect the working areas and organizations premises from unauthorized physical access, interference, or damage to university information or premises. It is further sub-divided into six sub-clauses denoted as control A.9.1.1 to control A.9.1.6 to assure proper security of working areas.

The subcategories are; physical perimeter security that requires the organizations to protect areas that contain information and information facilities using barriers such as walls and manned gates; physical entry controls that require organization to protect their information and facilities containing information using sufficient entry controls to ensure that only authorized persons are permitted access; secure offices, rooms and facilities that require organizations to design and apply physical security for facilities rooms and offices; protecting against damaged caused by external and environmental threats whether natural or man-made; Design and application of physical guidelines and protection for working in secure areas; and control and isolation of public access, delivery and loading areas to avoid unauthorized access.

ii. Equipment Security

Control A.9.2 of the standard deals with the security of the organization’s equipment. It requires that organizations should protect their assets from damage, loss, compromise or theft and disruption of activities resulting from such breaches. The control is further broken down into seven sub-clauses denoted as A.9.2.1 to A.9.2.7 in order to fully exhaust the aspects of equipment security and disposal (Calder & Watkins, 2008).

Control A.9.2.1 that requires the organizations to site or protect the equipment in order to reduce the risks from unauthorized access, hazards, and environmental threats. According to ISO 27002, there are a number of controls that needs to be considered in equipment siting and protection. They include; situating equipment in places that are free from unnecessary interference or access by persons without permission; storage and information processing facilities bearing sensitive information should not be positioned in such a way that passers-by can overlook; items that require special protection must be isolated to reduce the risk of damage, loss, interference or compromise; ISO 27002 also recommends that organizations should reconsider their internal policies about smoking, drinking or eating within the proximity of information processing equipment; the organizations should also consider the dangers of information leakage (Calder & Watkins, 2008).

2.2.7 Asset management

IT asset management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. The ISO 19770-1 is a process related standard which outlines best practices for IT Asset Management in an organization. The latest revision dates to 2012 and breaks ITAM processes down into 4 tiers in a maturity matrix.

Assets are not only information in electronic form but include; hardware, software, infrastructure, outsourced services, people, and everything else that provide value to the universities (Calder & Watkins, 2008).

IT asset management (also called IT inventory management) is an important part of an organization's strategy. It usually involves gathering detailed hardware and software inventory information which is then used to make decisions about hardware and software purchases and redistribution. IT inventory management helps organizations manage their systems more effectively and saves time and money by avoiding unnecessary asset purchases and promoting the harvesting of existing resources (Kerzner & Kerzner, 2017). Organizations that develop and maintain an effective IT asset management program further minimize the incremental risks and related costs of advancing IT portfolio infrastructure projects based on old, incomplete and/or less accurate information.

i. **Hardware and Software Asset Management**

Hardware asset management entails the management of the physical components of computers and computer networks, from acquisition through disposal (Hassan, 2018). Common business practices include the request and approval process, procurement management, life cycle management, redeployment, and disposal management. A key component is capturing the financial information about the hardware life cycle which aids the organization in making business decisions based on meaningful and measurable financial objectives. Software Asset Management is a similar process, focusing on software assets, including licenses, versions, and installed endpoints.

ii. **Assets Owners**

Asset owner is the human resource who use and utilize the information system. These owners basically are persons who are accountable for ensuring that the assets and information related to those assets are protected from unauthorized access, use, and modification (Calder & Watkins, 2008). Control A.7.1.2 from ISO 27001:2005 Annex A requires that an organization maintains in their Information Security Management System (ISMS) all their assets and have a nominated owner who is a member of staff who will be responsible for those assets. The nominated owners must sign memoranda as agreement to the ownership of the asset. The asset owner can delegate ownership of the asset to another owner who takes the responsibility of the delegated assets. Asset ownership is therefore important because it ensures that each asset assigned to an asset owner is properly managed and protected.

iii. **Assets Inventory**

ISO 27001 Control A.7.1.1 requires that organizations should identify all assets that are valuable to them then draw and maintain an inventory of those assets. It requires that each asset must be identified in the asset inventory and their full descriptions recorded including nominated asset owners. According to ISO27002, the types of assets that need to be identified and maintained in the asset inventory include; information assets, software assets, physical assets, services, people, and intangible assets such as brand and reputation (Calder & Watkins, 2008).

iv. **Acceptable use of Assets**

ISO/IEC 27001 (2013) control A.8.1.3 requires that organizations should document and implement the protocols for the acceptable use of information assets, services, and systems by employees, contractors, and other third parties. The particular focus here is an acceptable use policy on emails, mobile devices, internet, and other information systems outside the organization’s fixed boundaries.

v. **Role of IT asset management in Universities**

The IT Asset Management function is the primary point of accountability for the life-cycle management of information technology assets throughout the organization. The implementation of specific controls may be delegated by the owner, as appropriate, but the owner remains responsible for the proper protection of assets, including information classification (Rabah, 2007).

Included in this responsibility are development and maintenance of policies, standards, processes, systems and measurements that enable the organization to manage the IT Asset Portfolio with respect to risk, cost, control, IT Governance, compliance, and business performance objectives established by the business. IT Asset Management uses integrated software solutions that work with all departments that are involved in the procurement, deployment, management and expense reporting of IT assets.

2.2.8 Business Continuity Management

The term BC/DR implies that the business can continue to run, even in the case of major incidents that are classified as disasters, which can be grouped into two general categories (Schmidt, 2006): natural disasters, such as a flood or tsunami, or those caused by humans, such as terrorism or accidents.

The disturbances can be minor or major, and based on the type of the incident, appropriate measures can be initiated. In most cases, BC alone is sufficient to deal with the events. However, when BC is used in the context of DR, the implication is that the business is recovered at a secondary site so that business activities can continue there (Liu, *et al*, 2008)

Moreover, BCM is a holistic way of managing BC and the corresponding policies and processes in the event of disruptive incidents. The ISO standard 22301:2012 defines BCM as “the holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities” (Estall, 2012). It means a BCM solution should be extensive and detailed and should follow a cycle so that the solution can continuously be improved. For this purpose, ISO recommends the plan-do-check-act (PDCA) cycle, which is depicted in Figure 2 below.

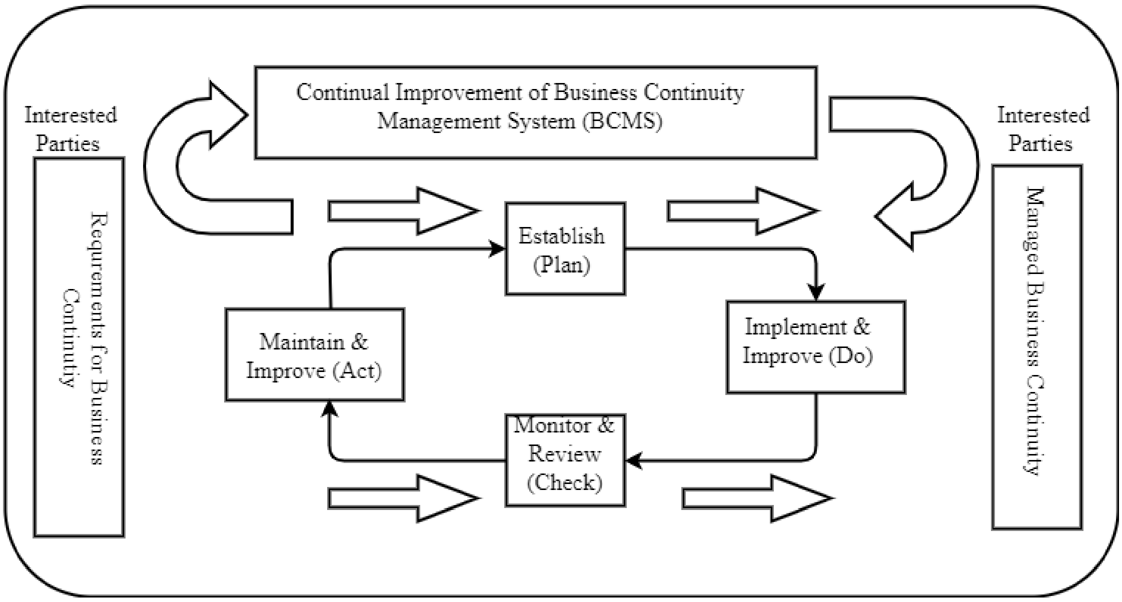

Interested Parties
Requirements for Business Continuity
Continual Improvement of Business Continuity Management System (BCMS)
Establish (Plan)
Implement & Improve (Do)
Monitor & Review (Check)
Maintain & Improve (Act)
Interested Parties
Managed Business Continuity

Figure 2: Plan-Do-Check-Act Cycle

Additionally, BCM consists of several phases, each with multiple steps, to realize implementing a BCM framework. The mapping between BCM steps and the PDCA cycle steps is listed in Table 2 below adapted from (Saint-Germain, 2005).

Table 2: PDCA phases and business continuity management

PDCA Phases	BCM Steps
Plan	Create a business strategy, business objectives, and business continuity management standards.
Do	Perform business analysis steps, such as business inventory, risk analysis, and business impact analysis. Create a business continuity plan. Document the steps.
Check	Perform testing and auditing on the solution. In the case of gaps or missing elements, initiate mitigation activities
Act	Based on test results, auditing results, gap analysis, and assessments performs steps to improve the overall solution. Maintain the business continuity management system.

Apart from ISO standards that can be benchmarked by universities, there are also other standards that can also be considered international standards, and these include: From the National Institute for Standards and Technology (NIST 800-34); Information Technology Service Continuity Management (ITSCM); Control Objectives for Information and related Technology (COBIT); From the US National Fire Protection Association (NFPA 1600); and The US Health Insurance Portability and Accountability Act (HIPAA). It is critical; therefore, to implement information security practices within the organizational context given that each organizational composition of business drivers and risk tolerances vary from each other (Caralli & Wilson, 2004).

2.3 Existing Models for Assessing Information Security Maturity

A security model is very crucial for enterprises as well as universities because it will give an idea of how the prototype or the artefact would behave and also operate in the real world. It is important for every computing design activity to examine the model to understand the working of the system. The following section discusses existing models that are similar to information security maturity.

2.3.1 SSE-CMM -Capability Maturity Model (CMM)

SSE-CMM is the Capability Maturity Model (CMM) for System Security Engineering (SSE). SSE-CMM consists of two parts, namely; the Model for process security techniques, projects and organizations, and Assessment methods to know the maturity process (Kurniawan, & Riadi, 2018).

The staged representation was used in the CMM. A maturity level in the staged approach is a defined and enclosed step in improvement, consisting of a number of key process areas (KPA) specific to that stage. KPAs are the basic structuring elements, which all models have in common (Steenbergen, 2005). A KPA describes related practices of a certain process issue e.g. project management or IT security. The staged approach of CMMI defines five maturity levels for an organizational process. Every maturity level is the foundation for the next level and cannot be omitted.

The continuous representation is used in Integrated Product Development – CMM and in Systems Engineering – Capability Model (Bate, *et al*, 1995). It "offers a flexible approach to process improvement" The organization has the latitude in selecting the KPA that should be improved. Thus, the organizations are able to improve single KPAs e.g. an organization focuses on the improvement of a specific process-related trouble spot, respectively a less developed capability (Chrissis, 2003). But, the latitude in improvement is restricted to the dependencies between the KPAs. The continuous approach uses in contrast to the staged approach Capability Levels for describing the state of improvement.

The difference between maturity and capability levels is that a capability level only classifies the ability of an organization within a certain KPA, for example, IT security or maintenance of EA deliverables, whereas a maturity level classifies the overall ability of an enterprise level process, for example, EA management or software development. Thus, a maturity level is derived from the capability levels of the KPAs.

2.3.2 ICS-SCADA Cyber Security Maturity Assessment Model

The project of ICS-SCADA was used to measure the level of cyber security maturity in Critical Sectors in the EU. It is considered a critical part of the infrastructure analysis in the EU. The model approach was that it was subdivided into three sub-areas which were further expanded into nine operating sub-dimensions (Camarinha-Matos, & Afsarmanesh, 2007). The dimensions were legislation; which covered on the jurisprudence and law matters in the EU partner states in terms of ICS-SCADA security enhancements. It delved on regulations, policy activities and responsibilities at each member state as shown below according to Green, *et al* (2017).

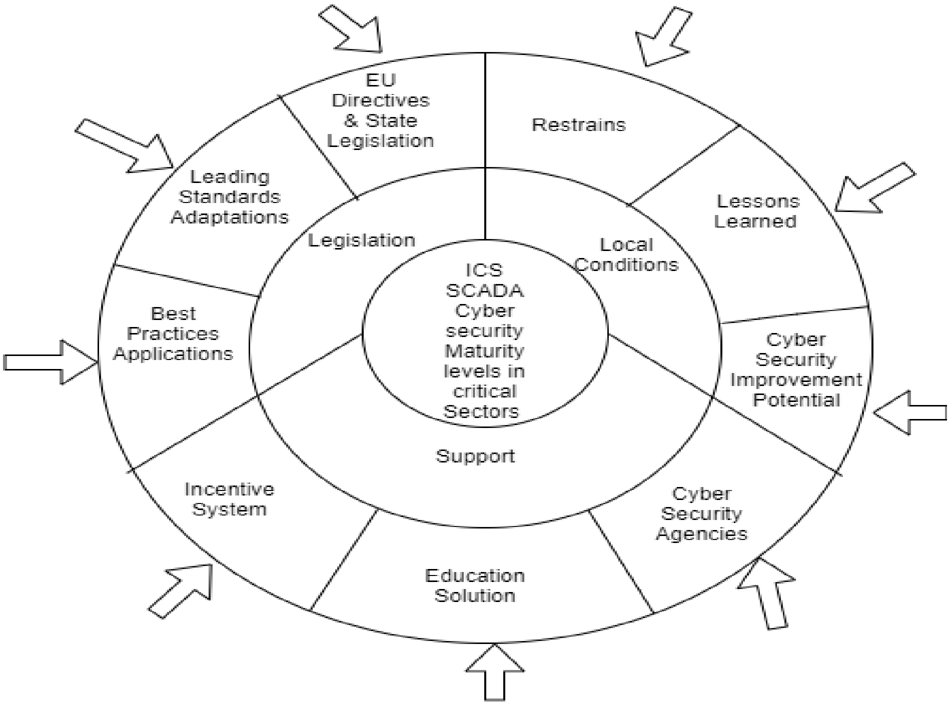

EU Directives & State Legislation
Restrains
Leading Standards Adaptations
Lessons Learned
Legislation
Local Conditions
ICS SCADA Cyber security Maturity levels in critical Sectors
Best Practices Applications
Cyber Security Improvement Potential
Support
Incentive System
Cyber Security Agencies
Education Solution

Figure 3: Dimensions of ICS-SCADA Security Maturity Model

The Support; the execution principle shows how proficient a particular member is in towards advancement of the cyber maturity model by actively improving through participation in the continual improvement of cyber security maturity (McIlmurray, 2008). It shows approaches through which activities of improving information security are driven towards and propagated in existing infrastructure.

Also the conditions locally; where the execution of the model domain reports the merits and the demerits of the in terms of the success of the model. The positive impacts of the ICS-SCADA system are used for future improvement.

The ICS-SCADA operating Dimensions continued to be expanded into further thematic operating sub-domains according to specific areas structured to allow comparisons between member countries (Green, 2017).

Table 3:I: CS-SCADA Cyber Security Maturity Model Dimensions

OPERATING MODEL DIMENSION	OPERATING MODELS SUB-DIMENSION	DESCRIPTION
Legislation	EU Directives & State Legislation	How do the EU and the Member States create policy landscapes to support ICS-SCADA cyber security?
	Leading Standards Adaptation	Do the Member States utilize industry standards to enhance ICS-SCADA security in Critical Information Infrastructure?
	Good Practices Adaptation	Do the Member States develop a systematic approach to collect and exchange good practices among Critical Service providers?
	Good Practices Adaptation	Do Member States support Critical Service providers and encourage them to improve ICS-SCADA cyber security?
Support	Incentive System	Do Member States support Critical Service providers and encourage them to improve ICS-SCADA cyber security?

The Operating Model Sub-Domains are the specific core areas which determine the maturity level of ICS-SCADA cyber security in individual Member of the EU. To be able to compute the specific measure of the maturity level an underlying questionnaire was used to score and evaluate each Operating Model Sub-Dimension (Sahin, 2018). The questionnaires were divided into questions corresponding to the nine sub-dimensions; Create - How is the process developed? Implement - How is the process deployed? Monitor - How is the process reported and monitored? Modify - How is the process adapted and changed. The questions were described with reference to the lifecycle of a process.

The answers for each question were scored against a 5 level scale with clearly defined, question independent criteria. To ensure the reliability of the results, when answers were gathered during the interview, assessment criteria were not shared with the interviewed stakeholders. The maturity levels considered for the purpose of the study were: Basic – activities aren't conducted, Developing - activities are under development or conducted on the ad-hoc manner, Established - activities are regularly conducted on the basic level, Advanced - activities are implemented with a deep understanding of ICS-SCADA specific requirements, Leading - activities are implemented in the level that exceeds current, basic needs (are designed to address needs which arrival is foreseen) (Rauter, 2018).

To complement the analysis, information on additional non-standard activities around cyber security in ICS-SCADA area for the individual Member States should have been taken into consideration. The mixed research methodology (qualitative and quantitative) provides advantages by relegating qualitative analysis to an exploratory tool (Creswell, 2006). It gives a broader perspective over the cyber security maturity subject and enables to capture patterns and make a statistical analysis which makes the study more comprehensive.

2.3.3 Information Security Maturity Model for NIST Cyber Security Framework

The National Institute of Standards and Technology (NIST) have issued a framework to provide guidance for organizations within critical infrastructure sectors to reduce the risk associated with cyber security (Gordon, 2018). From the University perspective, it's clear that NIST CSF is not comprehensive to address all information security related processes that are addressed in some of the existing frameworks. The main objective of the framework is to manage cyber security risks within the organizations that implement it.

The NIST CSF consists of three main parts in which, cyber security is considered as a risk that is managed through the enterprise risk management process (NIST, 2014). Therefore it can be considered as a risk-based framework. NIST CSF, as a framework, has the following nature; Focused on information security high-level requirements and Applicable for the development of information security program and policy.

The profile part of the NIST CSF is focused on tracking the organization progress in implementing the gaps to move from the current state to the defined target. NIST CSF provides Tiers as a visionary tool that allows organizations to understand their cyber security risk characteristics. However, the Tiers do not provide organizations with a mechanism to measure the progress of implementing NIST CSF or their maturity level and information security processes capabilities. Therefore, a maturity model is needed to measure information security processes capabilities. The main objective of a maturity model is to identify a baseline to start improving the security posture of an organization when implementing NIST CSF (Haya, 2018).

2.3.4 Oil and Natural Gas Subsector Cyber security Capability Maturity Model (Ong-C2m2)

The model arises from a combination of existing cyber security standards, frameworks, programs, and initiatives. The model provides flexible guidance to help organizations develop and improve their cyber security capabilities. As a result, the model practices tend to be at a high level of abstraction, so that they can be interpreted for organizations of various structures and sizes (Harder, & Tokarski, 2018).).

The model is organized into 10 domains. Each domain is a logical grouping of cyber security practices. The practices within a domain are grouped by objective target achievements that support the domain (Keller, 2018). The illustration according to Onyeji, *et al*,(2014) is as shown below in figure 4.

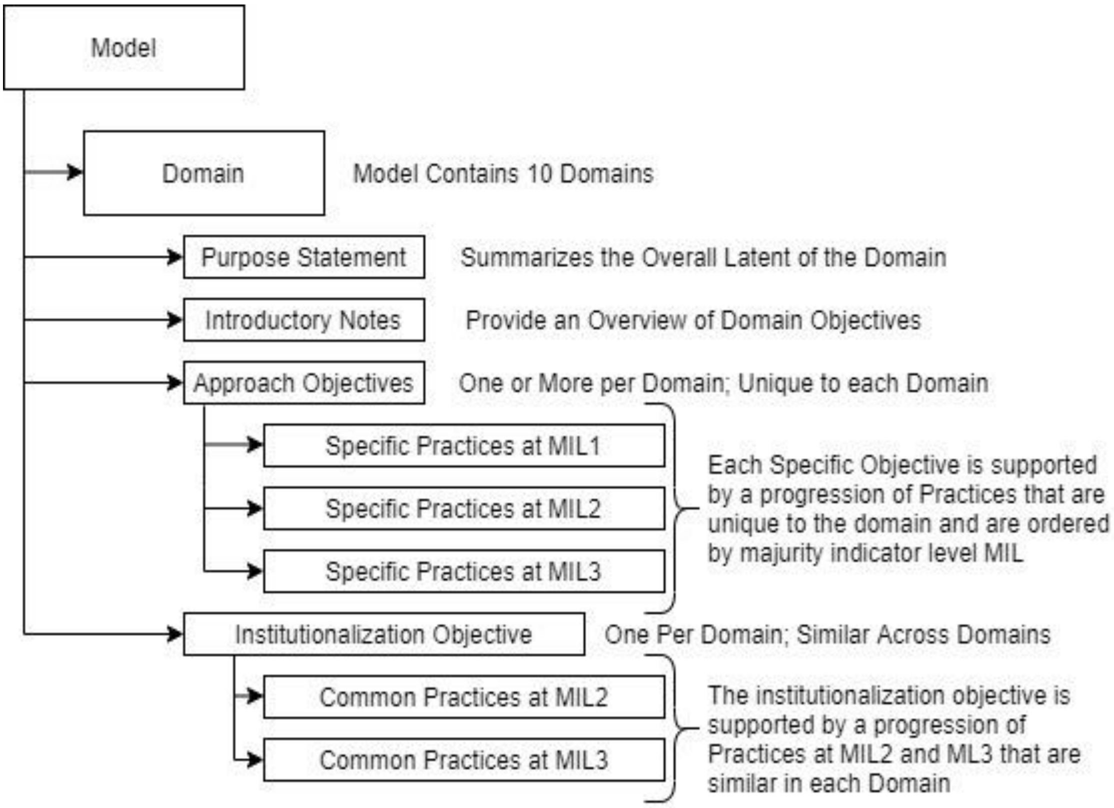

Model
Domain
Model Contains 10 Domains
Purpose Statement
Summarizes the Overall Latent of the Domain
Introductory Notes
Provide an Overview of Domain Objectives
Approach Objectives
One or More per Domain; Unique to each Domain
Specific Practices at MIL1
Specific Practices at MIL2
Specific Practices at MIL3
Each Specific Objective is supported by a progression of Practices that are unique to the domain and are ordered by majurity indicator level MIL
Institutionalization Objective
One Per Domain; Similar Across Domains
Common Practices at MIL2
Common Practices at MIL3
The institutionalization objective is supported by a progression of Practices at MIL2 and ML3 that are similar in each Domain

Figure 4: Oil and Natural Gas Subsector Cyber security Capability Maturity Model

The model defines four maturity indicator levels, MIL1 through MIL3, which apply independently to each domain in the model (Curtis, & Mehravari, 2015). The MILs define a dual progression of maturity: an approach progression and an institutionalization progression.

The domain-specific objectives and practices describe the progression of the approach to cyber security for each domain in the model. Approach refers to the completeness, thoroughness, or level of development of activity in a domain. As an organization progresses from one MIL to the next, it will have more complete or more advanced implementations of the core activities in the domain. At MIL1, while only the initial set of practices for a domain is expected, an organization is not precluded from performing additional practices at higher MILs (Keller, 2018)

The ONG-C2M2 is meant to be used by an organization to evaluate its cyber security capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cyber security investments. An organization performing an evaluation against the model uses that evaluation to identify gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements plans to address the gaps. As plans are implemented, business objectives change, and the risk environment evolves, the process is repeated.

2.3.5 Infosys IT Security Maturity Model (INFOSeMM)

The traditional information security objectives are confidentiality, integrity, and availability. Achieving these three objectives does not mean achieving security. Security is achieved by the prevention of attacks against information systems and from achieving the organization's mission despite attacks and accidents (Saleh, 2011). Infosys IT security Maturity Model (INFOSeMM) has been developed with the objective of assessing an organization's level of preparedness in handling cyber threats (Narasimhalu,*et al*, 2004)

According to Narasimhalu,*et al* (2004), ISM is defined to be a four-level model which categorizes an organization into inactive, reactive, streamlined and proactive with respect to its current status based on a study of the IT security gap analysis. Each organization can be assigned a three letter IT security Maturity index that starts with the poorest rating of DDD to the most desirable rating of AAA.

The framework developed allows Infosys to engage in three main types of assessment and resulting mitigation related projects (Jalote, 2000). The three main categories are IT Security Maturity assessment, Regulation compliance and Vulnerability, and threat assessment and mitigation. The Vulnerability and threat assessment and mitigation can be further subdivided into twenty-four small scale assignments in order to provide for those customers who would like to take small steps towards reaching their desired IT security maturity.

The INFOSeMM IT Security Maturity Model framework has been developed with the goal of including all the major factors outlined in the frameworks, specifications, and methodologies mentioned above. These well thought out frameworks and methodologies can be applied, either in part or as a whole, in both determining a business' INFOSeMM maturity level and in helping it to progress to the desired level

They call the four-level model INFOSeMM, standing for INFOSYS IT Security Maturity Model. The maturity levels are determined by a business' posture towards reviewing and revising its vulnerabilities along three main dimensions – Infrastructure, Intelligence and Practices (Jansen, 2010). We call these the three pillars of IT security maturity level of any organization. It is these three pillars that ensure the stability of an organization from an information security perspective (Subashini & Kavitha, 2011). The diagrammatic representation of information security pillars is as shown below in figure 5 below.

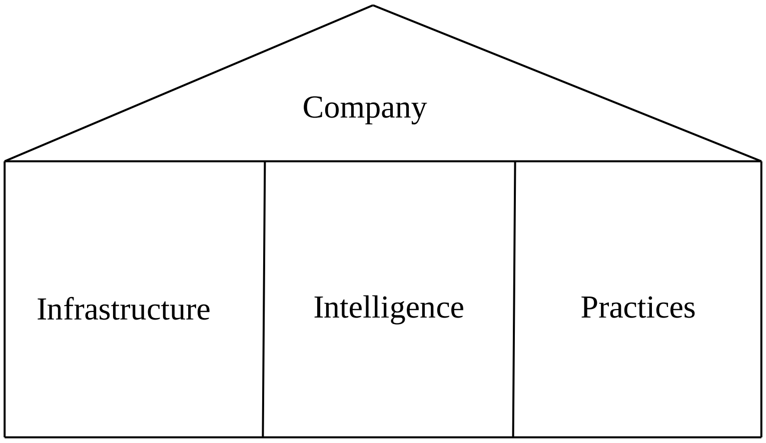


Figure 5: INFOSeMM- Infrastructure, Intelligence, and Practices

Each of the three pillars can, in turn, be defined in terms of their key components. The Network vulnerabilities which include issues related to firewalls, VPNs, Network forensics, advanced boundary controller. The System vulnerabilities which include issues related to Operating Systems, Servers, Domains, Security Architecture (Subashini & Kavitha, 2011). And also, Environment vulnerabilities having issues related to earthquakes, environmental pollution, and terrorism.

In intelligence section application vulnerabilities are dealt with including issues related to malicious code, application forensics, and access control of applications. The data vulnerabilities section issues related to privacy, confidentiality, unauthorized disclosure, non-delivery or misguided information (Johnstone, 2015).

Finally, Practices of human resource vulnerabilities which includes information security awareness amongst employees and others interacting with the company and monitoring the violations and enforcement of the security policies (Da Veiga & Eloff, 2010). The processes include issues such as creating, maintaining and retiring information security-related policies.

2.3.6 Risk Maturity of Maritime Logistics and Supply Chain (Mlosc) Services.

The primary objective is to reduce the gap within the existing risk management policy. According to Kalogeraki, *et al* (2018), existing model in use had significant limitations in terms of capturing the specific security requirements of ICTs and control/monitoring devices, such as IoT platforms, satellites and time installations, which are primary functioning for the provision of Maritime Logistics and Supply Chain (MLoSC) services.

Therefore in a bid to address the cyber security shortcomings they adopted a risk assessment methodology capable of addressing the security particularities and specificities of the complex nature of SCADA infrastructures and Cyber-Physical Systems (CPSs) of the Maritime Logistics Industry.

The approach identified high value asset vulnerabilities and threats to estimate the cyber-risks and their cascading effects within the supply chain (Kalogeraki, *et al* (2018). They introduced a set of subsequent security assessment services. The utilization of these services was then demonstrated through a critical, real-life SCADA scenario that indicated how they can facilitate supply chain operators in comprehending the threat landscape of their infrastructures and guide them how to adopt optimal mitigation strategies to counter or eliminate their cyber-risks.

Critical infrastructure ICS in Maritime such as dockside container cranes, straddle-carriers and autonomous vehicles supporting stevedoring procedures and transporting containers in a commercial port with GPS and optical recognition port operations contain SCADA, DCSs, and PLCs (Ljøsne, 2019)

The key issues focused on risk management methodologies for maritime logistics environments that did not pay attention to the cyber-security nature of their infrastructures and to adequately address the security requirements of the business processes associated with global supply chains.

The complex infrastructure in consideration was SCADA system. It is highly utilized in Maritime Logistics and Supply Chains (MLoSC) because of composite interconnected systems playing a vital role in the transportation, storage and delivery of goods and services. MLoSC services usually involve various and multiple types of Critical Infrastructure, mainly in the transportation sector and exhibit intra-sector and cross-border dependencies.

They used a tailor made tool Multidimensional, Integrated, Risk Assessment Framework and Dynamic, Collaborative Risk Management Tools for Critical Information Infrastructures (MITIGATE) system. MITIGATE is to assess the individual, cumulative and propagated risk of an IT-based supply chain, having in mind the cyber interconnections and interdependencies between the various entities within an MLoSC. It assessed he threats affecting all the business partners involved in the MLoSC and estimates the threats of the MLoSC as a whole via a collaborative environment.

Using MITIGATE they were able to protect the expected individual, cumulative and propagated risks within an ICS infrastructure. They derived risk values that were utilized to generate a baseline security strategy for MLoSCs. Also, identifying the least necessary security controls for each participant within the supply chain. This enables MLoSC participants to fine-tune their security strategies according to their business role as well as their dependencies.

The contributions of this study illustrates that maritime, logistics and transport supply chain services have common characteristics and face similar challenges concerning cyber security. MITIGATE met their requirements and particularities because of their related business process.

To this end, the MITIGATE system supported a number of security assessments that can be used by heterogeneous MLoSC infrastructures of different types, sizes and business activities. Their findings implemented the risk assessment services on an indicative SCADA scenario and has proved that the MITIGATE approach can be successfully applied to complex MLoSC systems, such as SCADA infrastructure, can estimate effectively their cyber-risks and drive the risk mitigation actions.

However, the MITIGATE evidence-driven Risk Assessment methodology provided security assessment services while considering only the cyber-nature of CPSs. It did not put into consideration integration of incident management practices to estimate and handle the combination of physical and cyber-risks on such infrastructure.

2.3.7 Information Security Maturity of an Enterprise Using Fuzzy AHP

The solution is based on hierarchical multilevel information security gap analysis model for ISO 27001:2013 security standard. The measurement of organizations information security maturity under uncertain environment was based on fuzzy set applied to Analytic Hierarchical Process (AHP). The IS maturity index (ISMl) was calculated by following formula:

$$ISMI = \sum_{i=1}^{n} W(C_i).ISMI(C_i), \sum_{i=1}^{n} W(C_i). = 1$$

Equation 1: Fuzzy APH IS Maturity Index

Where W (Ci) is the weight of ith control, "n"=114, is the number of controls in each ISO: 27001:2013.After calculation, the obtained ISMI can be mapped to 6 stages of IS development road-map.

On the other hand in their papers, Itrada *et al*, (2014), Al-Mayahi and S. P. Mansoor (2012) did not mention a group of decision-makers as well as uncertainty in their judgments. Similarly, Nasser (2017), let the weights of controls as:

W (C1) = W (C2) =…= W (Cn) = 1/n.

Equation 2: Weighted Controls for Fuzzy APH

Their main goal was to quantify different factors in information security determination. They applied fuzzy AHP approach to determine important weights and indicators. The weights of various factors were defined to find the most influential factors on the total information security maturity level. Data was obtained from Yemeni Academy for Graduate Studies.

The quantification process considered ISO/IEC 27001: 2013. They took into consideration 14 security control clauses, 35 Control Objectives having 114 Controls. Considering that each security clause (A5-A18) covers one or more objective, each of them has a number of security controls TUDOR (2006).

Similarly in order to determine the level of IS maturity they suggested adoption of COBiT considering its 6-stage roadmap to determine the level of maturity. The breakdown of considered maturity levels suggested by the authors is as shown below, also accordingly with Saleh and Nasser (2017).

Table 4: Maturity Level Assessment Criteria

Maturity Index	Maturity Level
0 – 0.50	0 – Non Existent
0.51 -1.50	1 – Initial / Adhoc
1.51 – 2.50	2 – Repeatable But Intuitive
2.51 – 3.50	3 – Defined Process
3.51 – 4.50	4 – Managed and Measurable
4.51-5.00	4 – optimized

The method considered for the study and even other maturity models do not deal with subjectivity of human aspects. Also, do not consider measures of consistency among respondents or group of decision makers especially in maturity level assessment criteria.

2.3.8 Electricity Subsector Cyber security Capability Maturity Model (Es-C2m2)

The model focuses towards reducing cyber intrusions in the implementation and management of cyber security practices associated with information technology (IT) and operations technology (OT) assets within the surrounding environments of energy sector in United States

The model has been successful in strengthen energy sector cyber security capabilities enabling the organizations to effectively and consistently evaluate and benchmark cyber security capabilities. In addition they have been able to Share knowledge, best practices, and relevant references across organizations as a means to improve cyber security capabilities (Haller, *et al.*, 2010). It has gone a leap in modernizing and making priority options to improve cyber security investment.

It is designed such that it offers a self-evaluation tool for organization which is made available to the respective organization on request. The evaluation tool kit can be used for assessment in a cycle of one day although it can be adapted for more rigorous evaluation (Stevens, 2014). In addition it is also poised to inform the development of new cyber security programs.

The model can be adapted by energy organizations of all types, structures and sizes, owing to its high level of abstraction and also its level of integration to both traditional and emerging enterprise IT assets. It suggests an enterprise risk management strategy that is aligned to cyber security management strategy. The C2M2's cyber security risk management benefits organization in corporate decision on impact, tolerance and risk response.

It was successful in creating a cyber-security architecture that identified the organizational critical assets and coming up with the critical controls to protect valued assets. They were able to gauge the organizational cyber security objectives. Cyber security requirements (confidentiality, integrity, and availability) were ether enabled or inhibited by how the security controls are designed and applied to assets within the function; in other words, by the cyber security architecture (Stevens, 2014).

2.4 Information Security Maturity Model

The design of IT security Maturity Model is to come up with a metric for assessing an organization's level of preparedness in handling security threats. The following section discusses the modelling process

2.4.1 Information Security Maturity Model Design

To ensure information security, it is vital to build security in-design and adapt a security architecture which makes sure that regular security-related processes are deployed correctly. In their research work, Mahmoodi *et al,* (2017) noted that, there's a continued rise in the number of maturity models yearly in different application areas. However, it can be noted that none of the areas of concerns have concentrated on the provision of a specific maturity model for universities. These maturity model are intended as a tool to evaluate the ability of organizations to meet the objectives of security (Carvalho, 2018), IT management (Becker *et al*. 2009, IT Governance Institute 2007), or knowledge management (Kulkarni & Freeze 2004).

The business process management (BPM) also has an array of maturity models postulated (Hammer 2007, Lee *et al*. 2007, Rohloff 2009, Rosemann & de Bruin 2005, Weber et al. 2008), which is probably necessitates the high importance of process orientation and continuous process improvement for organizational design (Wolf & Harmon 2010). In practice, the overall adoption of maturity models is expected to increase (Scott 2007), a prediction corroborated by the numerous proprietary models proposed by software companies and consultancies. Recent studies report increasing academic interest in maturity models (Becker *et al*. 2010). This postulate that different sectorial sectors of human facets will be having their own individual suited maturity models.

Maturity models usually include a sequence of levels, based on the assumption of predictable patterns of evolution and change, (or stages) that together form an anticipated, desired, or logical path from an initial state to maturity (Becker *et al*. 2009, Gottschalk 2009, Kazanjian & Drazin 1989). In this regard, maturity levels indicate an organization's current (or desirable) capabilities as regards a specific class of entities (Rosemann & de Bruin 2005). Maturity models are commonly applied to assess the as-is situation, to derive and prioritize improvement measures, and to control progress (Svensson & Lanander, 2018).

2.4.2 Purposes of Maturity Models

With maturity models representing theories of stage-based evolution, their basic purpose consists in describing stages and maturation paths. Accordingly, characteristics for each stage and the logical relationship between successive stages need to be explicated (Kuznets 1965). As for their application in practice, maturity models are expected to disclose current and desirable maturity levels and to include respective improvement measures. The intention is to diagnose and eliminate deficient capabilities (Rummler & Brache, 1990).

According to, Rummler & Brache (1990) metaphorically refer to such tools as engines for continuously improving systems, roadmaps for guiding organizations, and blueprints for designing new entities. Maturity model serves a descriptive purpose of use if it is applied for as-is assessments where the current capabilities of the entity under investigation are assessed with respect to given criteria (Becker *et al*. 2009). The maturity model is used as a diagnostic tool (Maier *et al*. 2009). The assigned maturity levels can then be reported to internal and external stakeholders.

Also maturity model serves a prescriptive purpose of use on identifying desirable maturity levels and provides guidelines on improvement measures (Becker et al. 2009). "Specific and detailed courses of action are suggested." (Maier *et al*. 2009)

They serve a comparative purpose of use if it allows for internal or external benchmarking. Given sufficient historical data from a large number of assessment participants, the maturity levels of similar business units and organizations can be compared (De Bruin *et al*. 2005, Maier *et al*. 2009).

2.4.3 Design of Maturity Models

The development of maturity models is viewed as a matter of design science research by some IS researchers (Becker *et al*. 2009, Mettler & Rohner 2009). Design science research seeks to create innovative artifacts that are useful for coping with human and organizational challenges (Hevner *et al*. 2004). In this context, Mettler & Rohner (2009) raised the question which artifact type according to the categories given by March & Smith (1995) maturity models actually are.

They suggest that maturity models are “somehow in-between” (Mettler & Rohner 2009) models and methods as they combine state descriptions (models of distinct maturity levels) with activities (methods for conducting assessments, recognizing the need for action, and selecting improvement measures).

The evaluation of artefacts is an essential part of design science research (Hevner *et al*. 2004, March & Smith 1995). Supposed to be innovative and useful, artefacts are commonly evaluated “with respect to the utility provided for the class of problems addressed” (Hevner *et al*. 2004). Accordingly, maturity models refer to the process of maturity model design, others to qualities and components of maturity models as design products.

As for the process of maturity model design, de Bruin et al. (2005) & Becker *et al*. (2009) suggest procedure models. De Bruin *et al*. (2005) propose six phases intended to guide the design of a descriptive maturity model and its advancement for prescriptive and comparative purposes. Becker *et al*. (2009) derive requirements and a procedure model from Hevner *et al*. (2004) design science guidelines. They distinguish eight phases that provide “a manual for the theoretically founded development and evaluation of maturity models” (Becker *et al*. 2009). Though ensuring well-structured and well-documented design processes, both procedure models tell little about design principles.

As for maturity models the design products, qualities and components need to be considered. Whereas qualities represent desirable properties or dimensions of value, components and their interplay shape a maturity model’s structure (Georgiadou, 2019). On the one hand, there are quality taxonomies that apply to (conceptual) modelling in general (Bogdanova & Snoeck, 2019).

Exemplary qualities are correctness, relevance, flexibility, understand ability, implement-ability, and economic efficiency. On the other hand, Simonsson *et al*. (2007), as well as (Manderscheid, 2018), suggest qualities particularly geared to capability assessment models. According to Simonsson *et al*. (2007), a good capability assessment model has to be valid, reliable, and cost-efficient Manderscheid (2018), Postulate empirical foundation, software tool support, standardization, flexibility, benchmarking applicability, certification, disclosure of potential for improvement, evidence of a correlation between maturity model adoption and performance.

As for the components, Ofner *et al*. (2009) recommend dividing maturity models into domain reference models, for example, the domain or scope that is assessed and assessment models on how maturity levels are assigned to particular elements of the domain reference model. On a coarse level, (Pöppelbuß & Röglinger, 2011) suggest structuring maturity models hierarchically into multiple layers. On a detailed level, (Manderscheid, 2018) define a meta-model including components such as competence objects, maturity levels, criteria, and methods for data collection and analysis. Hüner, *et al*. (2009) identify the following components: levels, descriptors, descriptions for each level, dimensions, process areas, activities for each process area, and a description of each activity as performed at a certain maturity level.

2.4 Theories Informing the Study

The theories on information security simply state the motivation behind all attempts by an organization to secure information against threats and create resources that can later improve organizational performance. Information will degrade over time without adequate controls implemented for its protection. In terms of the taxonomy of information systems theories presented by Gregor (2006), describing how and why the phenomenon of information security occurs.

The theory on information security originates from the area of information systems, built entirely from concepts that relate to the information and the breadth of systems that it can reside on. It applies to different levels, including strategies to protect the information used by individuals, groups, organizations and also protects information shared between organizations. The results are that, depending on the information affected, degradation over time may reduce the usefulness of the resource and thus lead to the potential erosion of competitive advantage or organizational success (Huda, 2019).

2.4.1 The use of Technology Acceptance Model (TAM)

Technology Acceptance Model (TAM) is used as the foundation in this study for two reasons; (i) it is easy to be applied and (ii) provide a better understanding on the relationship amongst the variables used in the study (Amin, 2008). Furthermore, it is one of the most influential models which have been widely used in the studies of the determinants of information system acceptance (Ramayah & Jantan, 2004).

Tam was introduced in 1989 by Fred D. Davis, TAM is an information systems theory that models how users come to accept and use technology. TAM is an adaptation of TRA and specifically tailored for modeling user acceptance of information systems (Venkatesh, 2000; Ramayah & Jantan, 2004; Sun & Zhang, 2006; Amin, 2007a; Chung, 2008).

TAM is established generally to provide an explanation of the determinants of technology acceptance and capable of explaining user behavior across a broad range of end-user technologies and user populations while at the same time being parsimonious and theoretically justified (Alrafi, 2006; Amin, 2007b; Amin, Baba & Muhammad, 2007; Amin, 2008; Chung, 2008). The model proposes that when users are presented with a particular technology, two particular beliefs namely perceived usefulness and perceived ease of use affected their behavioral intention to use the system. TAM asserts that the influence of external variables upon user behavior is mediated through user beliefs and attitudes. Beliefs connote a degree of instrumentality tied to action whereas attitudes are purely effective. Beliefs relate to an individual’s subjective assessment that performing some behavior will result in a specific consequence, whereas attitudes relate to an individual’s positive or negative affective feelings about performing the behavior (Seo & Park, 2019).

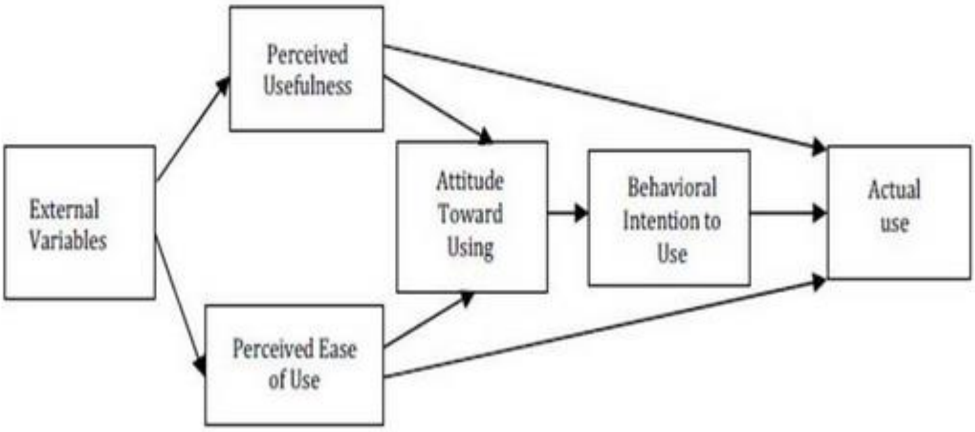


Figure 6: TAM Ali H. Al-Badi, Abdullah S. Al-Rashdi & Taher A. Ba-Omar, 2011 Technology Acceptance: Course and Teaching Surveys Case Study at Sultan Qaboos University.

Technology Acceptance Model has been studied in various setting. For example, Leong (2003) has conducted a study on the robustness of TAM after a decade of its establishment to find out whether TAM is still valid after rapid changes in systems and technologies. He replicated Davis *et al*. (1989) and used Ms. Access as the application software in his study. The results supported the applicability of TAM in the recent technologies where it showed that the two salient beliefs in TAM still provide significant effects on the usage of the tested technology.

A longitudinal study examining technology acceptance by school teachers in Hong Kong has been carried out by Hu, Clark & Ma (2003). They found that perceived usefulness was the most important determinant of teachers' acceptance of PowerPoint application. However, contrary to Davis *et al*. (1989), perceived ease of use failed to show a significant effect on intention.

According to Kang & Namkung, (2019), this contrary result might be due to job relevancy was perceived far more important than ease of use. Thus, even how easy the technology is, it will still not be used if it is perceived as not useful or relevance in one's job. In Malaysia, Md Noor, Hashim, Haron & Ariffin (2005), have studied the effect of perception of trust, risk and sharing on the intention to share and actual sharing of information at the customer to community (C2C) travel and tourism websites. Contradictory to other TAM findings, this study found perceived usefulness and ease of use of knowledge sharing website did not contribute to the intention-behaviour.

Ignatius & Ramayah (2005) provide an empirical investigation on Course Website Acceptance Model (CWAM) which is a modification from TAM (Davis et al., 1989) in investigating course website acceptance amongst students in universities and they suggested that culture may have a potential effect on the adoption of information technologies especially in the developing countries.

Amin (2008) presented a study on factors influencing the intentions of customers in Malaysia to use mobile phone credit cards and found TAM variables have significantly affected customer intention to use mobile phone credit cards. Previously, Amin et al. (2007) have conducted an examination on mobile banking acceptance by Malaysian customers where they added perceived credibility, perceived self-efficacy and normative pressure with TAM. They discovered all elements are significant factors of behavioural intention except for normative pressure where this factor has no significant effect on the intention to use mobile banking.

Besides mobile banking, studies have also been conducted on the acceptance of internet banking in Malaysia. According to a study on the impact of ethnicity on internet banking adoption which selected Malay and Chinese ethnic groups and compared their perceptions on internet banking adoption. It was found that Malays and Chinese perceived trust as the most influential factor of internet banking adoption in Malaysia. However, the Chinese also put a higher emphasis on perceived usefulness than the Malays. This result might be due to the cultural traits where the Chinese tend to put more emphasis on the benefits they will get before adopting any technology (Md Nor, 2008).

Another study on internet banking adoption was conducted by Lallmahamood (2007) who found perceived security and privacy as the second important element in internet banking adoption after perceived usefulness. He found perceived usefulness, ease of use and credibility have explained approximately 53.2% of the variance in intention to adopt internet banking.

Ramayah, Mohd Suki and Ibrahim (2005) have examined technology acceptance of online bill payment system and found support for the applicability of TAM in explaining intention to use online bill payment system among postgraduate students in Malaysia. TAM has also been tested in taxation environment. Online tax services have been established to offer more convenience and accessibility of tax services and information to the taxpayers.

Wang (2002) has conducted an empirical study on the adoption of electronic filing systems in Taiwan and found extended TAM contributes 62% of explained variance in behavioural intention. The results showed perceived usefulness, ease of use and credibility did have a significant effect on the behavioural intention with perceived ease of use contributed more to intention as compared to the other variables.

A study to investigate the determinants of user acceptance of online tax payment has been conducted in Taiwan by Hung *et al.* (2006). However, in Taiwan, the online tax filing and online tax payment facilities are incorporated into one system and are named as Online Tax Filing and Payment System FPS). They have employed decomposed TPB theory which also includes the TAM variables in explaining Taiwanese taxpayers in accepting the FPS. The findings showed that the model explained 72% of the variance in intention and both TAM variables were significant determinants of intention to use the FPS.

2.4.2 Technology Adoption

The emergence of electronic government so-called e-government is the evidence of successful utilization of information system in government organizations. Internet technology is proven to be the most powerful and popular means of delivering government around the world (Wangpipatwong, Chutimaskul & Papasratorn, 2008).

A study to identify factors related to the benefits and barriers of e-government adoption has been conducted by Gilbert and Balestrini (2004). They found nine factors important to government's adoption where three of them namely less time, cost and avoiding interaction; are related to benefits while the other six particularly experience, information quality, financial security, low stress, trust, and visual appeal are factors that are related to the barriers of adoption.

They concluded that the adoption rate will not likely be increased if factors related to barriers are not properly addressed. Hence, users' acceptance has a critical impact on the success of the system adopted. If users are not willing to accept a new information system, it will not bring full benefits to the organization that has made.

According to Melucci & Paggiaro, (2019), the usage of a system can be an indicator of information system success. Whether the system is regarded as good or bad depends on how the users perceived the system. If the users perceived that the system is useless and did not accept the system, then that system cannot be regarded as an effective system, however, if the users perceived that the systems are used and accept it, then the system has achieved its goal on efficiency and effectiveness.

In other words, no matter how good the system is, without users, the system would still be a failure. As such, in ensuring the success of any developed systems, it is vital to find out reasons why people decide to use or not to use the information system and determine factors that may affect their acceptance of those systems.

2.6 Summary of Reviewed Literature

As a result of the survey to related literature, a number of factors contribute to threats facing the integrity, confidentiality, and availability of organizational information along with many countermeasures. Threats to information systems security include unauthorized access, changing of information, and the destruction of protective infrastructure that helps preserve the confidentiality, integrity, and availability of the information. Various threats persistently target exposures or vulnerabilities and ultimately have an adverse impact on the information.

It was also noted that repeatedly information protection decisions are made in an ad hoc manner, based on the IT department's prior experience with vulnerabilities and the threats that they currently know about. Thus, risks tend not to be systematically managed or are managed by the wrong people.

Organizational security controls are defined as an appropriate mix of physical, technical or operational security controls. The goal of controls is to mitigate the risks to information. Controls are used to protect information by reducing the risk posed by exposures or vulnerabilities arising from threats. A strong set of protective controls can provide an organization with an effective defence capability and an organization's capabilities provide the best defence against the existing array of competitive forces.

Information resources are crucial to supporting organizational performance by providing prospects for the establishment of competitive advantage and as such, preservation of information-based, intangible resources is a significant imperative for organizations. For the financial returns to an organization to be sustainable, the resources that support them must also be sustainable. The longevity of the of an organization's competitive advantage also depends on the speed at which its supporting resources degrade.

Many organizations outsource information security risk assessments because they do not have in-house competency to perform this vital service. They hire experts to perform risk assessments, and the resulting assessment is only as good as the experts who perform it. Often the consumers of such services have no way to understand if the risk assessment performed for them is adequate for their enterprise.

From the survey to existing models, SSE-CMM for System Security Engineering (SSE) that primarily concerns on the improvement of a specific process-related trouble spot and it is heavily influenced by the CMMI five layer capability maturity model was considered. The project on ICS-SCADA Cyber Security Maturity Assessment Model dealing with regulations, policy activities and responsibilities at each member state in the EU. The Cyber Security Maturity Framework for NIST for information security determination was also reviewed. The main objective of the framework is to manage cyber security risks within the organizations that implement it.

Finally reviewed was Oil and Natural Gas Subsector Cyber security Capability Maturity Model (Ong-C2m2) arising from a combination of existing cyber security standards, frameworks, programs, and initiatives derived from benchmark domain-specific practices against ONG-C2M2 cyber security practices for industrial control systems.

2.7 Research Gap

Often, the computing infrastructure is set up without the IT staff having a clear understanding of the organization's mission- or business-related needs. This leads to a gap between the organization's operational requirements and its related information security needs. From the literature, the researcher has noted that there is a gap in the existing models. Organizations fail to establish the effect of the infrastructure weaknesses on information assets. The discussion below seeks to elaborate on gaps in already existing models in different domains.

The SSE-CMM for System Security Engineering (SSE) focuses on the improvement of a specific process-related trouble spot and it is heavily influenced by the CMMI five layer capability maturity models. While the project on ICS-SCADA Cyber Security Maturity Assessment Model, delved on regulations, policy activities and responsibilities at each member state in the EU. The Cyber Security Maturity Framework for NIST aside from being a framework is not comprehensive to address all information security related processes. The main objective of the framework is to manage cyber security risks within the organizations that implement it.

On the other hand, Oil and Natural Gas Subsector Cyber security Capability Maturity Model (Ong-C2m2) though arising from a combination of existing cyber security standards, frameworks, programs, and initiatives has limitation in that it is derived from benchmark domain-specific practices against ONG-C2M2 cyber security practices which are not applicable to a university. Although the existing models examined seek to measure maturity, not much of concerns are in line with information security maturity in universities.

MITIGATE aided to detect expected individual, cumulative and propagated risks within an ICS infrastructure. They derived risk values that were utilized to generate a baseline security strategy for MLoSCs. MITIGATE is evidence-driven Risk Assessment methodology provided security assessment services while considering only the cyber-nature of CPSs

In fuzzy AHP approach it determined important weights and indicators. They took into consideration all the 14 security control clauses, 35 Control Objectives having 114 Controls. Having derived weights from ISO/IEC 27001: 2013 and getting controls from COBIT, it did not consider subjectivity of human aspects especially on control levels

The models and frameworks reviewed considered a holistic view to come up with diverse approaches to improve organizational information security. The missing link between security risks and the specific impact on organizational IS security using a measurable model and an index / rating provided the motivation to pursue the work reported in this document.

The approach in the industry and specifically the university’s towards information security maturity should consider University Information security maturity (UISM) based on ISO 27001 best practices as a benchmark standard. This study, therefore, aims to bridge the gap by designing an organizational focused University Information

Security Maturity (UISM) with a more comprehensive approach that incorporates key elements of ISO/IEC 27001.

2.8 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 (Kombo & Tromp, 2006). 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 shows the prototype Implementation Conceptual framework. The formula derivation conceptual framework is as shown in Figure 7 below.

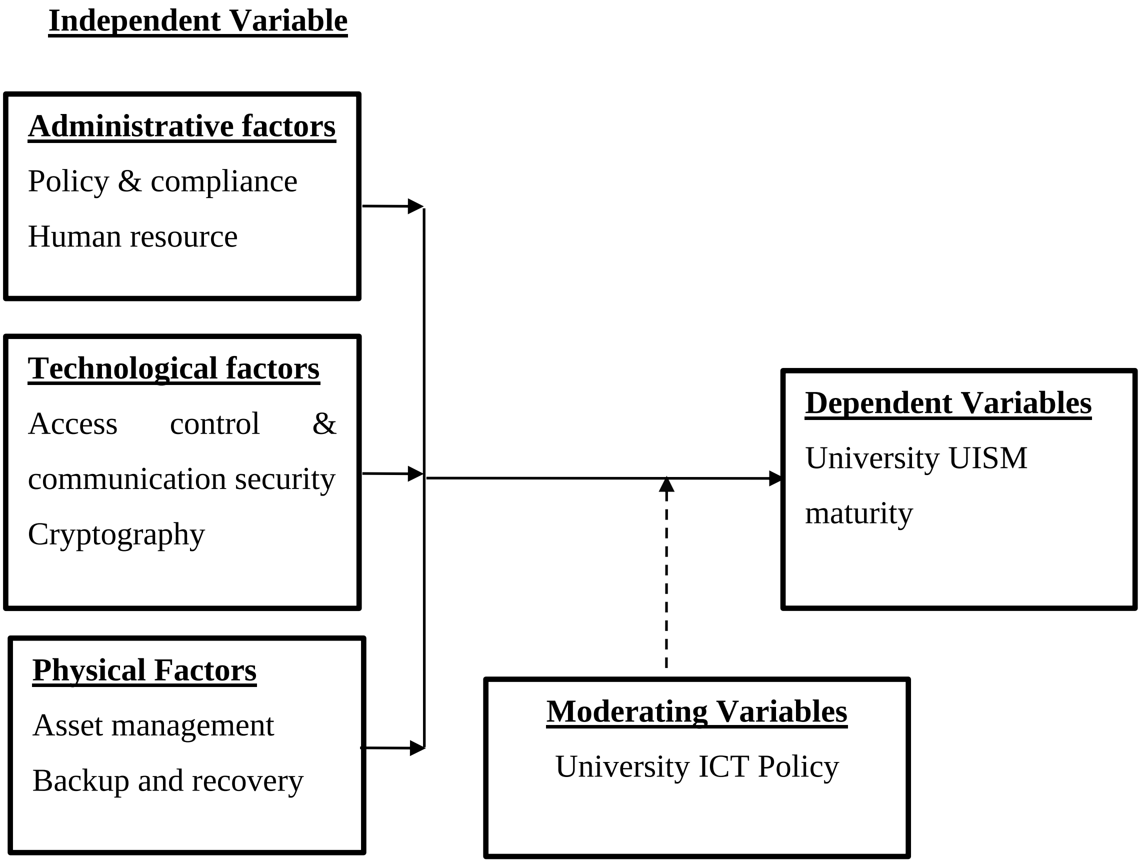


Figure 7: Formula derivation Conceptual framework

The proposed conceptual framework above has three key areas of concerns. The independent variables drawn from the ISO/IEC 27001 standard, the specific university policy and the dependent variable University Information Security Maturity (UISM). The three independent variables, administrative, physical and technical factors were derived from literature review in the previous section. The university policy depends on the respective information security guidelines and practices within the university. Overall upon consideration of the different factors in the independent variables, the maturity will be computed based on the weighted emphasis of each particular factor and therefore will serve to inform Maturity in Information Security.

Stage two of the conceptual framework which will guide the implementation of the prototype is shown in figure 8 below.

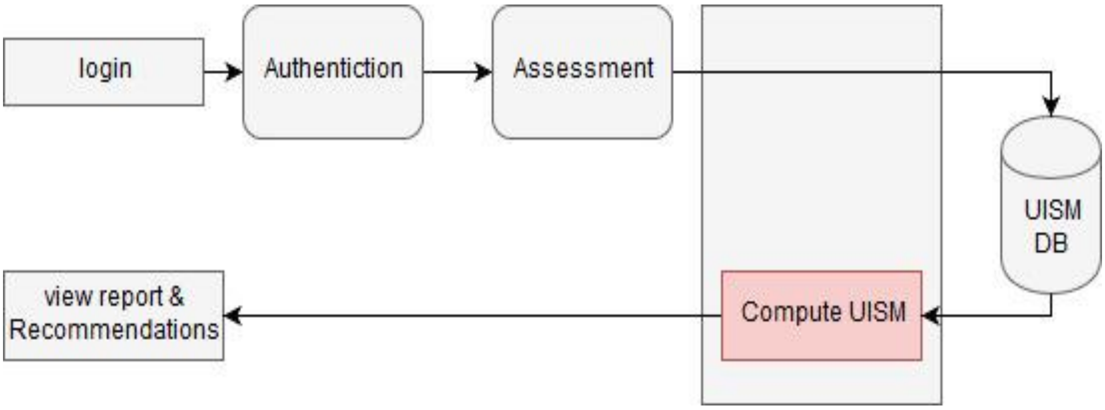


Figure 8: Prototype implementation Conceptual framework

The prototype will have the following modules; User Registration module, User login and authentication module that will be regulating access to only authorized users, Risk assessment module that will prompt users to express their concerns in regard to information technology maturity, database module that will store user information and assessment scores, and information processing module that will compute UISM from the weights that will be stored and security posture information that will be provided by the users. In addition, the prototype will have a module to display UISM information and provide a mechanism for downloading the UISM index report and recommendations.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

Drawing informed decisions for further inferences requires accurate, timely and reliable data. University data in this study is very critical for information decisions that require development of a model to guide future security landscape of an organization. In seeking answers to the aforementioned research questions, the study utilized mixed research methodology that combined design science and scientific methodologies. Data gathered ascertained the level of agreement on the various aspects of the ISO 27001 standard. Obtained data was subjected to validity and reliability test through face validity check and a pilot study prior to analysis and further inferences in the next chapter.

3.1.1 Population

Data collection involved 74 public and private universities in Kenya according to CUE report of 2018. Data received from universities were cleaned, collated and entered into one main excel sheet and analysed according to the following variables: administrative, technical and physical security factors. Descriptive statistics, which included frequency tables, percentages and ratios, were used to analyse the data.

3.1.2 Sample size

Sample constitutes a finite part of statistical population whose properties are studied to gain information about the whole population. Sampling on the other hand is the act, process or technique of selecting a suitable sample which represents the whole population to determine its characteristics (Webster, 1985). According to Orodho (2003) certain sampling methods are applicable depending on what the population constitutes. These study adopted purposive sampling technique to obtain data from ICT personnel's of different universities because they form part of study population who can effectively establish cause of information security challenges in universities. The sample constitute at least 6 key personnel: Senior Management, ICT Manager, Database Administrator, Network Administrator, System Administrator and ICT Student Support, the sample elements ware then selected using simple random sampling. According to Mugenda and Mugenda (2009) a good sample should be large enough and logically between 10 and 30 per cent of the study population. Nassiuma's (2000) was employed to calculate the exact sample size as shown below.

Equation 3: Formula for Sample Size Computation (Nassiuma's 2000)

$$n = \frac{NC^2}{C^2 \ + (N-1)e^2}$$

Where: n = sample size

N= population Sample

C = coefficient of variation (0.5)

e = error margin (0.05)

The total sampling frame is 444 personnel's considering the 6 key ICT staff and 74 universities in Kenya. Taking consideration of Nassiuma's formula the sample size can be computed as shown below:

$$n = \frac{444(0.5)^2}{0.5^2 \ + (444-1)0.05^2}$$

n = 81.768

$n \ \approx$ 82 Respondents

Therefore the proportionate sample size should not be less than 82 respondents. Therefore for this study 120 respondents were drawn from the accessible population of 444 elements.

3.2 Data Collection Instruments

An online Questionnaire was developed and tested before being rolled out for data collection in universities, by subjecting Cronbach alpha test. An online questionnaire is desirable because of low cost, adequacy of time for respondents to give responses, it is free of interviewer's biases and a large number of respondents may be reached, (Kothari, 2004). The tool validation was also subjected to general face validity test by administering to a group of experts in ICT field to check on questions content coverage. .

3.3 Data Analysis

Data collection tool reliability and validity was determined by undertaking Two Tailed Anova of coefficients (Conroy, 2016). The obtained confidence of validity with sufficient Cronbach alpha test loading exceeding 0.8 formed the basis for main data collection exercise.

3.3.1 Instrument Face Validity

The instrument's reliability is very important in determining the level of stability and internal consistency of an instrument. To obtain reliability value of an instrument, face validity was carried out. The flowchart in figure 9 below shows the steps followed to achieve reliability.

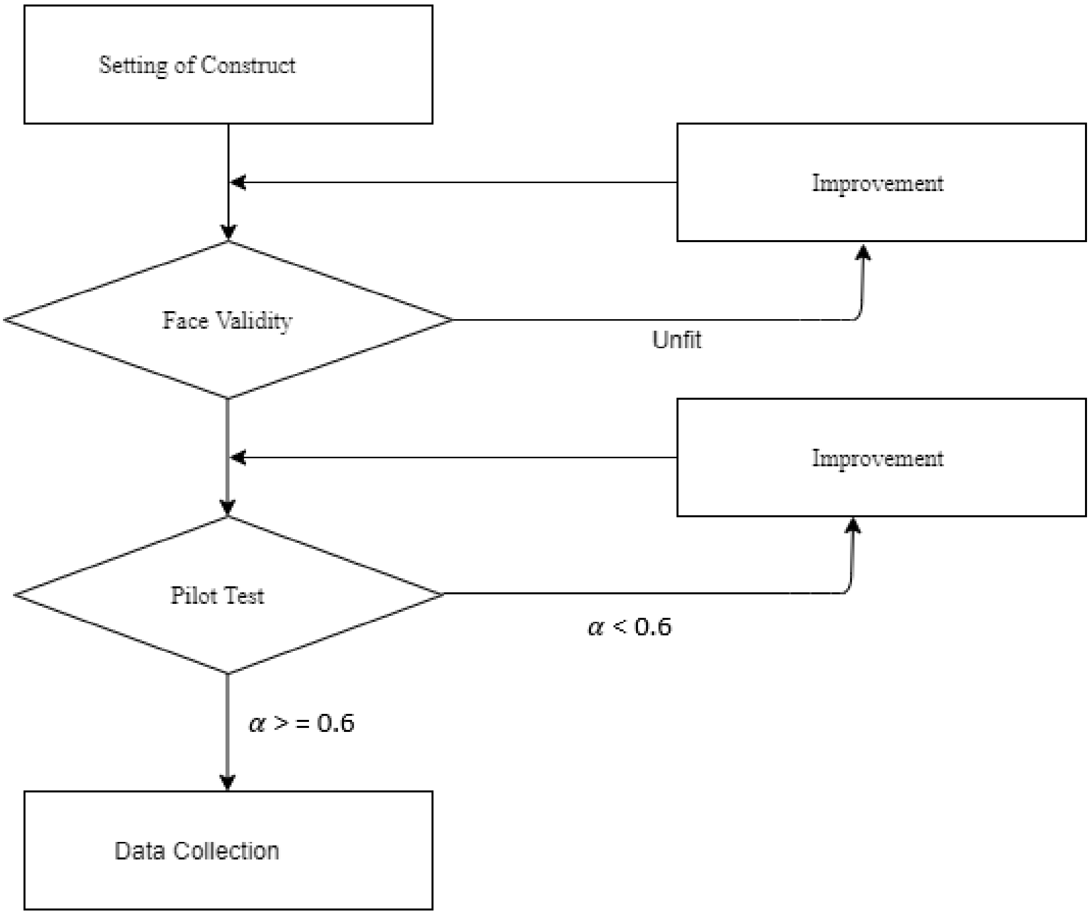


Figure 9: Pilot test flowchart

Foremost face validity was undertaken by administering the questionnaire to a team of expert's knowledgeable in information security. Secondly, a pilot test was then conducted on respondents who were later not involved in the actual study. The respondents were then given room to provide comments and feedback on grammatical errors and vague sentences.

3.3.2 Sample Determination for Cronbach Alpha Test

A Single Coefficient of Cronbach Alpha Test was done assuming the null hypothesis to be Zero. The value of Cronbach alpha ranges from zero to one with the higher values implying the items are measuring the same dimension (Mohamad *et al* 2018*)*. However, with the sample size calculation, researchers (Yurdugül, 2008; Bonett, 2002), have agreed that sample size can be calculated to determine sufficient sample to assess the internal consistency of a research instrument.

Sample size for Single Coefficient alpha was calculated using Microsoft Excel. The formulation was from (Bonett, 2002; Wright, 2015) based on the formula given;

Equation 4: Formula for Single Coefficient Alpha (Bonett, 2002; Wright, 2015)

$$n = \left[\left\{\left(\frac{2k}{k-1}\right)\left(Z\,\alpha/_{2} + Z_{\beta}\right)^{2}\right\}\Big/\ln\left(\bar{\delta}\right)^{2}\right] + 2$$

Taking Into Consideration: $\delta = \frac{1-\text{Null Hypothesis}}{1-\text{Alternative Hypothesis}}$

By using formula above and taking into consideration the data collection tool composed of 36 ratters represented byκ(should not be zero) and the value of Cronbach's alpha at (null hypothesis and the expected value of Cronbach's alpha) δwith the Reliability of measurement (null hypothesis and alternative hypothesis identified at 0.0 and 0.7, respectively). Power is set at 90% and the value of alpha α at 0.05. The minimum sample size required was based computed below based on Bonett shown above;

Computations:

α = 0.05

β = 0.1

κ = 36

Null Hypothesis = 0.0

Alternative Hypothesis = 0.7

$$\delta = \frac{1-0.0}{1-0.7} = 3.333$$

$$n = \left[\frac{\left\{ \left(\frac{2(36)}{36-1} \right) (Z_{0.025} \ = 1.96 \ + Z_{0.1} \ = 1.282)^2 \right\}}{\ln(3.333)^2} \right] + 2$$

$n = 16.9186 \approx 17$

Therefore, the minimum sample size$n$ required for two Coefficientalpha study is approximately 17 samples.

3.3.3 Content validity

Internal consistency of data collection instruments is an adequate measure for testing reliability and validity of data collected for analysis. One of these tests for internal consistency is Cronbach's alpha (Cronbach 1951; Nunnally 1979). A value of Cronbach's alpha between 0.6 and 0.8 is acceptable (Wim *et al*, 2008). The Anova table of pilot test for Cronbach alpha determination is as shown below in table 5.

Table 5: Anova Table

Source of Variation	*SS*	*Df*	*MS*	*F*	*P-value*	*F crit*
Rows	255.8273	15	17.05515	12.08527	4.56E-26	1.684431
Columns	23.15954	37	0.625933	0.443536	0.998383	1.432365
Error	783.2352	555	1.411235			
Total	1062.222	607				

In this study, it was found that the overall value of Cronbach Alpha is exceeding 0.8 and it's considered to be very high and acceptable. Table 6 below shows the overall value of Cronbach Alpha for 17 respondents being 0.917.

Table 6: Cronbach Alpha

Cronbach Alpha	**N of Items**
0.917255.	17

It can be concluded that the scale used to measure the individual construct in the data collection instrument is reliable.

3.4 Model Development

Proposed information security maturity model for universities considers ISO/IEC 27001specific clauses relevant to universities. The model considers relevant clauses and weighted risk factors to determine university information security level. The model is presented in an equation format as shown below;

Equation 5: UISM Formula Derivation

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

Where; $\boldsymbol{W_1}$, $\boldsymbol{W_2}$, $\boldsymbol{W_3}$ **. . .** $\boldsymbol{W_n}$, respectively are the weights determined through field data collection by this study.

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

The weights were then rated as; not performed, performed in formerly, planned, well defined, quantitatively performed and continuously improving according to ISO/IEC 27001 maturity standard. Once the weighted scores were obtained, university information security maturity was then computed following the proposed formula above. The model operated in the premise that the cumulated factors and its combined indicators determine the maturity in information security.

The summary of ISO/IEC 27001 focus areas included in model development are administrative controls with focus on Information Security Policies, defining how an institution expresses its intent with regard to information security. Also, human resource security, assessing on institution's safeguards and processes for ensuring that all employees are qualified for and understand their roles and responsibilities of their job duties, and that access is removed once employment is terminated. Finally, Compliance which Assess an institution’s processes for staying current with legal and contractual requirements to protect sensitive information assets.

The technical controls looks into Cryptographic policies which is the art of protection of institutional information and communication through the use of codes. The Cryptographic codes are responsible for key management (encryption). The

Communications Security assesses institution’s formalized policies, procedures, and controls, which assist in network management and operation and Access Control which deals with the use of administrative, physical, or technical security features to manage how users and systems communicate and interact with other information resources.

Physical and Environmental Security which assess on an institution's steps taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. It includes information security aspects of business continuity management which assess an institution’s business continuity after unforeseen circumstances takes place.

A mature institution has a managed and an organized method for the development of procedures to ensure the continuity of operations under extraordinary circumstances, including the maintenance of measures to ensure the privacy and security of its information resources. Upon consideration of ISO/IEC relevant areas in universities has a product of factor on the individual weight, we can come up with a University Information System Security Maturity (UISM).

3.5 Goal Question Metrics Approach for UISM Model Realization

The thesis adopted GQM for model realization. It started with a top-down definition of explicit measurement goals. The goal of our concept was to realize an UISM model by refining several questions that break down the issue into its major sub components. Each question was then refined into metrics that provide information to answer the questions. Measurement data was then interpreted bottom-up. As the metrics were defined with an explicit goal in mind, the information provided by the metrics were then interpreted and mapped with respect to the goal to conclude whether or not it attained its intended objective.

3.5.1 The Measurement Concept of GQM Paradigm

The result of the application of the Goal Question Metric approach is the specification of a measurement system targeting a particular set of issues and rules for the interpretation of the measurement data (Wolski, *et al,* 2018). Figure 10 below shows a representation of GQM approach process (Basili & Weiss, 1984).

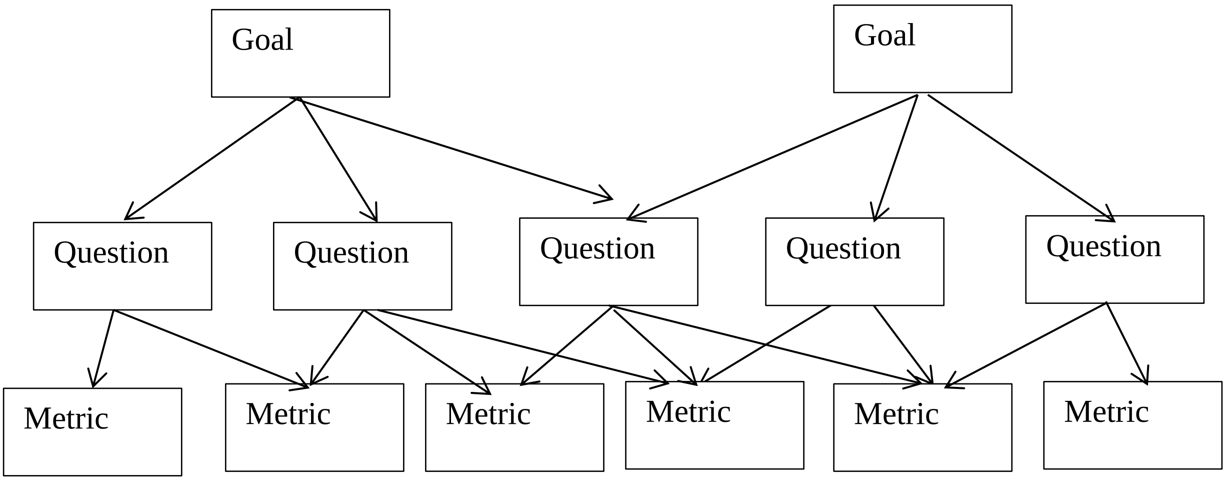


Figure 10: Modified Goal Question Metrics Approach

The measurement model has three levels, the Conceptual level representing the goal. This is defined for an object, with respect to various models of quality, from different points of view, relative to a particular environment.

The Operational level contains the set of questions used to characterize the way the assessment of a specific goal is going to be performed based on some characterizing model. Questions try to characterize the object of measurement for example product, process and resource with respect to a selected quality issue and to determine its quality from the selected viewpoint (Polančič & Cegnar, 2017). Finally, the Quantitative level is about metric which is the standard for measuring or evaluating something, especially one that uses figures or statistics: measurements (Florac & Carleton, 1999). A set of data is associated with every question in order to answer it in a quantitative way.

3.5.2 Application of GQM

User data goals and associated measurement were developed following the Goal Question Metrics approach. The respondent’s data from different institutions of higher learning was captured using goal template which entailed the data collection instruments. Using this template, each goal is described. The resultant output was then analysed considering the respondent's score for improvement.

3.6 Prototype Implementation

A prototype was developed to actualize the proposed model discussed. A prototype is the making of a working model of a product to exhibit the achievability of the concept. The model was later refined for final consideration into the working software prototype (Chowdhury *et al*, 2018). It guided on how simple or troublesome it will be to execute the web based model. It additionally allowed stakeholders to remark on the ease of use and handiness of the user interface (UI) plan and gave a chance to survey the fit between the product devices chosen and the client needs (Osborn, 2017). The illustration of Rapid application development according to Hassan *et al*, (2017)is as shown below.

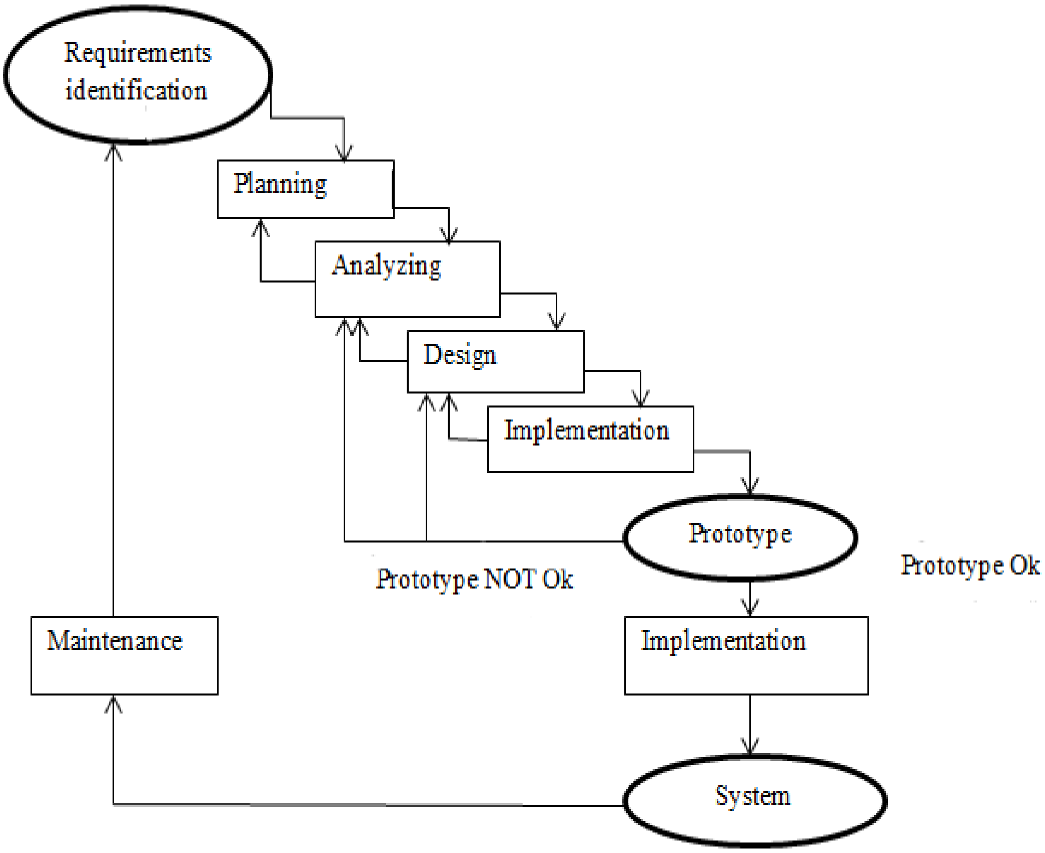


Figure 11: Rapid Prototyping Model

3.6.1 Prototype Evaluation

The model envisioned was evaluated using the ‘IT-Systems as such Goal-based evaluation approach’ (Kavakli, & Loucopoulos, 2005). Testing the prototype enabled the concept to be evaluated for proof of concept (Menold, 2017). Operational and technical based approach was used to reveal how the set objectives were being achieved. The evaluation involved the evaluators and end beneficiary stakeholders (Stufflebeam, & Zhang, 2017).

The evaluation criterion was based on the specification and description. The proposed Web-based model for university information security maturity was evaluated according to University registration with a view to confirm if the prototype was able to capture the name of the institution and the registered number. Also Information input with an emphasis to know if it allowed for the input of university data by the responsible ICT officer and enter information regarding the information security risk factors.

In addition, according to maturity assessment computation and upon supplying necessary input data, the model appropriately computed the maturity index of the particular university. The system also provided the maturity level to appropriately inform on areas for improvement. Finally it was able to track Maturity logs for maturity improvement or deterioration of an institution.

3.7 Proof of Concept Approach for Model Implementation

In software development, proof of concept is often used to describe several distinct processes with different objectives and participant roles (Mao, *et al,* 2017). Through proof of concept a partial solution involving employees in universities took part in using the web based model to test their information security posture and ascertain whether the system satisfies some aspect of the requirement (Fielding *et al,* 2017). This allowed verification on whether the model conform in-line to expected solution.

3.7.1 Proof of Concept Procedure

The proof of concept approach followed Model View Controller (MVC) pattern presented below in figure 11. It guided best on coming up with a product from initial weak zero (initial stage) to full production for a final market-ready item (Segura, 2018). Similarly, the (POC) operation provided a Minimum Viable Product (MVP) that resulted after a successful implementation of the prototype. (Schmidts, 2018).

The UISM MVP is an early version of maturity assessment model replica of an intended final product. The obtained MVP can be used to test marketability and usability with potential users or customers (Jiménez, 2017).

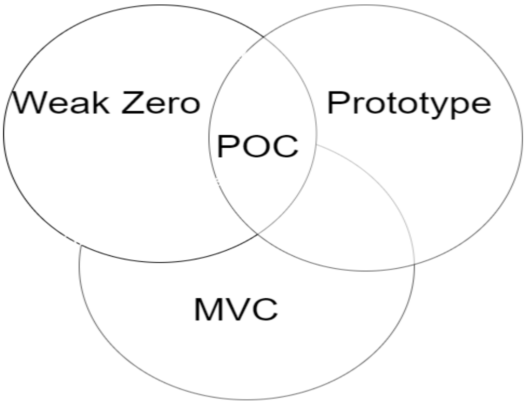


Figure 12: Modified Proof of concept approach

To prove that the model designed is an achievable solution, a proof of concept has been built. Chapter 5 contains a description of how this proof of concept has been implemented and a discussion on the design considerations. Furthermore, descriptions of the use cases that are defined for the proof of concept are given. The proof of concept has been simulated and tested. The results of these simulations and tests are used to validate the model and proof of concept. This process is described in Chapter 5.

3.8 Ethical Consideration

During data collection and model testing, several ethical considerations were adhered. The researcher obtained information that furthers the purpose of this study. The ethical consideration was in line with regulating authorities' requirements. Data was collected from universities after obtaining consent from the institutions. This was done by having an introductory letter from the Institute of postgraduate and research of Kabarak University and also, a permit obtained from the National Commission for Science Innovation and Technology (NACOSTI).

The information that was obtained from the respondents was treated with strict confidentiality. Respondents were not solicited to obtain data. During the data collection process, the respondent's self-respect and esteem were not violated. Also, data obtained for the purpose of the model design was not misinterpreted or distorted in any form during reporting.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND DISCUSSION

4.0 Introduction

This chapter presents analysis and findings of the study as set out in the research methodology. The results were presented using the “ISO 27001 based model to determine university information security maturity under uncertainty” as envisioned in the previous chapter. The study objectives were; to determine the critical information security risk factors that impact on security of universities based on ISO 27001, to explore the existing models used in assessing information security maturity, to design a model to determine university information security maturity and to implement the model to determine university information security maturity level & finally, verify the prototype for computing information security maturity in universities.

Data Analysis looks for patterns or trends across the results, to track progressions or to seek out repetition of certain results to build up a strong case. More so, quantitative analysis deals with data in the form of numbers and uses mathematical operations to investigate their properties (Walliman, 2011). The chapter covers the demographic information, and the findings based on the objectives. The findings were then presented in tables, frequencies, and percentages with explanations being given in prose thereafter.

4.1 Response Rate

Data collection was done by using simple random sampling procedure administered through an online Questionnaire. From the study sampling frame 120 respondents responded and returned their questionnaires. This response rate was sufficient and representative conforming to Mugenda & Mugenda (2003) stipulation that a population response rate of 50% is adequate for analysis and reporting; a rate of 60% is good while a response rate of 70% and over is excellent.

4.1.1 Background Data

To be sure that what was found in the questionnaires actually represented what was measured, a section of the questionnaire was designed to capture background data on respondents as well the specific organization category they represented. The Background data, therefore, further ensured validity and reliability of the questionnaires used as data collection tools. The approach also agrees with Roe & Just (2009), that inferences that can be tied back to previous findings and the ability of study results to be transferable to other studies, populations, settings and time, and answers research questions better exhibit validity and reliability.

4.1.2 Respondents General Information

Individual respondent's data included institution category type of the respondent and their position in the university. The combination of institution type and the position held in the university yielded the following results.

Table 7: Respondents Institution Type

Variable	Frequency	Percent
Public	93	77.5
Private	27	22.5
Total	120	100.0

From the responses in Table 7above it showed that a majority of respondents constituted employees from public universities (77.5% of the sample size) whereas 22.5% of the total sample size were drawn from private universities. This is attributed to the higher number of public universities compared to private universities in Kenya. According to Commission of University Education (CUE) report of 2018, there are more public universities compared to private universities in Kenya.

4.1.3 Current Position

The current position of different personalities who participated in the research from different cadres of a higher learning institution are as shown below in table 8.

Table 8: Position in the University

Variable	Frequency	Percent
Senior management	5	4.2
ICT manager	7	5.8
Database Administrator	8	6.7
Network administrator	16	13.3
System administrator	30	25
ICT student support	36	30
Others	18	15
Total	120	100.0

The finding showed that System administrators were (25%) and Network administrator (13.3 %), confirming that the respondents in the study constituted respondents who were knowledgeable and experienced in ICT. Therefore, their opinions make an informative judgement on information technology infrastructure situation within the university. Similarly, it is observable that ICT student support constituted (30 %), with the least being senior management 4.2 %. The ICT managers and Database administrators constituted 5.8 % & 6.7 % respectively.

4.1.4 ISO certification in universities

The ISO certifications in universities accordingly with the number of universities ascribing to the different standards are shown below in table 9.

Table 9: ISO Certification in Universities

	ISO Certified	ISO 9001 Certified	ISO 27001 Certified
No	10	20	77
Yes	110	100	43
Total	120	120	120

From the findings it can be concluded that majority of organizations having ISO certification, specifically are ISO 9001 certified. The findings are supported by carol *et al* (2018), that ISO 9001 is the mostly widely adopted ISO standard in practice. Equally, compared with having ISO 9001 there's slightly few organizations who are certified that ascribe to ISO 27001 compliance. .

In contrast it can be observed that organizations that have complied with ISO 27001 are in addition ISO 9001 certified. According to Barafort *et al* (2018), it is becoming more common for organizations to have a need to obtain and maintain multiple ISO certifications. One common combination of certifications that continues to gain popularity is ISO 9001:2015 (ISO 9001) and ISO/IEC 27001:2013 (ISO 27001).

4.2 Descriptive Analysis

Descriptive statistics were used to analyse the data whereby relative frequencies, mean scores, and standard deviation were used to describe the data. The statistics were based on information security maturity scale of 1 to 5. With Performed Informally = 1; Planned = 2; well defined = 3; Quantitatively Controlled = 4; Continuously Improving = 5; NOTE: 5 is the highest level of maturity).

4.2.1 Administrative Factors

The descriptive statistics for construct administrative factors with 12 data item is as shown below in Table 10.

Table 10: Administrative Factors

Statement	PI%	P%	WD%	QC%	CI%
1.Our institution have an information security policy that has been approved by management	6.7	6.7	26.7	38.3	21.7
2.The policy been published and communicated to all relevant parties	10.0	10.0	32.5	26.7	20.8
3.Our institution review the policy at defined intervals to encompass significant change and monitor for compliance	9.2	10.0	36.7	23.3	20.8
4.All individuals interacting with university systems receive information security awareness training	8.3	10.8	31.7	32.5	16.7
5.The information security programs clearly state responsibilities, liabilities, and consequences	10.0	6.7	34.2	32.5	16.7

6. Our institution have a process for revoking system access when there is a position change or when responsibilities change	5.0	13.3	26.7	34.2	20.8
7. Our institution have a process for revoking system and building access and returning assigned assets	5.8	19.2	30.0	30.0	15.0
8. Our institution have an enforceable data protection policy that covers personally identifiable information (PII)	7.5	13.3	35.8	24.2	19.2
9. Standard operating procedures is periodically evaluated for compliance with your organization's security policies, standards, and procedures	5.0	17.5	27.5	29.2	20.8
10. We perform independent audits on information systems to identify strengths and weaknesses	3.3	15.8	26.7	33.3	20.8
11. Audit tools are properly separated from development and operational system environments to prevent any misuse or compromise	8.3	16.7	31.7	29.2	14.2
12. Our institution provide guidance for the community on export control laws	12.5	20.0	35.0	20.8	11.7

Key: PI=Performed Informally; P=Planned; WD=Well Defined; QC=Quantitatively Controlled and CI=Continuously Improving

With regards to administrative factors, 38.3% of the respondents stated that their institution have an information security policy that has been approved by management that is quantitatively controlled. Similarly 35.8% affirmed that they have an enforceable data protection policy that covers personally identifiable information (PII) that is well defined. The findings conform to the findings of Nebyu (2018). In contrast, 3.3 % maintains that they performed informally in carrying out independent audits on information systems to identify strengths and weaknesses.

The study found that respondents affirmed that the standard operating procedure was quantitatively controllable with organization's security policies, standards, and procedures which affirm Jennex & Durcikova (2019) findings. They also reported that they have Quantitatively Controlled Standard operating procedures that is periodically evaluated for compliance with organization's security policies, standards, & procedures, as well information security programs that clearly state responsibilities, liabilities, and consequences as represented by 29 % and 32.5 % respectively. It was also noted that respondents had a quantitatively controllable process for revoking system and building access & returning assigned assets (30.0%), a controlled information security programs that clearly state responsibilities, liabilities, and consequences (34.2%).

However, it was observed that 32.5% agreed that all individuals interacting with university systems receive information security awareness training and that the situation was well defined. Additionally, it was noted that the policy was well defined, published and communicated to all relevant parties(32.5%) as well as audit tools are properly separated from development and operational system environments to prevent any misuse or compromise(31.7%).

4.2.2 Technological Factors

The descriptive statistics for the construct technological factors with 12 data item is as shown below in Table 11.

Table 11: Technological Factors

Statement	**PI** %	**P** %	**WD**%	**QC**%	**CI** %
1.Our institution have an authentication system in place that applies higher levels of authentication to protect resources with higher levels of sensitivity	4.2	17.5	34.2	25.0	19.2
2.Our institution require encryption on mobile (i.e., laptops, tablets, etc.) computing devices	9.2	20.2	34.5	22.7	13.4

3.In our institution, the policy enforce usage guidance established for mobile computing devices (regardless of ownership) that store, process, or transmit institutional data	8.3	16.7	36.7	28.3	10.0
4.Our institution have standards for isolating sensitive data and procedures and technologies in place to protect it from unauthorized access and tampering	5.0	24.2	30.0	25.8	15.0
5. Our institution have a telework policy that addresses multifactor access and security requirements for the end point used	9.2	19.2	39.2	21.7	10.8
6. Our institution use appropriate/vetted encryption methods to protect sensitive data in transit	10.0	15.8	40.8	18.3	15.0
7. Our policies indicate when encryption should be used (e.g., at rest, in transit, with sensitive or confidential data, etc.)	12.5	17.5	34.2	25.0	10.8
8. Standards for key management documented and employed	6.7	24.2	30.0	23.3	15.8
9. Our institution maintain security configuration standards for information systems and applications	6.7	13.3	39.2	25.8	15.0
10. Changes to information systems tested, authorized, and reported	5.8	11.7	39.2	30.0	13.3
11. Our your institution have a process for posture checking, such as current antivirus software, firewall enabled, OS patch level, etc., of devices as they	10.0	13.3	36.7	23.3	16.7

connect to your network					
12. Our institution have a process for routinely monitoring logs to detect unauthorized and anomalous activities	9.2	13.3	28.3	30.8	18.3

Key: PI=Performed Informally; P=Planned; WD=Well Defined; QC=Quantitatively Controlled; CI=Continuously Improving

The findings indicated that the majority of respondents (40.8%) significantly agreed that their institution use appropriate/vetted encryption methods to protect sensitive data in transit that is well defined, while 4.2% opine that their institution perform informally in having an authentication system in place that applies higher levels of authentication to protect resources with higher levels of sensitivity.

In addition some respondents agree that their organizations have well defined process for changing information systems that is tested, authorized, and reported (39.2 %). At the same time, a significant number of respondents (39.2%) pointed out that they had a well-defined telework policy that addresses multifactor access and security requirements for the endpoint used as well as that they have standards for isolating sensitive data and procedures and technologies in place to protect it from unauthorized access and tampering (30.0%).

Implementation of security policy is imperative for organizations. The study findings indicated that over half of the respondents (36.7%) opine that the policy enforce usage guidance established for mobile computing devices (regardless of ownership) that store, process, or transmit institutional data Similar to suggestions of Eloff (2002) who postulated that an organization must use a code of best practice. Furthermore, security configuration standards and Standards for key management were also not well developed with 30.0 % having a continuously improving policy usage.

On the other hand, 36.7% agreed that their institutions have a well-developed process for posture checking, such as current antivirus software, firewall enabled, OS patch level of devices as they connect to the network which is a good technological practice to improve information security maturity similar to findings of Shulman, (2018).

Despite this technological development, 30.8% opine that the process for routinely monitoring logs to detect unauthorized and anomalous activities and having authentication system in place that applies higher levels of authentication to protect resources with higher levels of sensitivity was still continuously improving.

4.2.3 Physical Factors

The descriptive statistics for construct physical factors with 12 data item is as shown below in Table 12.

Table 12: Physical Factors

Statement	PI%	P %	WD%	QC%	CI %
1. Our organization has identified critical information assets and the functions that rely on them	4.2	14.2	32.5	30.8	18.3
2. Our institution classify information to indicate the appropriate levels of information security	4.2	15.0	33.3	30.8	16.7
3. Our institution have a process for revoking system and building access and returning assigned assets	3.3	17.5	35.8	30.0	13.3
4. Our institution have a media-sanitization process that is applied to equipment prior to disposal, reuse, or release	4.2	18.3	37.5	26.7	13.3
5. Our institution have processes in place to monitor the utilization of key system resources and to mitigate the risk of system downtime	3.3	15.8	40.0	29.2	11.7
6. We have Methods used to detect and eradicate known malicious code transported by electronic mail, the web, or removable media	6.7	18.3	30.8	27.5	16.7
7. Our institution have a records management or data governance policy	7.5	15.8	30.8	29.2	16.7

that addresses the life cycle of both paper and electronic records at your institution					
8. Our institution's data centres include controls to ensure that only authorized parties are allowed physical access	5.0	10.8	39.2	25.0	20.0
9. Our institution have a process for issuing keys, codes, and/or cards that require appropriate authorization and background checks for access to these sensitive facilities	5.0	13.3	36.7	27.5	17.5
10. Our institution follow vendor-recommended guidance for maintaining equipment	3.3	12.5	37.5	37.5	9.2
11. There are processes in place to detect the unauthorized removal of equipment, information, or software	2.5	16.8	32.8	31.9	16.0
12. Our institution have preventative measures in place to protect critical hardware and wiring from natural and man-made threats	3.3	10.0	37.5	35.0	14.2

Key: PI=Performed Informally; P=Planned; WD=Well Defined; QC=Quantitatively Controlled and CI=Continuously Improving

According to Table 12, majority of the respondents (40.0%) agree that they have a well-defined processes in place to monitor the utilization of key system resources and to mitigate the risk of system downtime. They also agreed they have processes in place to monitor the utilization of key system resources and to mitigate the risk of system downtime for issuing keys, codes, and/or cards that require appropriate authorization and background checks for access to these sensitive facilities are well performed in their institution. This view was supported by 40% who points out that their institution have processes in place to monitor the utilization of key system resources and to mitigate the risk of system downtime. This ultimately improves the overall information security maturity.

However, security risk was evidenced by 18.3% who lamented that Methods used to detect and eradicate known malicious code is still at planning stages. Similarly, 37.5% reports that they have a well-defined institutional media-sanitization process that is applied to equipment prior to disposal, reuse, or release. This assessment was supported by 30.8% who report that their institution is planning for records management or data governance policy that addresses the life cycle of both paper and electronic records at the institution.

It was evident from the finding that only 35.8% assert that their institutions have a well-defined process for revoking system and building access and returning assigned assets, which is seen to be a good indicator of information security Cruz (2013). Similarly, respondents acknowledged that there are processes in place to detect the unauthorized removal of equipment, information, or software and that there is a continuous improvement in following vendor-recommended guidance for maintaining equipment indicating that the distribution of responses was nearly equal proportions across the maturity scale.

On the other hand, 37.5% reported that they have preventative measures in place to protect critical hardware and wiring from natural and man-made threats. In conclusion, all the respondents agreed that at least organization have processes in place to detect unauthorized removal of equipment, information, or software that is not planned informally.

4.2.4 University Information Security Maturity

Mean Descriptive Statistics for University Information Security was duly analysed and presented in table 13.

Table 13: Descriptive Statistics for University Information Security Maturity

	N	Mean	Std. Deviation
Administrative factors	120	3.3743	.92569
Technological factors	120	3.2057	.88817
physical infrastructure	120	3.3694	.83422
UISM	120	3.7778	.92616
Valid N (listwise)	120		

Regarding university information security maturity, it was noted that administrative process, information security infrastructure and physical infrastructure was not well developed as indicated by their means of 3.3743, 3.2057 and 3.3694 respectively. Consequently, the university information security maturity overall index was 3.7778 indicating that the level of maturity performance was at an average level and more remedial information security measures are still required.

4.3 Correlation Analysis

Pearson Correlation was used in this analysis. Pearson Correlation coefficient is a statistical measure of the strength of and direction of relationship between two variables. The correlation coefficient represents the effect size between two variables and tells in which degree they correlate in a straight line. The correlation coefficient can range from +1, which is a perfect positive relationship between two variables, till -1 which is a perfect negative relationship. A coefficient of zero means, that there is no relationship between two variables. Field (2009) mentions, that the measure of Cohen (1988, 1992) can be used as a guideline when measuring the correlation coefficient. Correlation in this study was undertaken to establish the relationship between each of the three independent variables; Administrative, Technical and Physical Factors on Information Security Maturity Model.

4.3.1 Administrative Factors and University Information Security Maturity

Table 14: Correlation between Administrative Factors and University Information Security Maturity

		Administrative Factors	UISM
Administrative Factors	Pearson Correlation	1	.723**
	Sig. (2-tailed)		.000
	N	120	120
UISM	Pearson Correlation	.723**	1
	Sig. (2-tailed)	.000	
	N	120	120

**. Correlation is significant at the 0.01 level (2-tailed).

Therefore the findings of the Pearson’s r, correlation showed that there exists a statistically significant positive relationship between administrative factors and university information security maturity ($r=.723^{**}p<0.01$).This means that when administrative factors are Continuously Improving, the information security maturity at the university will be at its highest level. Conversely, when these factors are under Performed, then its maturity will be low.

4.3.2 Correlation between Technological Factors and University Information Security Maturity

Table 15: Correlation between Technological Factors and University Information Security Maturity

		Technological factors	UISM
Technological factors	Pearson Correlation	1	.636**
	Sig. (2-tailed)		.000
	N	120	120
UISM	Pearson Correlation	.636**	1
	Sig. (2-tailed)	.000	
	N	120	120

**. Correlation is significant at the 0.01 level (2-tailed).

The results indicate that there exists a statistically significant positive relationship between Technological factors and university information security maturity (r=.636**p<0.01). This means that when Technological factors are improved, the information security maturity at the university will be at its highest level. Equally, when these factors are lacking, then its maturity will be low.

4.3.3Correlation between Physical Factors and University Information Security Maturity

Table 16: Correlation between Physical Factors and University Information Security Maturity

		Physical Factors	UISM
Physical Factors	Pearson Correlation	1	.735**
	Sig. (2-tailed)		.000
	N	120	120
UISM	Pearson Correlation	.735**	1
	Sig. (2-tailed)	.000	
	N	120	120

**. Correlation is significant at the 0.01 level (2-tailed).

According to table 16 above, it is observed that there exist a statistically significant positive relationship between Physical factors and university information security maturity (.735**p<0.01). This means that when Physical factors are put in place, the information security maturity at the university will increase. In the same way, when these factors are deficient, then it will decrease Information Security Maturity.

4.4. Regression Analysis

The regression analysis was achieved by running the respondents responses on the statistical package to establish the effect of independent on dependent variables. Regression was conducted in order to predict the university information security maturity by using Administrative, Technological and Physical Factors. Multiple linear regressions were employed.

4.4.1 Multi-Collinearity Analysis

The Variance Inflation Factor (VIF) was used to identify the correlation between independent variables and the strength of the correlation. VIFs start at 1 and have no upper limit. A value of 1 indicates that there is no correlation between this independent variable and any others. VIFs between 1 and 5 suggest that there is a moderate correlation, but it is not severe enough to warrant corrective measures. VIFs greater than 5 represent critical levels of multi-collinearity where the coefficients are poorly estimated, and the p-values are questionable (Ballantine, 2018).

From the finding, all the factors had a VIF near 1, which shows that multicollinearity does not affect it and we can trust this coefficient and p-value with no further action. Therefore independent variables can be used in regression analysis to model the relationship between the independent variables (administrative factor, technological factor and physical factor's) and the dependent variable (University information security maturity UISM).

Table 17: Collinearity Statistics

Model	**Collinearity Statistics**	
	Tolerance	**VIF**
Administrative Factors	.364	2.745
Technological Factors	.243	4.110
Physical Factors	.255	3.915

a. Dependent Variable: University Information Security Maturity

Multicollinearity statistics showed all VIF values for the three independent variables ranged from 2.43 to 3.64.These values were within the standard range (VIF<10) and at best case being (VIF<5).It is reported that Variables with multi-collinearity signs may give misleading results. Therefore this assumption was not violated and can be concluded that the variables accurately associates the variance in the outcome variable.

4.4.2 Model Summary

The overall determination of the model was analysed and determined. The output is as shown in table 18 below.

Table 18: Model Summary

Model	R	R Square	Adjusted R Square	Std. The error of The Estimate
1	.781[a]	.610	0.600	.586

A. Predictors: (Constant), Physical Factors, Technological Factors, Administrative Factors

The model summary shows that 61 % in the University Information Security Maturity can be explained by the variables: Physical Factors, Technological Factors, and Administrative Factors with a standard error of .586.

4.4.3 Overall Significance of the Model

The Significance of The Model was analysed using F-statistics.

Table 19: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
	Regression	62.281	3	20.760	60.517	.000[b]
	Residual	39.793	116	.343		
	Total	102.074	119			

A. Dependent Variable: University Information Security Maturity

B. Predictors: (Constant), Physical Factors, Technological Factors, Administrative Factors

It was notable that the model was statistically significant at 0.05, r^2= .610, F (3, 116)=60.517; p <0.05. It can also be inferred that the three independent variables were significantly different in predicting University Information Security Maturity.

From the output r²value, it can be noted that the three independent variables have a combined effect size of r²= .610on University Information Security Maturity. There still remains a gap to be addressed on the remaining 41% of the model which can be attributed to multidimensional nature of Information Security and further enhancement of factors under assessment. Neter *et al* (1996) agrees that the value of r²depends on the field of study and assessment factors.

4.4.4 Regression Coefficients/weights

Table 20: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.821	.228		3.595	.000
	Administrative Factors	.436	.096	.436	4.541	.000
	Technological Factors	-.157	.123	-.151	1.284	.202
	Physical Factors	.590	.127	.532	4.634	.000

a. Dependent Variable: University Information Security Maturity

The Regression Equation

Equation 6: The Regression Equation

$$Y = C + \beta 1_{x1} + \beta 2_{x2} + \beta 3_{x3} + e$$

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:

$$\begin{aligned} UISM = {} & .821 + (.436 * \text{ Administrative Factors}) \\ & + (-.157 * \text{ Technological Factors}) + (.590 * \text{ Physical Factors}) \\ & + .586 \end{aligned}$$

The tested regression model relating to University information security maturity to its drivers was of the form;UISM $= C + \beta1_{x1} + \beta2_{x2} + \beta3_{x3} + e$. Where UISM = maturity score; C = the UISM intercept when x is zero; β1, β2, β3, are regression weights attached to the variables; x1 = Administrative Factors; x2= technological factors; x3 = physical factors; and e allows for errors. The output of regression equation is such that x1 is $.436$. While x2 produced $-.157$and x3 was $.590$. From the confirmations P values it can be noted that x2 varies inversely with the administrative and physical factors. The P value of .202 is as a result ofcomplex and multidimensional nature of information security aspects. Overly, considering the overall F test significance in ANOVA and the type of study undertaken x2 is justified for inclusion in model development.

4.4 Derivation of Weights for UISM Mathematical Model

The weights considered for the model are based on statistical data obtained from the previous section. The weighted value for each factor was then considered for model development by incorporating into a web-based computational logic.

4.4.1 Mathematical Modelling

Mathematical models are designed to describe physical systems by equations or, more in general, by logical and computational structures (Menghi, 2019). 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 (Çalişkan, 2019).

Systems of the real world are generally nonlinear (Zhang *et al*, 2020). 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 the 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 (Ricca *et al,* 2020). The next section outlines the process of model derivation.

4.4.2 UISM Mathematical Model

For the 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 is performed informally while 5 being the highest meant that the organization process was are continuously improving which is a desired characteristic in information security maturity. 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 the proposed model for analysis in chapter 3 was actualized by having weighted coefficients obtained from the regression model being used to determine university information Security maturity.

Equation 7: Determine University Information Security Maturity

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

Where;W_i,. . . W_n, respectively are the weights determined through data collection exercise by the study. The obtained weights are adopted from the regression equation above. Were; the output of regression equation is such that W_1 is $.436$ while W_2 produced $-.157$and W_3 was $.590$

While; ***Ri*,. . . *Rn*** respectively are the weighted indicators that determine the state of a particular risk security factor. The weight depends on the score entered by the individual university has per the level of agreements on the respective weights within allowed range of 0 to 5 on each security concern presented on the interface of the web based model developed and presented in the chapter 5.

4.4.3 Model Design Scenarios

Suppose all the assessment questions have constant coefficients, such that

$W=W_1=W_2=... W_,$

Then, the weight will be W, whereby;

Equation 8: Mathematical Maturity Model

$$UISM = WR_1+WR_2+WR_3+ \ ...\ +WR_n.$$

Since W is common,

$$UISM= W (R_1+R_2+R_3+ \ ...\ +Rn)$$

4.4.4 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 were; 6*36 = 216.

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

Equation 9: Percentage Maturity Factor

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

Therefore;

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

Hence;

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

In the view of the above, the relevant weight for the UISM model based on 36 Assessment questions was **0.005**;

The value of the maturity factor of UISM could be represented as a percentage factor (UISM %) as shown in equation 5 below;

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

Hence

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

4.4.5 UISM 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 5 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 achieve is deduced according to ISO 27001 requirement which includes; state of non-compliance, initial compliance, and basic compliance, acceptable and full compliance respectively (Siponen & Willison, 2009).

4.5 UISM Model Metrics

Information Security Maturity of an organization was determined as shown in equation 5, which represented the compliance level of the organization to ISO 27001 standard, and second computing UISM as shown in equation 10 which represents the organization's deficit score or gap for it to attain full compliance to ISO 27001 standard. There are therefore five model scenarios which are explained in sections

4.6.1 to 4.6.5, namely; non-compliance, initial compliance, and basic compliance, acceptable and full compliance

4.5.1 State of Full Compliance

For an 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 was the process is continuously improving according to ISO 27001 compliance will be determined by the model taking into consideration some of the organization scores for the 36 information security assessment questions is equal to 216.

Equation 10: Desired State of Full Compliance and Continuous Improvement in the Process

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

By substituting back to the equation in equation 5,

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

Equations 10 above depicts that the user and their organizations are fully compliant to the specific requirements of ISO 27001 standard at ideal value of UISM=100% and that it is fully compliant and process are continuously improving.

4.5.2 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 the equation in equation 5,

Equation 11: Acceptable State of Compliance Entails Organizations Being Conscious about Their Security Needs.

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

Equations 11 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 an acceptable level of compliance to the specific requirements of ISO 27001 standard at assumption value of UISM=75% and above.

4.5.3 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 are 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 the equation in equation 5,

Equation 12: Basic Compliance State Usually Centred on the Business Activities of the Organization and the Protection of Core Systems

$\boldsymbol{UISM = \frac{1}{2}(0.0046(216) = 50\%}$ *;*

Equations 12 from the basic compliance state it depicts two restrictions that are faced at this stage: First, financial restriction and spending on systems that do not add value to the income of the business. Second, organizations classify their initial investments in security as completed. The user and their organizations have a basic level of compliance to the specific requirements of ISO 27001 standard at UISM=50%. The organization will have a perception that their systems are protected and they become unaware of the threats and vulnerabilities.

4.5.4 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 the equation in equation 5,

Equation 13: Initial Starting Point for any Organization

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

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

4.5.5 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 the equation in equation 5,

Equation 14: Non-Compliance State is characterized by None Existence of Policies and Procedures

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

From Equations 14 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 %.

4.5.6 Maturity Threshold Scores

The working of the maturity model assessment threshold scale is such that the threshold scores which are on a scale of 0 to 5 were pegged at 4. This score denotes that the organization agrees to be compliant to the requirements of ISO 27001 standard. Score 5, which denote that the organization process is in the desired state and continuously improving in line with ISO 27001 compliance standard requirements. This meant that the organization's 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) mean that the organization's 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 with the threshold scores.

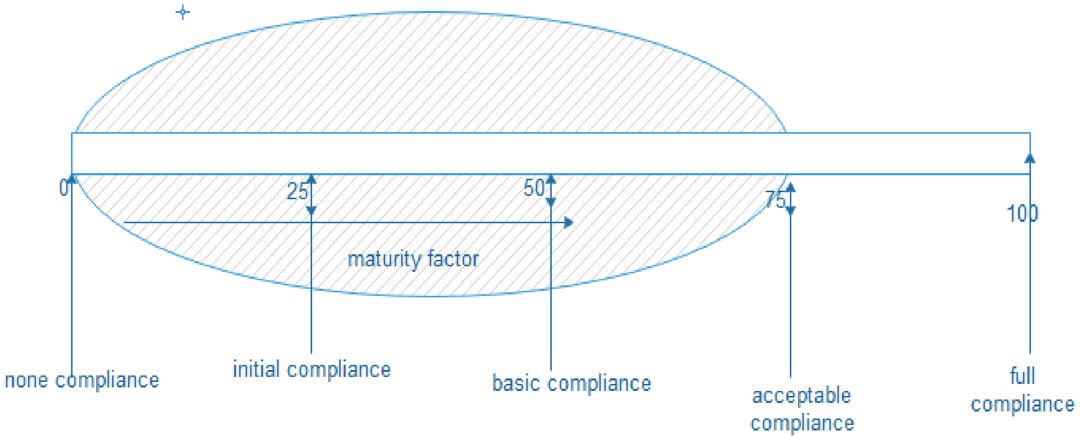


Figure 13: Assessment Scale

As presented in the equations, 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 are 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 information security index computation logic is provided and a guiding recommendation report is determined based on risks associated with the index in the next chapter on model implementation for the organization to take into account so as to remain secure.

CHAPTER FIVE

MODEL IMPLEMENTATION

5.1 Introduction

This chapter discusses the process that was followed to implement the ISO 27001 based model to determine university information security maturity under uncertainty. The Goal Question Metric approach (GQM) was used in coming up with the project overall goal realization. It also describes the 5 steps functional decomposition process that was followed in model development as described in section 5.2.5.

5.1.1 Metrics Model Mapping Approach

The Goal Question Metric (GQM) approach is based upon the assumption that for an organization to measure in a purposeful way it must first specify the goals for itself and its projects, then it must trace those goals to the data that are intended to define those goals operationally, and finally provide a framework for interpreting the data with respect to the stated goals (Basili & Rombach, 1988).

Accordingly, the findings from the regression equation were mapped in three levels. The conceptual level (GOAL) consisting of the dependent variable – university information security maturity (UISM). The Operational level (QUESTION) that takes into consideration the data items in each of the independent variables; Administrative factors, Technological factors, and physical environmental security. Finally, the metrics derivation based on the individual itemized factor in the independent variables as quantitatively operationalized according to statistical findings. The weights are attached to each particular information security independent variables as shown in the previous section as per the regression equation.

Therefore in taking the considerations on metrics to compute university information security maturity, measurement is defined in a top-down fashion since the objective should be focused, based on goals and the model. The GQM approach to realize the model is as shown in figure 14 below.

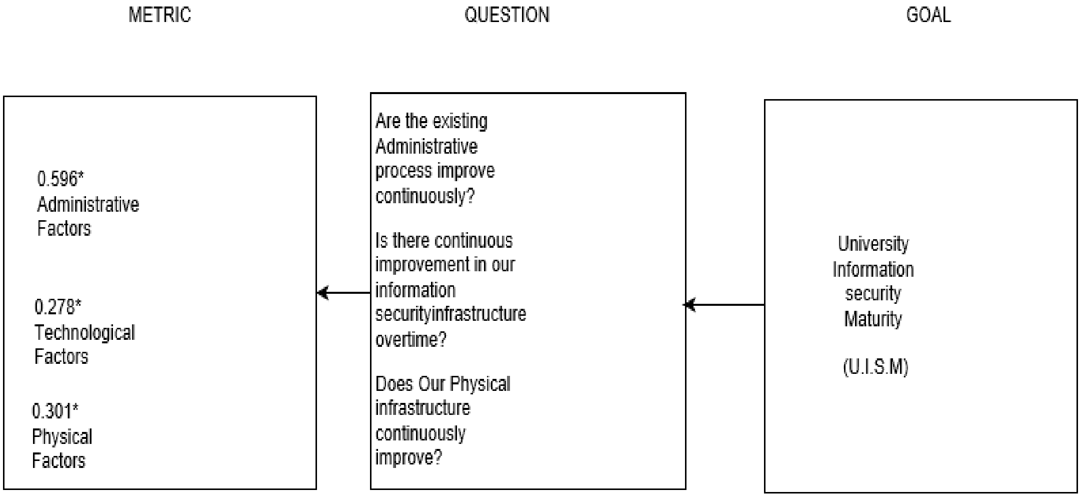

METRIC
QUESTION
GOAL
0.596* Administrative Factors
0.278* Technological Factors
0.301* Physical Factors
Are the existing Administrative process improve continuously?
Is there continuous improvement in our information securityinfrastructure overtime?
Does Our Physical infrastructure continuously improve?
University Information security Maturity
(U.I.S.M)

Figure 14: Information Security Maturity GQM

The envisaged weights that determine university information security maturity are illustrated as shown above in figure 14.The weights are obtained from the regression equation in the previous chapter. The questions that are desired to obtain information security are also shown in the diagram question section. Finally, the overall goal is determined by taking into consideration the specific itemized question in the information security determinant factor that brings in data items that have been operationalized to come up with the weights for each of the independent variables.

5.2 University Information Security Maturity Model Design

Functional decomposition which is a top-down representation of a process was adopted in model design. Functional decomposition is a term that engineers use to describe a set of steps in which they break down the overall function of a device, system, or process into its smaller parts (Mall, 2018). The design overview is explained in 6 sections; namely, section 5.2.1 to section 5.2.6 that describes the process that was followed in the realization of the model explained in the GQM in the previous section.

5.2.1 Model Objectives

The core objective of this study is to come up with a model that enables universities to determine their maturity in information security. The platform enables universities to audit their information technology infrastructure taking into consideration the ISO 27001 standard. The standard becomes relevant because it serves as a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization’s information risk management processes (Fauzi,*et al,* 2018). The existing scenario in universities is gauged on perpetrated number of attacks on information technology infrastructure which gives a red flag to the organization to implement remedial measures. The measures implemented are put in place once the attack has taken place and also sometimes organization patch software after an incidence attack has occurred. The envisioned model determines information security maturity by enabling IT staff to forecast their maturity in security by answering specific questions. Once the organization has gauged its maturity level it then informs the organizations appropriately on infrastructure investments and red tapes areas of concern, therefore, informing on the necessary defence in-debt strategy to be adopted.

5.2.2 Model Functional Overview

Towards realizing the concept the model was implemented using open source tools. The model was developed with PHP for server-side scripting, MySQL for the backend, JQuery in interactive functions. The model ensured that all users are registered before allowing them to access any of the system functionality. All successful and unsuccessful attempts to access system functionality in addition to maturity level computation for the organization were recorded and encrypted to ensure data security. The model implementation functional overview sections are shown in table 21 below;

Table 21: Model Functional Overview

Model Functionality	Function realization
1. User authentication and security	The proposed model ensured that all users are registered before allowing them to access any of the system functionality. All successful and unsuccessful attempts to access system functionality in addition to all information security maturity computation were stored in an encrypted format.
2. User registration	All users are required to register prior to accessing any of the system functionality. Utmost care is taken at the entry point of the system to ensure the details of particular organizations are secured.
3. User de-registration	Organizations can deregister and drop all maturity related records of their organizations whenever necessary.
4. Measurement metric	The model considers each itemized question as per the information security maturity factor and multiplies with associated weighted value.
5. Maturity level Computation	The model enables users to use a web interface to access predefined questions that can be used to gauge organizational information security maturity.
6. Report generation	Once the participant organization has gauged its maturity they are provisioned a report with relevant maturity recommendation for improvement.

5.2.3 System Participants

The participating entities in university information security maturity are composed of; System users, System Administrators, Domain registrar, and hosting service providers.

i. **System Users:** This is the appointed personnel in a particular organization given authority to login into the platform and determines information security maturity. They should be able to answer a specific set of questions that seeks to compute maturity and therefore supply the information into maturity database. Once information is supplied then it can be weighted and summated to obtain maturity level of the particular organization. The user can, therefore, download a maturity report with a relevant recommendation report.

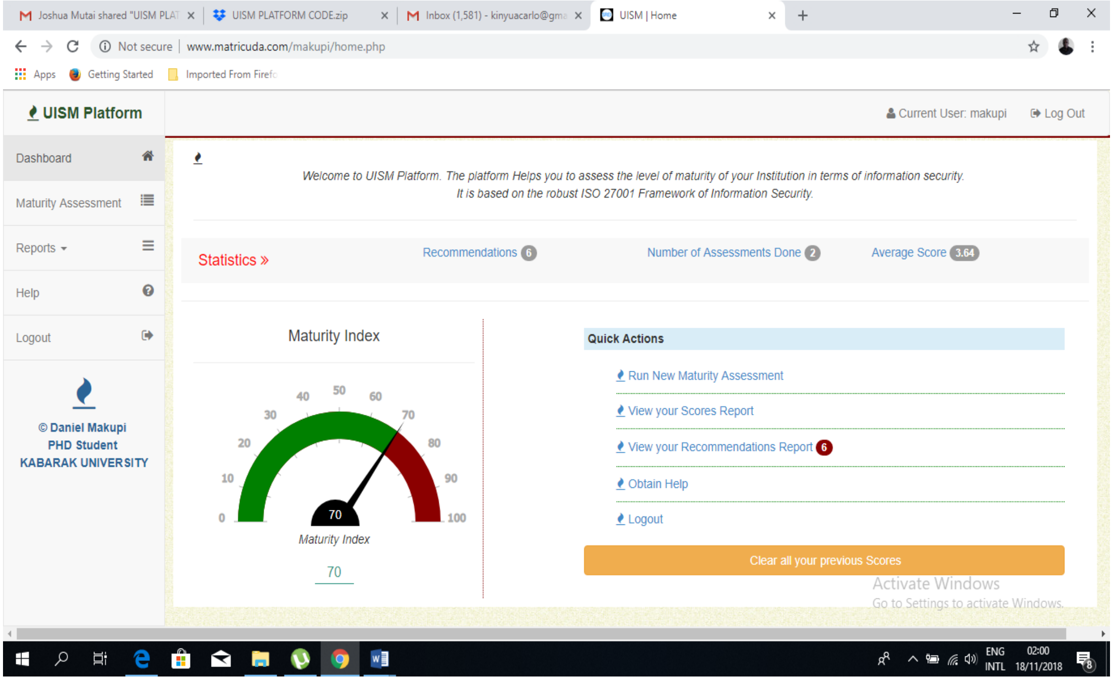
ii. **Administrators:** The administrators have the overall privileges to register and deregister organizations. They are vested with the rights of performing any necessary upcoming changes in the model. They also provide organizational user support when needed. Also, the administrators have the internal view of how maturity level information security indicators are mapped in the physical storage.

iii. **Domain registrars:** The domain registrar is the organizations that register domain names. To get the address of a domain one has to register with a domain registrar. The domain could be on companies or institutions or individual name. The registration of domain names is done through InterNic, a body that manages databases of all registered domains so far and is collaboration between US National Science Foundation, AT & T and Network solutions (Zhang, 2018). Therefore for these model to be accessible online the reservation and registered domain was done with a domain registrar.

iv. **Hosting service provider:** The web hosting service providers are the organization hosting the model in their servers. The model hosted is then accessible 24/7 online for organizations to register and login to determine their maturity and also obtain their information security maturity report. The web server also ensurestwo-way communication between organizations and the hosted site.

5.2.4 Components Interface

The main interface to the system was composed of a web application running on a web browser provisioning the predefined questions that determine information security maturity. The users are able to login and from one common dashboard are able to access the interface are shown in Figure 15 below.



Welcome to UISM Platform. The platform Helps you to assess the level of maturity of your Institution in terms of information security. It is based on the robust ISO 27001 Framework of Information Security.

© Daniel Makupi
PHD Student
KABARAK UNIVERSITY

Figure 15: The User Interface of UISM

5.2.5 Processes Required for Achieving System Functionality

The process followed to achieve system functionality adopted rapid application approach discussed in section 3.5 and depicted in Figure 10. RAD emphasizes working software and user feedback over strict planning and requirements recording (Mall, 2018). Because of its agile approach, it suits the development of university information security maturity in that it has a faster turnaround. The process involved the following steps;-

i. **Gathering requirements:** The requirements for the proposed model were inferred from literature and refined using results from the user survey presented in chapter 4.

ii. **Quick design:** The system was designed taking into consideration its conceptual process flow. The flowchart below showed the system subcomponents and direction process flow. The quick design process flow is shown in figure 16 below.

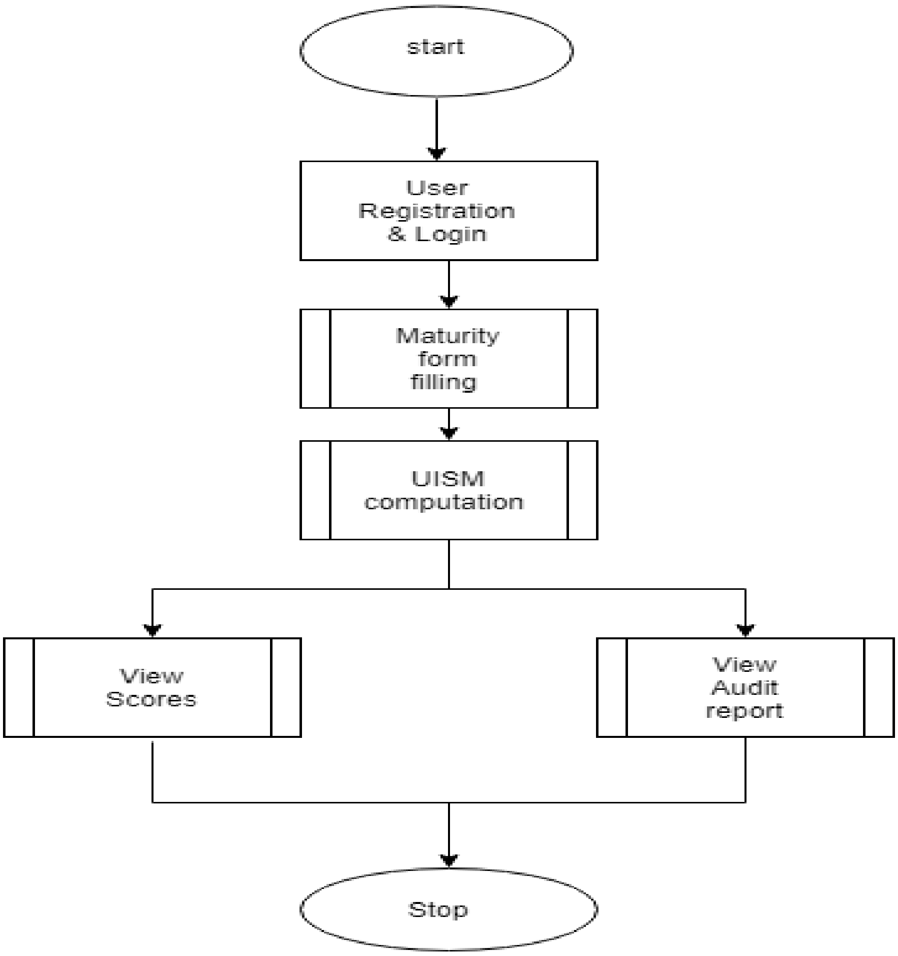


Figure 16: UISM Quick Design Process Flow

iii. **Build prototype:** A prototype was then built using PHP programming language, the MySQL database and hosted online on a domain acquired as part of the development process.

iv. **Evaluation and refinement of requirements:** The system requirements were refined on an on-going basis using feedback from the system development, deployment, and testing process.

v. **Design, code, and test final product:** Once the requirements were found to be satisfactory a final version of the system was completed and tested with real users in a pilot study. Feedback from this stage informed some additional development and refinement of the system logic and the user interfaces design.

5.3 Design and Testing of University Information Security Maturity (UISM) Model

The core objective of this research is to come up with a model that computes information security maturity of a specific organization. A conceptual model to graphically represent the system was designed with input from existing models in literature such as the SCADA information security maturity model and Oil and Natural Gas Subsector Cyber security Capability Maturity Model (Ong-C2m2) ,(Ramon & Zajac, 2018). The model incorporates three main components; the users, system administrators, and the hosting service providers. This section presents the system logic and database design. In addition, the testing results and an evaluation report of the prototype are also presented. There are four main functions of the system; organization registration, filling assessment details, computation of UISM and detailed audit report for information security maturity. An overview of the system flowchart is depicted in Figure 17**.**

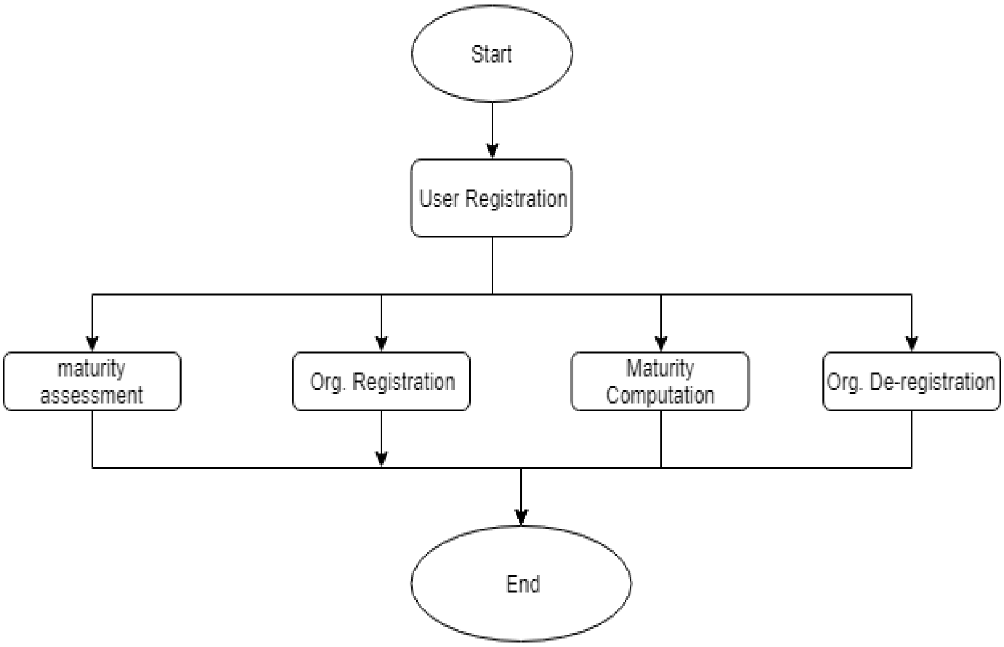


Figure 17: Flow chart of UISM prototype

5.3.1 Entity Relationship Diagram

The entity-relationship diagram (ERD) was used to graphically illustrate the maturity model conceptual implementation. It depicts the entities and relations between entities in the model. ER modelling is a diagrammatic technique used to represent the conceptual model of the relational database. The entity is a real-world object or concept described in a database whereas attributes are properties of the entity measuring the appropriateness of attribute groupings into relational schemas (Balaji *et al*, 2018). The Entity relationship diagram (ERD) for university information security maturity with four tables for data storage is as depicted below in figure 18.

i. Organization user registration and login authentication information: user_id, user_name. Email_ID, maturity, and password (SHA1 cryptographic algorithm).

ii. Maturity Questions: category_id, category_name.

iii. System Questions information: Category_id, question_id, recommendation, threshold_score.

iv. Maturity information: user_id, question_id, assessment_date, assessment_score.

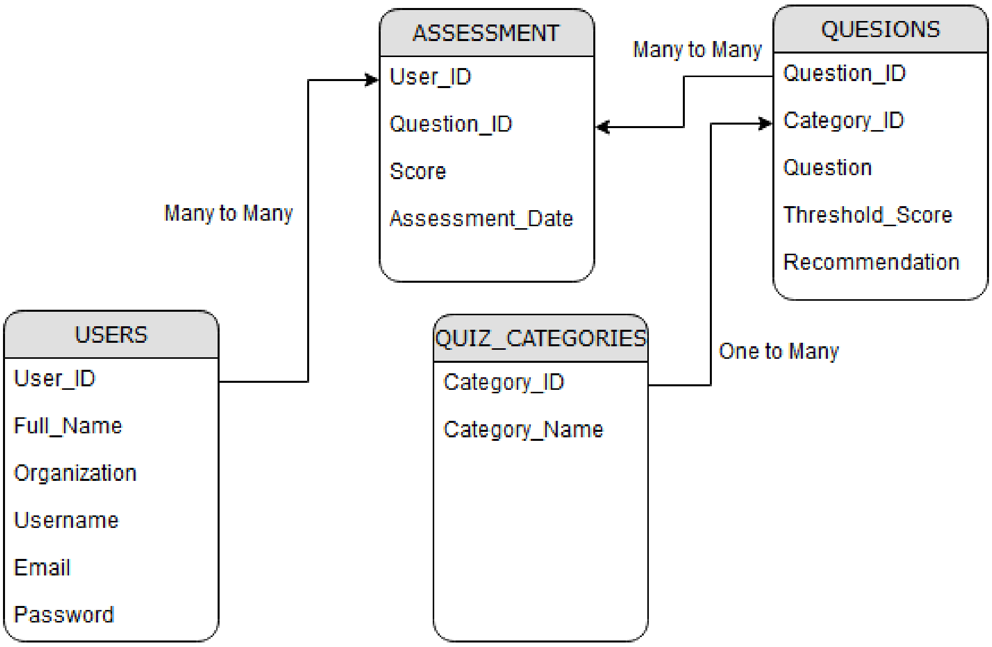


Figure 18: Entity Relationship Diagram

5.3.2 Organization Registration

The registration process is the entry point into the system and caters for the two types of system users, namely; guests and the specific organizations that would what to assess their information security maturity. The guests must register by providing their details. Also, the specific organization must register to be able to get an opportunity to access the online maturity assessment form that will determine particular organization maturity. The user registration process is outlined in Figure 19 as shown below;

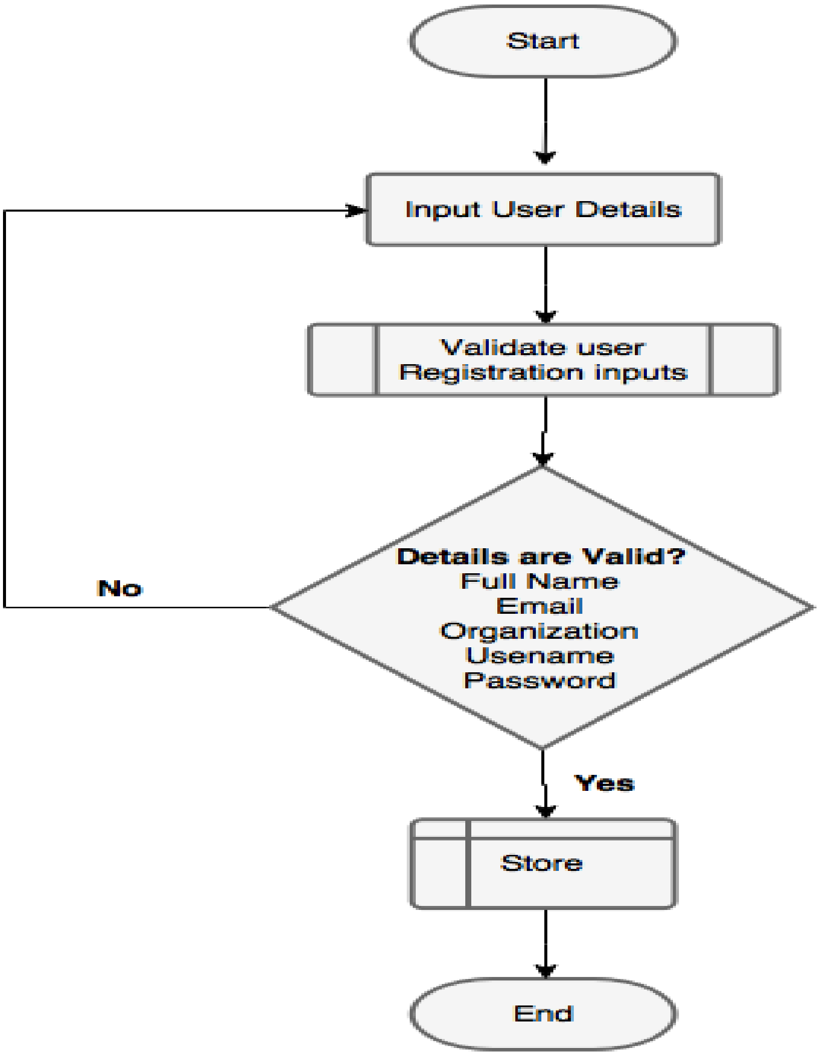


Figure 19: Registration Process Flowchart

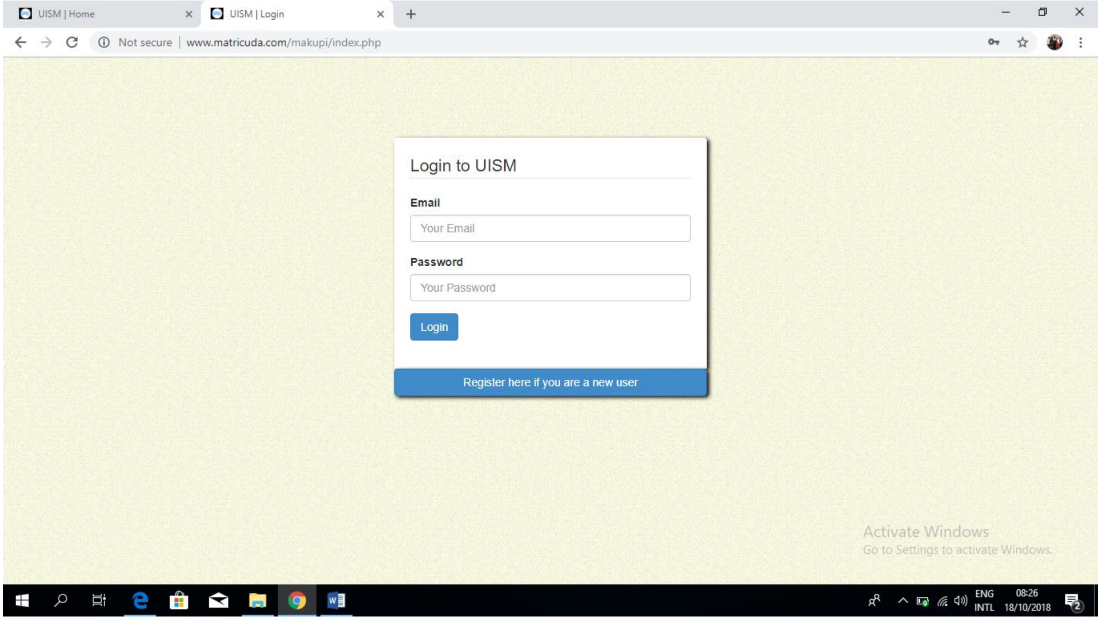


Figure 20: Registration GUI

The graphical user interface for data entry by appointed personnel within the specific university is as shown above in figure 20.

5.3.3 Information Security Maturity Module

The maturity information regarding particular organization dependent on information supplied is displayed in this section. It is able to consider the Likert scale range from 0 to 5 accordingly in conformity with proposed accepted criticality scale in 114 ISO/IEC 27001 (Annex I) and 27002 standard controls scoring in a scale from 0 (noncompliance) to 5 (continually improving) (Kurniawan & IRiadi, 2018). The organizations supply predefined maturity questions to maturity database. Once information is captured the model utilizes maturity formula to compute information security maturity of the organization. Figure 21 below depicts the flowchart of information security maturity computation logic. The user interaction interface for maturity assessment is shown in figure 22.

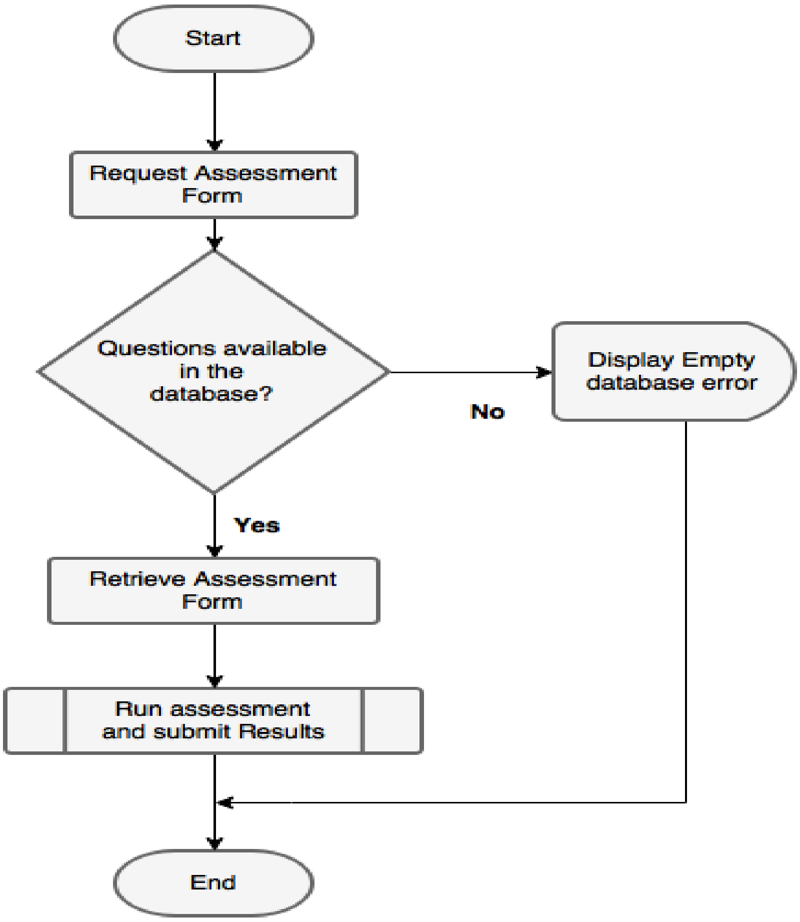
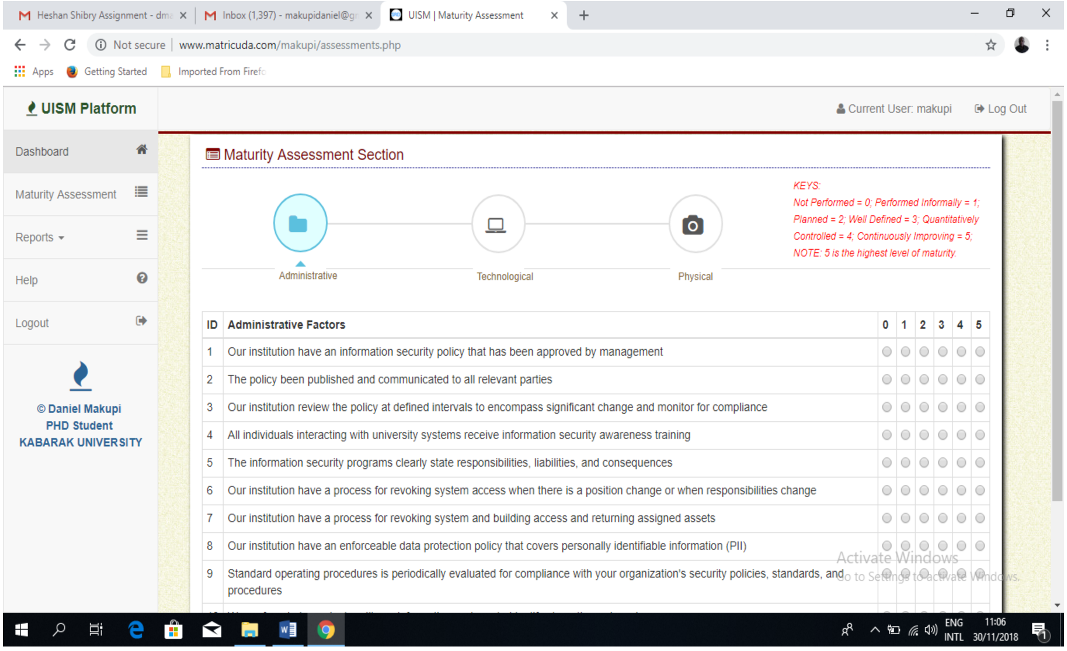

Start
Request Assessment Form
Questions available in the database?
No
Display Empty database error
Yes
Retrieve Assessment Form
Run assessment and submit Results
End

Figure 21: Maturity Computation logic flowchart



Maturity Assessment Section

KEYS:
Not Performed = 0; Performed Informally = 1; Planned = 2; Well Defined = 3; Quantitatively Controlled = 4; Continuously Improving = 5;
NOTE: 5 is the highest level of maturity.

ID	Administrative Factors	0	1	2	3	4	5
1	Our institution have an information security policy that has been approved by management	○	○	○	○	○	○
2	The policy been published and communicated to all relevant parties	○	○	○	○	○	○
3	Our institution review the policy at defined intervals to encompass significant change and monitor for compliance	○	○	○	○	○	○
4	All individuals interacting with university systems receive information security awareness training	○	○	○	○	○	○
5	The information security programs clearly state responsibilities, liabilities, and consequences	○	○	○	○	○	○
6	Our institution have a process for revoking system access when there is a position change or when responsibilities change	○	○	○	○	○	○
7	Our institution have a process for revoking system and building access and returning assigned assets	○	○	○	○	○	○
8	Our institution have an enforceable data protection policy that covers personally identifiable information (PII)	○	○	○	○	○	○
9	Standard operating procedures is periodically evaluated for compliance with your organization's security policies, standards, and procedures	○	○	○	○	○	○

Figure 22: User Interface for Maturity Assessment

5.3.4 Model Code Logic

The maturity regression equation implementation logic is realized in a prototype for overall goal realization. This model explains the output value as university information security maturity gave different sets of input data items. Linear regression modelling is a specific form of regression modelling that assumes that the output can be explained using a linear combination of the input values (Preacher *et al,* 2006). Also, it conforms accordingly to simulation modelling that takes the form of computer programs, where logical arithmetic operations are performed in a prearranged sequence. This provides an added flexibility in model formulation and permits a high degree of realism to be achieved, which is particularly useful when uncertainties are an important aspect of decision making. The code logic realized in the web based model is as shown in Table 22 below.

Table 22: Model code Logic

```
<?php
        include_once 'dbconnect.php';
        $user_id = $_SESSION['usr_id'];

$sql = "SELECT ROUND(100*((0.821+SUM(user score*weight)+
0.586)/(0.821+SUM(5*weight) + 0.586)),1) FROM `maturity_assessment`WHERE
user_id='$user_id' ";
        $result = mysqli_query($con,$sql);
        $data = mysqli_fetch_array($result);
        $uism = $data[0];

        if($uism == 0){
                echo 0;
        }else{
                echo $uism;
        }

?>
```

‘

The University Information Security Maturity is realised by taking the maturity weight of each of the maturity factor and multiplying with each individual organizational score. The maturity “questions” are sectioned per category and each weighted score is multiplied by the associated organizational position.

5.3.5 Maturity Score Module

The maturity scores module captures information as supplied by users and considers the university information security maturity computation for the relevant maturity factor score. The scores about particular information security factor are then provisioned to a user from the web-based interface in any format of their choice. The user can, therefore, receive a report regarding their organization in information security maturity. This report is itemized according to predefined data items of the ISMS 27001 checklist. Upon receiving the report then the user will be able to know which specific area they need to be able to implement defence-in-depth. The module is able to classify the reports based on organization information including the time of assessment done and the particular responsibility employee who performed maturity assessment on behalf of the organization. The diagrammatic representation is depicted in flowchart figure 23 and user interface presentation score logic shown in figure 24.

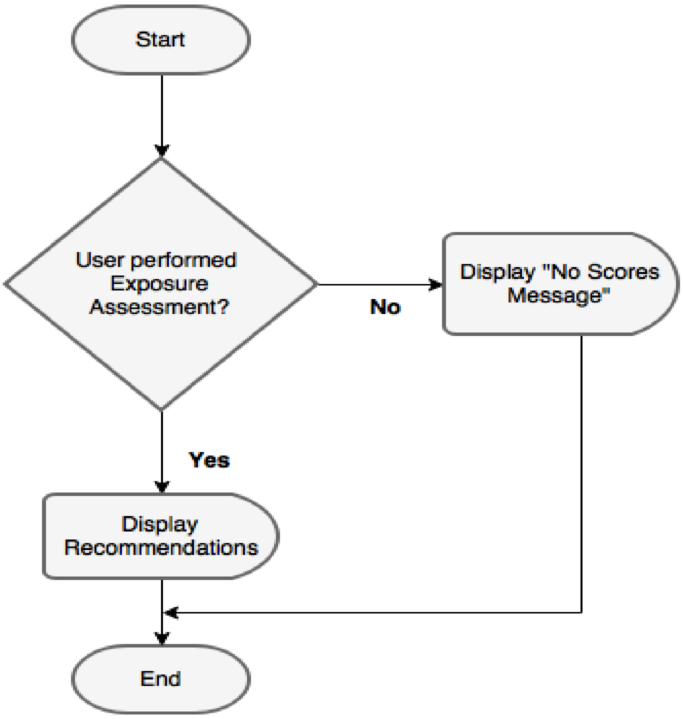

Start
User performed Exposure Assessment?
No
Display "No Scores Message"
Yes
Display Recommendations
End

Figure 23: Maturity Score Flowchart

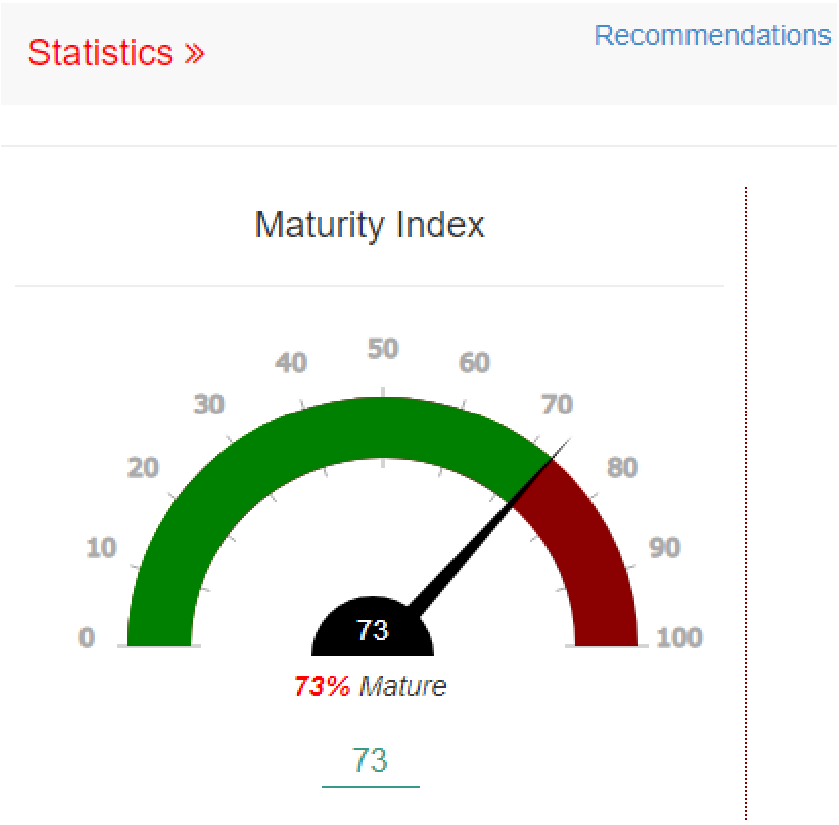


Figure 24: Maturity Scores GUI

5.3.6 Maturity Report Module

The reporting module retrieves report as supplied from the individual data item. The data items once supplied is associated with specific recommended report for the course of action that organizations should adopt. The advisory report contains information regarding what the organization should do to attain reasonable maturity level. Finally, the user can be able to generate the report securely from the web interface in the preferred format. The maturity report flowchart is as shown in Figure 25 below with the user interface in figure 26.

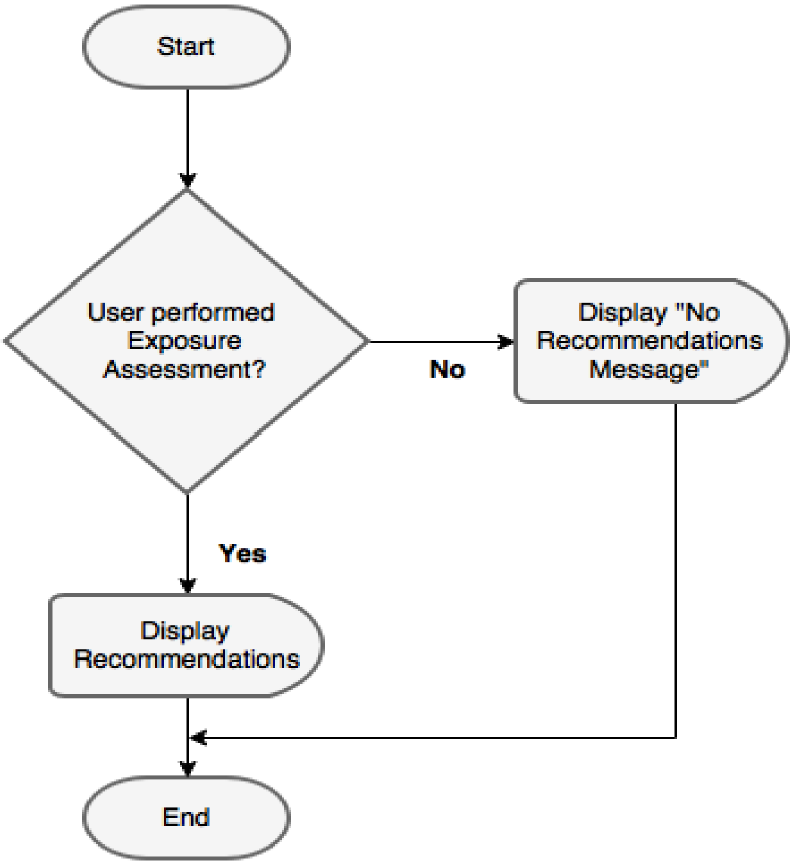
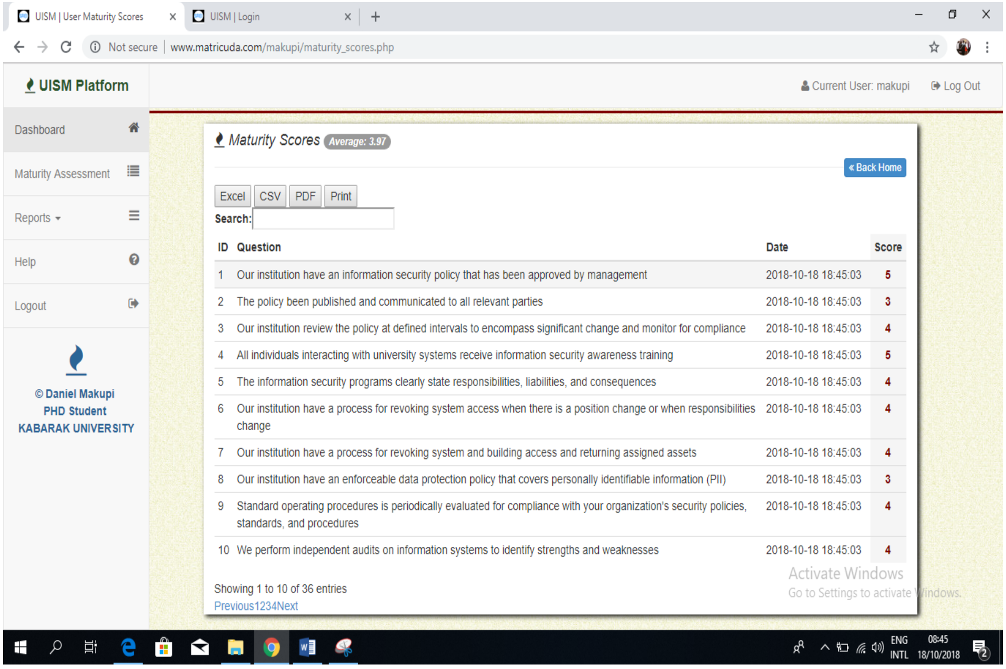

Start
User performed Exposure Assessment?
No
Display "No Recommendations Message"
Yes
Display Recommendations
End

Figure 25: Maturity report Flowchart



Maturity Scores Average: 3.97

Search:

ID	Question	Date	Score
1	Our institution have an information security policy that has been approved by management	2018-10-18 18:45:03	5
2	The policy been published and communicated to all relevant parties	2018-10-18 18:45:03	3
3	Our institution review the policy at defined intervals to encompass significant change and monitor for compliance	2018-10-18 18:45:03	4
4	All individuals interacting with university systems receive information security awareness training	2018-10-18 18:45:03	5
5	The information security programs clearly state responsibilities, liabilities, and consequences	2018-10-18 18:45:03	4
6	Our institution have a process for revoking system access when there is a position change or when responsibilities change	2018-10-18 18:45:03	4
7	Our institution have a process for revoking system and building access and returning assigned assets	2018-10-18 18:45:03	4
8	Our institution have an enforceable data protection policy that covers personally identifiable information (PII)	2018-10-18 18:45:03	3
9	Standard operating procedures is periodically evaluated for compliance with your organization's security policies, standards, and procedures	2018-10-18 18:45:03	4
10	We perform independent audits on information systems to identify strengths and weaknesses	2018-10-18 18:45:03	4

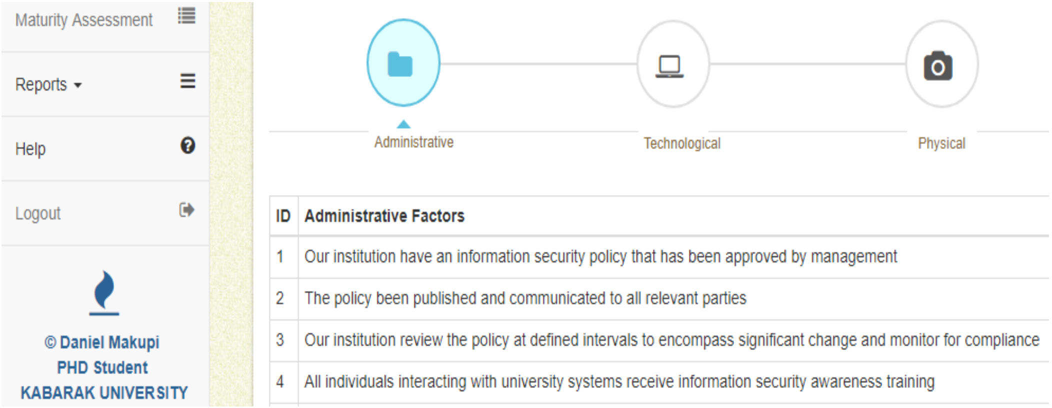
Showing 1 to 10 of 36 entries

Previous1234Next

Figure 26: Maturity report Assessment

5.3.7 User Support Module

The user support module helps users in navigating maturity prototype by being given guidance on how to interact and use the system. The users are given a step to step guidance on prototype usage. The different sections of the system are provided on responsive buttons that have particular subjects regarding the maturity prototype. The user interface interaction is as shown in figure 27 below.



ID	Administrative Factors
1	Our institution have an information security policy that has been approved by management
2	The policy been published and communicated to all relevant parties
3	Our institution review the policy at defined intervals to encompass significant change and monitor for compliance
4	All individuals interacting with university systems receive information security awareness training

Figure 27: UISM User support

5.3.8 The Home Page Display

The home page display presents the user interface that the user interacts on. This section has a responsive tab's that will guide the user to different sections of the prototype. From the interface is where the presentations of maturity index are displayed. It, in addition, facilitates the re-entering of results and scores and also deleting previous scores. If the user is not interested to delete the scores then the scores can remain on the prototype portal for future comparisons. The user interface abstracts the users from the internal logic implementation of the model in the web-based prototype. The user interfaces home page is shown in Figure 28 below.

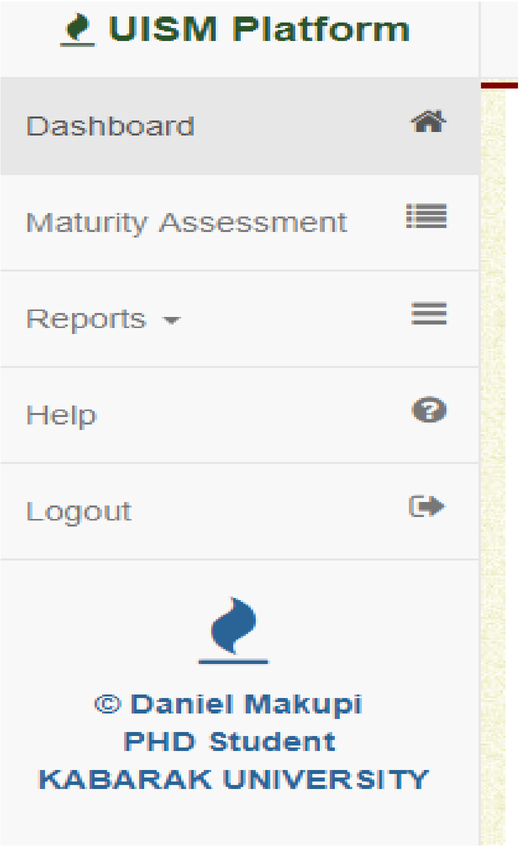
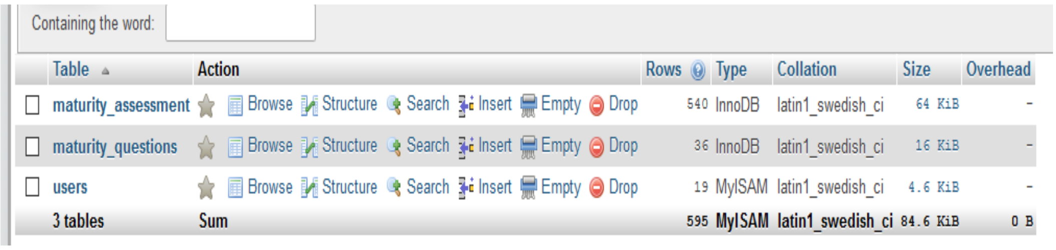


Figure 28: Home Page Display

5.3.9 UISM Physical Database Schema

The physical database schema for model realization into the actual database implementation is described. Physical database design, the creation of efficient data storage, and retrieval mechanisms on the computing platform are salient in the implementation of efficient databases (Jin *et al*, 2018). The translation of the ERD diagram discussed in section 5.3.1 above is realized physically in the internal schema as depicted in Figure 29 below.

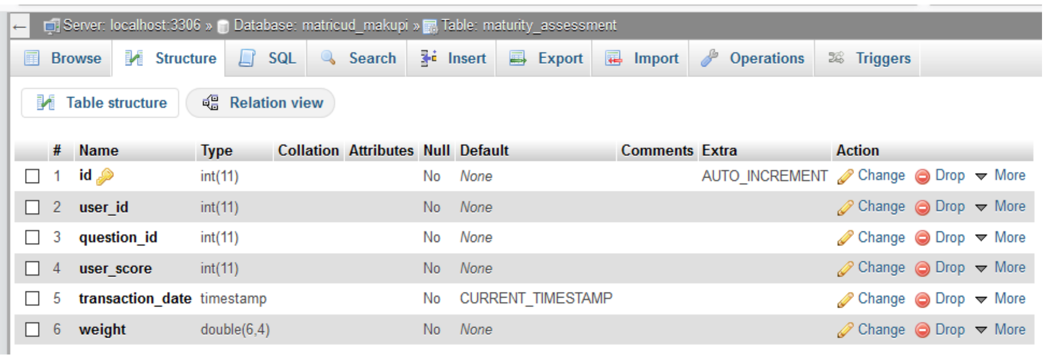


Containing the word:

	Table	Action	Rows	Type	Collation	Size	Overhead
□	maturity_assessment	☆ Browse Structure Search Insert Empty Drop	540	InnoDB	latin1_swedish_ci	64 KiB	-
□	maturity_questions	☆ Browse Structure Search Insert Empty Drop	36	InnoDB	latin1_swedish_ci	16 KiB	-
□	users	☆ Browse Structure Search Insert Empty Drop	19	MyISAM	latin1_swedish_ci	4.6 KiB	-
	3 tables	Sum	595	MyISAM	latin1_swedish_ci	84.6 KiB	0 B

Figure 29: Physical Schema for All Tables

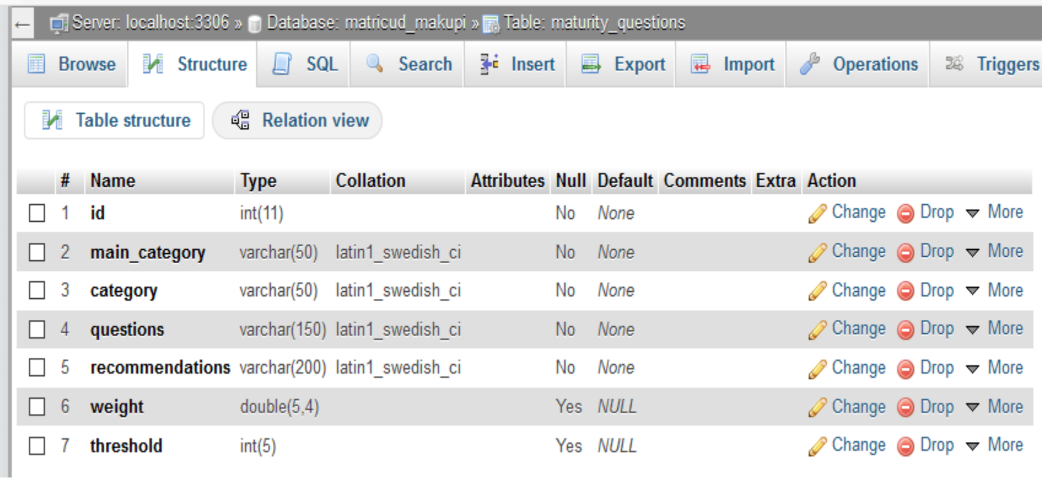
The maturity determination table structure is as shown below in figure 30.



	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
□	1	**id**	int(11)			No	*None*		AUTO_INCREMENT	Change Drop More
□	2	**user_id**	int(11)			No	*None*			Change Drop More
□	3	**question_id**	int(11)			No	*None*			Change Drop More
□	4	**user_score**	int(11)			No	*None*			Change Drop More
□	5	**transaction_date**	timestamp			No	CURRENT_TIMESTAMP			Change Drop More
□	6	**weight**	double(6,4)			No	*None*			Change Drop More

Figure 30: Maturity Assessment Table structure

The maturity questions to be filled by the relevant organizations table structure is as shown below in figure 31

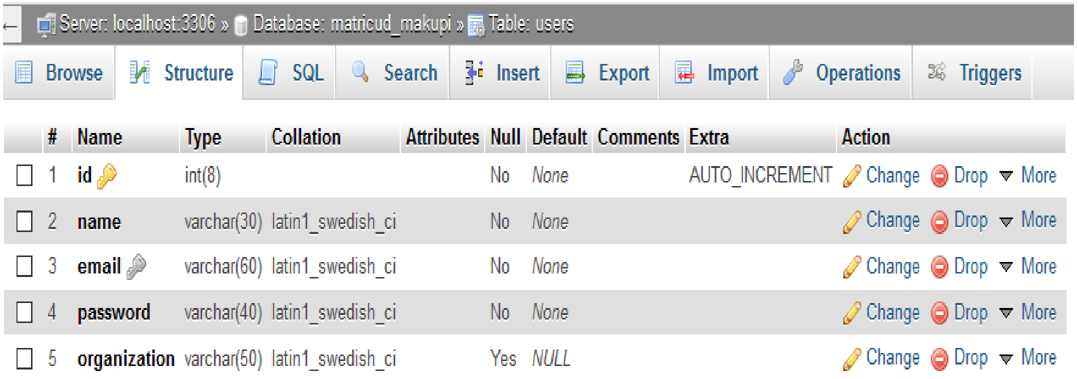


	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
□	1	**id**	int(11)			No	*None*			Change Drop More
□	2	**main_category**	varchar(50)	latin1_swedish_ci		No	*None*			Change Drop More
□	3	**category**	varchar(50)	latin1_swedish_ci		No	*None*			Change Drop More
□	4	**questions**	varchar(150)	latin1_swedish_ci		No	*None*			Change Drop More
□	5	**recommendations**	varchar(200)	latin1_swedish_ci		No	*None*			Change Drop More
□	6	**weight**	double(5,4)			Yes	*NULL*			Change Drop More
□	7	**threshold**	int(5)			Yes	*NULL*			Change Drop More

.

Figure 31: Maturity Questions Table Structure

The details of responsibility users for the particular organizations is as shown below in figure 32.


Server: localhost:3306 » Database: matricud_makupi » Table: users
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Triggers

	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
□	1	id	int(8)			No	None		AUTO_INCREMENT	Change Drop More
□	2	name	varchar(30)	latin1_swedish_ci		No	None			Change Drop More
□	3	email	varchar(60)	latin1_swedish_ci		No	None			Change Drop More
□	4	password	varchar(40)	latin1_swedish_ci		No	None			Change Drop More
□	5	organization	varchar(50)	latin1_swedish_ci		Yes	NULL			Change Drop More

Figure 32: Users Table Structure

5.4 Proof-of-Concept

The viability of the concept and demonstration of workability was done to ascertain the model practical potential. Prototyping was used as a valuable exercise to allow visualization of product functioning by providing an interactive model end product design, navigation, and layout. According to Hallgrimsson (2012) prototypes plays an important role for designers by allowing a physical realization of the idea for problem-solving.

The model for computing information security maturity (UISM) was realized using PHP for server-side scripting, Cascading style sheets version 3 (CSS3) for front end responsiveness and JAVASCRIPT for dynamic and interactive web content. The open source development tools notepad++ editor for editing, MySQL as a database for storage and Apache for local hosting. The prototype was later hosted online available at www.matricuda.com/makupi.The model was able to compute information security maturity of a higher learning institution and offered recommendation on areas of concerns that the organization needed to improve.

5.4.1 Alpha Testing for Web Based Model Evaluation

The goal-centred view of system effectiveness was used to first determine the task objectives of the system, and then to develop criterion measures to assess how well the objectives are being achieved. Effectiveness is determined by comparing performance to objectives (Salimi & Rezaei, 2018). An example of the goal-centred view of systems effectiveness would be to compare actual costs and benefits to budgeted costs and benefits (Perez, 2018). Utilization-Focused Evaluation begins with the premise that evaluations should be judged by their utility and actual use; therefore, evaluators should facilitate the evaluation process and design any evaluation with careful consideration of how everything that is done, from beginning to end, will affect use. Use concerns show how real people in the real world apply evaluation findings and experiences in evaluation process. Therefore, the focus in utilization-focused evaluation is on the intended use by intended users.

The approach adopted in system evaluation was "goal-based evaluation and IT-system as such". This is because the evaluation was performed according to some predefined business goals and that the object of evaluation is the IT-system functioning process. IT-systems as such allow the evaluator to decide if the goals have been fulfilled. The IT system as such works as an Alpha testing approach were the assessment of the model is done on site before actual roll out in production environment. Discussion on whether the system's functionality meets the business goals is presented in Table 23 shown below.

Table 23: Goal-Based Evaluation and IT-System as Such

	Goal	Evaluation Results
i.	**User registration:** The goal was to ensure users get registered and be able to supply their credentials. Also, the user's data is protected using encryption.	The prototype succeeded in capturing user details upon registration by the concerned organization authorized personnel. Also, user credential detail was able to be captured and protected using encryption schemes for security
ii.	**User Authentication and login:** The user should be able to supply correct user registration as per user credentials from stored data in the database before being allowed to access the system.	The system allowed users to supply correct details as per stored login credentials stored in the database. There was a password match between existing credentials in the database upon login by the user.
iii.	**Computation logic:** The system	The system was able to capture the assessment

	should be able to capture the assessment details used for maturity computation. It should be able to allow users to submit a specific question.	details used for maturity computation. The system was able to compute maturity using the data item specific questions in the assessment.
iv.	**University information security maturity Computation:** The model should be able to compute information security maturity using the different information security determinant factors as represented as independent variables.	The prototype succeeded in computing information security maturity upon supply of specific questions by users. The specific questions supplied and using the model formula the prototype was able to compute maturity and provision the level on a graphical user interface (GUI)
v.	**Maturity Scores and recommendations records:** The model to be able to give a report based on scores determining the level of information security maturity on maturity and facilitate documentation of the report.	The model was able to utilize the model to compute maturity and provide relevant recommendation for a particular security risk factor. Also, it was able to allow individual organizations to export data in different formats accordingly.
vi.	**User support:** The model should be user-friendly and easy to navigate for users.	The model was user-friendly and users have provisioned a user-friendly interface for assessment of information security. The system had a responsive interface which is easy to navigate and also users can utilize its functionalities with ease.

5.4.2 Verification and Validation of the Model

The model was implemented in two stages. Firstly data was collected and validated for the development of the model. Secondly, the coefficient values realized in the regression equation was then realized by using the values to develop a web based prototype for information security maturity. The realised prototype was subjected to alpha based pre-testing at every step of model implementation while taking into consideration the users views of model and how it meets their individual organizational information security demands.

5.4.3 Coefficient Values for Model Development

The importance of validity cannot be compromised in any research work; this is the reason why validity was considered as a prime force that can direct the use of research findings. The selected data sources were checked for their validity and sufficient attention was paid in the selection of data sources. The outcome of data collection from various sources was cross-checked to ensure the validity in the research findings. On the other hand, the data collection methods which were used in this research work were analysed and scrutinized before their use in this research work. The choice of conducting interviews and questionnaires was paid considerations by considering their potential impact and conformance with the research scenario. The data were collected from different sources, at a different time and in different situations. This diversity helped in attaining a richer amount of data and by cross-checking results.

5.4.4 Model for Prototype Implementation

Information security maturity model was designed and implemented using open source tools. The prototype was able to allow users to provide their individual organizational credentials and perform an assessment. The system successfully was able to capture the details of users and encrypt details. The individual score record logs were also captured with timestamps attached to each information security research question in each assessment row. The system was able to successfully retrieve recommendations records based on user maturity scores.

5.5 The Limitations of Information Security Maturity Model for Universities

Information security maturity model does come with some drawbacks. One of which is that when organizations use UISM, they look at each level as a target. They make their goal to reach the next level up. This can be a dangerous thought because if you become fixated on reaching the next level, you begin to lose perspective and forget that the real goal is to actually improve the processes. According to Jugdev & Thomas (2002) in examining maturity models from four different resource-based models perspectives in order to assess whether having a higher maturity level in project management bring competitive advantage to an organization or not. Their article concludes that maturity models have some characteristics but not all of a strategic asset, thus cannot present a competitive advantage. This conclusion based on their observation that although “maturity models are a component of project management they are not a holistic representation of the discipline.”

Similarly, the Information security maturity model does not specify a particular way of achieving those goals. In order to achieve them one needs to think in a flexible way. The goals will only be achieved if the organization's processes are taken into account, as each organization is different so the steps needed for process improvement will be different. Just because one organization follows the rules set by the UISM it does not guarantee that it will be successful as there are other factors involved.

Another disadvantage is that UISM only helps if it is put into place early in the software development process (Jugdev & Thomas, 2002). For example, if there is a process that is in a crisis then UISM will not help overnight. It cannot be used as an emergency method of recovering from a difficult position since UISM is based on software maturity models that lack a theoretical basis. Accordingly, it can be concluded that there is no global standard for maturity models which is one of its shortcomings and this is because maturity models are a new concept and need further considerations and clarifications by both researchers and companies.

Finally, UISM is concerned with the improvement of management related activities. Whilst this is a big issue in the software development process it is not necessarily the most important thing to look at. Improved quality of code may be a vital issue in the context of software.

5.6 Challenges of Using Information Security Maturity Model

Security challenges are seldom solved by technology alone. However, all technology implemented should be as good as it can be, and act as the fundamental on which everything else is built. Information security should be a continuous research process for in-depth strategies to ensure confidentiality, integrity, and availability. Organizations should be able to make information security investment decision in line with their organizational requirements based on their maturity in regard to information security.

Security maturity is a continuous process which begins from technology. Various attacks perpetrated on information infrastructure have been as a result of unpatched server, or a misconfigured router or firewall, presenting a worrying tendency for organizations to take their eye off the technology ball (Shulman, 2018). While it may be impossible to prevent all attacks through the use of technology, the implementation of best practice can ensure that it is much harder for attackers to be successful.

From a review of literature, it shows that many organizations fail to fully utilize their existing investment in passive-defence security technology (Bao *et al*, 2010). Often, devices are bought and implemented to solve a specific requirement and are rarely reviewed when that requirement has been met. The answer to a new security challenge may lie with an existing technology asset, such as a firewall that may also run application-aware IPS that could be an enforcement point for integrating endpoint protection. Security technology is a huge asset involving investment, therefore, it is import for organizations to proactively operate and understand their security ecosystem by continuously assessing information security infrastructure against pre-set goals.

5.7 Incidental Application Areas of the Information Security Maturity Model for Universities (UISM).

The model for university information security maturity was initially envisioned to determine information security by taking into considerations specific coefficients and providing a recommendation report to the organization. Aside from the core objectives of the study other potential application areas emerged at the course of model development and system design. These additional application areas proposed by users confirm Kelly's (2007), observations that people often use innovations in ways not originally envisioned.

5.7.1 Auditing Tool for Information Security

The university information security maturity model (UISM) not only becomes applicable to universities but can be scaled to other organizations. The model becomes applicable because sometimes information technology infrastructure in universities can be similar to other organization like banks, hospitals, and Sacco's. Therefore not only is a tool for determining maturity in information security for universities but can be applicable to other types of organization.

5.7.2 Government Compliance Tool

The government can use the model by utilizing it as an automated tool to determine university information technology infrastructure position. The government periodically audits compliance in government institution by ensuring organizations adhere to minimum standard requirements. Since the model is based on the ISO 27001 standard which is almost universally accepted for information security maturity compliance then the government can adopt the university information security maturity model to ascertain compliance.

5.7.3 Used As a Diagnostic Tool

The maturity model can be used as a descriptive tool if it is applied for as-is assessments where the current capabilities of the entity under investigation are assessed with respect to given criteria (Becker *et al*. 2009). The maturity model can be used as a diagnostic tool (Maier *et al*. 2009). The assigned maturity levels can then be reported to internal and external stakeholders.

5.7.4 Determination Tool for Desirable Maturity Level

Information security maturity model can also be used to identify desirable maturity levels and provides guidelines on improvement measures (Becker *et al*. 2009). “Specific and detailed courses of action are suggested.” (Maier *et al.* 2009).

5.7.5 Used For Internal and External Benchmarking

A maturity model can serve as a comparative tool for internal or external benchmarking. Given sufficient historical data from a large number of assessment participants, the maturity levels of similar business units and organizations can be compared (de Bruin *et al.* 2005, Maier *et al*. 2009).

CHAPTER SIX

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

In this thesis, the maturity model implemented for universities is discussed. The model for university information security maturity model (ISMM) is as a tool 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. It defines a process that manages, measures, and controls all aspect of security. It relies on three core indicators for benchmarking and as an aid to understanding the security needs in an organization. These indicators are goal-driven to achieve security needs.

6.1.1 University Information Security Maturity Model Compliance States (UISM)

It is hard for security practitioners and decision makers to know what level of protection they are getting from their investments in security. It is even harder to estimate how well these investments can be expected to protect their organizations in the future as security policies, regulations and the threat environment are constantly changing (Beres, *et al.*, 2009). An information system would transition between several distinct vulnerability states. The first state is hardened and it occurs when all security-related corrections, usually patches, have been installed. The second is vulnerable and it occurs when at least one security-related correction has not been installed. The final state is compromised and it occurs when it has been successfully exploited (Arbaugh *et al*, 2000).

Within the different states, metrics were used to indicate how secure the organization is so that the window of exposure can be minimized by security operation teams in the organization by following a standard patching process to eliminate vulnerability and any associated risks. The security team either deploys patches after the vulnerability is first disclosed or updates signatures that are associated with attacks. The longer the window of exposure, the more the organization is exposed to attacks and exploits. Therefore the magnitude of risks is minimized if organizations are conscious about their security needs (Saleh, 2011). The UISM considered four levels of compliance. Security improves as the organization moves up the five levels from none, initial, basic and acceptable compliances.

6.1.2 UISM Metric and Core Indicator

The principle that was followed was based on the premise that **"what you can't measure, you can't manage"** accordingly agreed with (Guldneret *et, al*. 2018). Therefore four core indicators were developed to manage and measure the compliance with the UISM. Each indicator had its own key performance indicators that showed the overall compliance with the model. The four indicators were domain specific rather than being process specific but they measured the aspect of structure, the management, the practices and the overall performance of the organization in information security.

The specific practices were intended as a guide for those responsible for the activities to draw their attention to good practices and to assist them to evaluate the practices at their organization. For each individual item, six responses are called for, but on items that are not applicable to the organization, they were assumed as non-compliance and were not ignored but used in the overall determination of security maturity. If the data item is applicable for the organization then a 6 point Linkert scale according to ISO 27001 maturity standard consisting of scores from 0 to 5 was used to determine how well the practices are carried out. An overall rating of all domains reflected the compliance with the maturity model.

6.2 Conclusions of Information Security Maturity Model for Universities

This study was based on the premise for the need for an information security maturity model for universities based upon the ISO 27001 standard. The model developed aids in carrying out benchmarking and performance improvement. It is a complete maturity model for carrying out continuous performance improvement. The objective of the model was to provide an organization with a way to conduct a self-study of its security implementation. Compliance with the model determines the results. The goals exist for the five different levels of compliance that organization should purpose to achieve. For an organization to achieve the highest level of security objective it should continuously measure and audit its security implementation.

By having control over the security needs of the organization, monitoring the systems, being aware of threats and benchmarking by comparing the organization itself to other similar organizations and to international standards the organizations achieve full compliance to the model.

Upon unacceptable compliance level, a maturity level indicator metric raises a red flag for organizations that their security is weak and improvements are required in a recommendation report. Through central management of all security-related issues and policies, an organization achieves full compliance. University Information security maturity model measurement indicators are domain specific rather than being process specific but measure the aspect of the structure, the management, the practices and the overall performance of the organization in term of its security.

A model to determine information security maturity for universities was developed and implemented. The solution was able to effectively compute information security maturity of an organization and also provide a recommendation report. The recommendation report is generated for each of the predetermined data items which make the report informative to some extent of exact specification on the infrastructure investment which informs budgeting. The use of the model and assessment of maturity required expertise domain experience in information technology.
Conclusions related to the specific objectives are discussed in sections 6.2.1 to 6.2.2.

6.2.1 Research Question1: What Are The Critical Security Risk Factors That Impact On The Security Of Universities Based On ISO 27001?

From this study, the most critical security risk factor is the human factor represented by administrative factors. The findings conform to findings of Bulgurcu *et al*., (2010) contractors and people within an organization are the greatest assets to that organization because of the value they bring in. however, they are considered to be the weakest link in information security. According to ISO 27001's control 8; human resource security is most important because the security of information in any organization is the responsibility of the employees and other people within that organization.

Although some security threats and breaches are as a result of non-human factors, most of these threats and breaches are widely propagated by humans either accidentally or maliciously (Brauch, 2011). The security risk factor contributes immensely to the model for the computation of university information security maturity (UISM). Accordingly, the finding of the Spearman's rho correlation showed that there exists a statistically significant relationship between administrative factors and university information security maturity ($r=0.675^{**}$; $p<0.01$).This means that when administrative factors are Continuously Improving, the information security maturity at the university will be at its highest level. Conversely, when these factors are under Performed, then its maturity will be low.

6.2.2 Research Question 2: What Are the Existing Models Used In Assessing Information Security Maturity?

A majority of organizations believe that they can buy information security (Jenkins, 2003). Organizations tend to spend money to solve information security problem however it's pivotal enough to highlight certain preliminary perceptions, or rather misconceptions; organizations have regarding the information security discipline. Information security does not exist in a box by itself and that consequently, organizations will have to be concerned with information security, not as a product but a process (Sommer, 2003).

Organizations should not take the view that for every security problem there is a technological solution. Therefore technical products will not solve all their information security problems. They shouldn't take a piecemeal approach to information security, placing a wholly inappropriate degree of reliance on technology. It must be realized that information security is a holistic discipline of which no one component may be ignored (Baskerville, 1998).

The problem, however, lies therein that if security is conceived as principally a technological problem, the focus is drawn away from the other two equally important components of information security, namely physical security, and non-technological/procedural security.

In order to ensure that security requirements are met Eloff (2002) postulates that an organization must use a code of best practice to assess a policy and related procedures; combine that with benchmarking methods to be able to compare with other organizations; and include the compliance results of internal guidelines to determine if the security objectives are met. One such mechanism is the measurement of information security process maturity. In order to have a better understanding of the Information concepts and dimensions, researchers discussed four related models on information security maturity.

The SSE-CMM-Capability Maturity Model (CMM) for System Security Engineering (SSE) focuses on the improvement of a specific process-related trouble spot, while the project on ICS-SCADA Cyber Security Maturity Assessment Model, delved on regulations, policy activities and responsibilities at each member state in the EU. The Cyber Security Maturity Framework for NIST aside from being a framework is not comprehensive to address all information security related processes. The main objective of the framework is to manage cyber security risks within the organizations that implement it. On the other hand, Oil and Natural Gas Subsector Cyber security

6.2.3 Research Question 3: How Can a Model Determine The Maturity Level of Information Security in Universities be Designed?

The development of maturity models was viewed as a matter of design science research. Design science research seeks to create innovative artefacts that are useful for coping with human and organizational challenges (Hevner *et al.* 2004). In this context, Mettler & Rohner (2009) raised the question which artefact type according to the categories given by March and Smith (1995) maturity models actually are. They suggest that maturity models are in between (Mettler and Rohner 2009) models and methods as they combine state descriptions (for example models of distinct maturity levels) with activities (for example methods for recognizing the need for action, conducting assessments and selecting improvement measures).

As for the process of maturity model design, de Bruin et al. (2005) and Becker *et al.* (2009) suggest procedure models. De Bruin *et al.* (2005) propose six phases intended to guide the design of a descriptive maturity model and its advancement for prescriptive and comparative purposes. Becker *et al*. (2009) derive requirements and a procedure model from Hevner *et al*. (2004) design science guidelines. They distinguish eight phases that provide “a manual for the theoretically founded development and evaluation of maturity models” (Becker *et al*. 2009). Though ensuring well-structured and well-documented design processes, we utilized the regression model from data analysis results in chapter four of this study.

The linear mathematical approach proposed in chapters three was then realized by building into a web-based logic. The model coefficients were obtained from the regression equation from analysis results while security variables were the scores of information security related data items provided based on ISO 27001 standard checklists with a range of 0 to 5. Therefore the design of the model was based on analysed data from questions according to ISO 27001 as the standard of IT Security best practices.

6.2.4 Research Question 4: How Can The Model Determine University Information Security Maturity Level be Implemented?

To ensure that security-related tasks are deployed correctly organizations need to build-in security in both planning and the design phases and adopt a specific security architecture. Security requirements must be linked to business objectives. For this study, we identified three core tenets that impact organizational security namely, physical and environmental security, administrative security and technological security. In order to identify and explore the strength and weaknesses of a particular organization's security, a wide range model has been developed. This model is proposed as an information security maturity model (UISM) for universities and it is intended as a tool to evaluate the ability of organizations to meet the objectives of security.

In order to identify and explore the strength and weaknesses of a particular organization's security, a wide range model has been developed. The purpose is to identify a gap between the practice and theory which then can be closed by following a process-oriented approach. We introduce a maturity model that provides a starting point for security implementation, a common and shared vision of security, and a framework for prioritizing actions. Moreover, this information security model has five compliance levels and four core indicators to benchmark the implementation of security in organizations.

The model was implemented using a web-based prototype. It was designed as a web-based application using PHP as a server-side language, JQuery for frontend interactions, and MySQL as a database engine. The model contains a database for storing assessment questions information, assessment scores information and system users' information. Also, interaction and integration between the database and the user interface were also realized. The model relies on the assessment information stored in the database to compute and determine university information security maturity. The model displays the results in a graphical and easy-to-read graphical view. Based on the same score the model generates an associated recommendation score for a particular security data item.

6.2.5 Research Question 5: Can The Model Compute University Information Security Maturity?

With maturity models representing theories of stage-based evolution, their basic purpose consists of describing stages and maturation paths. Accordingly, characteristics for each stage and the logical relationship between successive stages need to be explicated (Kuznets 1965). As for their application in practice, maturity models are expected to disclose current and desirable maturity levels and to include respective improvement measures. The intention is to diagnose and eliminate deficient capabilities (Rummler & Brache 1990). Rummler & Brache (1990) metaphorically refer to such tools as engines for continuously improving systems, roadmaps for guiding organizations, and blueprints for designing new entities. Typically, the following application-specific purposes of use are distinguished accordingly and confirmed by the model implemented.

The model was descriptive enough because it serves its purpose of use if achieving "as-is assessments" where the current capabilities of the entity under investigation are assessed with respect to given criteria (Becker *et al*. 2009). The maturity model is used as a diagnostic tool (Maier *et al*. 2009). The assigned maturity levels can then be reported to internal and external stakeholders.

It meets its prescriptive purpose of use by indicating desirable maturity levels and provides guidelines on improvement measures (Becker *et al.* 2009). "Specific and detailed courses of action are suggested which in line with suggestions of." (Maier *et al*. 2009).

It also meets the comparison objective by comparability through internal and external benchmarking with other organizations. Given sufficient historical data from a large number of assessment participants, the maturity levels of similar business units and organizations can be compared (de Bruin *et al*. 2005, Maier *et al*. 2009).

The relevant maturity index and expert information security report on areas of concern for the different universities who participated and also approached to use the model to audit and determine their information security maturity is discussed in section 6.3 below.

6.3 Expert Sample Beta Testing Maturity Assessment Reports

An information security determination report for different Universities in Kenya who logged in and did a maturity assessment has part of model testing for their respective Universities are discussed. Some of the institutions participated in the data collection during model design. The institutions assessed are both public and private universities. The following recommendation reports illustrated in the next section represents an information security position for the different institutions respectively. The assessment was done by ICT personnel in the universities. The report seeks to illustrate how the model can compute information security maturity for particular organizations. An information security maturity index will be illustrated followed by the relevant information security report for the university.

i. Organization "A" Information Security Maturity Determination and Report.

The organization below is a private chartered university in Kenya. The following maturity index of organization A illustrates its maturity in information security as done by ICT administrator.

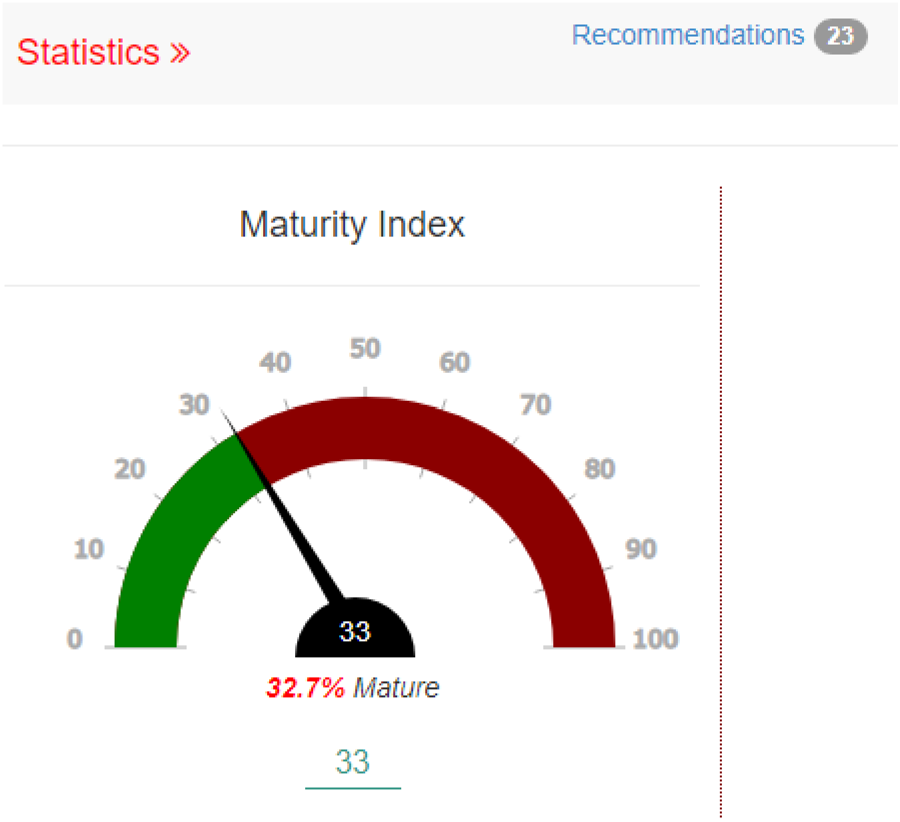
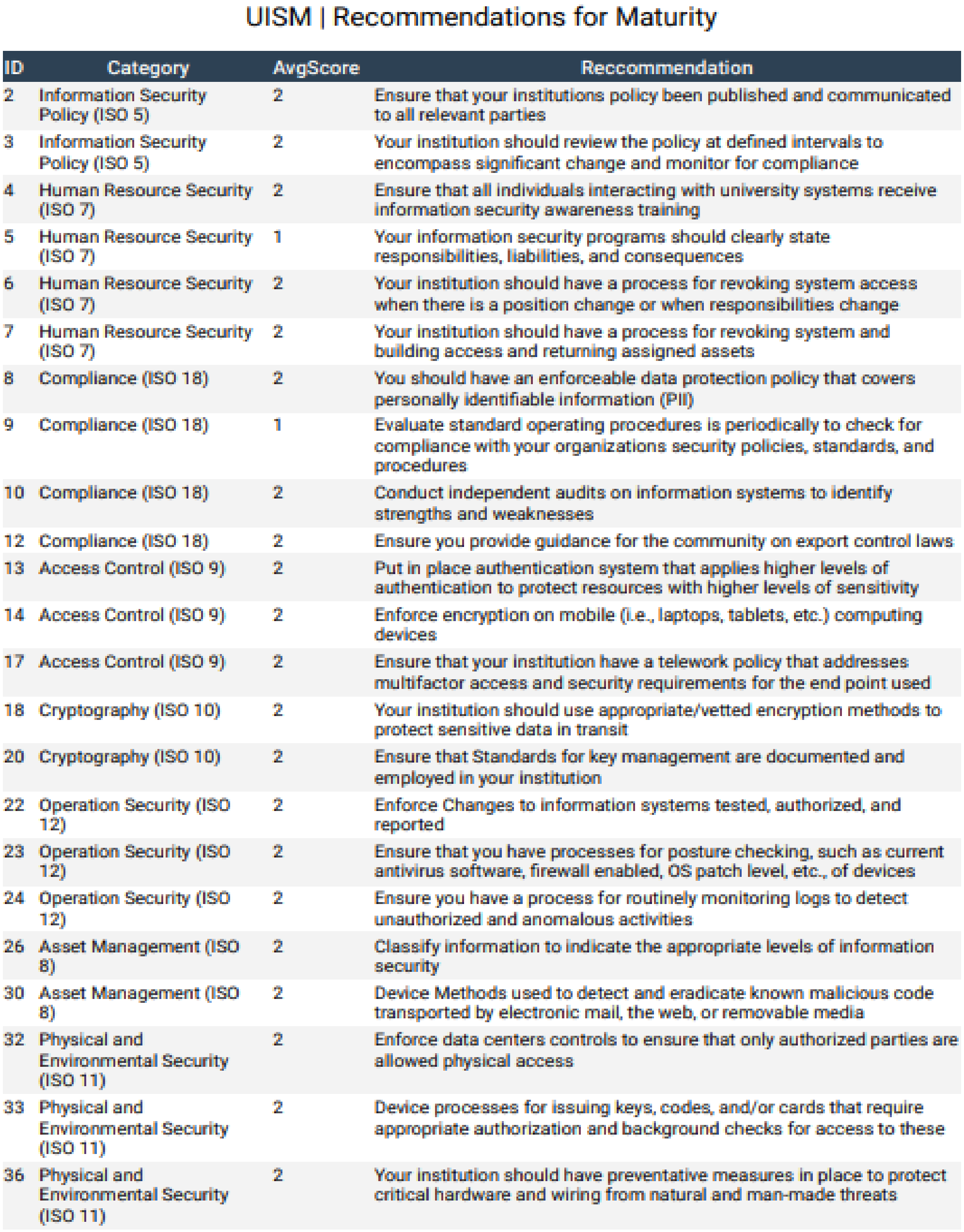


Figure 33: Maturity scores of organization “A”

The relevant recommendation report for the organization “**A**” based on information security areas of concern for improvement is as shown in table 24.

Table 24: Recommendation Report For the Organization" A".



UISM | Recommendations for Maturity

ID	Category	AvgScore	Reccommendation
2	Information Security Policy (ISO 5)	2	Ensure that your institutions policy been published and communicated to all relevant parties
3	Information Security Policy (ISO 5)	2	Your institution should review the policy at defined intervals to encompass significant change and monitor for compliance
4	Human Resource Security (ISO 7)	2	Ensure that all individuals interacting with university systems receive information security awareness training
5	Human Resource Security (ISO 7)	1	Your information security programs should clearly state responsibilities, liabilities, and consequences
6	Human Resource Security (ISO 7)	2	Your institution should have a process for revoking system access when there is a position change or when responsibilities change
7	Human Resource Security (ISO 7)	2	Your institution should have a process for revoking system and building access and returning assigned assets
8	Compliance (ISO 18)	2	You should have an enforceable data protection policy that covers personally identifiable information (PII)
9	Compliance (ISO 18)	1	Evaluate standard operating procedures is periodically to check for compliance with your organizations security policies, standards, and procedures
10	Compliance (ISO 18)	2	Conduct independent audits on information systems to identify strengths and weaknesses
12	Compliance (ISO 18)	2	Ensure you provide guidance for the community on export control laws
13	Access Control (ISO 9)	2	Put in place authentication system that applies higher levels of authentication to protect resources with higher levels of sensitivity
14	Access Control (ISO 9)	2	Enforce encryption on mobile (i.e., laptops, tablets, etc.) computing devices
17	Access Control (ISO 9)	2	Ensure that your institution have a telework policy that addresses multifactor access and security requirements for the end point used
18	Cryptography (ISO 10)	2	Your institution should use appropriate/vetted encryption methods to protect sensitive data in transit
20	Cryptography (ISO 10)	2	Ensure that Standards for key management are documented and employed in your institution
22	Operation Security (ISO 12)	2	Enforce Changes to information systems tested, authorized, and reported
23	Operation Security (ISO 12)	2	Ensure that you have processes for posture checking, such as current antivirus software, firewall enabled, OS patch level, etc., of devices
24	Operation Security (ISO 12)	2	Ensure you have a process for routinely monitoring logs to detect unauthorized and anomalous activities
26	Asset Management (ISO 8)	2	Classify information to indicate the appropriate levels of information security
30	Asset Management (ISO 8)	2	Device Methods used to detect and eradicate known malicious code transported by electronic mail, the web, or removable media
32	Physical and Environmental Security (ISO 11)	2	Enforce data centers controls to ensure that only authorized parties are allowed physical access
33	Physical and Environmental Security (ISO 11)	2	Device processes for issuing keys, codes, and/or cards that require appropriate authorization and background checks for access to these
36	Physical and Environmental Security (ISO 11)	2	Your institution should have preventative measures in place to protect critical hardware and wiring from natural and man-made threats

ii. Organization “B” Information Security Maturity Determination and Report.

The organization below is a chartered public university in Kenya. The following maturity index of organization “**B**” illustrates its maturity in information security as done by ICT administrator. Figure 34 below illustrates its maturity index.

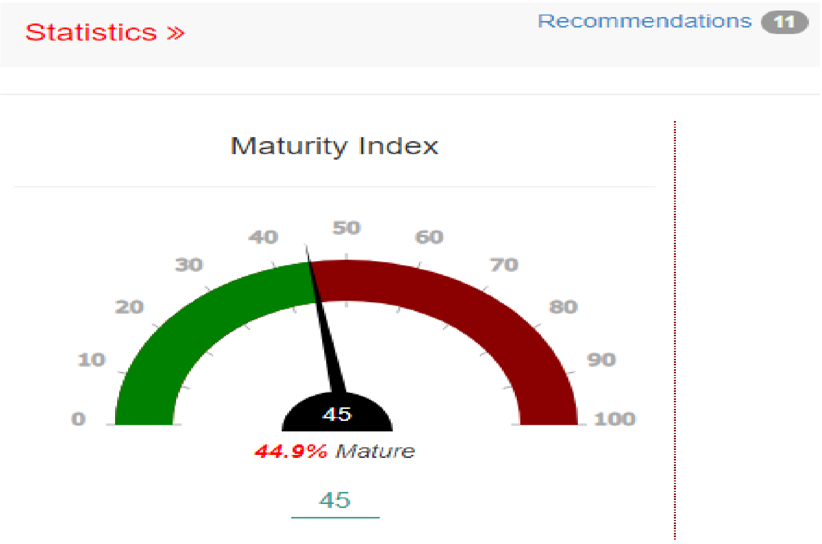
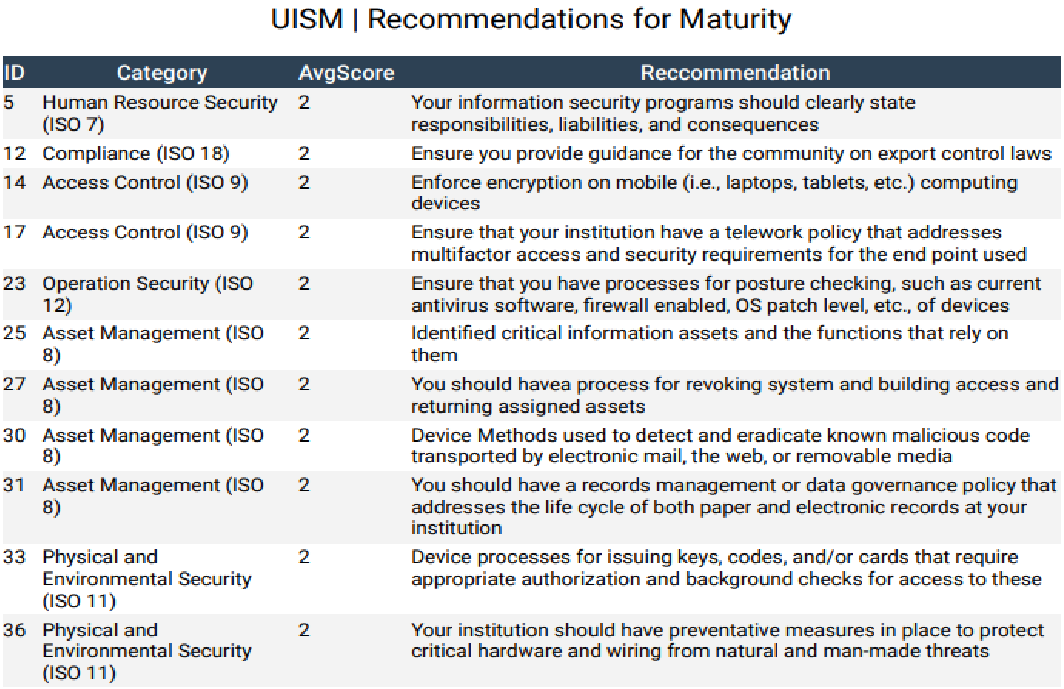


Figure 34: Maturity Scores of Organization “B”

The relevant recommendation report for organization “**B**” based on information security areas of concern for improvement is as shown below in Table 25.

Table 25: The Relevant Recommendation Report for the Organization “B”.



UISM | Recommendations for Maturity

ID	Category	AvgScore	Reccommendation
5	Human Resource Security (ISO 7)	2	Your information security programs should clearly state responsibilities, liabilities, and consequences
12	Compliance (ISO 18)	2	Ensure you provide guidance for the community on export control laws
14	Access Control (ISO 9)	2	Enforce encryption on mobile (i.e., laptops, tablets, etc.) computing devices
17	Access Control (ISO 9)	2	Ensure that your institution have a telework policy that addresses multifactor access and security requirements for the end point used
23	Operation Security (ISO 12)	2	Ensure that you have processes for posture checking, such as current antivirus software, firewall enabled, OS patch level, etc., of devices
25	Asset Management (ISO 8)	2	Identified critical information assets and the functions that rely on them
27	Asset Management (ISO 8)	2	You should havea process for revoking system and building access and returning assigned assets
30	Asset Management (ISO 8)	2	Device Methods used to detect and eradicate known malicious code transported by electronic mail, the web, or removable media
31	Asset Management (ISO 8)	2	You should have a records management or data governance policy that addresses the life cycle of both paper and electronic records at your institution
33	Physical and Environmental Security (ISO 11)	2	Device processes for issuing keys, codes, and/or cards that require appropriate authorization and background checks for access to these
36	Physical and Environmental Security (ISO 11)	2	Your institution should have preventative measures in place to protect critical hardware and wiring from natural and man-made threats

It can be noted that information security maturity is at 44% almost achieving state of basic compliance. The report above is a comprehensive report on what the institution needs to improve on and invest in IT infrastructure.

iii. Organization "C" Information Security Maturity Index Determination and Report.

The organization below is a chartered public university in Kenya. The following maturity index of organization "**C**" illustrates its maturity in information security as done by network administrator.

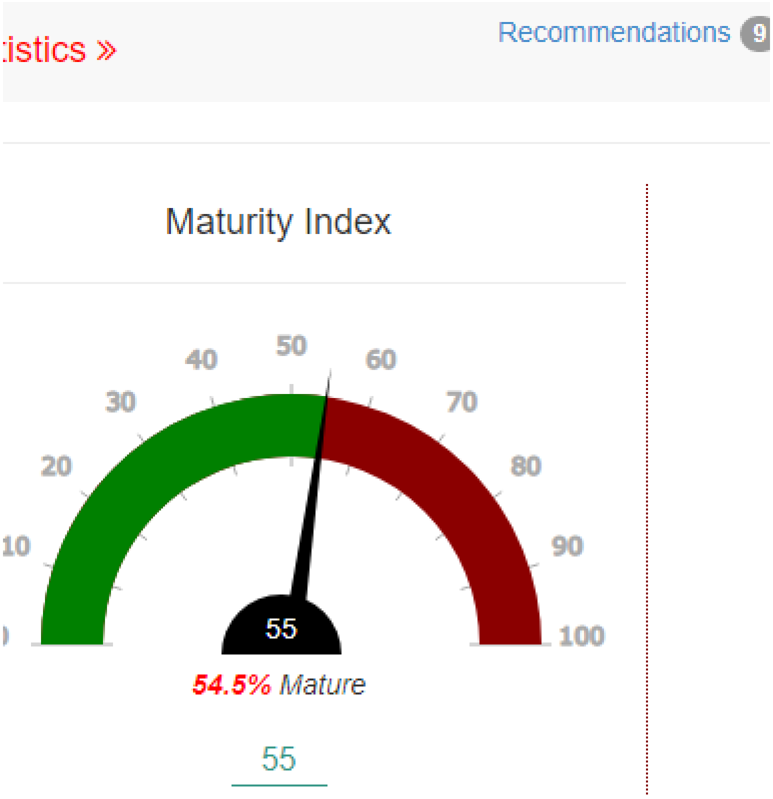
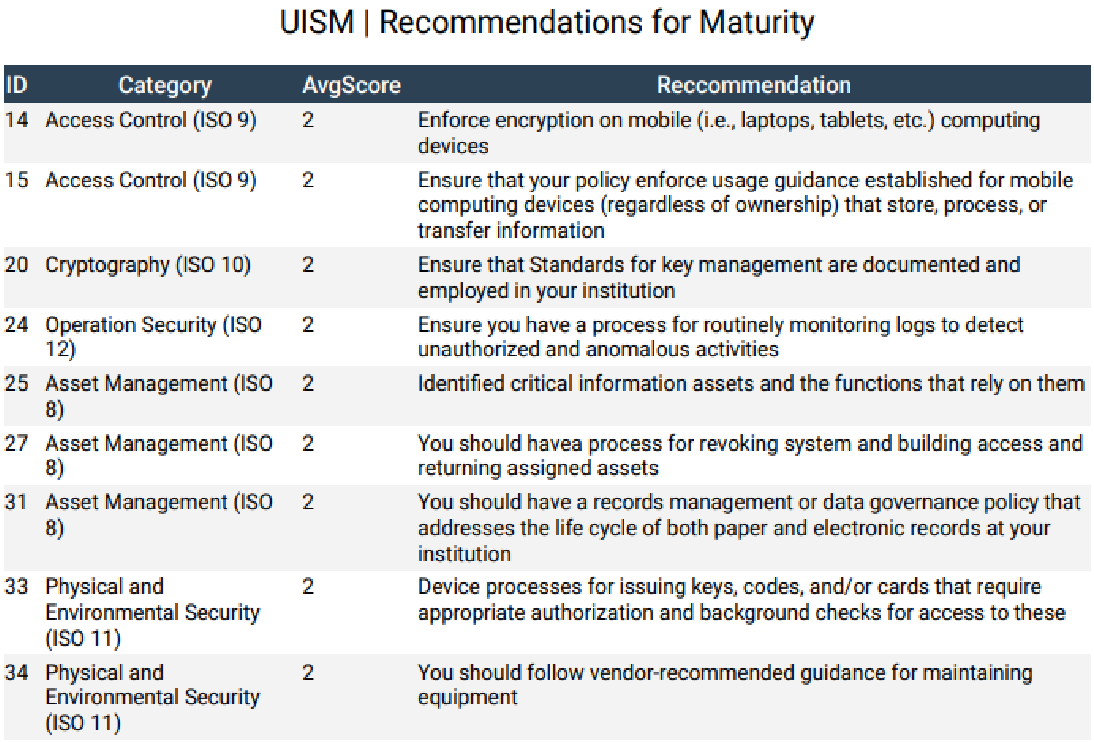


Figure 35: Maturity Scores of Organization "C"

The relevant recommendation report for organization "**C**" based information security areas of concern for improvement is as shown in Table 26.

Table 26: The Relevant Recommendation Report for the Organization "C".



UISM | Recommendations for Maturity

ID	Category	AvgScore	Reccommendation
14	Access Control (ISO 9)	2	Enforce encryption on mobile (i.e., laptops, tablets, etc.) computing devices
15	Access Control (ISO 9)	2	Ensure that your policy enforce usage guidance established for mobile computing devices (regardless of ownership) that store, process, or transfer information
20	Cryptography (ISO 10)	2	Ensure that Standards for key management are documented and employed in your institution
24	Operation Security (ISO 12)	2	Ensure you have a process for routinely monitoring logs to detect unauthorized and anomalous activities
25	Asset Management (ISO 8)	2	Identified critical information assets and the functions that rely on them
27	Asset Management (ISO 8)	2	You should havea process for revoking system and building access and returning assigned assets
31	Asset Management (ISO 8)	2	You should have a records management or data governance policy that addresses the life cycle of both paper and electronic records at your institution
33	Physical and Environmental Security (ISO 11)	2	Device processes for issuing keys, codes, and/or cards that require appropriate authorization and background checks for access to these
34	Physical and Environmental Security (ISO 11)	2	You should follow vendor-recommended guidance for maintaining equipment

The organization is at the state of basic compliance. The organizations should focus on improving information security process by improving on the recommended areas as shown in the report.

iv. Organization "D" Information Security Maturity Index Determination and Report.

The organization below is a public state university in Kenya. The following maturity index of organization "D" illustrates its maturity in information security as done by an IT staff.

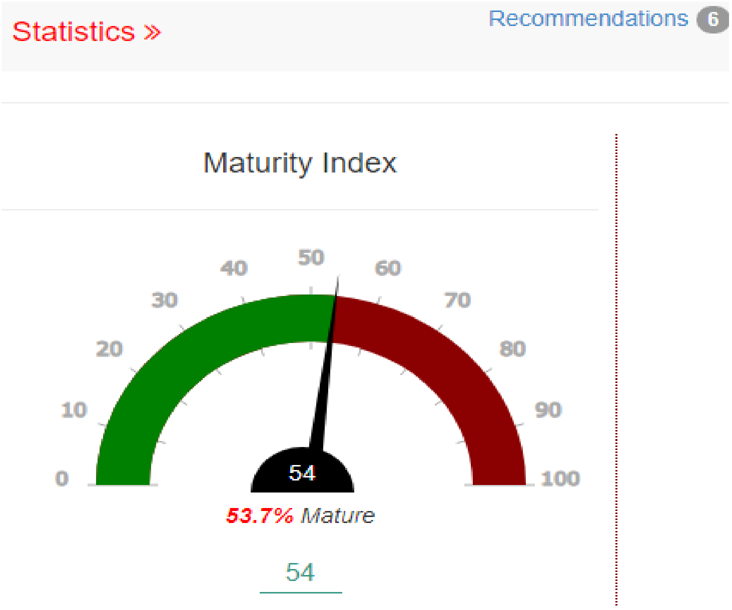
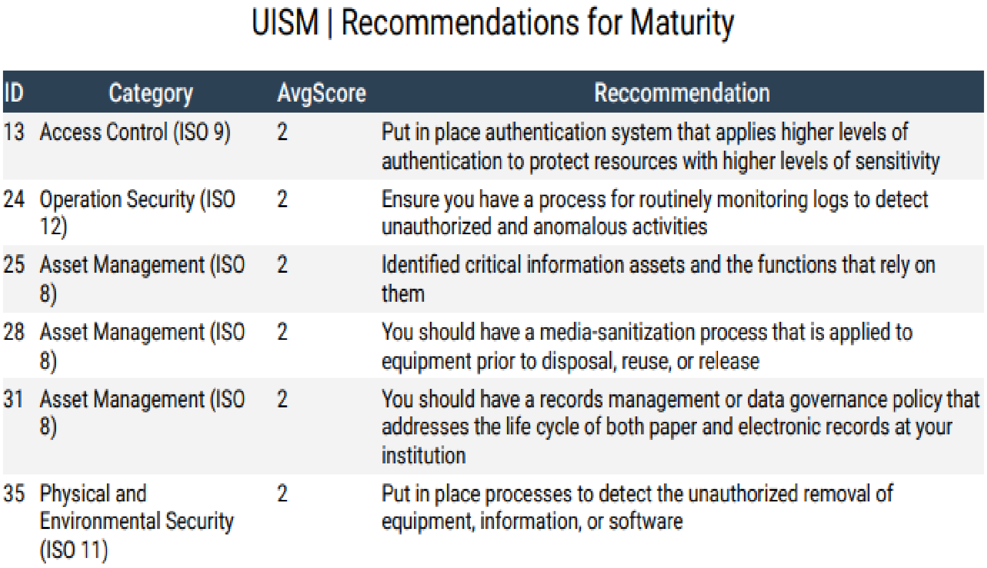


Figure 36: Maturity Scores of Organization "D".

It can be noted that the organization is mature in information security. At a 54% level of maturity, the organization is at a state of basic compliance. Its information security is continuously improving hence the organization should continue with its information security approach.

Table 27: The Relevant Recommendation Report for the Organization "D".

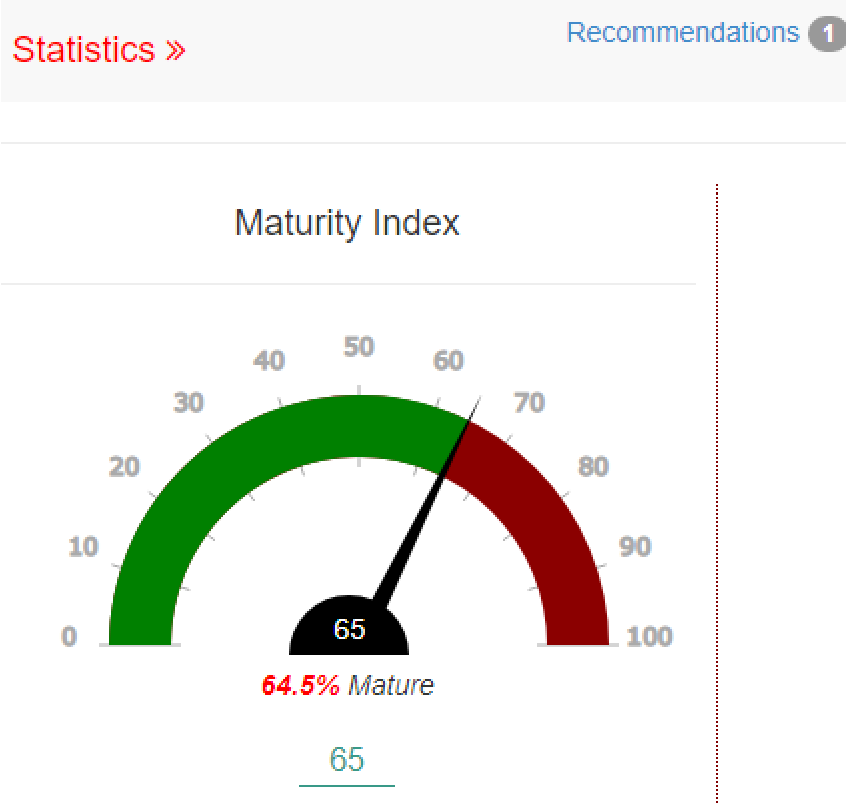


UISM | Recommendations for Maturity

ID	Category	AvgScore	Reccommendation
13	Access Control (ISO 9)	2	Put in place authentication system that applies higher levels of authentication to protect resources with higher levels of sensitivity
24	Operation Security (ISO 12)	2	Ensure you have a process for routinely monitoring logs to detect unauthorized and anomalous activities
25	Asset Management (ISO 8)	2	Identified critical information assets and the functions that rely on them
28	Asset Management (ISO 8)	2	You should have a media-sanitization process that is applied to equipment prior to disposal, reuse, or release
31	Asset Management (ISO 8)	2	You should have a records management or data governance policy that addresses the life cycle of both paper and electronic records at your institution
35	Physical and Environmental Security (ISO 11)	2	Put in place processes to detect the unauthorized removal of equipment, information, or software

v. Organization “E” Information Security Maturity Index Determination and Report.

The organization below is a private university in Kenya. The following maturity index of organization E illustrates its maturity in information security as done by ICT administrator.



Statistics »

Recommendations 1

Maturity Index

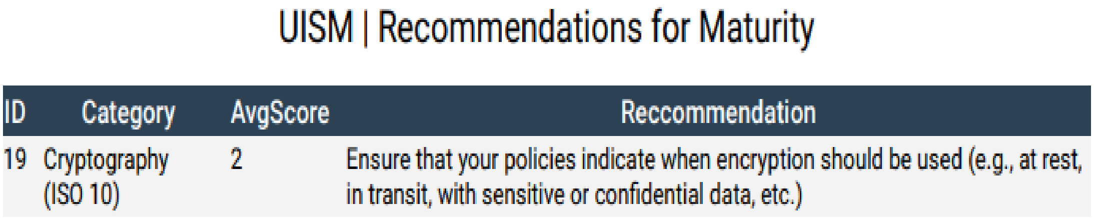
64.5% Mature

65

Figure 37: Maturity Scores of Organization “E”.

Maturity scores of organization “**E**” The relevant recommendation report for organization E based information security areas of concern for improvement is as shown below in Table 28.

Table 28: The Relevant Recommendation Report for the Organization “E”.



UISM | Recommendations for Maturity

ID	Category	AvgScore	Reccommendation
19	Cryptography (ISO 10)	2	Ensure that your policies indicate when encryption should be used (e.g., at rest, in transit, with sensitive or confidential data, etc.)

The following section discusses information security maturity of public universities in Kenya. The determination was done by ICT personnel in the universities respectively. The organization is at stage of basic compliance and moving towards state of acceptable compliance.

vi. **Organization "F" Information Security Maturity Index Determination.**

The organization below is a public chartered university in Kenya. The following maturity index of organization F illustrates its maturity in information security as done by ICT in charge.

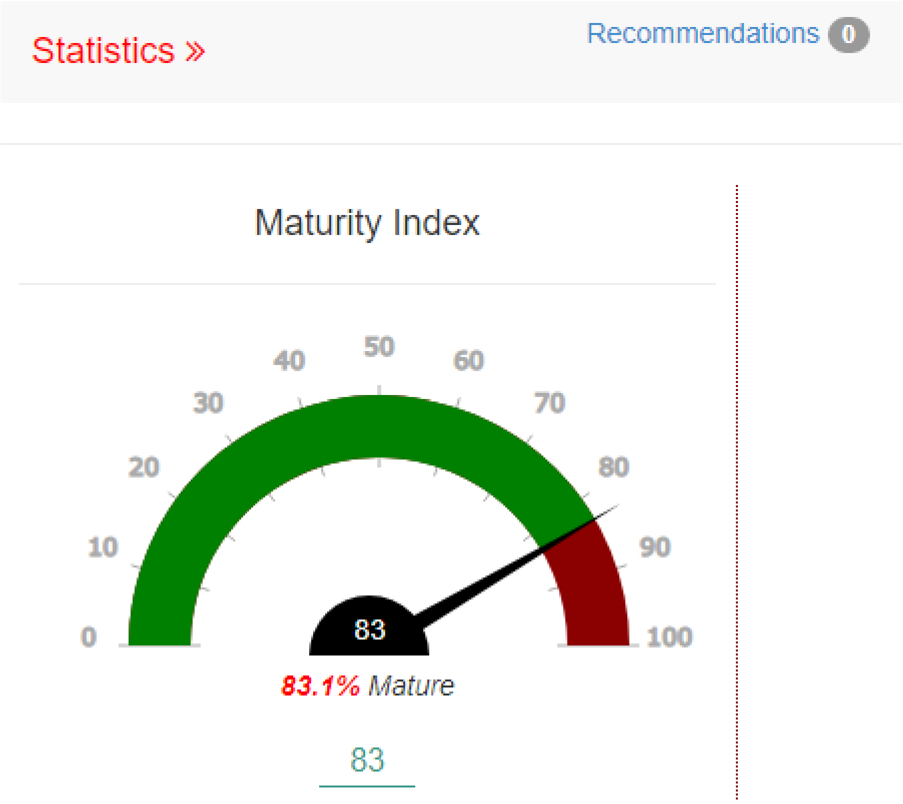


Figure 38: Maturity Scores of Organization "F".

The organization is at stage of acceptable compliance as shown from its maturity index at 83%. The organization should continue with its information technology strategy.

6.4 Comparison of IT Security Performance

The model computes information security maturity for the different organizations both public and private universities and considers both organizations equally. It can be noted that there's no disparity in information security determination either way in public and private universities. The difference in maturity depends on ICT infrastructural investments of the organization and also the relevant university information security and general ICT policy.

6.5 Areas for Further Study

This work presented a state of the art on the subject of maturity models specifically for universities. Future research will help Maturity Models become more relevant for both extended academia units and the industry. In this study, we also described the concepts which form the foundation of maturity models. A description of the different aspects of current maturity models was presented, combining knowledge from the different security risk factors analysed.

The findings from the study may not be applicable for other types of organizations, especially if the organizations are different in terms of environmental, organizational and internal structure. Although the choice of the quantitative survey method in this research was adequate for obtaining data to answer the research questions, future research may adopt a different method to unravel certain phenomena related to information security management. Future studies may employ a qualitative research design involving a case study or observation. Other possible methods to be used could be an integrative triangulation approach, combining both quantitative and qualitative design involving in-depth interviews with top-level managers.

As future work resulting from this study, we concluded that current maturity assessment methods focus on highly complex and specialized tasks being performed by competent assessors in an organizational context. These tasks mainly focus on manually collecting evidence to substantiate the maturity level calculation. Because of the complexity of these methods, maturity assessment becomes an expensive and burdensome activity for organizations.

A mathematical linear approach for carrying out benchmarking and performance improvement was developed. This model of best practices can be considered a maturity model which implies a complete system with continuous improvement. The objective of the model is to provide an organization with a way to conduct a self-study of its security implementation. The result was measured in terms of compliance with the model. There are five compliance levels and each level consists of goals. An organization that continuously measure and audit its security implementation achieves the highest level and it will achieve the objectives of security.

As such, one major area to invest is to develop methods and techniques to automate maturity assessment. Due to the widespread modelling practices in business domains, assisted by modelling tools, it's possible to have access, for processing, to the data created and managed by these tools. Also, the recent state of the art demonstrating how business processes and Enterprise Architecture model, in general, can be represented as ontologies has raised the potential relevance of the semantic techniques for the automated processing of these models.

Furthermore, there are other possible areas to be explored such as the national legislation and other external influences on UISM. Finally, the limitation is brought about by the constraints of finance, time and manpower resources. A research exercise such as this is a learning process which requires further research and enhancements including additional labour or aids. Future research with more resources in terms of time, money and manpower would be able to utilize the findings of this study to further explore the many domains or facets of information security management.

6.5.1 The Commercialization of the UISM

The University Information Security Maturity model (UISM) developed was subjected to user acceptance testing for organizations acceptability and its overall adoption. However, during acceptance testing organizations cited issues regarding the sensitivity of information attributed to their data used inthe computation of maturity. The protection of data using hashing and further organizational awareness program for the assurance of data and information protection should be done.

The findings from this study will, therefore, serve as a basis for the following future research undertakings with the sole objective of launching it as a commercially viable service.

i. Developing partnerships with hosting service providers for further development, testing, and commercialization of the UISM system.

ii. The field testing of the UISM to establish the factors influencing potential use and adoption.

iii. The development of a business model to ensure the sustainability of the UISM service.

These activities require a significant amount of time and resources and could not be undertaken within the time allocated for this study.

6.5.2 The Role of Risk, Convenience and Perceived Benefits in Influencing User Intention for Adoption and Use of UISM

It was established in this study that the respondents were willing to take higher levels of risk if the associated convenience and benefits were significant enough. There is a need to further investigate the relationship between the risk involved in using a service or system in relation to the convenience and perceived benefits that can be gained from it. This is a useful direction for further exploration.

6.5.3 A Security Model for the Delivery of UISMvia A Web-Based Platform.

The model addresses the issue of security in the use of the UISM model. Security in this regard refers to the assurance that user's information like maturity details would not be utilized by third parties to gain competitive advantage and also achieve more benefits. Therefore there's a need to establish how genuine the persons are when searching for information and confirming Information Security Maturity of a particular organization. Towards extending this model to factor in security features both in the actual technical aspects as well as in the actual use procedures lying outside the prototype the user ensures user and business registration processes.

6.5.4 Towards an Effective Delivery of University Information Security Maturity.

The prototype for the delivery of Web-based information security maturity model via a web interface to compute the UISM is feasible. The reason for the use of a web-based maturity monitoring interface is to standardize the inquiry and provision of UISM given that the user answers specific predefined data items that determine maturity in Information Security Infrastructure.

6.5.5 Investigating the User Trust Development Process for UISM.

Significant barriers were found to exist in the process of piloting the system prototype. It is therefore important to examine the role of security, privacy, cost and credibility in the adoption of the Web-based services in general and computation of

UISM in particular. The order in which trust is built is also a fruitful area of investigation. Respondents in the study began by understanding the service, questioning the security of the system and then the credibility of the platform upon computation and recommendation report obtained from the system. The issue of cost did not arise but would probably be the next issue in the sequence of concerns once the project has been commercially rolled out and accepted as a standard.

6.5.6 A Business Model for the Sustainable Delivery of UISM Using Web-Based Interface.

The lack of a suitable business models has in the number of instances or partners to provide information on various infrastructure investment, maturity data and innovative IT solutions will close down in the first few months or years of operation. In order to make the UISM solution sustainable, a suitable business model will be required to ensure that the service is affordable and available for users and significant to stakeholders.

6.6 Recommendations

Establishing that the risk management mechanism is the approach which has the most influence on ISM would benefit both future researchers and practitioners. The traditional tendency to manage information security from a technological perspective and within the information system entity may not be sufficient.

In conclusion, this research has provided invaluable input to both theory and practice. The empirical contribution has added value to previous and contemporary studies and thus further strengthens the existing application of social and technical theory and the integrated system theory in the information systems domain. In exploring technical contributions to ISM, the risk management mechanism was found to be the major predictor. In addition, as far as the social factors are concerned, the organization structure, awareness and training culture, and technical barriers were the contributors. All three factors were found to correlate significantly with the risk management mechanism. Surprisingly, the perceptions of individuals who were the key players in information security management in the organization do not have a significant impact on ISM. Furthermore, the analyses of the empirical evidence obtained appear to support the new theoretical perspective named the integrated social and technical system. The following citation best captures the demand for, and hidden danger embodied in, the discipline of information security management.

Security, like risk, is a capacious concept, perilously capable of meaning all things to all corners. Like risk, security provokes strong emotions and licenses extraordinary exercise of power. But, whereas risk threatens, security promises. And in this power of promise what it cannot deliver lays a particular danger (Zedner, 2003).

REFERENCES

Albuquerque Junior, A. E. D., & Santos, E. M. D. (2015). Adoption of information security measures in public research institutes. *JISTEM-Journal of Information Systems and Technology Management*, *12*(2), 289-315.

Arcuri, A. (2018). An experience report on applying software testing academic results in the industry: we need usable automated test generation. *Empirical Software Engineering*, *23*(4), 1959-1981.

Adhikary, N., & Gurumoorthy, B. (2017). Direct global editing of STL mesh model for product design and rapid prototyping. *Rapid Prototyping Journal*, *23*(4).

Arbaugh, W.A., W.L. Fithen, and J. McHugh, Windows of Vulnerability: A Case Study Analysis.IEEE Computer, 2000. **33**(12): p. 52 – 59.

Alexander, R. D., & Panguluri, S. (2017). Cyber security Terminology and Frameworks. In *Cyber-Physical Security* (pp. 19-47). Springer International Publishing.

Avena-Koenigsberger, A., Misic, B., & Sporns, O. (2018). Communication dynamics in complex brain networks. *Nature Reviews Neuroscience*, *19*(1), 17.

Alavi, M., & Leidner, D. E. (1999). Knowledge management systems: issues, challenges, and benefits. *Communications of the AIS*, *1*(2es), 1.

Armstrong, N., Brewster, L., Tarrant, C., Dixon, R., Willars, J., Power, M., & Dixon-Woods, M. (2018). Taking the heat or taking the temperature? A qualitative study of a large-scale exercise in seeking to measure for improvement, not blame. *Social Science & Medicine*, *198*, 157-164.

Annane, D., Lerolle, N., Meuris, S., Sibilla, J., & Olsen, K. M. (2019). Academic conflict of interest. *Intensive care medicine*, *45*(1), 13-20.

Al-Mayahi and S. P. Mansoor, “ISO 27001 gap analysis – case study ". In: Proceedings of the International Conference on Security and Management (SAM ’12), Las Vegas, 2012.

Blumenthal, D., Causino, N., Campbell, E., & Louis, K. S. (1996). Relationships between academic institutions and industry in the life sciences—an industry survey. *New England Journal of Medicine*, *334*(6), 368-374.

Brown, J. S., & Duguid, P. (1998). Organizing knowledge. *California management review*, *40*(3), 90-111.

Boehmer, W. (2008, August). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In *Emerging Security Information,* *Systems and Technologies, 2008. SECURWARE'08. Second International Conference on* (pp. 224-231). IEEE.

Brannen, J. (2017). Combining qualitative and quantitative approaches: an overview. In *Mixing methods: Qualitative and quantitative research* (pp. 3-37). Routledge.

Berger, A., & Lafferty, J. (2017, August). Information retrieval as statistical translation. In *ACM SIGIR Forum* (Vol. 51, No. 2, pp. 219-226). ACM.

Bob, B., Ellen, M., & Dan, G. (2001). Information security is an information risk management. Proceedings of the 2001 workshop on new security paradigms. Cloudcroft: ACM Press.

Boltz, J., Doring, E., & Gilmore, M. (1999, November). Information security risk assessment practices of leading organizations. General Accounting Office/Accounting and Information Management Division.

Balaji, B., Bhattacharya, A., Fierro, G., Gao, J., Gluck, J., Hong, D. ... & Bergés, M. (2018). Brick: Metadata schema for portable smart building applications. *Applied Energy*.

Becket, B (1988). Introduction to Cryptology. Blackwell Scientific Publications. ISBN 0-632-01836-4. OCLC 16832704. Excellent coverage of many classical ciphers and cryptography concepts and of the "modern" DES and RSA systems.

Bate, R. et al.:. A Systems Engineering Capability Maturity Model SM, Version 1.1.Technical report. Software Engineering Institute (SEI), Carnegie Mellon University.Pittsburgh, USA. 1995.

Bradshaw, S. (2015). Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cyber security.

Beres, Y., et al., Using security metrics coupled with predictive modeling and simulation to assesssecurity processes, in Proceedings of the 2009 3rd International Symposium on empirical software Engineering and Measurement. 2009, IEEE Computer Society [download]. p. 564-573.

Bogdanova, D., & Snoeck, M. (2019). CaMeLOT: An educational framework for conceptual data modelling. *Information and Software Technology*.

Bisbee, S. F., Moskowitz, J. J., Becker, K. F., Peterson, E. K., & Twaddell, G. W. (2017). *U.S. Patent No. RE46, 513*. Washington, DC: U.S. Patent and Trademark Office.

Barnes, J. C. (2004). *Business Continuity and HIPAA: Business Continuity Management in the Health Care Environment*. Rothstein Associates Inc.

Bertagna, L., Deparis, S., Formaggia, L., Forti, D., & Veneziani, A. (2017). The LifeV library: engineering mathematics beyond the proof of concept. *arXiv preprint arXiv:1710.06596*.

Barafort, B., Mesquida, A. L., & Mas, A. (2018). Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context. *Computer Standards & Interfaces*, *60*, 57-66.

Brown, L. T. (2019). Sustainability Strategies for Non-profit Organizations during General Economic Downturns.

Çalişkan, E., Aksakal, E., Çetinyokuş, S., & Çetinyokuş, T. (2019). Hybrid Use of Likert Scale-Based AHP and PROMETHEE Methods for Hazard Analysis and Consequence Modelling (HACM) Software Selection. *International Journal of Information Technology & Decision Making*, *18*(05), 1689-1715.

Cohen, J. (1992). A power primer. Psychological Bulletin, 112(1), 155.

Cohen, J. (1988). Statistical power analysis: A computer program. Routledge.

Calder, A., &Watkins, S. (2008). Information technology governance: A manager's guide to data security and ISO 27001/ISO 27002. Kogan Page Ltd.

Chowdhury, A. Z. M., Bhowmik, A., Hasan, H., & Rahim, M. S. (2018). Analysis of the Veracities of Industry Used Software Development Life Cycle Methodologies. *arXiv preprint arXiv:1805.08631*.

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

Clinton, C., & Sridhar, D. (2017). *Governing global health: who runs the world and why?*. Oxford University Press.

Chief Information Officer Council: A Practical Guide to Federal Enterprise Architecture. http://www.gao.gov/bestpractices/bpeaguide.pdf. 2001. (Cite 2009-06-05).

Cronholm, S., & Goldkuhl, G. (2003). Strategies for information systems evaluation-six generic types. *Electronic Journal of Information Systems Evaluation*, *6*(2), 65-74.

Creswell, J. W., Shope, R., Plano Clark, V. L., & Green, D. O. (2006). How interpretive qualitative research extends mixed methods research. *Research in the Schools*, *13*(1), 1-11.

Curtis, P. D., & Mehravari, N. (2015, April). Evaluating and improving the cyber security capabilities of the energy critical infrastructure. In *Technologies for Homeland Security (HST), 2015 IEEE International Symposium on* (pp. 1-6). IEEE.

Chaturvedi, R. (2018). Evaluation and refinement of web application architecture framework.

Carvalho, J. V., Rocha, Á., Vasconcelos, J., & Abreu, A. (2018). A health data analytics maturity model for hospitals information systems. *International Journal of Information Management*.

Camarinha-Matos, L. M., & Afsarmanesh, H. (2007). A comprehensive modeling framework for collaborative networked organizations. *Journal of Intelligent Manufacturing*, *18*(5), 529-542.

Checkel, J. T. (2001). Why comply? Social learning and European identity change. *The international organization*, *55*(3), 553-588.

Chatzipoulidis, A., & Mavridis, I. (2009). Evolving Challenges in Information Security Compliance. In MCIS (p. 75).

Davies, S. J. (Ed.). (2007). *Security supervision and management: The theory and practice of asset protection*. Butterworth-Heinemann.

DeVellis, R.F. (2003). Scale development: Theory and applications (2nd ed.). Thousand Oaks, CA: Sage Publications.

Deka, G. C. (2018). NoSQL Web Crawler Application. In *Advances in Computers* (Vol. 109, pp. 77-100). Elsevier.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196-207.

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. *Information Systems Management*, *22*(1), 77-85.

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

Estall, H. (2012). *Business continuity management systems: Implementation and certification to ISO 22301*. BCS, The Chartered Institute.

E. Kurniawan, I. Riadi, “Security Level Analysis of Academic Information Systems Based on Standard ISO 27002:2013 Using SSE-CMM”, International Journal of Computer Science and Information Security, IJCSIS, vol. 16, no. 1, pp. 139-147, 2018.

Floyd, F.J., & Widaman, K.F. (1995). Factor analysis in the development and refinement of clinical assessment instruments. Psychological Assessment, 7(3), 286-299.

Fielding, R. T., Taylor, R. N., Erenkrantz, J. R., Gorlick, M. M., Whitehead, J., Khare, R., & Oreizy, P. (2017, August). Reflections on the REST architectural style and principled design of the modern web architecture (impact paper award). In *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering* (pp. 4-14). ACM.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of advanced nursing*, *62*(1), 107-115.

Fauzi, R., Supangkat, S. H., & Lubis, M. (2018, August). The PDCA Cycle of ISO/IEC 27005: 2008 Maturity Assessment Framework. In *International Conference on User Science and Engineering* (pp. 336-348). Springer, Singapore.

Florac, W. A., & Carleton, A. D. (1999). *Measuring the software process: statistical process control for software process improvement*. Addison-Wesley Professional.

Elsbach, K. D., & Bechky, B. A. (2007). It's more than a desk: Working smarter through leveraged office design. *California management review*, *49*(2), 80-101.

Finley, S. (2017). *Multi-Disciplinary Probabilistic Design with High Fidelity 3-Dimensional Computer Modeling and Simulation* (Doctoral dissertation, Clarkson University).

Frey, C. B., & Osborne, M. A. (2017). The future of employment: how susceptible are jobs to computerization?. *Technological Forecasting and Social Change*, *114*, 254-280.

Ganek, A. G., & Corbi, T. A. (2003). The dawning of the autonomic computing era. *IBM Systems Journal*, *42*(1), 5-18.

Guldner, A., Garling, M., Morgen, M., Naumann, S., Kern, E., & Hilty, L. M. (2018). Energy Consumption and Hardware Utilization of Standard Software: Methods and Measurements for Software Sustainability. *From Science to Society* (pp. 251-261). Springer, Cham.

Green, B., Prince, D. D. C., Busby, J. S., & Hutchison, D. (2017). “How long is a Piece of String": Defining Key Phases and Observed Challenges within ICS Risk Assessment.

Green, B., Krotofil, M., & Abbasi, A. (2017, November). On the Significance of Process Comprehension for Conducting Targeted ICS Attacks. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy* (pp. 57-67). ACM.

Garcia, M. L. (2007). *Design and evaluation of physical protection systems*. Elsevier.

Goroff, D., Polonetsky, J., & Tene, O. (2018). Privacy Protective Research: Facilitating Ethically Responsible Access to Administrative Data. *The ANNALS of the American Academy of Political and Social Science*, *675*(1), 46-66.

Georgiadou, E. (2019). *A holistic method for improving software product and process quality* (Doctoral dissertation, Middlesex University).

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical Evidence on the Determinants of Cyber security Investments in Private Sector Firms. *Journal of Information Security, 9*(02), 133.

Hüner, K. M., Ofner, M., & Otto, B. (2009, March). Towards a maturity model for corporate data quality management. In *Proceedings of the 2009 ACM symposium on Applied Computing* (pp. 231-238). ACM.

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior, 81*, 282-293.

Hassan, A. A., Gupta, Y., Rao, R. T., & Anders, B. R. (2018). *U.S. Patent No. 9,870,028*. Washington, DC: U.S. Patent and Trademark Office.

Haya, G. M. (2018). *Collaboration Framework and Artifact for Information Security* (Doctoral dissertation, The Claremont Graduate University).

Harder, D. L., & Tokarski, K. O. (2018). The Power to Change a Social System. In *Organizational Behaviour and Human Resource Management* (pp. 49-72). Springer, Cham.

Hurd, I. (2017). *International organizations: politics, law, practice*. Cambridge University Press.

Hussain, S. (2017). *Corporate Governance-Effective Performance Evaluation of the Board*. eBookIt. com.

Hassan, W. N. W., Yusoff, Y., & Mardi, N. A. (2017). Comparison of reconstructed rapid prototyping models produced by 3-dimensional printing and conventional stone models with different degrees of crowding. *American Journal of Orthodontics and Dentofacial Orthopedics, 151*(1), 209-218.

Hsu, C., Lee, J. N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information systems research*, *23*(3-part-2), 918-939.

Hoyle, D. (2017). *ISO 9000 Quality Systems Handbook-updated for the ISO 9001: 2015 Standard: Increasing the Quality of an Organization's Outputs*. Taylor & Francis.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information security technical report*, *13*(4), 247-255.

Herrmann, D. S. (2007). Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI. Boca Raton, FL: Auerbach Publications.

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management, 43*, 165-172.

Hallgrimsson, B. (2012) Prototyping and Model Making for Product Design. Laurence King Publishing. ISBN 9781856698764.

Haller, J., Merrell, S. A., Butkovic, M. J., & Willke, B. J. (2010). *Best practices for national cyber security: Building a national computer security incident management capability*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Indonesian national standard. Information Technology - Security Techniques - Information Security Management Systems - Requirements (ISO / IEC 27001: 2005) (in Indonesian Language).

ISO/IEC, (2005). ISO/IEC 27001:2005 *Information Technology. Security Techniques. Specification for an Information Security Management System.* Geneva, Switzerland: ISO/IEC.

ISO 27001 Annex A – An overview of 2013 revision. (2017). 27001Academy. Retrieved 13 May 2017, from https://advisera.com/27001academy/knowledgebase/overview-of-iso-270012013-annex-a/

ISACA, Control Objectives for Information and related Technology (COBITÆ), retrieved 04/12/2007, from www.isaca.org, visited in August 2007.

Iriqat, Y. M., Ahlan, A. R., & Molok, N. N. A. (2019, April). Information Security Policy Perceived Compliance Among Staff in Palestine universities: An Empirical Pilot study. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)* (pp. 580-585). IEEE.

James Gannon, *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century*, Washington, D.C., Brassey's, 2001, ISBN 1-57488-367-4.

Risch, K. (2009, August). Security compliance: the next frontier in security research. In Proceedings of the 2008 workshop on New security paradigms (pp. 71-74). ACM.

Jayanthi, M. K. (2017, March). Strategic Planning for Information Security-DID Mechanism to befriend Cyber Criminals to assure Cyber Freedom. In *Anti-Cyber Crimes (ICACC), 2017 2nd International Conference on* (pp. 142-147). IEEE.

Jansen, W. (2010). *Directions in security metrics research*. Diane Publishing.

Jiménez, J. M. H., Nichols, J. A., Goseva-Popstojanova, K., Prowell, S., & Bridges, R. A. (2017). Malware detection on general-purpose computers using power consumption monitoring: A proof of concept and case study. *arXiv preprint arXiv:1705.01977*.

Jayanthi, M. K. (2017, March). Strategic Planning for Information Security-DID Mechanism to befriend Cyber Criminals to assure Cyber Freedom. In *Anti-Cyber Crimes (ICACC), 2017 2nd International Conference on* (pp. 142-147). IEEE.

Jin, Z., Baik, C., Cafarella, M., & Jagadish, H. V. (2018, June). Beaver: Towards a Declarative Schema Mapping. In *Proceedings of the Workshop on Human-In-the-Loop Data Analytics* (p. 10). ACM.

Johansson, E., & Elvin, G. (2017). The impact of organizational culture on information security during the development and management of IT systems: A comparative study between Japanese and Swedish banking industry.

Johnstone, P. (2015). *Cybercrime and the Law: A Critical Review of Current Legislative Provisions to Tackle Cybercrime* (Doctoral dissertation, Trinity College Dublin).

Jennex, M. E., & Durcikova, A. (2019). Integrating IS Security With Knowledge Management: What Can Knowledge Management Learn From IS Security Vice Versa? In *Effective Knowledge Management Systems in Modern Society* (pp. 267-283). IGI Global.

Jalote, P. (2000). *CMM in practice: processes for executing software projects at Infosys*. Addison-Wesley Professional.

Jin, Z., Baik, C., Cafarella, M., & Jagadish, H. V. (2018, June). Beaver: Towards a Declarative Schema Mapping. In *Proceedings of the Workshop on Human-In-the-Loop Data Analytics* (p. 10). ACM.

Janowitz, M. (2017). *The professional soldier: A social and political portrait*. Simon and Schuster.

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

Kothari, C. R. (2004). *Research Methodology: Methods and techniques*. New Age International.

Kurniawan, E., & Riadi, I. (2018). Security level analysis of academic information systems based on standard ISO 27002: 2003 using SSE-CMM. *arXiv preprint arXiv:1802.03613*.

Kaur, H. (2017). *Lost and Found Web Application for Cal Poly Pomona Students* (Doctoral dissertation, California State Polytechnic University, Pomona).

Khajouei, H., Kazemi, M., & Moosavirad, S. H. (2017). Ranking information security controls by using the fuzzy analytic hierarchy process. *Information Systems and e-Business Management*, *15*(1), 1-19.

K. Judev and J. Thomas, “Project management maturity models: The silver bullets of competitive advantage?” Project Management Journal, vol. 33, 2002

Cavalli, E., & Loucopoulos, P. (2005). Goal modeling in requirements engineering: Analysis and critique of current methods. *Information modeling methods and methodologies: Advanced topics in database research* (pp. 102-124). IGI Global.

Kouns, J., & Minoli, D. (2011). *Information technology risk management in enterprise environments: A review of industry practices and a practical guide to risk management teams*. John Wiley & Sons.

K. Rabah., (2007). Summary of IT Security Compliance Solutions & Best Practices v1.0 module 11. Global Open Versity, Vancouver Canada

Katz, J., & Townsend, J. B. (2000). The role of information technology in the" Fit" between culture, business strategy and organizational structure of global firms. *Journal of Global Information Management (JGIM)*, *8*(2), 24-35.

Kephart, J. O. (2005, May). Research challenges of autonomic computing. In *Proceedings of the 27th international conference on Software engineering* (pp. 15-22). ACM.

K. Judev and J. Thomas, “Project management maturity models: The silver bullets of competitive advantage?” Project Management Journal, vol. 33, 2002.

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analyzing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *The Journal of Strategic Information Systems*, *26*(1), 39-57.

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analyzing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *The Journal of Strategic Information Systems*, *26*(1), 39-57.

Kolomeec, M., Gonzalez-Granadillo, G., Doynikova, E., Chechulin, A., Kotenko, I., & Debar, H. (2017, August). Choosing Models for Security Metrics Visualization. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security* (pp. 75-87). Springer, Cham.

Kalogeraki, E. M., Papastergiou, S., Mouratidis, H., & Polemi, N. (2018). A novel risk assessment methodology for SCADA maritime logistics environments. *Applied Sciences*, *8*(9), 1477.

Liang, S., Zhang, Y., Guo, J., Dong, C., Liu, Z., & Jia, C. (2017, July). Efficient Format-Preserving Encryption Mode for Integer. In *Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on* (Vol. 2, pp. 96-102). IEEE.

Louw, C., & Von Solms, B. (2018, June). Smartphone Usage and Security Maturity: A South African Student Evaluation. In *ECCWS 2018 17th European Conference on Cyber Warfare and Security* (p. 268). Academic Conferences and publishing limited.

Liu, J., Yang, T., Li, Z., & Zhou, K. (2008, December). TSPSCDP: A time-stamp continuous data protection approach based on pipeline strategy. In *Frontier of Computer Science and Technology, 2008. FCST'08. Japan-China Joint Workshop on* (pp. 96-102). IEEE.

López, A. J. G., Márquez, A. C., Sanz, J. A., Kobbacy, K. A., Shariff, S. M., Le Page, E., & González-Prida, V. (2017). Asset Management for Buildings within the Framework of Building Information Modeling Development. In *Optimum Decision Making in Asset Management* (pp. 121-138). IGI Global.

Liu, C., Xiong, H., Papadimitriou, S., Ge, Y., & Xiao, K. (2017). A proactive workflow model for healthcare operation and management. *IEEE Transactions on Knowledge and Data Engineering*, *29*(3), 586-598.

Liu, C. W., Huang, P., & Lucas, H. (2017). IT Centralization, Security Outsourcing, and Cyber security Breaches: Evidence from the US Higher Education.

Ljøsne, M. J. (2019). *Network Scanning Industrial Control Systems: A Vulnerability Analysis* (Master's thesis).

Lyons, S. T., Duxbury, L. E., & Higgins, C. A. (2006). A comparison of the values and commitment of private sector, public sector, and parapublic sector employees. *Public administration review*, *66*(4), 605-618.

McIntyre, M. H.: An Integrated Product Development Framework. In Reliability and Maintainability Symposium. Pages 23–25. Anaheim, USA. 1998. IEEE Press.

Mahmoodi, S., Durak, U., Gerlach, T., Hartmann, S., & D’Ambrogio, A. (2017, April). Extending the CMMI Engineering Process Areas for Simulation Systems Engineering. In *Simulation Science* (pp. 193-207). Springer, Cham.

Mitchell, E. T. (2018). Issues and Implications in Technology and Collection Management. *Technical Services Quarterly, 35*(2), 175-186.

Mao, K., Capra, L., Harman, M., & Jia, Y. (2017). A survey of the use of crowdsourcing in software engineering. *Journal of Systems and Software, 126,* 57-84.

Mugenda, O. Mugenda, and G. Mugenda. "A.(2003)." *Research methods Quantitative and Qualitative Approaches. Nairobi: ACTS*.

Mall, R. (2018). *Fundamentals of software engineering*. PHI Learning Pvt. Ltd.

Menold, J., Jablokow, K., Simpson, T., & Seuro, R. (2017, August). Evaluating the Discriminatory Value and Reliability of Ideation Metrics for Their Application to Concept Development and Prototyping. In *ASME 2017 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference* (pp. V007T06A034-V007T06A034). American Society of Mechanical Engineers.

Malik F. SalehManagement Information Systems, Chair Prince Mohammad Bin Fahd University Al Khobar, 31952, Saudi Arabia, 2011.

M. F. Saleh," Information Security Maturity Model," International Journal of Computer Science and Security (IJCSS), Vol.5, Issue 3, pp: 316-337

M. Dey, “Information security management - a practical approach, “In Proceedings of AFRICAN 2007, Member, IEEE

Menghi, C., Nejati, S., Briand, L., & Parache, Y. I. (2020, June). Approximation-refinement testing of compute-intensive cyber-physical models: An approach based on system identification. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering* (pp. 372-384).

Makupi, D. (2017). Understanding Security Status of an Online Banking Infrastructure. *Mara International Journal of Scientific & Research Publications.*

Mari, L., Wilson, M., & Maul, A. (2020). Measurement across the Sciences.

Manderscheid, J. (2018). Process Improvement and Innovation: Identification and Planning of Process Redesign Ideas.

McIlmurray, S. J. (2008). *Competency development in the digital age: A study of the learning practices of cyber security professionals* (Doctoral dissertation, Teachers College, Columbia University).

McKinney Jr, E. H., & Yoos, C. J. (2019). Information as a difference: toward a subjective theory of information. *European Journal of Information Systems*, 1-15.

McSwiggan, L. C., Marston, J., Campbell, M., Kelly, T. B., & Kroll, T. (2017). Information-sharing with respite care services for older adults: a qualitative exploration of carers' experiences. *Health & Social Care in the Community*, *25*(4), 1404-1415.

National Association of State Chief Information Officers (NASCIO) USA: Enterprise Architecture Maturity Model. www.nascio.org/publications/ documents/NASCIO-EAMM.pdf. 2003. (cited 2009-06-05).

Nasser, “Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen, ” International Journal of scientific research in Multidisciplinary Studies, Vol. 3, Issues 11, pp. 5 – 14, DEC. 2017

Neter, J., Wasserman, W., & Kutner, M. H. (1985). *Applied linear statistical models: regression, analysis of variance, and experimental designs* (No. 469). McGraw-Hill/Irwin.

Nyanchama, M. (2005). Enterprise Vulnerability Management and Its Role in Information Security Management. *Information Systems Security*, *14*(3), 29-56.

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An Introduction to Information Security. *NIST Special Publication*, *800*, 12.

Narasimhalu, A. D., Dayasindhu, N., & Subramanian, R. (2004). INFOSeMM: Infosys IT Security Maturity Model: A Report.

Orodho, A. J. (2003). Essentials of educational and social science research methods. *Nairobi: masola publishers*, *54*, 71-82.

Onyeji, I., Bazilian, M., & Bronk, C. (2014). Cyber security and critical energy infrastructure. *The Electricity Journal*, *27*(2), 52-60.

Ortmeier, P. J. (2017). *Introduction to Security*. Pearson.

Oded Goldreich, *Foundations of Cryptography*, in two volumes, Cambridge University Press, 2001 and 2004.

Osborn, L. S. (2017). Intellectual Property Channeling for Digital Works. *Cardozo L. Rev.*, *39*, 1303.

Obama, B. (2010). *National security strategy of the United States (2010)*. Diane Publishing.

Planning, S. (2017). Risk Management Planning, Sustainability Risks Management, and Risk Stakeholders.

Park, W., & Ahn, S. (2017). Performance comparison and detection analysis in Snort and Suricata environment. *Wireless Personal Communications*, *94*(2), 241-252.

Prashar, A. (2017). Adopting the PDCA (Plan-Do-Check-Act) cycle for energy optimization in energy-intensive SMEs. *Journal of Cleaner Production*, *145*, 277-293.

Preacher, K. J., Curran, P. J., & Bauer, D. J. (2006). Computational tools for probing interactions in multiple linear regression, multilevel modeling, and latent curve analysis. *Journal of educational and behavioral statistics*, *31*(4), 437-448.

Pettigrew, A. M. (2014). *The politics of organizational decision-making*. Routledge.

Pasian, B. (2018). Project Management Maturity and Associated Modeling: A Historic, Process-Oriented View. *Developing Organizational Maturity for Effective Project Management* (pp. 1-24). IGI Global.

Polančič, G., & Cegnar, B. (2017). Complexity metrics for process models–A systematic literature review. *Computer Standards & Interfaces*, *51*, 104-117.

Pöppelbuß, J., & Röglinger, M. (2011, June). What makes a useful maturity model? a framework of general design principles for maturity models and its demonstration in business process management. In *Ecis* (p. 28).

Rauter, T., Iber, J., & Kreiner, C. (2018). Integrating Integrity Reporting Into Industrial Control Systems: A Reality Check. In *Solutions for Cyber-Physical Systems Ubiquity* (pp. 358-382). IGI Global.

Pham, H. C., Pham, D. D., Brennan, L., & Richardson, J. (2017). Information Security and People: A Conundrum for Compliance. *Australasian Journal of Information Systems*, *21*.

Ricca, F., Russo, A., Greco, S., Leone, N., Artikis, A., Friedrich, G., ... & Mileo, A. (2020). Proceedings 36th International Conference on Logic Programming (Technical Communications). *arXiv preprint arXiv:2009.09158*.

Qu, W. (2011). *A study of voluntary disclosure by listed firms in China* (No. Ph. D.). Deakin University.

Rabah, K. (2017). Implementation of Secure-key Establishment and Generation using Elliptic Curve Cryptographic Protocols. *Mara Research Journal of Computer Science & Security-ISSN 2518-8453, 1*(1), 79-99.

Restrepo, J. A. (2017). *Development and Application of a Risk-Based Online Body-of-Knowledge for the US Underground Coal Mining Industry: RISKGATE-US COAL* (Doctoral dissertation, Virginia Tech).

Riyanarto Sarno and Irsyat Iffano, ―Information Security Manajemen Syytem‖, Surabaya: ITSPress 2009 (in the Indonesian Language).

Robison, L. J., & Ritchie, B. K. (2016). *Relationship economics: The social capital paradigm and its application to business, politics and other transactions*. CRC Press.

Ramon, M. C., & Zajac, D. A. (2018). Cyber security Literature Review and Efforts Report. *Prepared for NCHRP Project*, 03-127.

Rodal Castro, P. (2016). Implementation plan for an ISMS according to ISO/IEC 27001: 2013.

Rodrigues, T., Delicato, F. C., Batista, T., Pires, P. F., & Pirmez, L. (2017). An approach based on the domain perspective to develop WSAN applications. *Software & Systems Modeling*, *16*(4), 949-977.

Roe, B. E., & Just, D. R. (2009). Internal and external validity in economics research: Tradeoffs between experiments, field experiments, natural experiments, and field data. *American Journal of Agricultural Economics*, *91*(5), 1266-1271.

Schellong, A. R. (2010). Benchmarking EU e-government at the crossroads: a framework for e-government benchmark design and improvement. *Transforming Government: People, Process and Policy*, *4*(4), 365-385.

Stufflebeam, D. L., & Zhang, G. (2017). *The CIPP evaluation model: How to evaluate for improvement and accountability*. Guilford Publications.

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

Sahin, C. (2018). Social Media Addiction Scale-Student Form: The Reliability and Validity Study. *Turkish Online Journal of Educational Technology-TOJET*, *17*(1), 169-182.

Saleh, M. F. (2011). Information security maturity model. *International Journal of Computer Science and Security (IJCSS)*, *5*(3), 21.

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.

Saleh, M. F. (2011). Information security maturity model. *International Journal of Computer Science and Security (IJCSS)*, *5*(3), 21.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.

Schneider, F. B. (2000). Enforceable security policies. *ACM Transactions on Information and System Security (TISSEC), 3*(1), 30-50.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. Risk management guide for information technology systems.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management, 39*(4), 60.

Segura, S., Troya, J., Durán, A., & Ruiz-Cortés, A. (2018). Performance metamorphic testing: A Proof of concept. *Information and Software Technology, 98*, 1-4.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Stouffer, K., Zimmerman, T., Tang, C., Lubell, J., Cichonski, J., & McCarthy, J. (2017). *Cyber security Framework Manufacturing Profile* (No. NIST Interagency/Internal Report (NISTIR)-8183).

Swanson, M. H., & Vogel, K. M. (2018). Big Data, intelligence, and analyst privacy: investigating information dissemination at an NSA-funded research lab. *Intelligence and National Security, 33*(3), 357-375.

Steger, M., Dorri, A., Kanhere, S. S., Römer, K., Jurdak, R., & Karner, M. (2018). Secure wireless automotive software updates using blockchains: A proof of concept. In *Advanced Microsystems for Automotive Applications 2017* (pp. 137-149). Springer, Cham.

Santoro, O., Lagermann, K., & Dechaene, T. (2018). *U.S. Patent Application No. 15/954,499*.

Stipp, David. *A Most Elegant Equation: Euler's Formula and the Beauty of Mathematics*. Basic Books, 2017.

Smith III, J. P. J., & Thompson, P. W. (2017). Quantitative reasoning and the development of algebraic reasoning. In *Algebra in the early grades* (pp. 117-154). Routledge.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267-270.

Seel, N. M. (2017). Model-based learning: a synthesis of theory and research. *Educational Technology Research and Development, 65*(4), 931-966.

Skurka, M. A. (2017). *Health information management: principles and organization for health information services*. John Wiley & Sons.

Spearman, C. General Intelligence, Objectively determined and measured. American Journal of Psychology, 15: 20 l-293, 1904.

Spalding, A. (2016). Restoring Pre-Existing Compliance through the FCPA Pilot Program. *U. Tol. L. Rev.*, *48*, 519.

Sprenger, C., & Lazareva, O. (2017). Corporate Governance and Investment: Evidence from Russian Unlisted Firms.

Svensson, M., Bertoni, A., & Lanander, M. (2018). ON KNOWLEDGE MATURITY AND BIASED NATURE OF STAGED DECISION MAKING IN A HIGH CONSEQUENCE INDUSTRY. In *DS92: Proceedings of the DESIGN 2018 15th International Design Conference* (pp. 465-476).

Schmidt, K. (2006). *High availability and disaster recovery: concepts, design, implementation* (Vol. 22). Springer Science & Business Media.

Schneier, B., Secrets, and Lies: Digital Security in a Networked World. 2000, New York: John Wiley & Sons, Inc.

Serengeti consulting group (2008).Bedrock City University (BCU) Secure Network Infrastructure. Module I Risk Management Plan a Case Study page 40.

Schmidts, O., Kraft, B., Schreiber, M., & Zündorf, A. (2018, May). Continuously evaluated research projects in collaborative decoupled environments. In *2018 IEEE/ACM 5th International Workshop on Software Engineering Research and Industrial Practice (SER&IP)* (pp. 2-9). IEEE.

Stevanović, "Maturity Models in Information Security," International Journal of Information and Communication Technology Research, vol.1, no.2, 2011.

Stevens, J. (2014). *Electricity subsector cyber security capability maturity model (es-c2m2)(case study)*. Carnegie-mellon Univ Pittsburgh Pa Software Engineering Inst.

Tuna, G., Kogias, D. G., Gungor, V. C., Gezer, C., Taşkın, E., & Ayday, E. (2017). A survey on information security threats and solutions for Machine to Machine (M2M) communications. *Journal of Parallel and Distributed Computing*, *109*, 142-154.

Turban, E., Whiteside, J., King, D., & Outland, J. (2017). Implementation Issues: From Globalization to Justification, Privacy, and Regulation. An *Introduction to Electronic Commerce and Social Commerce* (pp. 383-413). Springer International Publishing.

Taft, T. H. (2017). *The Integration of IT Governance, Information Security Leadership and Strategic Alignment in Healthcare: A Correlational Study* (Doctoral dissertation, Capella University).

Tate, J., Beck, P., Ibarra, H. H., Kumaravel, S., & Miklas, L. (2018). *Introduction to storage area networks*. IBM Redbooks.

Tari Schreider, S. S. C. P., CISM, C., & CISO, I. (2017). *The Manager's Guide to Cyber security Law: Essentials for Today's Business*. Rothstein Publishing.

Thomsson, J. (2017). Organizational effects and management of information security: A cross-sectoral case study of three different organizations.

Varun Arora, ―Comparing Different Information Security Standards : COBIT vs ISO 27001, Carnegie Mellon University, Qatar.

von Solms, S. B. (2005). Information Security Governance–compliance management vs operational management. *Computers & Security*, *24*(6), 443-447.

Vosko, L. F., Grundy, J., Tucker, E., Thomas, M. P., Noack, A. M., Casey, R., ... & Mussell, J. (2017). The compliance model of employment standards enforcement: an evidence-based assessment of its efficacy in instances of wage theft. *Industrial Relations Journal*, *48*(3), 256-273.

Wójtowicz, A., & Chmielewski, J. (2017). Technical feasibility of context-aware passive payment authorization for physical points of sale. *Personal and Ubiquitous Computing*, 1-13.

Walsh, J. P., & Kosnik, R. D. (1993). Corporate raiders and their disciplinary role in the market for corporate control. *Academy of Management Journal*, *36*(4), 671-700.

Waschke, M. (2017). How Does Computer Security Work?. In *Personal Cyber security* (pp. 53-80). Apress.

Wolski, M., Walter, B., Kupiński, S., & Chojnacki, J. (2018). Software quality model for a research‐driven organization—An experience report. *Journal of Software: Evolution and Process*, *30*(5), e1911.

Wong, M., Farooq, B., & Bilodeau, G. A. (2018). Discriminative conditional restricted Boltzmann machine for discrete choice and latent variable modeling. *Journal of choice modeling*, *29*, 152-168.

Webster, E. (1985). The growth of enterprise intangible investment in Australia. Information Economics and Policy, 12 128-154.

Yeap, G. (2013, December). Smart mobile SoCs driving the semiconductor industry: Technology trend, challenges, and opportunities. In *Electron Devices Meeting (IEDM), 2013 IEEE International* (pp. 1-3). IEEE.

Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine*, *55*(1), 26-33.

Zeegers, R. (2018). *Information Security Management Professional based on ISO/IEC 27001 Courseware–English*. Van Haren.

Zhang, J., Yan, Z., Geng, G., Lee, X., & Lee, J. H. (2018). Trademark Protection for Chinese Domain Names. *Journal of Internet Technology*, *19*(2), 315-324.

Zhang, Z., Li, H., Shi, Y., Zhang, S., & Yan, W. (2020). Cooperative optimal control for Lipschitz nonlinear systems over generally directed topologies. *Automatica*, *122,* 109279.

APPENDICES

APPENDIX I: Questionnaire

I am a student of Doctor of Philosophy in IT Security and Audit of Kabarak University carrying out research on "**An ISO 27001 Based Model to Determine University Information Security Maturity under Uncertainty**" .This is to request you to contribute in answering the following questions outlined here below as truthfully as you can. Please note that the information you provide will be used only for this academic purposes only.

SECTION A: GENERAL QUESTIONS

Please tick the most appropriate answer in this section

1. Indicate your institution type

   Public [ ] Private [ ]

2. Which one of the following best describes your position at the University?

Senior management	**[ ]**	ICT manager	**[ ]**
Database Administrator	**[ ]**	Network administrator	**[ ]**
System administrator	**[ ]**	ICT student support	**[ ]**

SECTION B: SPECIFIC QUESTIONS

In the scale of 0 to 5, please tick the most appropriate answer to the questions below in relation to policy, compliance, access control, communication security, cryptography, asset management and backup (***KEYS**: **Not Performed = 0; Performed Informally = 1; Planned = 2; Well Defined = 3; Quantitatively Controlled = 4; Continuously Improving = 5; NOTE: 5 is the highest level of maturity)***

1. **ADMINISTRATIVE FACTORS**

NO.	Questions	1	2	3	4	5
	Information Security Policies (ISO 5)					
1	Our institution has an information security policy that has been approved by management					

2	The policy has been published and communicated to all relevant parties					
3	Our institution review the policy at defined intervals to encompass significant change and monitor for compliance					
	Human Resource Security (ISO 7)					
4	All individuals interacting with university systems receive information security awareness training					
5	The information security programs clearly state responsibilities, liabilities, and consequences					
6	Our institution has a process for revoking system access when there is a position change or when responsibilities change					
7	Our institution has a process for revoking system and building access and returning assigned assets					
	Compliance (ISO 18)					
8	Our institution has an enforceable data protection policy that covers personally identifiable information (PII)					
9	Standard operating procedures are periodically evaluated for compliance with your organization's security policies, standards, and procedures					
10	We perform independent audits on information systems to identify strengths and weaknesses					
11	Audit tools are properly separated from development and operational system environments to prevent any misuse or compromise					
12	Our institution provides guidance for the community on export control laws					

2. TECHNOLOGICAL FACTORS

NO.	Questions	1	2	3	4	5
	Access Control (ISO 9)					
1	Our institution has an authentication system in place that applies higher levels of authentication to protect resources with higher levels of sensitivity					
2	Our institution require encryption on mobile (i.e., laptops, tablets, etc.) computing devices					
3	In our institution, the policy enforce usage guidance established for mobile computing devices (regardless of ownership) that store, process, or transmit institutional data					
4	Our institution has standards for isolating sensitive data and procedures and technologies in place to protect it from unauthorized access and tampering					
5	Our institution has a telework policy that addresses multifactor access and security requirements for the endpoint used					
	Cryptography (ISO 10)					
6	Our institution uses appropriate/vetted encryption methods to protect sensitive data in transit					
7	Our policies indicate when encryption should be used (e.g., at rest, in transit, with sensitive or confidential data, etc.)					
8	Standards for key management documented and employed					

	Operation Security (ISO 12)					
9	Our institution maintains security configuration standards for information systems and applications					
10	Changes to information systems tested, authorized, and reported					
11	Our your institution has a process for posture checking, such as current antivirus software, firewall enabled, OS patch level, etc., of devices as they connect to your network					
12	Our institution has a process for routinely monitoring logs to detect unauthorized and anomalous activities					

3. PHYSICAL FACTORS

NO	Questions	1	2	3	4	5
	Asset Management (ISO 8)					
1	Our organization has identified critical information assets and the functions that rely on them					
2	Our institution classify information to indicate the appropriate levels of information security					
3	Our institution has a process for revoking system and building access and returning assigned assets					
4	Our institution has a media-sanitization process that is applied to equipment prior to disposal, reuse, or release					
5	Our institution has processes in place to monitor the utilization of key system resources and to mitigate the risk of system downtime					
6	We have Methods used to detect and eradicate known malicious code transported by electronic mail, the web, or removable media					
7	Our institution has a records management or data governance policy that addresses the life cycle of both paper and electronic records at your institution					

	Physical and Environmental Security (ISO 11)					
8	Our institution's data centers include controls to ensure that only authorized parties are allowed physical access					
9	Our institution has a process for issuing keys, codes, and/or cards that require appropriate authorization and background checks for access to these sensitive facilities					
10	Our institution follow vendor-recommended guidance for maintaining equipment					
11	There are processes in place to detect the unauthorized removal of equipment, information, or software					
12	Our institution have preventative measures in place to protect critical hardware and wiring from natural and man-made threats					

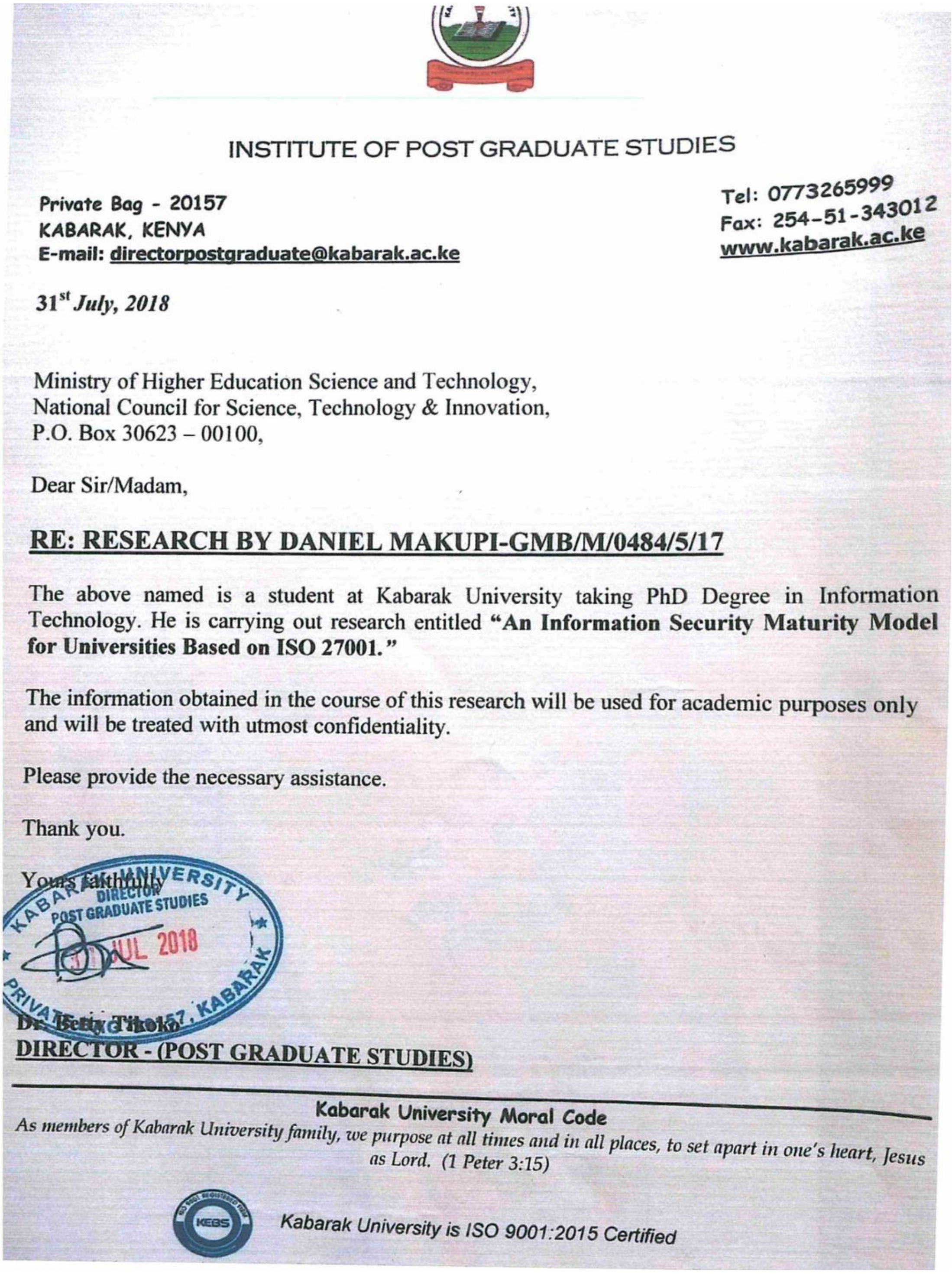
SECTION C: SPECIFIC QUESTIONS

In the scale of 0 to 5, please tick the most appropriate answer to the questions below in relation to your maturity in regard to information security for each specific factors listed below (***KEYS**: Not Performed = 0; Performed Informally = 1; Planned = 2; Well Defined = 3; Quantitatively Controlled = 4; Continuously Improving = 5; NOTE: 5 is the highest level of maturity)*

4. UNIVERSITY INFORMATION SECURITY MATURITY

NO.	Questions	1	2	3	4	5
	Our Administrative, Physical and technological security					
1	The existing Administrative process is continuously improving					
2	There’s continuous improvement in our information security infrastructure overtime					
3	Our Physical infrastructure is continuously improving					

APPENDIX II: University Transmittal Letter



INSTITUTE OF POST GRADUATE STUDIES

Private Bag - 20157
KABARAK, KENYA
E-mail: directorpostgraduate@kabarak.ac.ke

Tel: 0773265999
Fax: 254-51-343012
www.kabarak.ac.ke

31st July, 2018

Ministry of Higher Education Science and Technology,
National Council for Science, Technology & Innovation,
P.O. Box 30623 – 00100,

Dear Sir/Madam,

RE: RESEARCH BY DANIEL MAKUPI-GMB/M/0484/5/17

The above named is a student at Kabarak University taking PhD Degree in Information Technology. He is carrying out research entitled **"An Information Security Maturity Model for Universities Based on ISO 27001."**

The information obtained in the course of this research will be used for academic purposes only and will be treated with utmost confidentiality.

Please provide the necessary assistance.

Thank you.

Yours faithfully

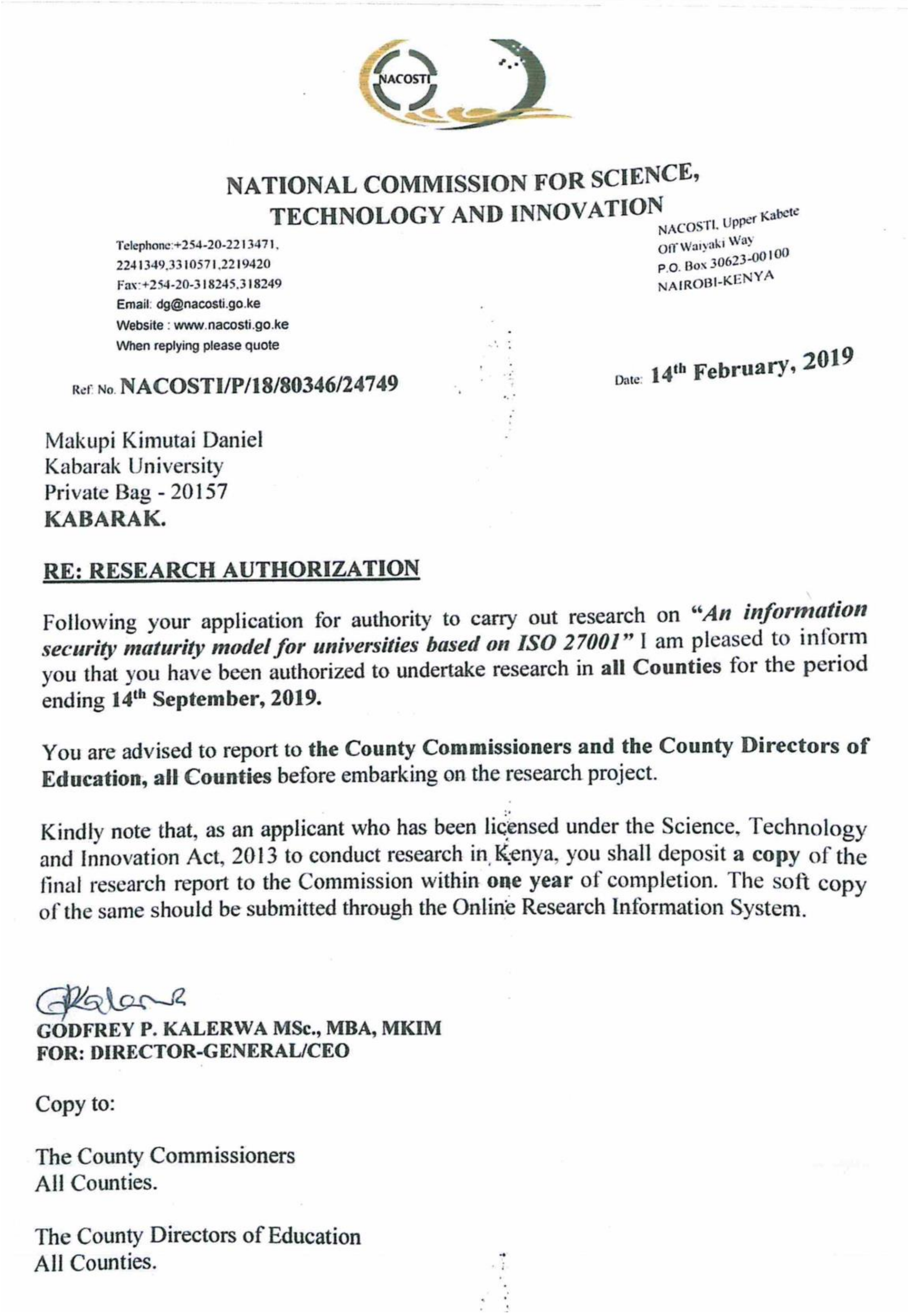
KABARAK UNIVERSITY
DIRECTOR
POST GRADUATE STUDIES
31 JUL 2018
PRIVATE BAG 20157, KABARAK

Dr. Betty Tikoko
DIRECTOR - (POST GRADUATE STUDIES)

Kabarak University Moral Code
As members of Kabarak University family, we purpose at all times and in all places, to set apart in one's heart, Jesus as Lord. (1 Peter 3:15)

Kabarak University is ISO 9001:2015 Certified

APPENDIX III: Nacosti Research Authorization



NACOSTI

NATIONAL COMMISSION FOR SCIENCE,
TECHNOLOGY AND INNOVATION

Telephone:+254-20-2213471,
2241349,3310571,2219420
Fax:+254-20-318245,318249
Email: dg@nacosti.go.ke
Website : www.nacosti.go.ke
When replying please quote

NACOSTI, Upper Kabete
Off Waiyaki Way
P.O. Box 30623-00100
NAIROBI-KENYA

Ref. No. **NACOSTI/P/18/80346/24749**

Date: **14th February, 2019**

Makupi Kimutai Daniel
Kabarak University
Private Bag - 20157
KABARAK.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on ***"An information security maturity model for universities based on ISO 27001"*** I am pleased to inform you that you have been authorized to undertake research in **all Counties** for the period ending **14th September, 2019.**

You are advised to report to **the County Commissioners and the County Directors of Education, all Counties** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit **a copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

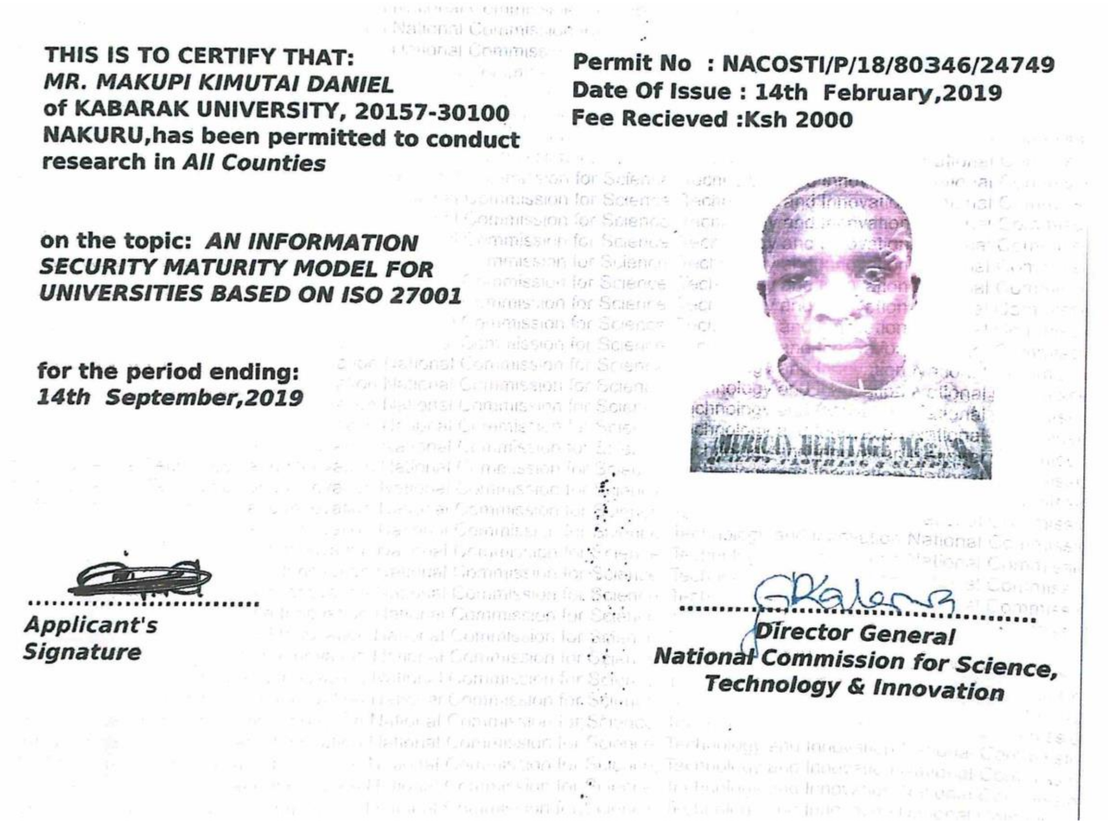
GODFREY P. KALERWA MSc., MBA, MKIM
FOR: DIRECTOR-GENERAL/CEO

Copy to:

The County Commissioners
All Counties.

The County Directors of Education
All Counties.

APPENDIX IV: Nacosti Research Permit



THIS IS TO CERTIFY THAT:
MR. MAKUPI KIMUTAI DANIEL
of KABARAK UNIVERSITY, 20157-30100
NAKURU,has been permitted to conduct
research in *All Counties*

Permit No : NACOSTI/P/18/80346/24749
Date Of Issue : 14th February,2019
Fee Recieved :Ksh 2000

on the topic: *AN INFORMATION SECURITY MATURITY MODEL FOR UNIVERSITIES BASED ON ISO 27001*

for the period ending:
14th September,2019

....
Applicant's Signature

...
Director General
National Commission for Science, Technology & Innovation

APPENDIX V: List of Universities in Kenya According to Commission of University Education (CUE)

	LIST OF UNIVERSITIES	YEAR OF CHARTER AWARD
Public Chartered Universities		
1.	University of Nairobi (UoN)	2013
2.	Moi University (MU)	2013
3.	Kenyatta University (KU)	2013
4.	Egerton University (EU)	2013
5.	Jomo Kenyatta University of Agriculture and Technology(JKUAT)	2013
6.	Maseno University (Maseno)	2013
7.	Dedan Kimathi University of Technology	2012
8.	Chuka University	2013
9.	Technical University of Kenya	2013
10.	Technical University of Mombasa	2013
11.	Pwani University	2013
12.	Kisii University	2013
13.	Masinde Muliro University of Science and Technology	2013
14.	Maasai Mara University	2013
15.	South Eastern Kenya University	2013
16.	Meru University of Science and Technology	2013
17.	Multimedia University of Kenya	2013
18.	Jaramogi Oginga Odinga University of Science and Technology	2013
19.	Laikipia University	2013
20.	University of Kabianga	2013
21.	University of Eldoret	2013
22.	Karatina University	2013
23.	Kibabii University	2015
24.	Embu University	2016
25	Kirinyaga University	2016

	Public University Constituent Colleges	
26.	Garissa University College (MU)	2011
27.	Murang'a University College (JKUAT)	2011
28.	Machakos University College (KU)	2011
29.	Rongo University College (MU)	2011
30.	Taita Taveta University College (JKUAT)	2011
31.	The Co-operative University College of Kenya (JKUAT)	2011
32.	Kaimosi Friends University College	2015
33.	Alupe University College (MU)	2015
34	Bomet University College	2017
Private Chartered Universities		
35.	University of Eastern Africa, Baraton	1991
36.	Catholic University of Eastern Africa (CUEA)	1992
37.	Daystar University	1994
38.	Scott Christian University	1997
39.	United States International University	1999
40..	St. Paul's University	2007
41.	Pan Africa Christian University	2008
42.	Africa International University	2011
43.	Kenya Highlands Evangelical University	2011
44.	Africa Nazarene University	2002
45.	Kenya Methodist University	2006
46.	Strathmore University	2008
47.	Kabarak University	2008
48.	Great Lakes University of Kisumu	2012
49.	KCA University	2013
50.	Mount Kenya University	2011
51.	Adventist University of Africa	2013
52	Scott Christian University	2012
53	Kabarak University	2008
Private University Constituent Colleges		

54.	Hekima University College (CUEA)	
55.	Tangaza University College (CUEA)	
56.	Marist International University College (CUEA)	
57.	Regina Pacis University College (CUEA)	
58.	Uzima University College (CUEA)	
59.	Koitaleel Samoei University College	
Institutions with Letter of Interim Authority (LIA)		
60.	Kiriri Women’s University of Science and Technology	
61.	Aga Khan University	
62.	GRETSA University	
63.	Presbyterian University of East Africa	
64.	Inoorero University	
65.	The East African University	
66.	GENCO University	
67.	Management University of Africa	
68.	Riara University	
69.	Pioneer International University	
70.	UMMA University	
71.	International Leadership University	
72.	Zetech University	
73	Lukenya University	
74.	KAG - EAST University	

APPENDIX VI: System Source Code

ALL SCORES SNIPPET

```
<?php
		if(!isset($_SESSION['usr_id'])) {
				header("Location: index.php");
		}
		include_once 'dbconnect.php';
		$user_id = $_SESSION['usr_id'];
		$sql   =   "SELECT   ROUND(100*((-2.128+SUM(user_score*weight))/(-
2.128+SUM(5*weight))),1)FROM maturity_assessment;";
		$result = mysqli_query($con,$sql);
		$data = mysqli_fetch_array($result);
		$output = $data[0];
		if($output>0){
				echo $output;
		}else{
				echo 0;
		}
?>

<?php
   session_start();
   if(!isset($_SESSION['usr_id'])) {
      header("Location: index.php");
   }
   include_once 'dbconnect.php';
?>
```

ASSESSMENT CODE SNIPPET

```
<!DOCTYPE html>
<html>
<head>
		<title>UISM | Maturity Assessment</title>
		<meta content="width=device-width, initial-scale=1.0" name="viewport" >
		<link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
		<link rel="stylesheet" href="css/style.css" type="text/css" />
		<link rel="stylesheet" href="css/style2.css" type="text/css" />
</head>
<body      style="background-image:      url('images/bg.jpg');background-attachment:
fixed;">
   <?php include 'sidenav.php' ?>
   <?php include 'topnav.php'?>
      <div class="container">
         <div     class="col-md-11"     style="box-shadow:     3px     2px     8px     0px
black;background: white; margin-top: 5%;margin-left:12%;display: inline-block"">
            <h4  style="color:  maroon;border-bottom:  1px  dotted  #000080;padding:
5px"><i class="fa fa-list-alt"></i> Maturity Assessment Section</h4>
            <div class="wizard">
               <div class="wizard-inner">
                  <div class="connecting-line"></div>
            <ul class="nav nav-tabs" role="tablist">
              <li role="presentation" class="active">
                <a href="#step1" data-toggle="tab" aria-controls="step1"
role="tab" title="Step 1">
                  <span class="round-tab">
                    <i class="fa fa-folder"></i>
                    <span><br></span>
                    <span><h6 style="margin-
top:15px;padding:5px;background-color:white;color: #8a6d3b;text-align:
center;">Administrative</h6></span>
                  </span>
                </a>
              </li>
              <li role="presentation" class="disabled">
                <a href="#step2" data-toggle="tab" aria-controls="step2"
role="tab" title="Step 2">
                  <span class="round-tab">
                    <i class="fa fa-laptop"></i>
                    <span><br></span>
                    <span><h6 style="margin-
top:15px;padding:5px;background-color:white;color: #8a6d3b;text-align:
center;">Technological</h6></span>
                  </span>
                </a>
              </li>
              <li role="presentation" class="disabled">
                <a href="#step3" data-toggle="tab" aria-controls="step3"
role="tab" title="Step 3">
                  <span class="round-tab">
                    <i class="fa fa-camera"></i>
                    <span><br></span>
                    <span><h6 style="margin-
top:15px;padding:5px;background-color:white;color: #8a6d3b;text-align:
center;">Physical</h6></span>
                  </span>
                </a>
              </li>
              <li>
                <span style="font-size: 12px;font-style: italic;text-
align:right;color:red;">
                  KEYS: <br> Not Performed = 0; Performed Informally = 1;
Planned = 2; Well Defined = 3; Quantitatively Controlled = 4; Continuously
Improving = 5; <br> NOTE: 5 is the highest level of maturity.
                </span>
              </li>
            </ul>
          </div>
          <form role="form" action="saves_scores.php" method="post">
            <div class="tab-content">
              <div class="tab-pane active" role="tabpanel" id="step1">
```

```
                <div class="step1">
                  <!--PULL ADMINISTRATIVE QUESTIONS HERE-->
                  <table class="table table-fixed table-bordered table-condensed">
                    <?php
                    $sql = "SELECT id, questions  FROM maturity_questions where main_category='Administrative Factors'";
                    $result = $con->query($sql);
                    if ($result->num_rows > 0) {
                      echo "<thead>
                          <tr>
                            <th>ID</th>
                            <th>Administrative Factors</th>

<th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th>
                          </tr>
                        </thead>";
                        while($row = $result->fetch_assoc()) {
                            $radioname = $row['id'];
                            echo "<tr>";
                            echo "<td width='2%'>" . $row["id"] . "</td>";
                            echo "<td width='86%'>" . $row["questions"] . "</td>";
                            for($i=0;$i<=5;$i++) {
                              echo "<td width='2%'><input type='radio' name='$radioname' value='$i' required='required'/></td>";
                            }
                            echo "</tr>";
                          }
                        } else {
                          echo "<span style='font-weight: bolder;color:darkred;'> Sorry There are no Questions Under Administrative Factors</span>";
                        }

                    ?>
                  </table>

                </div>
                <ul class="list-inline pull-right">
                  <li><button type="button" class="btn btn-primary next-step">Next <i class="fa fa-angle-double-right"></i></button></li>
                </ul>
              </div>
              <div class="tab-pane" role="tabpanel" id="step2">
                <div class="step2">
                  <!--PULL TECHNOLOGICAL QUESTIONS HERE-->
                  <table class="table table-bordered table-condensed table-hover table-sm">
                    <?php
                    $sql = "SELECT id, questions  FROM maturity_questions
where main_category='Technological Factors'";
                    $result = $con->query($sql);
                    if ($result->num_rows > 0) {
                      echo "<thead>
                      <tr>
                        <th>ID</th>
                        <th>Technological Factors</th>

<th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th>
                      </tr>
                    </thead>";
                      while($row = $result->fetch_assoc()) {
                        $radioname = $row['id'];
                        echo "<tr>";
                        echo "<td width='2%'>" . $row["id"] . "</td>";
                        echo "<td width='86%'>" . $row["questions"] . "</td>";
                        for($i=0;$i<=5;$i++) {
                          echo "<td width='2%'><input type='radio'
name='$radioname' value='$i' required='required'/></td>";
                        }
                        echo "</tr>";
                      }
                    } else {
                      echo "<span style='font-weight: bolder;color:darkred;'>
Sorry There are no Questions Under Technological Factors</span>";
                    }
                    ?>
                  </table>
                </div>
                <ul class="list-inline pull-right">
                  <li><button type="button" class="btn btn-default prev-step"><i
class="fa fa-angle-double-left"></i> Previous</button></li>
                  <li><button type="button" class="btn btn-primary next-
step">Next <i class="fa fa-angle-double-right"></i></button></li>
                </ul>
              </div>
              <div class="tab-pane" role="tabpanel" id="step3">
                <div class="step3">
                  <!--PULL PHYSICAL QUESTIONS HERE-->
                  <table class="table table-bordered table-condensed table-
hover">
                    <?php
                    $sql = "SELECT id, questions  FROM maturity_questions
where main_category='Physical Factors'";
                    $result = $con->query($sql);
                    if ($result->num_rows > 0) {
                      echo "<thead>
                      <tr>
                        <th>ID</th>
```

```
                                        <th>Question</th>

<th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th>
                                    </tr>
                                </thead>";
                                    while($row = $result->fetch_assoc()) {
                                        $radioname = $row['id'];
                                        echo "<tr>";
                                        echo "<td width='2%'>" . $row["id"] . "</td>";
                                        echo "<td width='86%'>" . $row["questions"] . "</td>";
                                        for($i=0;$i<=5;$i++) {
                                            echo "<td width='2%'><input type='radio'
name='$radioname' value='$i' required='required'/></td>";
                                        }
                                        echo "</tr>";
                                    }
                                } else {
                                    echo "<span style='font-weight: bolder;color:darkred;'>
Sorry There are no Questions Under Physical Factors</span>";
                                }
                                ?>
                            </table>
                        </div>
                        <ul class="list-inline pull-right">
                            <li><button type="button" class="btn btn-default prev-step"><i
class="fa fa-angle-double-left"></i> Previous</button></li>
                            <li><button onclick="return confirm('Are you sure you want to
Submit?');" id="submit_score" name="submit_score" type="submit" class="btn btn-
primary btn-info-full next-step"><i class="fa fa-save"></i> Submit</button></li>
                        </ul>
                         <div class="clearfix"></div>
                        </div>
                </form>
            </div>
        </div>
    </div>
<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/custom.js"></script>
<script src="js/custom2.js"></script>
</body>
</html>
```

CODE SNIPPET FOR COMPUTING AVERAGE SCORES

```
<?php
        if(!isset($_SESSION['usr_id'])) {
                header("Location: index.php");
        }
        include_once 'dbconnect.php';
        $user_id = $_SESSION['usr_id'];
        $sql = "select round(avg (a.user_score),2) from maturity_assessment a
inner join
                        users b on a.user_id=b.id";
        $result = mysqli_query($con,$sql);
        $data = mysqli_fetch_array($result);
        $output = $data[0];
        if($output>0){
                echo $output;
        }else{
                echo 0;
        }

?>
```

CODE SNIPPET TO CLEAR USER ASSESSMENTS

```
<?php
/**
 * Created by:J K. mutai
 * Date: 10/28/18
 * Time: 11:22 AM
 */

session_set_cookie_params(0);
session_start();
include_once 'dbconnect.php';
  $user_id = $_SESSION['usr_id'];
        $sql = "DELETE FROM maturity_assessment WHERE  user_id='$user_id'
";
        mysqli_query($con,$sql);
        header("Location: home.php");
?>
```

CODE SNIPPET TO COUNT USER ASSESSMENTS DONE

```
<?php
        if(!isset($_SESSION['usr_id'])) {
                header("Location: index.php");
        }
        include_once 'dbconnect.php';
        $user_id = $_SESSION['usr_id'];
        $sql = "select ROUND(count(a.id)/36,0) from maturity_assessment a inner
join users b on a.user_id=b.id where b.id=$user_id";
        $result = mysqli_query($con,$sql);
        $data = mysqli_fetch_array($result);
        $output = $data[0];
        if($output>0){
                echo $output;
        }else{
                echo 0;
        }
```

```
?>
```

CODE SNIPPET TO COUNT USER RECOMMENDATIONS

```
<?php
        if(!isset($_SESSION['usr_id'])) {
                header("Location: index.php");
        }
        include_once 'dbconnect.php';
        $user_id = $_SESSION['usr_id'];
        $sql = "select count(distinct(a.id))from maturity_questions a inner join
maturity_assessment b on a.id=b.question_id inner join
                        users c on b.user_id=c.id where
b.user_score<a.threshold and c.id=$user_id";
        $result = mysqli_query($con,$sql);
        $data = mysqli_fetch_array($result);
        echo $data[0];

?>
```

CODE SNIPPET FOR HELP SECTION

```
<?php
/**
 * Created by PhpStorm.
 * User: mutai
 * Date: 10/28/18
 * Time: 1:44 PM
 */
    session_start();
    if(!isset($_SESSION['usr_id'])) {
        header("Location: index.php");
    }
    include_once 'dbconnect.php';
?>
<!doctype html>
<html lang="en">
<head>
    <link rel="stylesheet" href="css/help.css">
    <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
    <link rel="stylesheet" href="css/style.css" type="text/css" />
    <meta charset="UTF-8">
    <meta name="viewport"
          content="width=device-width, user-scalable=no, initial-scale=1.0, maximum-
scale=1.0, minimum-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>UISM | Help</title>
</head>
<body>
<?php include 'topnav.php'?>
```

```
<?php include 'sidenav.php' ?>
  <div class="container">
    <div class="row" style="margin-top: 5%;margin-left: 8.5%; background:
white;padding: 10px;width: 100%;">
      <p style="font-family:Helvetica;font-weight: normal;font-style: oblique;text-
align: center;"><i class="fa fa-fire"></i><br>
        Welcome to UISM Platform Help Section.
        <br>Obtain Help on how to perform different tasks in the system. You only
need to
        click on the subject title to obtain Help.</p>

      <!--  START       -->
      <div class="accordion-container">
        <hr>
        <div class="set">
          <a href="#">
            <span class="fa fa-fire"></span> How to Run Maturity Assessment
            <i class="fa fa-plus"></i>
          </a>
          <div class="content">
            <p>
              <ul>
                <li>Goto Maturity Assessment item on the side menu or on the
Dashboard</li>
                <li>Answer all Administrative, Technological and Physical
questions </li>
                <li>Note: The Score is in a  scale of 0 to 5</li>
                <li>Confirm Submission on the Alert</li>
                <li>Submit the scores</li>
              </ul>
            </p>
          </div>
        </div>
        <div class="set">
          <a href="#">
            <span class="fa fa-fire"></span> How to Delete your Maturity Scores
            <i class="fa fa-plus"></i>
          </a>
          <div class="content">
            <p>
              <ul>
                <li>Goto the Dashboard</li>
                <li>Click on "Clear all your previous scores" button </li>
                <li>Confirm deletion on the Alert</li>
              </ul>
            </p>
          </div>
        </div>
        <div class="set">
          <a href="#">
```

```
            <span class="fa fa-fire"></span> How to View Maturity Recommendations
            <i class="fa fa-plus"></i>
          </a>
          <div class="content">
            <p>
            <ul>
              <li>Go to Reports on side menu then click "Maturity Recommendations" item </li>
              <li>OR Click "View your Recommendations Report" item on Dashboard</li>
            </ul>
            </p>
          </div>
        </div>
        <div class="set">
          <a href="#">
            <span class="fa fa-fire"></span> How to View Maturity Scores
            <i class="fa fa-plus"></i>
          </a>
          <div class="content">
            <p>
              <ul>
                <li>Go to Reports on side menu then click "Maturity scores" item </li>
                <li>OR Click "View your Scores Report" item on Dashboard</li>
              </ul>
            </p>
          </div>
        </div>
        <div class="set">
          <a href="#">
            <span class="fa fa-fire"></span> How to Interpret your UISM index Score
            <i class="fa fa-plus"></i>
          </a>
          <div class="content">
            <p>
              <ul>
                <li>On your Dashboard, your UISM score is presented as a SVG Gauge </li>
                <li>The scale is calculated as a percentage of 1-100</li>
                <li>The score is arrived at using a model formula: <br>
                  <span style="font-weight: bolder;color:red;font-style: oblique;">
                  U.I.S.M = -0.305+{0.596* Administrative Factors}+{0.278* Technological Factors}+{0.301* Physical Factors}+0.59
                  </span>

                </li>
                </ul>
              </p>
            </div>
          </div>
        </div>
        <!--   END       -->
      </div>
    </div>
<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/help.js"></script>
</body>
</html>
```

UISM COMPUTATION

```
<?php
        include_once 'dbconnect.php';
        $user_id = $_SESSION['usr_id'];


$sql = "SELECT ROUND(100*((0.821+SUM(user score*weight)+
0.586)/(0.821+SUM(5*weight) + 0.586)),1) FROM `maturity_assessment`WHERE
user_id='$user_id' ";
        $result = mysqli_query($con,$sql);
        $data = mysqli_fetch_array($result);
        $uism = $data[0];


        if($uism == 0){
                echo 0;
        }else{
                echo $uism;
        }


?>
```

HP

```
<?php
  session_start();
  if(!isset($_SESSION['usr_id'])) {
    header("Location: index.php");
  }
  include_once 'dbconnect.php';
?>

<!DOCTYPE html>
<html>
```

```
<head>
        <title>UISM | Home</title>
        <meta content="width=device-width, initial-scale=1.0" name="viewport" >
        <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
        <link rel="stylesheet" href="css/style.css" type="text/css" />
        <link rel="stylesheet" href="css/gauge.css" type="text/css" />
</head>
<body style="background-image: url('images/bg.jpg');background-attachment: fixed;">

  <?php include 'topnav.php'?>
  <?php include 'sidenav.php' ?>
  <div class="container">
    <div class="row" style="margin-top: 5%;margin-left: 8.5%; background: white;padding: 10px;width: 100%;">
      <div class="col-md-12">
        <span class="fa fa-fire"></span>
        <p style="font-family:Helvetica;font-weight: normal;font-style: oblique;text-align: center;">Welcome to UISM Platform. The platform Helps you to assess the level of maturity of your Institution in terms of information security.
        <br>It is based on the robust ISO 27001 Framework of Information Security.</p>
        <hr>
        <div class="row justify-content-center" style="background: #f8f8f8;padding: 6px;">
          <div class="col-md-3" style="color: red;font-weight: bolder;"><h4>Statistics <i class="fa fa-angle-double-right"></i></h4> </div>
          <div class="col-sm-3">
            <a href="maturity_recommendations.php" class="" style="display: inline-block;">Recommendations <span class="badge"><?php include 'count_recommendations.php'?></span></a><br>
          </div>
          <div class="col-sm-3">
            <a href="#" class="" style="display: inline-block;"> Number of Assessments Done <span class="badge"><?php include "count_assessmentsdone.php"?></span></a><br>
          </div>
          <div class="col-sm-3">
            <a href="maturity_scores.php" class="" style="display: inline-block">Average Score <span class="badge"><?php include "average_score.php";?></span></a>
          </div>
        </div>
        <div class="row"><hr>
          <div class="col-md-4" style="border-right: 1px dotted maroon;padding-right: 10px;">
            <h4 style="text-align: center;"> Maturity Index </h4>
            <hr>
<!--              BEGINNING OF GAUGE-->
            <div class="container A">
            <svg class="typeRange" height="165" width="330" view-box="0 0
330 165">

              <g class="scale" stroke="red"></g>

              <path class="outline" d="" />
              <path class="fill" d="" />
              <polygon class="needle" points="220,10 300,210 220,250
140,210" />
            </svg>
            <div class="output">30</div>
          </div>
          <p style="font-style: oblique;text-align: center;"><span style="color:
red;font-weight: bolder"><?php include 'uism.php'?>%</span> Mature</p>

          <input type="text" class="initialValue" value="<?php include
'uism.php'?>" hidden />
<!--                    ENDING OF GAUGE-->
        </div>
        <div class="col-md-7 pull-right" style="">
          <div class="col-md-12">
            <h5 class="bg-info" style="padding: 5px; font-weight:
bolder">Quick Actions</h5>
            <ul style="list-style-type: none;">
              <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="assessments.php"><h5><i class="fa fa-fire"></i> Run
New Maturity Assessment</h5></a></li>
              <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="maturity_scores.php"><h5><i class="fa fa-fire"></i>
View your Scores Report</h5></a></li>
              <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="maturity_recommendations.php"><h5><i class="fa fa-
fire"></i> View your Recommendations Report  <span class="badge"
style="background: darkred"><?php include
'count_recommendations.php'?></span></h5></a></li>
              <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="help.php"><h5><i class="fa fa-fire"></i> Obtain
Help</h5></a></li>
              <li style="padding-top: 2px;padding-bottom: 2px;"><a
href="logout.php"><h5><i class="fa fa-fire"></i> Logout</h5></a></li>
            </ul>
          </div>
          <div class="col-md-12">
            <a href="clear_assessments.php" class="btn btn-block btn-warning"
onclick="return confirm('Are you sure you want to Clear?');"><i class="fa fa-
trash"></i>
              Clear all your previous Scores</a>
          </div>

        </div>
```

```
                </div>

            </div>
        </div>
    </div>

<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/gauge.js"></script>
</body>
</html>

<?php
    session_start();
    if(!isset($_SESSION['usr_id'])) {
        header("Location: index.php");
    }
    include_once 'dbconnect.php';
?>

<!DOCTYPE html>
<html>
<head>
                <title>UISM | Home</title>
                <meta content="width=device-width, initial-scale=1.0" name="viewport" >
                <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
                <link rel="stylesheet" href="css/style.css" type="text/css" />
                <link rel="stylesheet" href="css/gauge.css" type="text/css" />
</head>
<body style="background-image: url('images/bg.jpg');background-attachment:
fixed;">

    <?php include 'topnav.php'?>
    <?php include 'sidenav.php' ?>
    <div class="container">
        <div class="row" style="margin-top: 5%;margin-left: 8.5%; background:
white;padding: 10px;width: 100%;">
            <div class="col-md-12">
                <span class="fa fa-fire"></span>
                <p style="font-family:Helvetica;font-weight: normal;font-style:
oblique;text-align: center;">Welcome to UISM Platform. The platform Helps you to
assess the level of maturity of your Institution in terms of information security.
                <br>It is based on the robust ISO 27001 Framework of Information
Security.</p>
                <hr>
                <div class="row justify-content-center" style="background:
#f8f8f8;padding: 6px;">
                    <div class="col-md-3" style="color: red;font-weight:
bolder;"><h4>Statistics <i class="fa fa-angle-double-right"></i></h4> </div>
                    <div class="col-sm-3">
                      <a href="maturity_recommendations.php" class="" style="display: inline-block;">Recommendations <span class="badge"><?php include 'count_recommendations.php'?></span></a><br>
                    </div>
                    <div class="col-sm-3">
                      <a href="#" class="" style="display: inline-block;"> Number of Assessments Done <span class="badge"><?php include "count_assessmentsdone.php"?></span></a><br>
                    </div>
                    <div class="col-sm-3">
                      <a href="maturity_scores.php" class="" style="display: inline-block">Average Score <span class="badge"><?php include "average_score.php";?></span></a>
                    </div>
                </div>
                <div class="row"><hr>
                    <div class="col-md-4" style="border-right: 1px dotted maroon;padding-right: 10px;">
                      <h4 style="text-align: center;"> Maturity Index </h4>
                      <hr>
<!--               BEGINNING OF GAUGE-->
                      <div class="container A">
                        <svg class="typeRange" height="165" width="330" view-box="0 0 330 165">

                          <g class="scale" stroke="red"></g>

                          <path class="outline" d="" />
                          <path class="fill" d="" />
                          <polygon class="needle" points="220,10 300,210 220,250 140,210" />
                        </svg>
                        <div class="output">30</div>
                      </div>
                      <p style="font-style: oblique;text-align: center;"><span style="color: red;font-weight: bolder"><?php include 'uism.php'?>%</span> Mature</p>

                      <input type="text" class="initialValue" value="<?php include 'uism.php'?>" hidden />
<!--               ENDING OF GAUGE-->
                    </div>
                    <div class="col-md-7 pull-right" style="">
                      <div class="col-md-12">
                        <h5 class="bg-info" style="padding: 5px; font-weight: bolder">Quick Actions</h5>
                        <ul style="list-style-type: none;">
                          <li style="padding-top: 2px;padding-bottom: 2px;border-bottom: 1px dotted green;"><a href="assessments.php"><h5><i class="fa fa-fire"></i> Run New Maturity Assessment</h5></a></li>
```

```
                                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="maturity_scores.php"><h5><i class="fa fa-fire"></i>
View your Scores Report</h5></a></li>
                                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="maturity_recommendations.php"><h5><i class="fa fa-
fire"></i> View your Recommendations Report  <span class="badge"
style="background: darkred"><?php include
'count_recommendations.php'?></span></h5></a></li>
                                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="help.php"><h5><i class="fa fa-fire"></i> Obtain
Help</h5></a></li>
                                <li style="padding-top: 2px;padding-bottom: 2px;"><a
href="logout.php"><h5><i class="fa fa-fire"></i> Logout</h5></a></li>
                            </ul>
                        </div>
                        <div class="col-md-12">
                            <a href="clear_assessments.php" class="btn btn-block btn-warning"
onclick="return confirm('Are you sure you want to Clear?');"><i class="fa fa-
trash"></i>
                                Clear all your previous Scores</a>
                        </div>

                    </div>
                </div>

            </div>
        </div>
    </div>

<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/gauge.js"></script>
</body>
</html>
```

CODE SNIPPET FOR DASHBOARD

```
<?php
    session_start();
    if(!isset($_SESSION['usr_id'])) {
        header("Location: index.php");
    }
    include_once 'dbconnect.php';
?>

<!DOCTYPE html>
<html>
<head>
                <title>UISM | Home</title>
                <meta content="width=device-width, initial-scale=1.0" name="viewport" >
                <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
                <link rel="stylesheet" href="css/style.css" type="text/css" />
                <link rel="stylesheet" href="css/gauge.css" type="text/css" />
</head>
<body style="background-image: url('images/bg.jpg');background-attachment:
fixed;">

    <?php include 'topnav.php'?>
    <?php include 'sidenav.php' ?>
    <div class="container">
        <div class="row" style="margin-top: 5%;margin-left: 8.5%; background:
white;padding: 10px;width: 100%;">
            <div class="col-md-12">
                <span class="fa fa-fire"></span>
                <p style="font-family:Helvetica;font-weight: normal;font-style:
oblique;text-align: center;">Welcome to UISM Platform. The platform Helps you to
assess the level of maturity of your Institution in terms of information security.
                <br>It is based on the robust ISO 27001 Framework of Information
Security.</p>
                <hr>
                <div class="row justify-content-center" style="background:
#f8f8f8;padding: 6px;">
                    <div class="col-md-3" style="color: red;font-weight:
bolder;"><h4>Statistics <i class="fa fa-angle-double-right"></i></h4> </div>
                    <div class="col-sm-3">
                        <a href="maturity_recommendations.php" class="" style="display:
inline-block;">Recommendations <span class="badge"><?php include
'count_recommendations.php'?></span></a><br>
                    </div>
                    <div class="col-sm-3">
                        <a href="#" class="" style="display: inline-block;"> Number of
Assessments Done <span class="badge"><?php include
"count_assessmentsdone.php"?></span></a><br>
                    </div>
                    <div class="col-sm-3">
                        <a href="maturity_scores.php" class="" style="display: inline-
block">Average Score <span class="badge"><?php include
"average_score.php";?></span></a>
                    </div>
                </div>
                <div class="row"><hr>
                    <div class="col-md-4" style="border-right: 1px dotted maroon;padding-
right: 10px;">
                        <h4 style="text-align: center;"> Maturity Index </h4>
                        <hr>
<!--                BEGINNING OF GAUGE-->
                        <div class="container A">
                            <svg class="typeRange" height="165" width="330" view-box="0 0
330 165">
```

```
                <g class="scale" stroke="red"></g>

                <path class="outline" d="" />
                <path class="fill" d="" />
                <polygon class="needle" points="220,10 300,210 220,250
140,210" />
              </svg>
              <div class="output">30</div>
            </div>
            <p style="font-style: oblique;text-align: center;"><span style="color:
red;font-weight: bolder"><?php include 'uism.php'?>%</span> Mature</p>

            <input type="text" class="initialValue" value="<?php include
'uism.php'?>" hidden />
<!--               ENDING OF GAUGE-->
          </div>
          <div class="col-md-7 pull-right" style="">
            <div class="col-md-12">
              <h5 class="bg-info" style="padding: 5px; font-weight:
bolder">Quick Actions</h5>
              <ul style="list-style-type: none;">
                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="assessments.php"><h5><i class="fa fa-fire"></i> Run
New Maturity Assessment</h5></a></li>
                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="maturity_scores.php"><h5><i class="fa fa-fire"></i>
View your Scores Report</h5></a></li>
                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="maturity_recommendations.php"><h5><i class="fa fa-
fire"></i> View your Recommendations Report <span class="badge"
style="background: darkred"><?php include
'count_recommendations.php'?></span></h5></a></li>
                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="help.php"><h5><i class="fa fa-fire"></i> Obtain
Help</h5></a></li>
                <li style="padding-top: 2px;padding-bottom: 2px;"><a
href="logout.php"><h5><i class="fa fa-fire"></i> Logout</h5></a></li>
              </ul>
            </div>
            <div class="col-md-12">
              <a href="clear_assessments.php" class="btn btn-block btn-warning"
onclick="return confirm('Are you sure you want to Clear?');"><i class="fa fa-
trash"></i>
                Clear all your previous Scores</a>
            </div>

          </div>
        </div>

      </div>
```

```
        </div>
    </div>

<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/gauge.js"></script>
</body>
</html>
```

(A) **MENU**

```
<nav class="navbar navbar-default sidebar" role="navigation" style="display: inline-block;position: fixed;">
    <div class="container-fluid">
        <!-- Brand and toggle get grouped for better mobile display -->
        <div class="navbar-header">
            <button type="button" class="navbar-toggle" data-toggle="collapse" data-target="#bs-sidebar-navbar-collapse-1">
                <span class="sr-only">Toggle navigation</span>
                <span class="icon-bar"></span>
                <span class="icon-bar"></span>
                <span class="icon-bar"></span>
            </button>
            <a class="navbar-brand" href="home.php" style="color: #2b542c;font-weight: bolder;font-size: large;"><i class="fa fa-fire"></i> UISM Platform</a>
        </div>
        <!-- Collect the nav links, forms, and other content for toggling -->
        <div class="collapse navbar-collapse" id="bs-sidebar-navbar-collapse-1">
            <ul class="nav navbar-nav">
                <li class="active"><a href="home.php">Dashboard<span style="font-size:16px;" class="pull-right hidden-xs showopacity fa fa-home"></span></a></li>
                <li ><a href="assessments.php">Maturity Assessment<span style="font-size:16px;" class="pull-right hidden-xs showopacity fa fa-list"></span></a></li>
                 <li class="dropdown">
                    <a href="#" class="dropdown-toggle" data-toggle="dropdown">Reports <span class="caret"></span><span style="font-size:16px;" class="pull-right hidden-xs showopacity fa fa-bars"></span></a>
                    <ul class="dropdown-menu forAnimate" role="menu">
                        <li><a href="maturity_scores.php">Maturity Scores <i class="fa fa-check"></i></a></li>
                        <li class="divider"></li>
                        <li><a href="maturity_recommendations.php">Recommendations <i class="fa fa-file"></i></a></li>
                    </ul>
                </li>
                <li ><a href="help.php">Help<span style="font-size:16px;" class="pull-right hidden-xs showopacity fa  fa-question-circle"></span></a></li>
                <li ><a href="logout.php">Logout<span style="font-size:16px;" class="pull-right hidden-xs showopacity fa fa-sign-out"></span></a></li>
            </ul>
            <div style="text-align: center;float: bottom;font-weight: bold;color:
#2a6496;">
                <span> <h1 class="fa fa-fire"></h1><br>© Daniel Makupi <br>PHD
Student <br> KABARAK UNIVERSITY </span>
            </div>
        </div>
    </div>
</nav>
```

LANDING PAGE

```
<?php
session_start();

if(isset($_SESSION['usr_id'])!="") {
                header("Location: home.php");
}
include_once 'dbconnect.php';

//check if form is submitted
if (isset($_POST['login'])) {

                $email = mysqli_real_escape_string($con, $_POST['email']);
                $password = mysqli_real_escape_string($con, $_POST['password']);
                $result = mysqli_query($con, "SELECT * FROM users WHERE email = '"
. $email. "' and password = '" . sha1($password) . "'");

                if ($row = mysqli_fetch_array($result)) {
                                $_SESSION['usr_id'] = $row['id'];
                                $_SESSION['usr_name'] = $row['name'];
                                header("Location: home.php");
                } else {
                                $errormsg = "Incorrect Email or Password!!!";
                }
}
?>

<!DOCTYPE html>
<html>
<head>
                <title>UISM | Login </title>
                <meta content="width=device-width, initial-scale=1.0" name="viewport" >
                <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
</head>
<body style="background-image: url('images/bg.jpg');">

<br><br><br><br><br>
<div class="container">
                <div class="row">
```

```
        <div class="col-md-4 col-md-offset-4" style="box-shadow: 3px
2px 8px 0px black; padding: 20px;border-radius: 4px 4px 0 0;background: white;">
            <form role="form" action="<?php echo
$_SERVER['PHP_SELF']; ?>" method="post" name="loginform">
                <fieldset>
                    <legend>Login to
UISM</legend>

                    <div class="form-group">
                        <label
for="name">Email</label>
                        <input type="text"
name="email" placeholder="Your Email" required class="form-control" />
                    </div>

                    <div class="form-group">
                        <label
for="name">Password</label>
                        <input
type="password" name="password" placeholder="Your Password" required
class="form-control" />
                    </div>

                    <div class="form-group">
                        <input type="submit"
name="login" value="Login" class="btn btn-primary" />
                    </div>
                </fieldset>
            </form>

            <span class="text-danger"><?php if (isset($errormsg))
{ echo $errormsg; } ?></span>
        </div>
        <a class="btn btn-primary col-md-4 col-md-offset-4 text-center"
href="register.php" style="box-shadow: 3px 2px 8px 0px black;">Register here if you
are a new user</a>
    </div>

</div>

<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
</body>
</html>
```

CODE SNIPPET FOR DISPLAYING MATURITY RECOMMENDATION

```
<?php
   session_start();
   if(!isset($_SESSION['usr_id'])) {
        header("Location: index.php");
    }
    include_once 'dbconnect.php';
?>

<!DOCTYPE html>
<html>
<head>
                <title>UISM | Recommendations for Maturity</title>
                <meta content="width=device-width, initial-scale=1.0" name="viewport" >
                <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
                <link rel="stylesheet" href="css/style.css" type="text/css" />
</head>
<body style="background-image: url('images/bg.jpg');">

    <?php include 'topnav.php'?>
    <?php include 'sidenav.php' ?>

    <div class="container">
        <div class="row">
            <div class="col-md-10" style="margin-top:6%;margin-left: 15%;box-shadow:
3px 2px 8px 0px black;background: white;">
                <h4 style="font-style: oblique"><i class="fa fa-fire"></i> Maturity
Recommendations <span class="badge"> <?php include
"count_recommendations.php";?> Recommendations</span></h4>
                <a class="btn btn-primary btn-xs pull-right" href="home.php"><i class="fa
fa-angle-double-left"></i> Back Home</i></a>
                <hr>
                <table class="table table-condensed table-hover"
id="recommendations_table">
                    <?php
                    $user_id = $_SESSION['usr_id'];
                    $sql = "select distinct(a.id),a.category,b.user_score,a.recommendations
from maturity_questions a inner join maturity_assessment b on a.id=b.question_id
inner join users c on b.user_id=c.id where b.user_score<a.threshold and
c.id=$user_id;";
                    $result = $con->query($sql);
                    if ($result->num_rows > 0) {
                        echo "<thead>
                                    <tr>
                                        <th>ID</th>
                                        <th>Category</th>
                                        <th style='background: whitesmoke'>AvgScore</th>
                                        <th>Reccommendation</th>
                                     </tr>
                                </thead>";
                        while($row = $result->fetch_assoc()) {
                            echo "<tr>";
                            echo "<td width='2%'>" . $row["id"] . "</td>";
                            echo "<td width='16%'>" . $row["category"] . "</td>";
```

```
              echo "<td width='4%' style='color:maroon;background:
whitesmoke;text-align: center;font-weight: bolder'>" . $row["user_score"] . "</td>";
              echo "<td width='78%'>" . $row["recommendations"] . "</td>";
              echo "</tr>";
            }
          } else {
            echo "<span style='font-weight: normal;color:red;'> Sorry There are no
Recommendations</span>";
          }
          ?>
        </table>
      </div>
    </div>
  </div>

<script src="js/jquery-1.10.2.js"></script>
<script src="js/jquery.dataTables.min.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/buttons.flash.min.js"></script>
<script src="js/buttons.html5.min..js"></script>
<script src="js/buttons.print.min.js"></script>
<script src="js/dataTables.buttons.min.js"></script>
<script src="js/jszip.min.js"></script>
<script src="js/pdfmake.min.js"></script>
<script src="js/vfs_fonts.js"></script>
  <script>$(document).ready(function() {
      $('#recommendations_table').DataTable( {
        dom: 'Bfrtip',
        buttons: [
          'excel', 'csv', 'pdf', 'print'
        ]
      } );
    } );
  </script>
</body>
</html>
```

CODE FOR MATURITY SCORES

```
<?php
  session_start();
  if(!isset($_SESSION['usr_id'])) {
    header("Location: index.php");
  }
  include_once 'dbconnect.php';
?>

<!DOCTYPE html>
<html>
<head>
```

```
        <title>UISM | User Maturity Scores</title>
        <meta content="width=device-width, initial-scale=1.0" name="viewport" >
        <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
        <link rel="stylesheet" href="css/style.css" type="text/css" />
</head>
<body style="background-image: url('images/bg.jpg');">

  <?php include 'topnav.php'?>
  <?php include 'sidenav.php' ?>

  <div class="container">
    <div class="row">
      <div class="col-md-10" style="margin-top:6%;margin-left: 15%;box-shadow:
3px 2px 8px 0px black;background: white;">
        <h4 style="font-style: oblique"><i class="fa fa-fire"></i> Maturity Scores
<span class="badge"> Average: <?php include "average_score.php";?></span></h4>
        <a class="btn btn-primary btn-xs pull-right" href="home.php"><i class="fa
fa-angle-double-left"></i> Back Home</i></a>
        <hr>
        <table class="table table-condensed table-hover" id="scores_table">
          <?php
          $user_id = $_SESSION['usr_id'];
          $sql = "select distinct(a.id),a.questions,b.transaction_date,b.user_score
from maturity_questions a
              inner join maturity_assessment b on a.id=b.question_id inner join
users c on b.user_id=c.id
              where c.id=$user_id;";
          $result = $con->query($sql);
          if ($result->num_rows > 0) {
            echo "<thead>
                  <tr>
                    <th>ID</th>
                    <th>Question</th>
                    <th>Date</th>
                    <th style='background: whitesmoke'>AvgScore</th>
                  </tr>
                </thead>";
            while($row = $result->fetch_assoc()) {
              echo "<tr>";
              echo "<td width='2%'>" . $row["id"] . "</td>";
              echo "<td width='80%'>" . $row["questions"] . "</td>";
              echo "<td width='16%'>" . $row["transaction_date"] . "</td>";
              echo "<td width='2%' style='color:maroon;background:
whitesmoke;text-align: center;font-weight: bolder'>" . $row["user_score"] . "</td>";
              echo "</tr>";
            }
          } else {
            echo "<span style='font-weight: normal;color:red;'> Sorry There are no
Maturity Assessment Scores</span>";
          }
          ?>
        </table>
      </div>
    </div>
  </div>

<script src="js/jquery-1.10.2.js"></script>
<script src="js/jquery.dataTables.min.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/buttons.flash.min.js"></script>
<script src="js/buttons.html5.min..js"></script>
<script src="js/buttons.print.min.js"></script>
<script src="js/dataTables.buttons.min.js"></script>
<script src="js/jszip.min.js"></script>
<script src="js/pdfmake.min.js"></script>
<script src="js/vfs_fonts.js"></script>
<script>$(document).ready(function() {
    $('#scores_table').DataTable( {
      dom: 'Bfrtip',
      buttons: [
        'excel', 'csv', 'pdf', 'print'
      ]
    } );
  } );
</script>
</body>
</html>
```

CODE SNIPPET FOR USER REGISTRATION

```
<?php
session_start();

if(isset($_SESSION['usr_id'])) {
        header("Location: home.php");
}
include_once 'dbconnect.php';

//set validation error flag as false
$error = false;

//check if form is submitted
if (isset($_POST['signup'])) {
        $name = mysqli_real_escape_string($con, $_POST['name']);
        $email = mysqli_real_escape_string($con, $_POST['email']);
        $organization = mysqli_real_escape_string($con, $_POST['organization']);
        $password = mysqli_real_escape_string($con, $_POST['password']);
        $cpassword = mysqli_real_escape_string($con, $_POST['cpassword']);

        //name can contain only alpha characters and space
```

```
		if (!preg_match("/^[a-zA-Z ]+$/",$name)) {
			$error = true;
			$name_error = "Name must contain only alphabets and space";
		}
		if(!filter_var($email,FILTER_VALIDATE_EMAIL)) {
			$error = true;
			$email_error = "Please Enter Valid Email ID";
		}
   if(!preg_match("/^[a-zA-Z ]+$/",$organization)) {
      $error = true;
      $organization_error = "Please Enter Valid Organization";
   }
		if(strlen($password) < 6) {
			$error = true;
			$password_error = "Password must be minimum of 6
characters";
		}
		if($password != $cpassword) {
			$error = true;
			$cpassword_error = "Password and Confirm Password doesn't
match";
		}
		if (!$error) {
			if(mysqli_query($con, "INSERT INTO
users(name,email,organization,password) VALUES('" . $name . "', '" . $email . "','" .
$organization . "', '" . sha1($password) . "')")) {
				$successmsg = "Successfully Registered! <a
href='index.php'>Click here to Login</a>";
			} else {
				$errormsg = "Error in registering...Please try again
later!";
			}
		}
}
?>

<!DOCTYPE html>
<html>
<head>
		<title>UISM | Registration</title>
		<meta content="width=device-width, initial-scale=1.0" name="viewport" >
		<link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
</head>
<body style="background-image: url('images/bg.jpg');">


<br><br><br>

<div class="container">
		<div class="row">
```

```
                        <div class="col-md-4 col-md-offset-4" style="box-shadow: 3px
2px 8px 0px black; padding: 20px;border-radius: 4px 4px 0 0;background: white;">
                                <form role="form" action="<?php echo
$_SERVER['PHP_SELF']; ?>" method="post" name="signupform">
                                        <fieldset>
                                                <legend>Register to
UISM</legend>

                                                <div class="form-group">
                                                        <label
for="name">Name</label>
                                                        <input type="text"
name="name" placeholder="Enter Full Name" required value="<?php if($error) echo
$name; ?>" class="form-control" />
                                                        <span class="text-
danger"><?php if (isset($name_error)) echo $name_error; ?></span>
                                                </div>

                                                <div class="form-group">
                                                        <label
for="name">Email</label>
                                                        <input type="text"
name="email" placeholder="Email" required value="<?php if($error) echo $email;
?>" class="form-control" />
                                                        <span class="text-
danger"><?php if (isset($email_error)) echo $email_error; ?></span>
                                                </div>

                  <div class="form-group">
                     <label for="name">Organization</label>
                     <input type="text" name="organization" placeholder="Enter
Organization" required value="<?php if($error) echo $organization; ?>" class="form-
control"  autocomplete="off"/>
                     <span class="text-danger"><?php if (isset($organization_error)) echo
$organization_error; ?></span>
                  </div>

                                                <div class="form-group">
                                                        <label
for="name">Password</label>
                                                        <input
type="password" name="password" placeholder="Password" required class="form-
control" />
                                                        <span class="text-
danger"><?php if (isset($password_error)) echo $password_error; ?></span>
                                                </div>

                                                <div class="form-group">
                                                        <label
for="name">Confirm Password</label>
```

```
              <input type="password" name="cpassword" placeholder="Confirm
Password" required class="form-control" />
                                                <span class="text-
danger"><?php if (isset($cpassword_error)) echo $cpassword_error; ?></span>
                                        </div>

                                        <div class="form-group">
                                                </i><input
type="submit" name="signup" value="Register" class="btn btn-primary" />
                                        </div>
                                </fieldset>
                        </form>
                        <span class="text-success"><?php if
(isset($successmsg)) { echo $successmsg; } ?></span>
                        <span class="text-danger"><?php if (isset($errormsg))
{ echo $errormsg; } ?></span>
                </div>
        </div>
        <div class="row">
                <a class="col-md-4 col-md-offset-4 text-center btn btn-primary"
href="index.php" style="box-shadow: 3px 2px 8px 0px black">Login Here if you
already Registered</a>
        </div>
</div>
<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
</body>
</html>
```

CODE FOR UISM COMPUTATION

```
<?php
//      if(!isset($_SESSION['usr_id'])) {
//              header("Location: index.php");
//      }
        include_once 'dbconnect.php';
        $user_id = $_SESSION['usr_id'];
        //$sql = "SELECT
ROUND(100*((0.285+SUM(user_score*weight))/(0.285+SUM(5*weight))),0)
FROM `maturity_assessment`WHERE user_id='$user_id' ";
        $sql = "SELECT ROUND(100*((-2.128+SUM(user_score*weight))/(-
2.128+SUM(5*weight))),1) FROM `maturity_assessment`WHERE user_id='$user_id'
";
        $result = mysqli_query($con,$sql);
        $data = mysqli_fetch_array($result);
        $uism = $data[0];

        if($uism == 0){
                echo 0;
        }else{
                echo $uism;
```

```
            }

?>

HP
<?php
   session_start();
   if(!isset($_SESSION['usr_id'])) {
      header("Location: index.php");
   }
   include_once 'dbconnect.php';
?>

<!DOCTYPE html>
<html>
<head>
            <title>UISM | Home</title>
            <meta content="width=device-width, initial-scale=1.0" name="viewport" >
            <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
            <link rel="stylesheet" href="css/style.css" type="text/css" />
            <link rel="stylesheet" href="css/gauge.css" type="text/css" />
</head>
<body style="background-image: url('images/bg.jpg');background-attachment:
fixed;">

   <?php include 'topnav.php'?>
   <?php include 'sidenav.php' ?>
   <div class="container">
      <div class="row" style="margin-top: 5%;margin-left: 8.5%; background:
white;padding: 10px;width: 100%;">
         <div class="col-md-12">
            <span class="fa fa-fire"></span>
            <p style="font-family:Helvetica;font-weight: normal;font-style:
oblique;text-align: center;">Welcome to UISM Platform. The platform Helps you to
assess the level of maturity of your Institution in terms of information security.
            <br>It is based on the robust ISO 27001 Framework of Information
Security.</p>
            <hr>
            <div class="row justify-content-center" style="background:
#f8f8f8;padding: 6px;">
               <div class="col-md-3" style="color: red;font-weight:
bolder;"><h4>Statistics <i class="fa fa-angle-double-right"></i></h4> </div>
               <div class="col-sm-3">
                  <a href="maturity_recommendations.php" class="" style="display:
inline-block;">Recommendations <span class="badge"><?php include
'count_recommendations.php'?></span></a><br>
               </div>
               <div class="col-sm-3">
```

```
          <a href="#" class="" style="display: inline-block;"> Number of
Assessments Done <span class="badge"><?php include
"count_assessmentsdone.php"?></span></a><br>
        </div>
        <div class="col-sm-3">
          <a href="maturity_scores.php" class="" style="display: inline-
block">Average Score <span class="badge"><?php include
"average_score.php";?></span></a>
        </div>
      </div>
      <div class="row"><hr>
        <div class="col-md-4" style="border-right: 1px dotted maroon;padding-
right: 10px;">
          <h4 style="text-align: center;"> Maturity Index </h4>
          <hr>
<!--             BEGINNING OF GAUGE-->
          <div class="container A">
            <svg class="typeRange" height="165" width="330" view-box="0 0
330 165">

              <g class="scale" stroke="red"></g>

              <path class="outline" d="" />
              <path class="fill" d="" />
              <polygon class="needle" points="220,10 300,210 220,250
140,210" />
            </svg>
            <div class="output">30</div>
          </div>
          <p style="font-style: oblique;text-align: center;"><span style="color:
red;font-weight: bolder"><?php include 'uism.php'?>%</span> Mature</p>

          <input type="text" class="initialValue" value="<?php include
'uism.php'?>" hidden />
<!--             ENDING OF GAUGE-->
        </div>
        <div class="col-md-7 pull-right" style="">
          <div class="col-md-12">
            <h5 class="bg-info" style="padding: 5px; font-weight:
bolder">Quick Actions</h5>
            <ul style="list-style-type: none;">
              <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="assessments.php"><h5><i class="fa fa-fire"></i> Run
New Maturity Assessment</h5></a></li>
              <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="maturity_scores.php"><h5><i class="fa fa-fire"></i>
View your Scores Report</h5></a></li>
              <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="maturity_recommendations.php"><h5><i class="fa fa-
fire"></i> View your Recommendations Report <span class="badge"
```

```
style="background:                    darkred"><?php                    include
'count_recommendations.php'?></span></h5></a></li>
                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px  dotted  green;"><a  href="help.php"><h5><i  class="fa  fa-fire"></i>  Obtain
Help</h5></a></li>
                <li     style="padding-top:     2px;padding-bottom:     2px;"><a
href="logout.php"><h5><i class="fa fa-fire"></i> Logout</h5></a></li>
              </ul>
            </div>
            <div class="col-md-12">
              <a href="clear_assessments.php" class="btn btn-block btn-warning"
onclick="return  confirm('Are  you  sure  you  want  to  Clear?');"><i  class="fa  fa-
trash"></i>
                Clear all your previous Scores</a>
            </div>

          </div>
        </div>

      </div>
    </div>
  </div>

<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/gauge.js"></script>
</body>
</html>

<?php
  session_start();
  if(!isset($_SESSION['usr_id'])) {
    header("Location: index.php");
  }
  include_once 'dbconnect.php';
?>

<!DOCTYPE html>
<html>
<head>
        <title>UISM | Home</title>
        <meta content="width=device-width, initial-scale=1.0" name="viewport" >
        <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
        <link rel="stylesheet" href="css/style.css" type="text/css" />
        <link rel="stylesheet" href="css/gauge.css" type="text/css" />
</head>
<body      style="background-image:      url('images/bg.jpg');background-attachment:
fixed;">

  <?php include 'topnav.php'?>
```

```
    <?php include 'sidenav.php' ?>
    <div class="container">
       <div class="row" style="margin-top: 5%;margin-left: 8.5%; background:
white;padding: 10px;width: 100%;">
          <div class="col-md-12">
             <span class="fa fa-fire"></span>
             <p style="font-family:Helvetica;font-weight: normal;font-style:
oblique;text-align: center;">Welcome to UISM Platform. The platform Helps you to
assess the level of maturity of your Institution in terms of information security.
             <br>It is based on the robust ISO 27001 Framework of Information
Security.</p>
             <hr>
             <div class="row justify-content-center" style="background:
#f8f8f8;padding: 6px;">
                <div class="col-md-3" style="color: red;font-weight:
bolder;"><h4>Statistics <i class="fa fa-angle-double-right"></i></h4> </div>
                <div class="col-sm-3">
                   <a href="maturity_recommendations.php" class="" style="display:
inline-block;">Recommendations <span class="badge"><?php include
'count_recommendations.php'?></span></a><br>
                </div>
                <div class="col-sm-3">
                   <a href="#" class="" style="display: inline-block;"> Number of
Assessments Done <span class="badge"><?php include
"count_assessmentsdone.php"?></span></a><br>
                </div>
                <div class="col-sm-3">
                   <a href="maturity_scores.php" class="" style="display: inline-
block">Average Score <span class="badge"><?php include
"average_score.php";?></span></a>
                </div>
             </div>
             <div class="row"><hr>
                <div class="col-md-4" style="border-right: 1px dotted maroon;padding-
right: 10px;">
                   <h4 style="text-align: center;"> Maturity Index </h4>
                   <hr>
<!--               BEGINNING OF GAUGE-->
                   <div class="container A">
                      <svg class="typeRange" height="165" width="330" view-box="0 0
330 165">

                         <g class="scale" stroke="red"></g>

                         <path class="outline" d="" />
                         <path class="fill" d="" />
                         <polygon class="needle" points="220,10 300,210 220,250
140,210" />
                      </svg>
                      <div class="output">30</div>
```

```
            </div>
            <p style="font-style: oblique;text-align: center;"><span style="color:
red;font-weight: bolder"><?php include 'uism.php'?>%</span> Mature</p>

            <input type="text" class="initialValue" value="<?php include
'uism.php'?>" hidden />
<!--              ENDING OF GAUGE-->
          </div>
          <div class="col-md-7 pull-right" style="">
            <div class="col-md-12">
              <h5 class="bg-info" style="padding: 5px; font-weight:
bolder">Quick Actions</h5>
              <ul style="list-style-type: none;">
                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="assessments.php"><h5><i class="fa fa-fire"></i> Run
New Maturity Assessment</h5></a></li>
                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="maturity_scores.php"><h5><i class="fa fa-fire"></i>
View your Scores Report</h5></a></li>
                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="maturity_recommendations.php"><h5><i class="fa fa-
fire"></i> View your Recommendations Report <span class="badge"
style="background: darkred"><?php include
'count_recommendations.php'?></span></h5></a></li>
                <li style="padding-top: 2px;padding-bottom: 2px;border-bottom:
1px dotted green;"><a href="help.php"><h5><i class="fa fa-fire"></i> Obtain
Help</h5></a></li>
                <li style="padding-top: 2px;padding-bottom: 2px;"><a
href="logout.php"><h5><i class="fa fa-fire"></i> Logout</h5></a></li>
              </ul>
            </div>
            <div class="col-md-12">
              <a href="clear_assessments.php" class="btn btn-block btn-warning"
onclick="return confirm('Are you sure you want to Clear?');"><i class="fa fa-
trash"></i>
                Clear all your previous Scores</a>
            </div>

          </div>
        </div>

      </div>
    </div>
  </div>

<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/gauge.js"></script>
</body>
</html>
```

INDEX

```
<?php
session_start();

if(isset($_SESSION['usr_id'])!="") {
        header("Location: home.php");
}
include_once 'dbconnect.php';

//check if form is submitted
if (isset($_POST['login'])) {

        $email = mysqli_real_escape_string($con, $_POST['email']);
        $password = mysqli_real_escape_string($con, $_POST['password']);
        $result = mysqli_query($con, "SELECT * FROM users WHERE email = '"
. $email. "' and password = '" . sha1($password) . "'");

        if ($row = mysqli_fetch_array($result)) {
                $_SESSION['usr_id'] = $row['id'];
                $_SESSION['usr_name'] = $row['name'];
                header("Location: home.php");
        } else {
                $errormsg = "Incorrect Email or Password!!!";
        }
}
?>

<!DOCTYPE html>
<html>
<head>
        <title>UISM | Login </title>
        <meta content="width=device-width, initial-scale=1.0" name="viewport" >
        <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
</head>
<body style="background-image: url('images/bg.jpg');">

<br><br><br><br><br>
<div class="container">
        <div class="row">
                <div class="col-md-4 col-md-offset-4" style="box-shadow: 3px
2px 8px 0px black; padding: 20px;border-radius: 4px 4px 0 0;background: white;">
                        <form role="form" action="<?php echo
$_SERVER['PHP_SELF']; ?>" method="post" name="loginform">
                                <fieldset>
                                        <legend>Login to
UISM</legend>
```

```
                    <div class="form-group">
                        <label
for="name">Email</label>
                        <input type="text"
name="email" placeholder="Your Email" required class="form-control" />
                    </div>

                    <div class="form-group">
                        <label
for="name">Password</label>
                        <input
type="password" name="password" placeholder="Your Password" required
class="form-control" />
                    </div>

                    <div class="form-group">
                        <input type="submit"
name="login" value="Login" class="btn btn-primary" />
                    </div>
                </fieldset>
            </form>

            <span class="text-danger"><?php if (isset($errormsg))
{ echo $errormsg; } ?></span>
        </div>
        <a class="btn btn-primary col-md-4 col-md-offset-4 text-center"
href="register.php" style="box-shadow: 3px 2px 8px 0px black;">Register here if you
are a new user</a>
    </div>

</div>

<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
</body>
</html>

<?php
session_start();

if(isset($_SESSION['usr_id'])!="") {
    header("Location: home.php");
}
include_once 'dbconnect.php';

//check if form is submitted
if (isset($_POST['login'])) {

    $email = mysqli_real_escape_string($con, $_POST['email']);
    $password = mysqli_real_escape_string($con, $_POST['password']);
    $result = mysqli_query($con, "SELECT * FROM users WHERE email = '"
. $email. "' and password = '" . sha1($password) . "'");

    if ($row = mysqli_fetch_array($result)) {
        $_SESSION['usr_id'] = $row['id'];
        $_SESSION['usr_name'] = $row['name'];
        header("Location: home.php");
    } else {
        $errormsg = "Incorrect Email or Password!!!";
    }
}
?>

<!DOCTYPE html>
<html>
<head>
    <title>UISM | Login </title>
    <meta content="width=device-width, initial-scale=1.0" name="viewport" >
    <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
</head>
<body style="background-image: url('images/bg.jpg');">

<br><br><br><br><br>
<div class="container">
    <div class="row">
        <div class="col-md-4 col-md-offset-4" style="box-shadow: 3px
2px 8px 0px black; padding: 20px;border-radius: 4px 4px 0 0;background: white;">
            <form role="form" action="<?php echo
$_SERVER['PHP_SELF']; ?>" method="post" name="loginform">
                <fieldset>
                    <legend>Login to
UISM</legend>


                    <div class="form-group">
                        <label
for="name">Email</label>
                        <input type="text"
name="email" placeholder="Your Email" required class="form-control" />
                    </div>

                    <div class="form-group">
                        <label
for="name">Password</label>
                        <input
type="password" name="password" placeholder="Your Password" required
class="form-control" />
                    </div>

                    <div class="form-group">
```

```
                                                    <input type="submit"
name="login" value="Login" class="btn btn-primary" />
                                              </div>
                                        </fieldset>
                                  </form>

                                  <span class="text-danger"><?php if (isset($errormsg))
{ echo $errormsg; } ?></span>
                            </div>
                            <a class="btn btn-primary col-md-4 col-md-offset-4 text-center"
href="register.php" style="box-shadow: 3px 2px 8px 0px black;">Register here if you
are a new user</a>
               </div>

</div>

<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
</body>
</html>
```

NAVIGATION CODES

(B) TOP MENU

```
<div style="position: fixed;width: 100%;display: inline-block;z-index: 1;border-
bottom: 3px solid maroon;height: 8.9%;">
  <nav class="navbar navbar-default" role="navigation">
    <div class="container-fluid">
      <div class="navbar-header">
        <button type="button" class="navbar-toggle" data-toggle="collapse" data-
target="#navbar1">
          <span class="sr-only">Toggle navigation</span>
          <span class="icon-bar"></span>
          <span class="icon-bar"></span>
          <span class="icon-bar"></span>
        </button>
        <a class="navbar-brand" href="home.php">UISM </a>
      </div>
      <div class="collapse navbar-collapse" id="navbar1">
        <ul class="nav navbar-nav navbar-right">
          <?php if (isset($_SESSION['usr_id'])) { ?>
            <li><p class="navbar-text"><i class="fa fa-user"></i> Current User:
<?php echo $_SESSION['usr_name']; ?></p></li>
            <li><a href="logout.php"><i class="fa fa-sign-out"></i> Log
Out</a></li>
          <?php } else { ?>
            <li><a href="index.php">Login</a></li>
            <li><a href="register.php">Sign Up</a></li>
          <?php } ?>
```

```
                </ul>
            </div>
        </div>
    </nav>
</div>
```

(C) **SIDE MENU**

```
<nav class="navbar navbar-default sidebar" role="navigation" style="display: inline-block;position: fixed;">
    <div class="container-fluid">
        <!-- Brand and toggle get grouped for better mobile display -->
        <div class="navbar-header">
            <button type="button" class="navbar-toggle" data-toggle="collapse" data-target="#bs-sidebar-navbar-collapse-1">
                <span class="sr-only">Toggle navigation</span>
                <span class="icon-bar"></span>
                <span class="icon-bar"></span>
                <span class="icon-bar"></span>
            </button>
            <a class="navbar-brand" href="home.php" style="color: #2b542c;font-weight: bolder;font-size: large;"><i class="fa fa-fire"></i> UISM Platform</a>
        </div>
        <!-- Collect the nav links, forms, and other content for toggling -->
        <div class="collapse navbar-collapse" id="bs-sidebar-navbar-collapse-1">
            <ul class="nav navbar-nav">
                <li class="active"><a href="home.php">Dashboard<span style="font-size:16px;" class="pull-right hidden-xs showopacity fa fa-home"></span></a></li>
                <li ><a href="assessments.php">Maturity Assessment<span style="font-size:16px;" class="pull-right hidden-xs showopacity fa fa-list"></span></a></li>
                 <li class="dropdown">
                    <a href="#" class="dropdown-toggle" data-toggle="dropdown">Reports <span class="caret"></span><span style="font-size:16px;" class="pull-right hidden-xs showopacity fa fa-bars"></span></a>
                    <ul class="dropdown-menu forAnimate" role="menu">
                        <li><a href="maturity_scores.php">Maturity Scores <i class="fa fa-check"></i></a></li>
                        <li class="divider"></li>
                        <li><a href="maturity_recommendations.php">Recommendations <i class="fa fa-file"></i></a></li>
                    </ul>
                </li>
                <li ><a href="help.php">Help<span style="font-size:16px;" class="pull-right hidden-xs showopacity fa  fa-question-circle"></span></a></li>
                <li ><a href="logout.php">Logout<span style="font-size:16px;" class="pull-right hidden-xs showopacity fa fa-sign-out"></span></a></li>
            </ul>

            <div style="text-align: center;float: bottom;font-weight: bold;color: #2a6496;">
            <span> <h1 class="fa fa-fire"></h1><br>© Daniel Makupi <br>PHD
Student <br> KABARAK UNIVERSITY </span>
         </div>
      </div>
   </div>
</nav>
```

LANDING PAGE

```
<?php
session_start();

if(isset($_SESSION['usr_id'])!="") {
            header("Location: home.php");
}
include_once 'dbconnect.php';

//check if form is submitted
if (isset($_POST['login'])) {

            $email = mysqli_real_escape_string($con, $_POST['email']);
            $password = mysqli_real_escape_string($con, $_POST['password']);
            $result = mysqli_query($con, "SELECT * FROM users WHERE email = '"
. $email. "' and password = '" . sha1($password) . "'");

            if ($row = mysqli_fetch_array($result)) {
                        $_SESSION['usr_id'] = $row['id'];
                        $_SESSION['usr_name'] = $row['name'];
                        header("Location: home.php");
            } else {
                        $errormsg = "Incorrect Email or Password!!!";
            }
}
?>

<!DOCTYPE html>
<html>
<head>
            <title>UISM | Login </title>
            <meta content="width=device-width, initial-scale=1.0" name="viewport" >
            <link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
</head>
<body style="background-image: url('images/bg.jpg');">

<br><br><br><br><br>
<div class="container">
            <div class="row">
                        <div class="col-md-4 col-md-offset-4" style="box-shadow: 3px
2px 8px 0px black; padding: 20px;border-radius: 4px 4px 0 0;background: white;">
```

```
                        <form role="form" action="<?php echo
$_SERVER['PHP_SELF']; ?>" method="post" name="loginform">
                                <fieldset>
                                        <legend>Login to
UISM</legend>

                                        <div class="form-group">
                                                <label
for="name">Email</label>
                                                <input type="text"
name="email" placeholder="Your Email" required class="form-control" />
                                        </div>


                                        <div class="form-group">
                                                <label
for="name">Password</label>
                                                <input
type="password" name="password" placeholder="Your Password" required
class="form-control" />
                                        </div>


                                        <div class="form-group">
                                                <input type="submit"
name="login" value="Login" class="btn btn-primary" />
                                        </div>
                                </fieldset>
                        </form>

                        <span class="text-danger"><?php if (isset($errormsg))
{ echo $errormsg; } ?></span>
                </div>
                <a class="btn btn-primary col-md-4 col-md-offset-4 text-center"
href="register.php" style="box-shadow: 3px 2px 8px 0px black;">Register here if you
are a new user</a>
        </div>

</div>

<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
</body>
</html>
```

CASCADING STYLE SHEETS

(A) GAUGE

```
/*GREENS: #4ac4ac, #399988, #0f4534, #0a1a17;*/
.output {
  line-height: 35px;
  width: 60px;
```

```
   height: 30px;
   background-color: black;
   color:white;
   border-radius: 60px 60px 0 0;
   position: absolute;
   top: 205px;
   left: 160px;
   text-align: center;
}

.initialValue {
   border: none;
   border-bottom: 1px solid #399988;
   color: #399988;
   display: block;
   width: 3em;
   background-color: transparent;
   margin: 1em auto;
   outline: none;
   font-size: 16px;
   text-align: center;
}
/*SVG*/

svg {
   margin: 0px;
   padding: 0;
   cursor: pointer;
}

svg.focusable {
   border: 1px solid #0f4534;
}

.outline,
.fill,
.center,
.needle,
.scale,
.output {
   pointer-events: none;
}

.outline {
   fill: darkred;
}

.fill {
   fill: green;
}
```

```
.needle {
   fill: #000000;
}

.scale {
   stroke: #aaa;
}

text {
   text-anchor: middle;
   dominant-baseline: alphabetic;
   font: 12px verdana, sans-serif;
   fill: #aaa;
}
```

(B) HELP

```
@import url("//cdnjs.cloudflare.com/ajax/libs/font-awesome/4.0.3/css/font-awesome.min.css");
.menu {
   position: fixed;
   top: 9%;
   left: 0;
   height: 90%;
   list-style-type: none;
   margin: 0;
   padding: 0;
   background: #fff4f5;
}
.menu li a{
   display:block;
   /*height:1em;*/
   width:4em;
   text-indent:-500em;
   line-height:4em;
   text-align:center;
   color: #000080;
   background: #fff4f5;
   position: relative;
   border-bottom: 1px dotted #000080;
   transition: background 0.3s ease-in-out;
}
.menu li a:before {
   font-family: FontAwesome;
   speak: none;
   text-indent: 0em;
   position: absolute;
   top: 0;
   left: 0;
   width: 100%;
   height: 100%;
   font-size: 1em;
}
.menu li a.search:before {
   content: "\f002";
}
.menu li a.archive:before {
   content: "\f187";
}
.menu li a.pencil:before {
   content: "\f040";
}
.menu li a.contact:before {
   content: "\f003";
}
.menu li a.about:before {
   content: "\f007";
}
.menu li a.home:before {
   content: "\f015";
}
.menu li a:hover{
   background: #10ceff;
   color: #fff;
}
.menu li.current a {
   background: #10ceff;
   color: #fff;
}
.menu li a.active {
   background: #10ceff;
   color: #fff;
}
.menu li a.active:after{
   position:absolute;
   left:4em;
   top:0;
   content:"";
   border:2.5em solid transparent;
   border-left-color:#10ceff;
   border-width: 2em 1em
}
.menu li{
   position:relative;
}
.menu li:after{
   content: attr(title);
   position:absolute;
```

```
    left:4em;
    top:0;
    height:4em;
    -webkit-box-sizing: border-box;
    -moz-box-sizing: border-box;
    box-sizing: border-box;
    text-transform:uppercase;
    background: #10ceff;
    padding:2em;
    transition: all 0.3s ease-in-out;
    visibility:hidden;
    opacity:0;
}
.menu li:hover:after{
    visibility:visible;
    opacity:1;
}
@media screen and (max-height: 34em){
    .menu li{
        font-size:70%;
    }
}


.stepwizard-step p {
    margin-top: 10px;
}

.stepwizard-row {
    display: table-row;
}

.stepwizard {
    display: table;
    width: 100%;
    position: relative;
}

.stepwizard-step button[disabled] {
    opacity: 1 !important;
    filter: alpha(opacity=100) !important;
}

.stepwizard-row:before {
    top: 14px;
    bottom: 0;
    position: absolute;
    content: " ";
    width: 100%;
    height: 1px;
```

```
   background-color: #ccc;
   z-order: 0;

}

.stepwizard-step {
   display: table-cell;
   text-align: center;
   position: relative;
}

.btn-circle {
   width: 30px;
   height: 30px;
   text-align: center;
   padding: 6px 0;
   font-size: 12px;
   line-height: 1.428571429;
   border-radius: 15px;
}
/* */

/* remove outer padding */
.main .row{
   padding: 0px;
   margin: 0px;
}

/*Remove rounded coners*/

nav.sidebar.navbar {
   border-radius: 0px;
}

nav.sidebar, .main{
   -webkit-transition: margin 200ms ease-out;
   -moz-transition: margin 200ms ease-out;
   -o-transition: margin 200ms ease-out;
   transition: margin 200ms ease-out;
}

/* Add gap to nav and right windows.*/
.main{
   padding: 10px 10px 0 10px;
}

/* .....NavBar: Icon only with coloring/layout.....*/

/*small/medium side display*/
@media (min-width: 768px) {
```

```
/*Allow main to be next to Nav*/
.main{
   position: absolute;
   width: calc(100% - 40px); /*keeps 100% minus nav size*/
   margin-left: 40px;
   float: right;
}

/*lets nav bar to be showed on mouseover*/
nav.sidebar:hover + .main{
   margin-left: 200px;
}

/*Center Brand*/
nav.sidebar.navbar.sidebar>.container   .navbar-brand,   .navbar>.container-fluid
.navbar-brand {
   margin-left: 0px;
}
/*Center Brand*/
nav.sidebar .navbar-brand, nav.sidebar .navbar-header{
   text-align: center;
   width: 100%;
   margin-left: 0px;
}

/*Center Icons*/
nav.sidebar a{
   padding-right: 13px;
}

/*adds border top to first nav box */
nav.sidebar .navbar-nav > li:first-child{
   border-top: 1px #e5e5e5 solid;
}

/*adds border to bottom nav boxes*/
nav.sidebar .navbar-nav > li{
   border-bottom: 1px #e5e5e5 solid;
}

/* Colors/style dropdown box*/
nav.sidebar .navbar-nav .open .dropdown-menu {
   position: static;
   float: none;
   width: auto;
   margin-top: 0;
   background-color: transparent;
   border: 0;
   -webkit-box-shadow: none;
```

```
        box-shadow: none;
    }

    /*allows nav box to use 100% width*/
    nav.sidebar .navbar-collapse, nav.sidebar .container-fluid{
        padding: 0 0px 0 0px;
    }

    /*colors dropdown box text */
    .navbar-inverse .navbar-nav .open .dropdown-menu>li>a {
        color: #777;
    }

    /*gives sidebar width/height*/
    nav.sidebar{
        width: 200px;
        height: 100%;
        margin-left: -160px;
        float: left;
        z-index: 8000;
        margin-bottom: 0px;
    }

    /*give sidebar 100% width;*/
    nav.sidebar li {
        width: 100%;
    }

    /* Move nav to full on mouse over*/
    nav.sidebar:hover{
        margin-left: 0px;
    }
    /*for hiden things when navbar hidden*/
    .forAnimate{
        opacity: 0;
    }
}

/* .....NavBar: Fully showing nav bar..... */

@media (min-width: 1330px) {

    /*Allow main to be next to Nav*/
    .main{
        width: calc(100% - 200px); /*keeps 100% minus nav size*/
        margin-left: 200px;
    }

    /*Show all nav*/
    nav.sidebar{
        margin-left: 0px;
        float: left;
    }
    /*Show hidden items on nav*/
    nav.sidebar .forAnimate{
        opacity: 1;
    }
}

nav.sidebar .navbar-nav .open .dropdown-menu>li>a:hover, nav.sidebar .navbar-nav
.open .dropdown-menu>li>a:focus {
    color: #CCC;
    background-color: transparent;
}

nav:hover .forAnimate{
    opacity: 1;
}
section{
    padding-left: 15px;
}
```

STYLES1

```
@import url("//cdnjs.cloudflare.com/ajax/libs/font-awesome/4.0.3/css/font-
awesome.min.css");
.menu {
    position: fixed;
    top: 9%;
    left: 0;
    height: 90%;
    list-style-type: none;
    margin: 0;
    padding: 0;
    background: #fff4f5;
}
.menu li a{
    display:block;
    /*height:1em;*/
    width:4em;
    text-indent:-500em;
    line-height:4em;
    text-align:center;
    color: #000080;
    background: #fff4f5;
    position: relative;
    border-bottom: 1px dotted #000080;
    transition: background 0.3s ease-in-out;
}
.menu li a:before {
    font-family: FontAwesome;
    speak: none;
    text-indent: 0em;
    position: absolute;
    top: 0;
    left: 0;
    width: 100%;
    height: 100%;
    font-size: 1em;
}
.menu li a.search:before {
    content: "\f002";
}
.menu li a.archive:before {
    content: "\f187";
}
.menu li a.pencil:before {
    content: "\f040";
}
.menu li a.contact:before {
    content: "\f003";
}
.menu li a.about:before {
    content: "\f007";
}
.menu li a.home:before {
    content: "\f015";
}
.menu li a:hover{
    background: #10ceff;
    color: #fff;
}
.menu li.current a {
    background: #10ceff;
    color: #fff;
}
.menu li a.active {
    background: #10ceff;
    color: #fff;
}
.menu li a.active:after{
    position:absolute;
    left:4em;
    top:0;
    content:"";
    border:2.5em solid transparent;
    border-left-color:#10ceff;
    border-width: 2em 1em
}
.menu li{
    position:relative;
}
.menu li:after{
    content: attr(title);
    position:absolute;
    left:4em;
    top:0;
    height:4em;
    -webkit-box-sizing: border-box;
    -moz-box-sizing: border-box;
    box-sizing: border-box;
    text-transform:uppercase;
    background: #10ceff;
    padding:2em;
    transition: all 0.3s ease-in-out;
    visibility:hidden;
    opacity:0;
}
.menu li:hover:after{
    visibility:visible;
    opacity:1;
}
@media screen and (max-height: 34em){
    .menu li{
       font-size:70%;
    }
}


.stepwizard-step p {
    margin-top: 10px;
}

.stepwizard-row {
    display: table-row;
}

.stepwizard {
    display: table;
    width: 100%;
    position: relative;
}

.stepwizard-step button[disabled] {
    opacity: 1 !important;
    filter: alpha(opacity=100) !important;
}

.stepwizard-row:before {
    top: 14px;
```

```
    bottom: 0;
    position: absolute;
    content: " ";
    width: 100%;
    height: 1px;
    background-color: #ccc;
    z-order: 0;

}

.stepwizard-step {
    display: table-cell;
    text-align: center;
    position: relative;
}

.btn-circle {
    width: 30px;
    height: 30px;
    text-align: center;
    padding: 6px 0;
    font-size: 12px;
    line-height: 1.428571429;
    border-radius: 15px;
}
/*ghsfdddddddddddddddddddddddddddddddddddddddddddddddddddd*/

/* remove outer padding */
.main .row{
    padding: 0px;
    margin: 0px;
}

/*Remove rounded coners*/

nav.sidebar.navbar {
    border-radius: 0px;
}

nav.sidebar, .main{
    -webkit-transition: margin 200ms ease-out;
    -moz-transition: margin 200ms ease-out;
    -o-transition: margin 200ms ease-out;
    transition: margin 200ms ease-out;
}

/* Add gap to nav and right windows.*/
.main{
    padding: 10px 10px 0 10px;
}
```

```
/* .....NavBar: Icon only with coloring/layout.....*/

/*small/medium side display*/
@media (min-width: 768px) {

  /*Allow main to be next to Nav*/
  .main{
    position: absolute;
    width: calc(100% - 40px); /*keeps 100% minus nav size*/
    margin-left: 40px;
    float: right;
  }

  /*lets nav bar to be showed on mouseover*/
  nav.sidebar:hover + .main{
    margin-left: 200px;
  }

  /*Center Brand*/
  nav.sidebar.navbar.sidebar>.container .navbar-brand, .navbar>.container-fluid
.navbar-brand {
    margin-left: 0px;
  }
  /*Center Brand*/
  nav.sidebar .navbar-brand, nav.sidebar .navbar-header{
    text-align: center;
    width: 100%;
    margin-left: 0px;
  }

  /*Center Icons*/
  nav.sidebar a{
    padding-right: 13px;
  }

  /*adds border top to first nav box */
  nav.sidebar .navbar-nav > li:first-child{
    border-top: 1px #e5e5e5 solid;
  }

  /*adds border to bottom nav boxes*/
  nav.sidebar .navbar-nav > li{
    border-bottom: 1px #e5e5e5 solid;
  }

  /* Colors/style dropdown box*/
  nav.sidebar .navbar-nav .open .dropdown-menu {
    position: static;
    float: none;
```

```
        width: auto;
        margin-top: 0;
        background-color: transparent;
        border: 0;
        -webkit-box-shadow: none;
        box-shadow: none;
    }

    /*allows nav box to use 100% width*/
    nav.sidebar .navbar-collapse, nav.sidebar .container-fluid{
        padding: 0 0px 0 0px;
    }

    /*colors dropdown box text */
    .navbar-inverse .navbar-nav .open .dropdown-menu>li>a {
        color: #777;
    }

    /*gives sidebar width/height*/
    nav.sidebar{
        width: 200px;
        height: 100%;
        margin-left: -160px;
        float: left;
        z-index: 8000;
        margin-bottom: 0px;
    }

    /*give sidebar 100% width;*/
    nav.sidebar li {
        width: 100%;
    }

    /* Move nav to full on mouse over*/
    nav.sidebar:hover{
        margin-left: 0px;
    }
    /*for hiden things when navbar hidden*/
    .forAnimate{
        opacity: 0;
    }
}

/* .....NavBar: Fully showing nav bar..... */

@media (min-width: 1330px) {

    /*Allow main to be next to Nav*/
    .main{
        width: calc(100% - 200px); /*keeps 100% minus nav size*/
        margin-left: 200px;
    }

    /*Show all nav*/
    nav.sidebar{
        margin-left: 0px;
        float: left;
    }
    /*Show hidden items on nav*/
    nav.sidebar .forAnimate{
        opacity: 1;
    }
}

nav.sidebar .navbar-nav .open .dropdown-menu>li>a:hover, nav.sidebar .navbar-nav
.open .dropdown-menu>li>a:focus {
    color: #CCC;
    background-color: transparent;
}

nav:hover .forAnimate{
    opacity: 1;
}
section{
    padding-left: 15px;
}

.wizard {
    margin: 5px auto;
    background: #fff;
}

.wizard .nav-tabs {
    position: relative;
    margin: 5px auto;
    margin-bottom: 0;
    border-bottom-color: #e0e0e0;
}

.wizard > div.wizard-inner {
    position: relative;
}

.connecting-line {
    height: 2px;
    background: #e0e0e0;
    position: absolute;
    width: 52%;
    margin: 0 auto;
    left: 0;
```

```
   margin-left: 10%;
   right: 0;
   top: 50%;
   z-index: 1;
}

.wizard .nav-tabs > li.active > a, .wizard .nav-tabs > li.active > a:hover, .wizard .nav-
tabs > li.active > a:focus {
   color: #555555;
   cursor: default;
   border: 0;
   border-bottom-color: transparent;
}

span.round-tab {
   width: 70px;
   height: 70px;
   line-height: 70px;
   display: inline-block;
   border-radius: 100px;
   background: #fff;
   border: 2px solid #e0e0e0;
   z-index: 2;
   position: absolute;
   left: 0;
   text-align: center;
   font-size: 25px;
}
span.round-tab i{
   color:#555555;
}
.wizard li.active span.round-tab {
   background: lightcyan;
   border: 2px solid #5bc0de;

}
.wizard li.active span.round-tab i{
   color: #5bc0de;
}

span.round-tab:hover {
   color: #333;
   border: 2px solid #333;
}

.wizard .nav-tabs > li {
   width: 25%;
}

.wizard li:after {
   content: " ";
   position: absolute;
   left: 46%;
   opacity: 0;
   margin: 0 auto;
   bottom: 0px;
   border: 5px solid transparent;
   border-bottom-color: #5bc0de;
   transition: 0.1s ease-in-out;
}

.wizard li.active:after {
   content: " ";
   position: absolute;
   left: 46%;
   opacity: 1;
   margin: 0 auto;
   bottom: 0px;
   border: 10px solid transparent;
   border-bottom-color: #5bc0de;
}

.wizard .nav-tabs > li a {
   width: 70px;
   height: 70px;
   margin: 20px auto;
   border-radius: 100%;
   padding: 0;
}

.wizard .nav-tabs > li a:hover {
   background: transparent;
}

.wizard .tab-pane {
   position: relative;
   padding-top: 50px;
}

.wizard h3 {
   margin-top: 0;
}
.step1 .row {
   margin-bottom:10px;
}
.step_21 {
   border :1px solid #eee;
   border-radius:5px;
   padding:10px;
}
```

```
.step33 {
   border:1px solid #ccc;
   border-radius:5px;
   padding-left:10px;
   margin-bottom:10px;
}
.dropselectsec {
   width: 68%;
   padding: 6px 5px;
   border: 1px solid #ccc;
   border-radius: 3px;
   color: #333;
   margin-left: 10px;
   outline: none;
   font-weight: normal;
}
.dropselectsec1 {
   width: 74%;
   padding: 6px 5px;
   border: 1px solid #ccc;
   border-radius: 3px;
   color: #333;
   margin-left: 10px;
   outline: none;
   font-weight: normal;
}
.mar_ned {
   margin-bottom:10px;
}
.wdth {
   width:25%;
}
.birthdrop {
   padding: 6px 5px;
   border: 1px solid #ccc;
   border-radius: 3px;
   color: #333;
   margin-left: 10px;
   width: 16%;
   outline: 0;
   font-weight: normal;
}


/* according menu */
#accordion-container {
   font-size:13px
}
.accordion-header {
   font-size:13px;
```

```
    background:#ebebeb;
    margin:5px 0 0;
    padding:7px 20px;
    cursor:pointer;
    color:#fff;
    font-weight:400;
    -moz-border-radius:5px;
    -webkit-border-radius:5px;
    border-radius:5px
}
.unselect_img{
    width:18px;
    -webkit-user-select: none;
    -moz-user-select: none;
    -ms-user-select: none;
    user-select: none;
}
.active-header {
    -moz-border-radius:5px 5px 0 0;
    -webkit-border-radius:5px 5px 0 0;
    border-radius:5px 5px 0 0;
    background:#F53B27;
}
.active-header:after {
    content:"\f068";
    font-family:'FontAwesome';
    float:right;
    margin:5px;
    font-weight:400
}
.inactive-header {
    background:#333;
}
.inactive-header:after {
    content:"\f067";
    font-family:'FontAwesome';
    float:right;
    margin:4px 5px;
    font-weight:400
}
.accordion-content {
    display:none;
    padding:20px;
    background:#fff;
    border:1px solid #ccc;
    border-top:0;
    -moz-border-radius:0 0 5px 5px;
    -webkit-border-radius:0 0 5px 5px;
    border-radius:0 0 5px 5px
}
```

```
.accordion-content a{
   text-decoration:none;
   color:#333;
}
.accordion-content td{
   border-bottom:1px solid #dcdcdc;
}



@media( max-width : 585px ) {

   .wizard {
      width: 90%;
      height: auto !important;
   }

   span.round-tab {
      font-size: 16px;
      width: 50px;
      height: 50px;
      line-height: 50px;
   }

   .wizard .nav-tabs > li a {
      width: 50px;
      height: 50px;
      line-height: 50px;
   }

   .wizard li.active:after {
      content: " ";
      position: absolute;
      left: 35%;
   }
}
```

JAVASCRIPTS

(A) **GAUGE**

```
var containersRy = document.querySelector(".container");
var svg = document.querySelector(".typeRange");
var output = document.querySelector(".output");
var outline = document.querySelector(".outline");
var fill = document.querySelector(".fill");
var center = document.querySelector(".center");
var needle = document.querySelector(".needle");

var initialValue = document.querySelector(".initialValue");
var rad = Math.PI / 180;
var NS = "http:\/\/www.w3.org/2000/svg";

var W = parseInt(window.getComputedStyle(svg, null).getPropertyValue("width"));
var offset = 40;
var cx = ~~(W / 2);
var cy = 160;

var r1 = cx - offset;
var delta = ~~(r1 / 4);

var initVal = initialValue.value;

var isDragging = false;

var x1 = cx + r1,
    y1 = cy;
var r2 = r1 - delta;

var x2 = offset,
    y2 = cy;
var x3 = x1 - delta,
    y3 = cy;

function drawScale() {
    sr1 = r1 + 5;
    sr2 = r2 - 5;
    srT = r1 + 20;
    var scale = document.querySelector(".scale");
    clearRect(scale)
    var n = 0;
    for (var sa = -180; sa <= 0; sa += 18) {
        var sx1 = cx + sr1 * Math.cos(sa * rad);
        var sy1 = cy + sr1 * Math.sin(sa * rad);
        var sx2 = cx + sr2 * Math.cos(sa * rad);
        var sy2 = cy + sr2 * Math.sin(sa * rad);
        var sxT = cx + srT * Math.cos(sa * rad);
        var syT = cy + srT * Math.sin(sa * rad);

        var scaleLine = document.createElementNS(NS, "line");
        var scaleLineObj = {
            class: "scale",
            x1: sx1,
            y1: sy1,
            x2: sx2,
            y2: sy2
        };
        setSVGAttributes(scaleLine, scaleLineObj);

        scale.appendChild(scaleLine);
        var scaleText = document.createElementNS(NS, "text");
        var scaleTextObj = {
            class: "scale",
            x: sxT,
            y: syT,
        };
        setSVGAttributes(scaleText, scaleTextObj);
        scaleText.textContent = n * 10;
        scale.appendChild(scaleText);

        n++

    }

}

function drawInput(cx, cy, r1, offset, delta, a) {

    var d1 = getD1(cx, cy, r1, offset, delta);
    var d2 = getD2(cx, cy, r1, offset, delta, a);

    drawScale();

    outline.setAttributeNS(null, "d", d1);
    fill.setAttributeNS(null, "d", d2);

    drawNeedle(cx, cy, r1, a);
}

function updateInput(p, cx, cy, r1, offset, delta) {

    var x = p.x;
    var y = p.y;
    var lx = cx - x;
    var ly = cy - y;

    var a = Math.atan2(ly, lx) / rad - 180;

    drawInput(cx, cy, r1, offset, delta, a);
    output.innerHTML = Math.round((a + 180) / 1.8);
    initialValue.value = Math.round((a + 180) / 1.8);
}

function getD1(cx, cy, r1, offset, delta) {

    var x1 = cx + r1,
        y1 = cy;
    var x2 = offset,
        y2 = cy;
```

```
   var r2 = r1 - delta;
   var x3 = x1 - delta,
      y3 = cy;
   var d1 =
      "M " + x1 + ", " + y1 + " A" + r1 + "," + r1 + " 0 0 0 " + x2 + "," + y2 + " H" +
(offset + delta) + " A" + r2 + "," + r2 + " 0 0 1 " + x3 + "," + y3 + " z";
   return d1;
}

function getD2(cx, cy, r1, offset, delta, a) {
   a *= rad;
   var r2 = r1 - delta;
   var x4 = cx + r1 * Math.cos(a);
   var y4 = cy + r1 * Math.sin(a);
   var x5 = cx + r2 * Math.cos(a);
   var y5 = cy + r2 * Math.sin(a);

   var d2 =
      "M " + x4 + ", " + y4 + " A" + r1 + "," + r1 + " 0 0 0 " + x2 + "," + y2 + " H" +
(offset + delta) + " A" + r2 + "," + r2 + " 0 0 1 " + x5 + "," + y5 + " z";
   return d2;
}

function drawNeedle(cx, cy, r1, a) {

   var nx1 = cx + 5 * Math.cos((a - 90) * rad);
   var ny1 = cy + 5 * Math.sin((a - 90) * rad);

   var nx2 = cx + (r1 + 15) * Math.cos(a * rad);
   var ny2 = cy + (r1 + 15) * Math.sin(a * rad);

   var nx3 = cx + 5 * Math.cos((a + 90) * rad);
   var ny3 = cy + 5 * Math.sin((a + 90) * rad);

   var points = nx1 + "," + ny1 + " " + nx2 + "," + ny2 + " " + nx3 + "," + ny3;
   needle.setAttributeNS(null, "points", points);
}

// helpers
function oMousePos(elmt, evt) {
   var ClientRect = elmt.getBoundingClientRect();
   return { //obj
      x: Math.round(evt.clientX - ClientRect.left),
      y: Math.min(Math.round(evt.clientY - ClientRect.top), cy)
   }
}

function clearRect(node) {
   while (node.firstChild) {
      node.removeChild(node.firstChild);
   }
}

function setSVGAttributes(elmt, oAtt) {
   for (var prop in oAtt) {
      elmt.setAttributeNS(null, prop, oAtt[prop]);
   }
}

// events
window.addEventListener("load", function() {
   var pa = (initVal * 1.8) - 180;
   var p = {}
   p.x = cx + r1 * Math.cos(pa * rad);
   p.y = cy + r1 * Math.sin(pa * rad);
   updateInput(p, cx, cy, r1, offset, delta)
}, false);

initialValue.addEventListener("input", function() {
   var val = this.value;
   var newVal = (!isNaN(val) && val >= 0 && val <= 100) ? val : 18;
   var pa = (newVal * 1.8) - 180;
   var p = {}
   p.x = cx + r1 * Math.cos(pa * rad);
   p.y = cy + r1 * Math.sin(pa * rad);
   updateInput(p, cx, cy, r1, offset, delta)
}, false);

svg.addEventListener("mousedown", function(evt) {
   isDragging = true;
   this.classList.add("focusable");
   var mousePos = oMousePos(svg, evt);
   updateInput(mousePos, cx, cy, r1, offset, delta);
}, false);
svg.addEventListener("mouseup", function(evt) {
   isDragging = false;
   this.classList.remove("focusable");
}, false);
svg.addEventListener("mouseout", function(evt) {
   isDragging = false;
   this.classList.remove("focusable");
}, false);

svg.addEventListener("mousemove", function(evt) {
   if (isDragging) {
      var mousePos = oMousePos(svg, evt);
      updateInput(mousePos, cx, cy, r1, offset, delta);
   }
}, false);
```

```
$(document).ready(function() {
   $(".set > a").on("click", function() {
      if ($(this).hasClass("active")) {
         $(this).removeClass("active");
         $(this)
            .siblings(".content")
            .slideUp(200);
         $(".set > a i")
            .removeClass("fa-minus")
            .addClass("fa-plus");
      } else {
         $(".set > a i")
            .removeClass("fa-minus")
            .addClass("fa-plus");
         $(this)
            .find("i")
            .removeClass("fa-plus")
            .addClass("fa-minus");
         $(".set > a").removeClass("active");
         $(this).addClass("active");
         $(".content").slideUp(200);
         $(this)
            .siblings(".content")
            .slideDown(200);
      }
   });
});

$(document).ready(function () {
   //Initialize tooltips
   $('.nav-tabs > li a[title]').tooltip();

   //Wizard
   $('a[data-toggle="tab"]').on('show.bs.tab', function (e) {

      var $target = $(e.target);

      if ($target.parent().hasClass('disabled')) {
         return false;
      }
   });

   $(".next-step").click(function (e) {

      var $active = $('.wizard .nav-tabs li.active');
      $active.next().removeClass('disabled');
      nextTab($active);
   });
   $(".prev-step").click(function (e) {

       var $active = $('.wizard .nav-tabs li.active');
       prevTab($active);

   });
});

function nextTab(elem) {
   $(elem).next().find('a[data-toggle="tab"]').click();
}
function prevTab(elem) {
   $(elem).prev().find('a[data-toggle="tab"]').click();
}


//according menu

$(document).ready(function()
{
   //Add Inactive Class To All Accordion Headers
   $('.accordion-header').toggleClass('inactive-header');

   //Set The Accordion Content Width
   var contentwidth = $('.accordion-header').width();
   $('.accordion-content').css({});

   //Open The First Accordion Section When Page Loads
   $('.accordion-header').first().toggleClass('active-header').toggleClass('inactive-
header');
   $('.accordion-content').first().slideDown().toggleClass('open-content');

   // The Accordion Effect
   $('.accordion-header').click(function () {
      if($(this).is('.inactive-header')) {
         $('.active-header').toggleClass('active-header').toggleClass('inactive-
header').next().slideToggle().toggleClass('open-content');
         $(this).toggleClass('active-header').toggleClass('inactive-header');
         $(this).next().slideToggle().toggleClass('open-content');
      }

      else {
         $(this).toggleClass('active-header').toggleClass('inactive-header');
         $(this).next().slideToggle().toggleClass('open-content');
      }
   });

   return false;
});
```