East African Scholars Journal of Engineering and Computer Sciences
Abbreviated Key Title: East African Scholars J Eng Comput Sci
ISSN 2617-4480 (Print) | ISSN 2663-0346 (Online) |
Published By East African Scholars Publisher, Kenya
OPEN ACCESS
Volume-2 | Issue-10 | Oct-2019 |
DOI:10.36349/EASJECS.2019.v02i10.008

Research Article

Implementing the Tool for Assessing Organisation Information Security Preparedness in E-Governance Implementation

Gladys Korir[1*], Dr. Moses Thiga[1] and Dr. Lamek Rono[1]
[1]Kabarak University, Kenya

*Corresponding Author
Gladys Korir

Abstract: The main objective of the study was to implement an information security self-assessment tool that can be used by governments to determine their preparedness in protecting e-governance systems against information security threats. The self-assessment tool utilises a web-based model containing specific information security elements and techniques against which different departments dealing with information security can assess their capability to defend e-governance systems. The study adopted two research methodologies; scientific- for collecting relevant data that was used to develop appropriate weights for different security variables and design research science- for developing and implementing the self-assessment tool. The study established that while the government have invested heavily in technical information security measures, it has, however, failed to evaluate and perform a routine review of its information security practices. This research contributes to existing knowledge on e-governance security by providing a method by which governments can use to assess their information security practices. The tool is recommended to be used by key information security personnel in Kenya's county governments to assess their information security preparedness and hence work towards improving their organisational information security practices.
Keywords: e-governance, information security, self-assessment, information security measures, organisation information security preparedness.

INTRODUCTION

In an age where globalisation and emerging technologies have taken root in every aspect of life (Backus, 2001), governments are now obligated to use new emerging and disruptive technologies to deliver public services. Governments are continually relying on information systems for efficient, accountable and transparent public service delivery. E-governance is becoming a formal way of providing improved public services. E-governance is the application of information and communication technologies to transform the efficiency, effectiveness, transparency and accountability of informational and transactional exchanges within government, between government departments, and to empower citizens through access and use of information (Bhatnagar, 2004). The resulting benefits of e-governance are less corruption, increased transparency, greater convenience, revenue growth, and cost reductions (Bhatnagar, 2004).

The purpose of e-governance is to support and streamline governance in government, for instance, improving operations between government, citizens and businesses, through effective use of ICTs (Backus, 2001). E-governance in Kenya has been supported momentously by the government as a hypothetical remedy for poverty-related problems and also improving governance (Ochara, 2008). In 2004, the Kenyan government approved the e-government strategy making the start of e-governance journey in Kenya (Wamoto, 2015). Since then, the government of Kenya initiated several e-governance systems with the aim of enhancing efficiency, transparency and democracy within public administration.

Among those initiatives are the Integrated Financial Management Information System (IFMIS) and the Integrated Personnel and Payroll Database (IPPD), which are operational in the ministries. Additional applications that have been rolled out include the Local Authorities Integrated Financial

Quick Response Code

Journal homepage:
http://www.easpublisher.com/easjecs/

Article History
Received: 23.09.2019
Accepted: 06.09.2019
Published: 27.10.2019

Operations Management Systems (LAIFOMS), Education Management Information System (EMIS), Integrated Taxation Management Systems (ITMS) currently known as ITAX, National integrated management Information system (NIMIS), Resource management system (RMS), online Selection and Recruitment System used by the public service commission as well as the Border control System in the Ministry of State for Immigration and Registration of persons (Wamoto, 2015). These systems have eased the burden of many citizens and improved government operation. However, the implementation of these systems has encountered several challenges which include cyber-attacks and information security breaches. It was reported that in 2015, the governments and government employees faced a lot of security breaches leading to financial loss and defamation of names (Serianu Cyber Threat Intelligence Team, 2016). For instance, in Garissa County government, passwords of senior county staffs were stolen and used to make illegal payments (Serianu Cyber Threat Intelligence Team, 2016). Also, the Ministry of Planning and Devolution IFMIS system was compromised by an inside attacker and stole login credentials of a government official who was in charge of approving tenders. The stolen credentials were used to approve fraudulent tender requests (Serianu Cyber Threat Intelligence Team, 2016). In May 2017, a ransomware attack hit the country, affecting most of the users running Windows operating systems. Phishing attacks targeting government's services and social media users were reported in 1st December 2014, where cyber criminals created fake websites and used them to collect login credentials, thereafter using the collected user's login details to advance their attacks (Business Daily, 2014).

Governments have accumulated a great deal of confidential information about their citizens, employees, customers, products, research, and financial status. Most of this information is collected, processed and stored electronically and transmitted across networks to other computers. Studies show that the security of e-governance in Kenya's government is at a high risk and information security threats against e-governance systems could cost the government millions of money (Serianu Cyber Threat Intelligence Team, 2016; Serianu Cyber Threat Intelligence, 2016a; Cisco, 2017).

In Kenya, information security in e-governance have been addressed using different approaches but still appear to be weak. For instance, the government of Kenya was reported to have lost over $171million to cyber-criminal by the end of 2017, which is said to be the highest record in East Africa (Cisco, 2017). Today's governments and organisations employ very sophisticated security tools and technologies like firewalls, encryption, access control management, and others to curb this challenge. Although technologies and tools are an integral part of effective information security practices, it is argued that they alone are not sufficient to address information security problems (Otero, 2014).

To improve overall information security, governments and organisations must assess their information security practices regularly so as to determine their security capability and thus review and update their information security practices to satisfy their specific security requirements and to overcome the challenge of the dynamic nature of information security threats (Otero, 2014).

The alarming facts related to e-governance success in Kenya (Serianu Cyber Threat Intelligence Team, 2016; Serianu Cyber Threat Intelligence, 2016a; Cisco, 2017), point to existent inadequacies and inefficiencies with regards to information security practices employed to secure e-governance systems. These realities also serve as motivators for finding innovative ways to assist governments and hence, other organisations improve their capabilities for securing their valuable information and systems. To this end, it is important that information security practices and techniques around e-governance systems be evaluated and updated on a regular basis. Enhancing information security in e-governance not only nurture secure e-governance services but also, creates confidence and trust among e-governance users; leading to the success of e-governance initiatives (Karokola, 2012)

In East Africa, Kenyan recorded the highest loss of $171 million to cybercriminals by the end of 2017. The public sector has been ranked as the sector facing the highest information and cybersecurity risks in Kenya. This is so, not because the government has not invested in ensuring information security, but because of a lack of realistic and prioritised strategies for improving organisational information security measures. The lack of a method or system for use in assessing the information security capability by key personnel in departments dealing with the implementation of e-governance in governments has caused governments to be reluctant in reviewing and updating their information security measures towards counteracting the dynamic nature of information security threats. This fact, therefore, necessitates the need for developing more efficient and innovative ways of dealing with the information security challenge. Departments responsible for critical government infrastructure need to have a consistent and iterative way of identifying, assessing and managing organisation information security. Adequate evaluation of information security measures employed in governments is crucial in sustaining sound security as well as protecting information assets. Traditional information security assessment methodologies like risk assessment and management, best practice frameworks and other ad hoc approaches must be strengthened and improved to assist governments with the process of information security management. In response to this, this study sought to develop a web-based information security self-assessment tool for assessing organisation information security processes to determine the preparedness of county governments in Kenya to curb information security threats.

LITERATURE REVIEW

Existing methodologies for Information security assessment

There are different existing methodologies for information security assessment developed by different organisations and researchers to assist organisations in assessing their information security preparedness. Most of the methodologies available are industry-specific. In this section, the study explored individual information security assessment tools available.

Baldrige Cyber Security Excellence Builder (BCEB)

The Baldrige Cybersecurity Excellence Builder is a self-assessment tool that helps organisations examine and understand the effectiveness of their cybersecurity risk management efforts and identify improvement opportunities in the context of their overall organisational performance (National Institute of Standards and Technology. (2019). This self-assessment tool mergers organisational assessment approaches from the Baldrige Performance Excellence Program (BPEP) with the concepts and principles of the Cyber Security Framework developed by NIST's Applied Cyber Security Division (ACD).

NIST Framework for cybersecurity risk self-assessing

This tool was developed by the National Institute of Standards and Technology NIST to assess cybersecurity risks during the implementation of the NIST cybersecurity framework. The tool forms a section of the NIST Cyber Security Framework (National Institute of Standards and Technology, 2018). The tool allows organisations to measure and assign values to their risks along with the cost and benefits of steps taken to reduce risks to an acceptable level. The self-assessment tool is designed to help organisations implementing the NIST Cyber Security Framework to improve their decision-making process about investment priorities.

Maryland Health Care Commission (MHCC) Cybersecurity self-assessment tool

This Cybersecurity Self-Assessment Tool was developed by the Maryland Health Care Commission (MHCC) to assist small health care providers in identifying gaps and potential risks in their cybersecurity processes (Maryland Health Care Commission, 2019). The tool is also used to provide guidance in the development and implementation of cyber protections where cybersecurity processes do not exist. The tool was developed using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which assembles standards, guidelines, and practices to evaluate cybersecurity. The tool guides users through assessing the organisational processes that address the five core functions of the NIST cybersecurity framework: 1) identify, 2) protect, 3) detect, 4) respond, and 5) recover. The scope of this self-assessment tool is within Maryland Healthcare in the United States of America and can only be adopted by other health institutions using the NIST cybersecurity framework. Its applicability is limited and cannot be scaled to other organisations.

FIFIEC Cybersecurity Assessment tool

Considering the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool on behalf of its members, to help institutions identify their risks and determine their cybersecurity maturity (Federal Financial Institutions Examination Council, 2017). The tool uses a list of questions to identify the level of risk and to assess the status of the existing cybersecurity programs. The Assessment's content is consistent with the policies of the FFIEC Information Technology Examination Handbook and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as industry-accepted cybersecurity best practices. The Assessment offers institutions a repeatable and measurable process of informing management of their risks and preparedness in cybersecurity. The Assessment comprises of two parts: Inherent Risk Profile and Cyber Security Maturity. The Inherent Risk Profile identifies the institution's inherent risk before implementing controls. The Cyber Security Maturity includes domains, assessment factors, components, and individual declarative statements across five maturity levels to identify specific controls and practices that are in place. While management can determine the institution's maturity level in each domain, the Assessment is not designed to identify an overall cybersecurity maturity level. The scope of this tool is that it's a risk assessment tool and is limited to FFIEC Information Technology Examination Handbook and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Information Security Risk Assessment

Information security risk assessment is a systematic approach used to identify organisations needs regarding information security requirement. It is used by information security best practices as part of the information security risk management process, which focuses on identifying the relevant risks and the appropriate controls for reducing or eliminating these identified risks. Risk assessment quantifies or qualitatively describes the information security risk and enables organisations to prioritise risks according to their seriousness. It determines the value of information assets, identifies the applicable threats and vulnerabilities that exist, identifies the existing controls and their effect on the risks identified, determines the potential consequences and finally prioritises them.

Common Information Security Risk assessment methodologies involve nine primary steps with help in conducting an information risk assessment (ISO/IEC 27000, 2016);

1. System understanding
2. Threat identification
3. Vulnerability identification
4. Control analysis
5. Likelihood determination
6. Impact analysis
7. Risk determination
8. Control recommendation
9. Results documentation

Technical Guide to Information Security Testing and Assessment

This is a technical guide developed by the National Institute of Standards and Technology that provides a guide to the basic technical aspects of conducting information security assessments (Scarfone, 2018). It presents a technical examination and testing methods and techniques that an organisation might use as part of an assessment. It also offers assessors insights on the execution and the potential effect they may have on networks and systems. For an assessment to be productive and have a positive impact on the security posture of a system, elements beyond the execution of testing and examination must support the technical process. Suggestions for these activities, including a robust planning process, root cause analysis, and tailored reporting, are also presented in the guide. The assessments focus on verifying that a particular security control meets requirements, at the same time identifying, validating, and assessing a system's exploitable security weaknesses. This guide's intention is not to give comprehensive information security testing or assessment program, but rather an overview of the key elements of technical security testing and assessment with emphasis on specific techniques, their benefits and limitations, and recommendations for their use (Scarfone, 2018).

Assessing Information security controls using Fuzzy theory

Otero (2014), in his dissertation, An Information Security Control Assessment Methodology for Organisations, developed a method for evaluating information security controls in organisations. The methodology, created using the Fuzzy Logic Toolbox of MATLAB based on fuzzy theory and fuzzy logic, uses fuzzy set theory which allows for a more accurate assessment of imprecise criteria than traditional methodologies (Otero, 2014).

Common Criteria – Common evaluation method

Common Criteria is a methodology for assessing the security of the system (Common Criteria, 2018). This methodology sets out the steps and actions that must be accomplished to validate the system's compatibility with the chosen level of confidence. The methodology includes a detailed description of how various provisions of the declaration of compliance with a given level of confidence in common criteria ought to be verified (Luiza Fabisiak, 2012). The outcome of the verification process is binary (pass/fail). However, until the assessment of a given module of declaration has been completed, its status is non-binding. This methodology does not aim to determine the actual level of system security. Its main objective is to test whether the security level declared by the manufacturer has been reached. Any non-compliance with the requirements for the declared level of confidence proves the declaration incompatible with the actual state and causes its rejection. Cases of non-compliance do not reduce the level of confidence in the tested product. This method is usually used when designing new solutions and products whose security has to be certified.

Data protection self-assessment tool

Data protection self-assessment is a self-assessment tool created by ICO (Information commissioner office), UK, to help organisations assess their compliance with data protection law (The Information Commission Office, 2019). It contains data protection assurance checklists that a controller or a processor uses to assess their compliance with common data protection laws that include information security, data sharing and privacy and records management. The information security section assesses an organisations compliance with data protection laws in the specific areas of information and cybersecurity policy and risk, mobile and home working, removable media, access controls and malware protection.

METHODOLOGY

This study adopted Design research science methodology to build the information security self-assessment tool. This study was mainly carried out in Uasin Gishu county government. The research target population included the county executive members, ICT staff, chief information security officers in the counties and information systems users and custodians within the county governments. This study used a structured questionnaire as the primary data collection instrument. The research used the secondary data sourced from governments, and which included: previous studies, books, academic magazines, periodicals, websites, electronic versions and agencies reports, and published articles related to the subject. A total of 5 respondents comprising of members of staff of Nakuru county government who met the selection criteria were sampled in this survey. A pilot test was carried out to detect weakness in design and instrumentation. To avoid misrepresentation and minimise errors, the researcher did a pre-test of the questionnaires before the actual data collection. Reliability Analysis was analysed using Cronbach's Alpha coefficient. Pearson correlation was used to test the nature of the relationship between the variables. The analysis and presentation were done with the aid of SPSS (Statistical Package for the Social Sciences).

Based on the above methodology, the development of the information security self-assessment tool was divided into the following steps;

i. awareness of the real-world problem and understanding the complexity of the problem
ii. suggestions for a tentative design
iii. developing the framework
iv. evaluating the proposed framework

DATA ANALYSIS, PRESENTATION AND DISCUSSION

Model Implementation

This section gives an elaborate description of how the information security self-assessment tool was designed, implemented and evaluated as a web-based model. It, therefore, fulfils objective three and four of the study. This study used Design research science methodology to come up with the information security self-assessment tool. Design science research (DSR) methodology is used when creating innovations and ideas that define technical capabilities through which the development process of a tool or model can be effectively and efficiently accomplished (Karokola, 2012).

System Objectives

The main objective of the OISP system is to provide an effective way in which key information security personnel in a county government can individually assess their organisation preparedness level in regards to information security. The system should be able to highlight the information security practices that require reviewing and update so as to protect e-governance systems appropriately hence improve citizen's trust in e-governance. Furthermore, the system should provide a detailed report on assessments done. The system is to be used as a platform for conducting information security assessments by county governments so that they can maintain a sound security level by updating their information security practices according to the recommendations suggested by the tool.

Model Requirements Specifications

Requirement specifications are a detailed description of the functions and capabilities a system should exhibit and constraints it should operate within. According to Somerville (2010), requirements specifications are grouped into two groups: functional and non-functional (business) requirements.

Functional Requirements

Somerville (2010) defines system functional requirements as statements describing services the system should provide. They define how a system should operate in particular situations and react to particular inputs (Sommervile, 2010). The following functional requirements were identified for the information security self-assessment tool:

1. The OISP platform should provide a friendly web-based interface for information security personnel to assess their security preparedness level.
2. The model is expected to provide information security personnel with an appropriate recommendation for improving their security preparedness level through a friendly and simple graphical interface.
3. The model is expected to provide the Chief information security officer with a detailed report on the overall preparedness level of the county government through a friendly and simple graphical interface.

Business Requirements

These are requirements that relate to the fundamental business of an organisation. Business (non-functional) requirements represent the constraints on the system and its functionalities; performance constraints; compliance with standards, (Somerville, 2010). In information security, any system adopted or implemented should ensure the confidentiality, integrity and availability of information. The study identified the following non-functional requirements.

1. The information security self-assessment tool should comply with the government of Kenya information security standards outlined in the GEA standard and guidelines for information security management outlined in the international best practices.
2. The tool should seamlessly integrate with existing information security management system.
3. The tool should be scalable.

System overview

The information security self-assessment tool was developed using PHP as a server-side scripting language, MySQL as a database engine, CSS3 for styling and jQuery for interactive functions. Security was enforced in the web-based model to ensure that all users would be authenticated before conducting any assessment or accessing any other system functionality. All users are required to log in, providing their unique log in details as assigned by the Chief information security officer. The chief information security officer registers all users according to their roles and responsibilities in information security and assigns them assessment questions according to their responsibilities.

The flowchart in figure 1 below represents the overall functionality of the OISP platform.

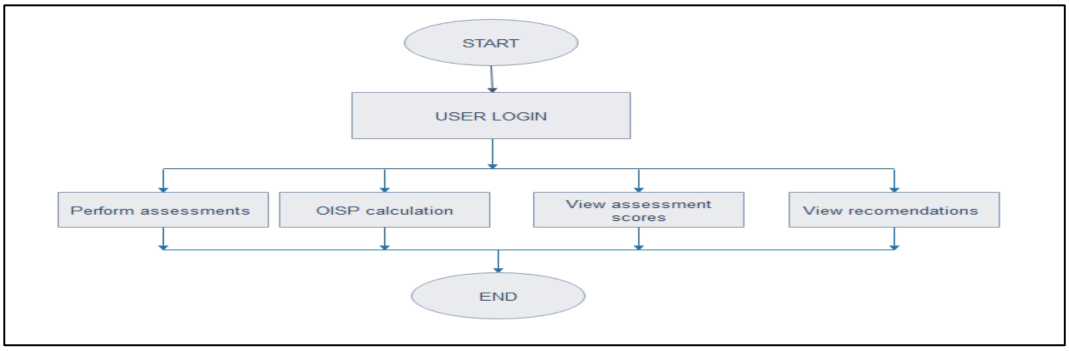


Figure 1: OISP system flowchart

Source; Researcher (2019)

System Contributors

During the implementation of the OISP platform, a number of partakers were involved, who include; system users and administrators, domain name registrar, and web hosting service provider.

1) **System users and administrators:** Users of OISP system are those who login successfully and are able to carry out assessments tasks within the OISP platform. They include key information security personnel in county governments that are responsible for information security management. The administrator position was reserved for a chief information security officer who is the lead player in the management of security risks in governments and organisations. Unlike the other system users, the CISO is able to register other personnel, and also view the overall scores of information security preparedness levels from all other user assessments. Furthermore, the CISOs are able to assign roles responsibilities to other personnel involved in information security management and update assessment checklists in case the current checklist changes.
2) **Domain registrars:** Domain name registrar are responsible for registration and reservation of the domain name for the OISP platform on the internet.
3) **Web host:** These are web hosting service providers who ensure that there is assured availability of the OISP system online by providing hosting space on their servers as well as services and technologies required for the webpages to be displayed on the Internet. The web server allows communication between users and the OISP platform.

OISP System architecture

This section describes the OISP system abstract model that defines the structure, behaviour and views of the system. It presents the modules that make up the OISP system, the entity-relationship diagram of the OISP model and the logical design of the OISP system.

OISP System modules

The OISP system has eight modules that work together to achieve the OISP system functionality.

a) **User login and authentication module:** This module ensures that only the registered users who have permission to access the functionality are allowed to access the system while others are denied access. The registered users are required to provide the email and password matching the ones assigned by the system administrator who is the CISO so as to be granted access.
b) **User Session Handling Module:** This module manages user sessions by creating a session when user logs in to the system, track all the user activities when the session is on and destroys the session when the user logs out of the system.
c) **Information security Assessment module:** This session pulls the assessment questions from the database and presents it on a Likert scale layout. The user goes through the questions and checks the appropriate answer depending on the level of implementation of their organisation's information security practices. After all the questions have been duly filled, the user submits it.
d) **Reports module:** This module presents the results of the submitted assessment to the user in a graphical display. The user can also download the assessment results and recommendations in the form of portable document format (pdf). Additionally, there is a separate admin report module that is only accessible to the CISO, where the CISO can view all other users' assessment reports and the overall organisation preparedness level.
e) **Core application logic:** This module contains logic that handles user requests by receiving, processes, and responding to them. Additionally, this module allows inputs to the database, performs arithmetic computations of the information security preparedness level.
f) **Settings module:** This module is only accessible to the system admin. It enables the CISO to register other system users by assigning them roles according to their responsibilities in information

security management and also add new roles. In addition, it allows the CISO to add and modify the assessment questions depending on the adopted practices of the organisation.

g) System database: The OISP model maintains a database that contains four main tables for storing information.

The OISP database contains four tables for storing different types of information;

1. **User information**: id, user_role_id, first_name, last_name, email, password, active

Table 1: tbl_users

Field	Type		Null	Key	Default		Extra
id	int(11)	7B	NO	PRI	(NULL)	0K	auto_increment
user_role_id	int(11)	7B	YES		(NULL)	0K	
first_name	varchar(255)	12B	YES		(NULL)	0K	
last_name	varchar(255)	12B	YES		(NULL)	0K	
email	varchar(255)	12B	YES		(NULL)	0K	
password	varchar(255)	12B	YES		(NULL)	0K	
active	tinyint(1)	10B	YES		(NULL)	0K	

Source: Research data (2019)

2. **User role information**: id, user_role

Table 2: tbl_user_role

Field	Type		Null	Key	Default		Extra
id	int(11)	7B	NO	PRI	(NULL)	0K	auto_increment
user_role	varchar(100)	12B	YES		(NULL)	0K	

Source: Research data (2019)

3. **System Questions information**: id, question, category, main_category, recommendation, category_weight, threshold, ciso, sysadmin, hr, netadmin, others

Table 3: tbl_system_questions

Field	Type		Null	Key	Default		Extra
id	int(11)	7B	NO	PRI	(NULL)	0K	auto_increment
question	varchar(255)	12B	YES		(NULL)	0K	
category	varchar(255)	12B	YES		(NULL)	0K	
main_category	varchar(255)	12B	YES		(NULL)	0K	
ciso	tinyint(1)	10B	YES		0	1B	
sysadmin	tinyint(1)	10B	YES		0	1B	
hr	tinyint(1)	10B	YES		0	1B	
netadmin	tinyint(1)	10B	YES		0	1B	
others	tinyint(1)	10B	YES		0	1B	
category_weight	double(12,6)	12B	YES		(NULL)	0K	
recommendation	varchar(255)	12B	YES		(NULL)	0K	
threshold	double(12,2)	12B	YES		(NULL)	0K	

Source: Research data (2019)

4. **Self-assessment information**: id, role_id, user_score, asst_date, qid, user_id.

Table 4: tbl_self_assessment_results

Field	Type		Null	Key	Default		Extra
id	int(11)	7B	NO	PRI	(NULL)	0K	auto_increment
qid	int(11)	7B	NO		(NULL)	0K	
user_id	int(11)	7B	NO		(NULL)	0K	
role_id	int(11)	7B	NO		(NULL)	0K	
user_score	int(11)	7B	NO		(NULL)	0K	
asst_date	timestamp	9B	NO		CURRENT_TIMESTAMP	17B	

Source: Research data (2019)

Entity-relationship diagram

The entity-relationship diagram for the OISP system is presented in figure 2 below.

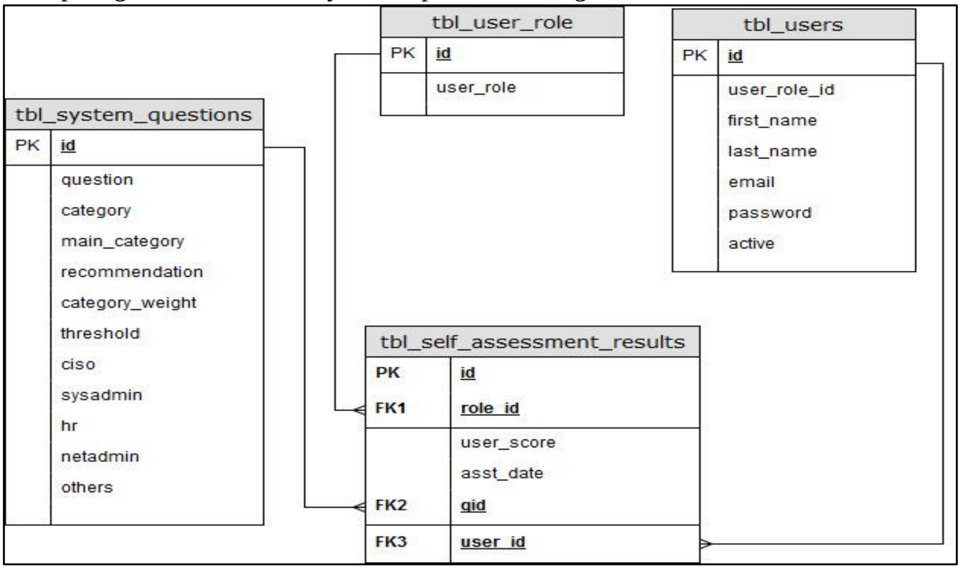


Figure 2: Entity relationship diagram

Source; researcher (2019)

OISP logical and physical design

The logical design of a system refers to an abstract representation of the data flows, inputs and outputs of the system. The physical design is a graphical representation of a system showing the system's internal and external entities, and the flows of data into and out of these entities. This section presents the logical design of the OISP system using flowcharts and user interface design of the implemented OISP modules.

User login and authentication module

This module manages logins and sessions on users. It allows registered users to access system functionality by referring to users' database. If the user is not registered, it denies them access and prompts them to provide correct usernames, passwords or register. Figure 3 below shows a flowchart representing the logic of the login system, while figure 4 presents a graphical user interface of the login component.

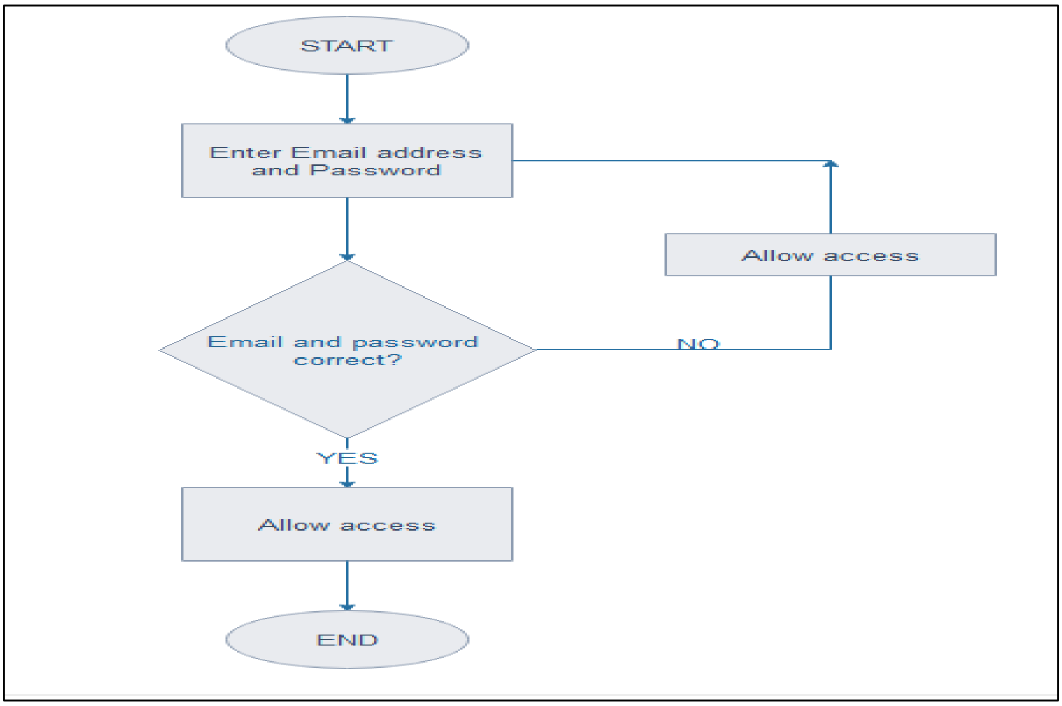


Figure 3: Login flowchart

Source: Researcher (2019)

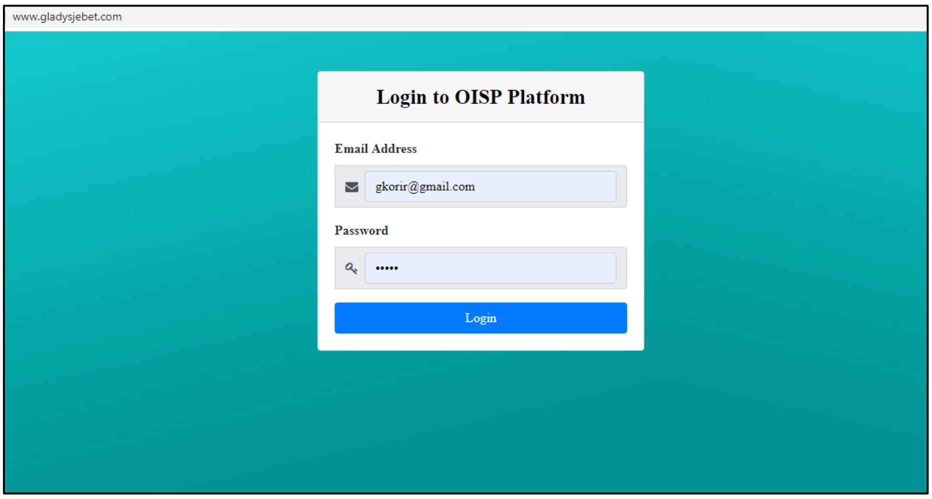


Figure 4: OISP login GUI
Source: Researcher (2019)

Information security Assessment module

Once a user has logged in, the user can perform an assessment using the information security self-assessment module. This module allows the user to perform self-assessment for their organisation/department by answering every assessment question on a Likert scale of 1 to 5. This module retrieves the questions from the database and presents it to the user in a Likert scale layout. Duly filled assessment form can be submitted to the database from where the information security preparedness level will be computed. Figure 5 below shows a flowchart presentation of the assessment logic, whereas figure 6 is the presentation of the graphical user interface of the information security assessment module.

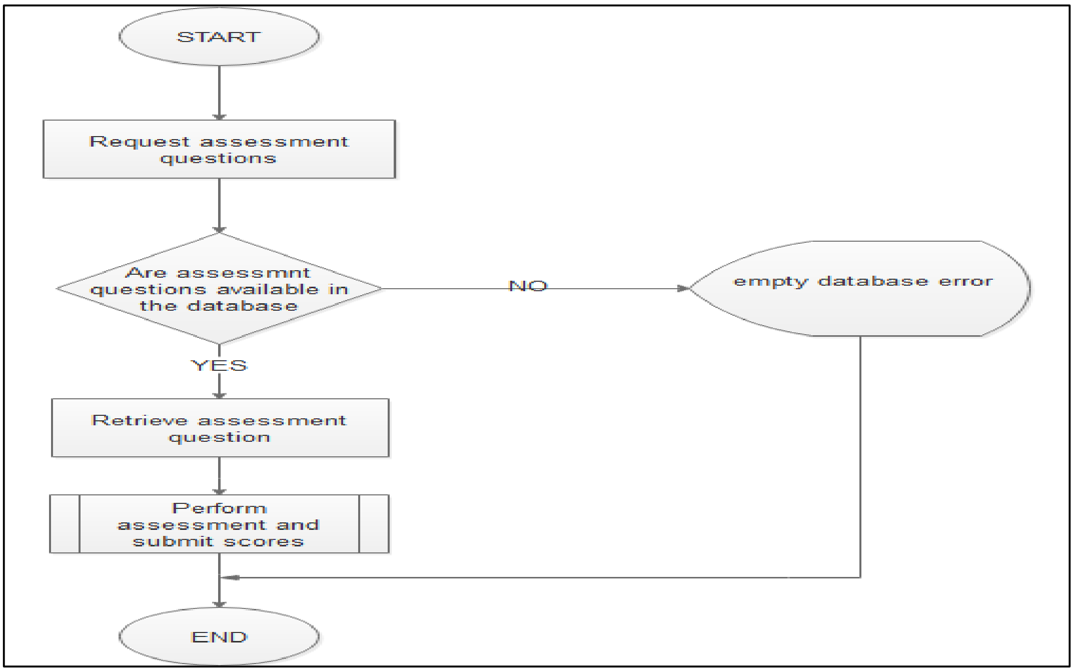


Figure 5: self-assessment module
Source: Researcher (2019)

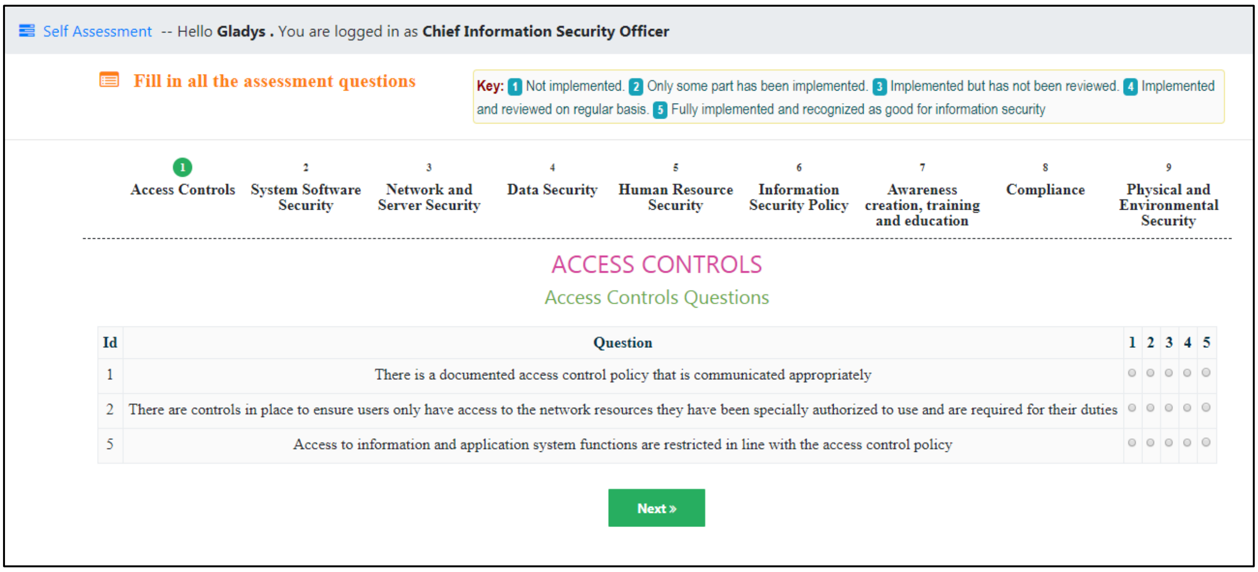


Figure 6: Self-assessment GUI

Source: Researcher (2019)

Reports module

This component of the OISP platform allows the user to read back their assessment scores for all the assessment questions submitted. It also allows the end-user to download the scores in a portable document format that can be printed. The reports module is further divided into user scores, recommendations and admin reports. Figure 7 illustrates the flowchart representation for retrieving the reports.

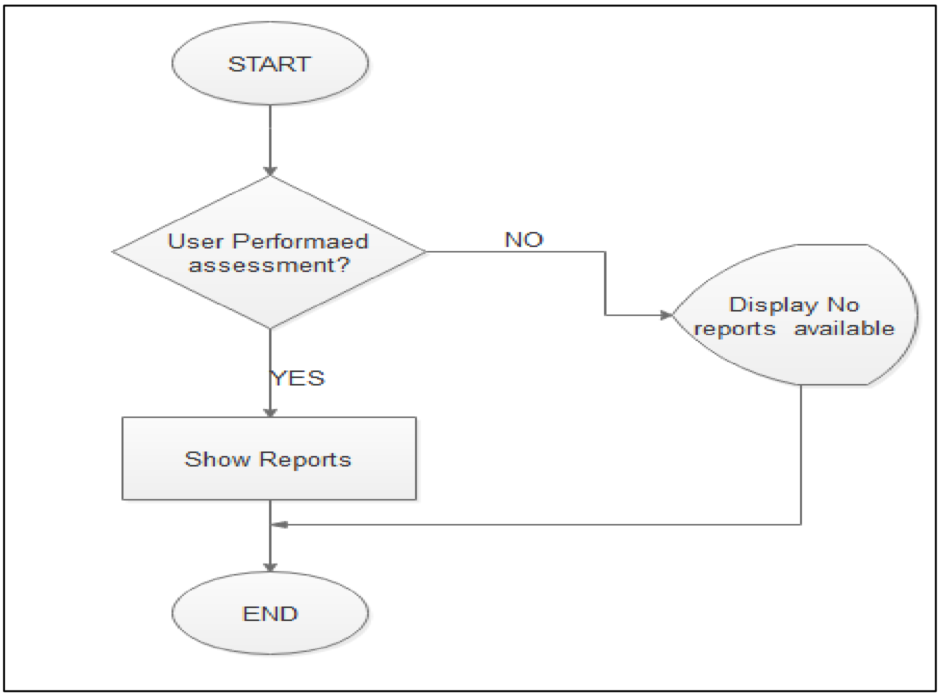


Figure 7: assessment report flowchart

Source Researcher (2109)

a) User scores reports

The figure 8 below shows the graphical user interface for the user scores reports

Your Self-Assessment Scores Per Question Average: 2.759 /5.000

Question ID	Question	Your Average Score (1-5)
1	There is a documented access control policy that is communicated appropriately	2.0000
2	There are controls in place to ensure users only have access to the network resources they have been specially authorized to use and are required for their duties	2.5000
5	Access to information and application system functions are restricted in line with the access control policy	2.0000
6	There are established procedures which list all requirements with regard to outsourcing any county Information Systems service or activities.	2.0000
7	There are anti?spyware, anti-phishing and cleanup software solutions to detect, prevent and remove any spyware threats, phishing attacks and trashed files regularly.	2.5000
8	There is a rollback software to keep track and record any changes made to the computers and allow the system to be restored to its original state from any chosen point in time.	3.5000
13	There is authentication systems to prevent unauthorized access to the countys server.	3.0000
14	There is routine backup for the data, safe storage of hard copy of server hardware specifications, installation information, installation software and passwords at an offsite location.	3.5000
15	The server is placed in a secure location, such as in a lockable cage, a locked room and place it with environmental controls.	3.0000
16	There are data classification, retention and destruction procedures for handling county data, media or materials that contain county sensitive information.	3.0000
18	There are policies on sharing, storing and transmitting of county data via ISPs, external networks or contractors systems.	4.0000
19	Use of cryptography techniques, hardware & software tokens and single sign on systems to control data access to the county internal and remote computer systems	3.0000

Figure 8: User Score report GUI

Source: Researcher (2019)

b) Recommendation reports

Figure 9 below shows the graphical user interface for the recommendation reports

Recommendations Report-- Hello **Gladys .** You are logged in as **Chief Information Security Officer**

Your Recommendations for Best Practice 16 Recommendations

Question ID	Your Average Score (1-5)	Recommendation
1	1.0000	You should have a documented access control policy that is communicated appropriately
2	1.0000	Controls should be in place to ensure users only have access to the network resources they have been specially authorized to use and are required for their duties
5	1.0000	Access to information and application system functions are restricted in line with the access control policy
6	1.0000	There are established procedures which list all requirements with regard to outsourcing any county Information Systems service or activities.
7	2.0000	There are anti?spyware, anti-phishing and cleanup software solutions to detect, prevent and remove any spyware threats, phishing attacks and trashed files regularly.
20	1.0000	Vital Countys business information or records are regularly backed up and stored in a different site.
27	1.0000	There are policies on protection of county assets to protect your countys hardware, software, data and people.
30	2.0000	Procedures for update and review existing information security policies
33	2.0000	Information security awareness trainings is mandatory to all staff and patrons at various levels.
34	2.0000	There are balanced set of key performance indicators (KPIs) and metrics used to provide the real insight into the effectiveness of security awareness programs.
37	1.0000	All the records within the county are protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative, regulatory, contractual and business requirements

Figure 9: Recommendation Reports GUI

Source: Researcher (2019)

c) Admin reports

Figure 10 below shows the graphical user interface for the administrator's reports

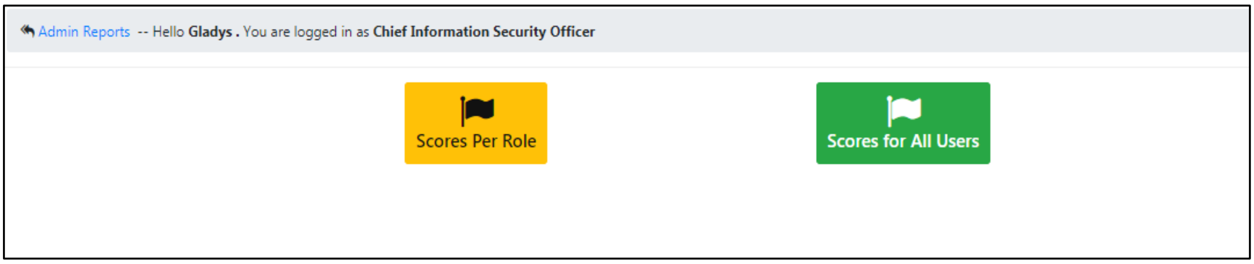
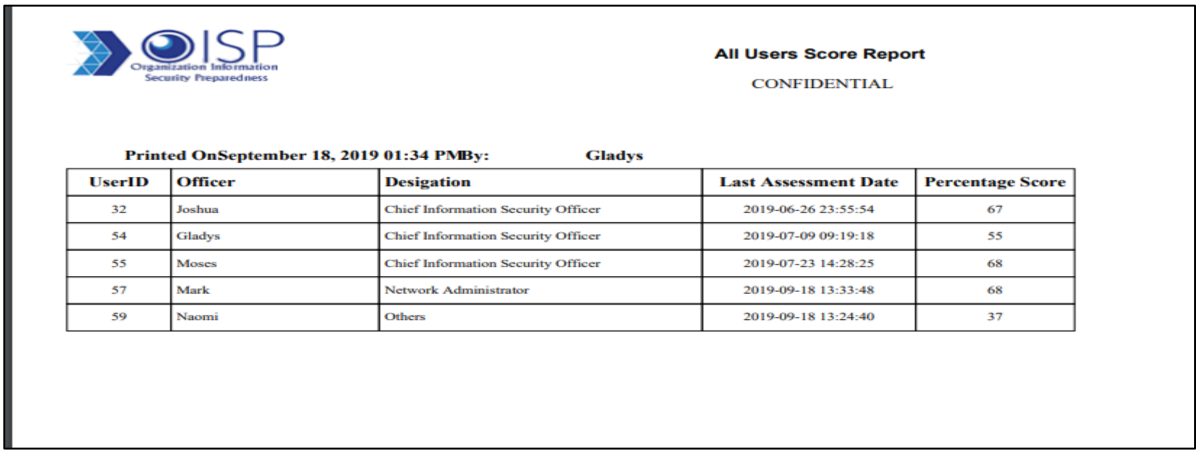


Figure 10: Admin Report GUI

Source: Researcher (2019)



OISP Organization Information Security Preparedness

All Users Score Report

CONFIDENTIAL

Printed OnSeptember 18, 2019 01:34 PMBy: Gladys

UserID	Officer	Desigation	Last Assessment Date	Percentage Score
32	Joshua	Chief Information Security Officer	2019-06-26 23:55:54	67
54	Gladys	Chief Information Security Officer	2019-07-09 09:19:18	55
55	Moses	Chief Information Security Officer	2019-07-23 14:28:25	68
57	Mark	Network Administrator	2019-09-18 13:33:48	68
59	Naomi	Others	2019-09-18 13:24:40	37

Figure 10: All users score report GUI

Source: Researcher (2019)

Setting module

The setting module enables the CISO to register other system users by assigning them roles according to their responsibilities in information security management and also add new roles. In addition, it allows the CISO to add and modify the assessment questions depending on the adopted practices of the organisation.

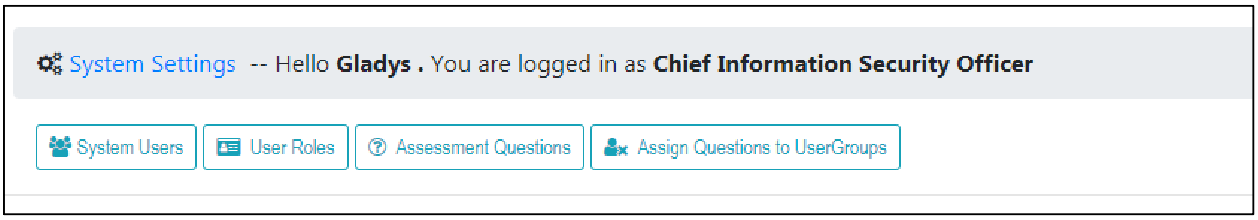


Figure 11: Setting GUI

Source: Researcher (2019)

a) System users' registration

This sub-module allows the CISO to register other users to the system according to the roles and responsibility in information security management. Figure 12 below shows the graphical user interface for this sub-module.

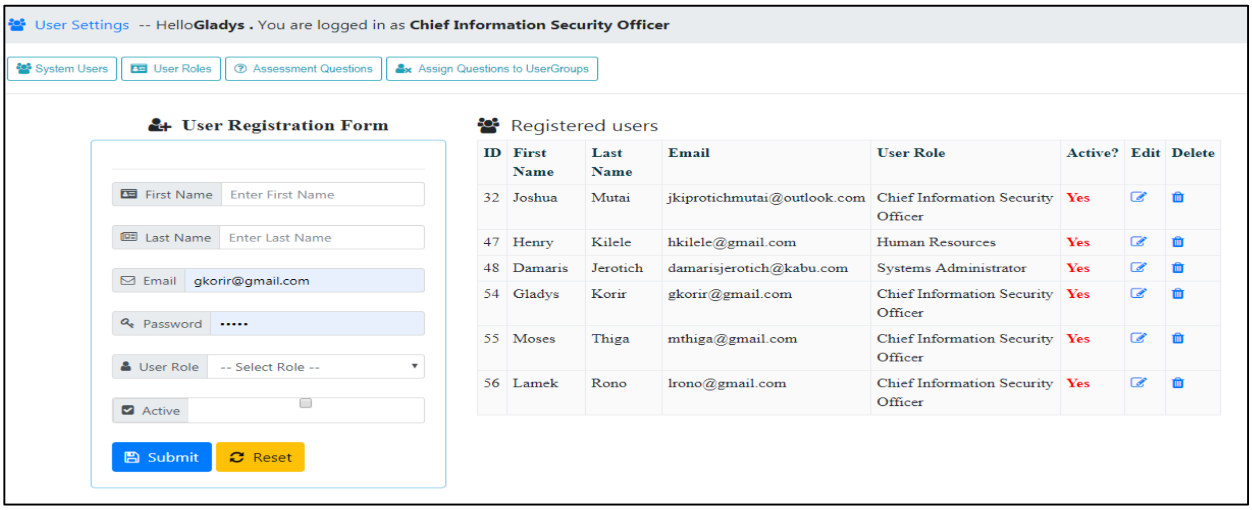


Figure 12: User registration GUI
Source: Researcher (2019)

b) User roles

This sub-module allows the CISO to add a new role to the system according to their need in information security management. Figure 13 below shows the graphical user interface for this sub-module.

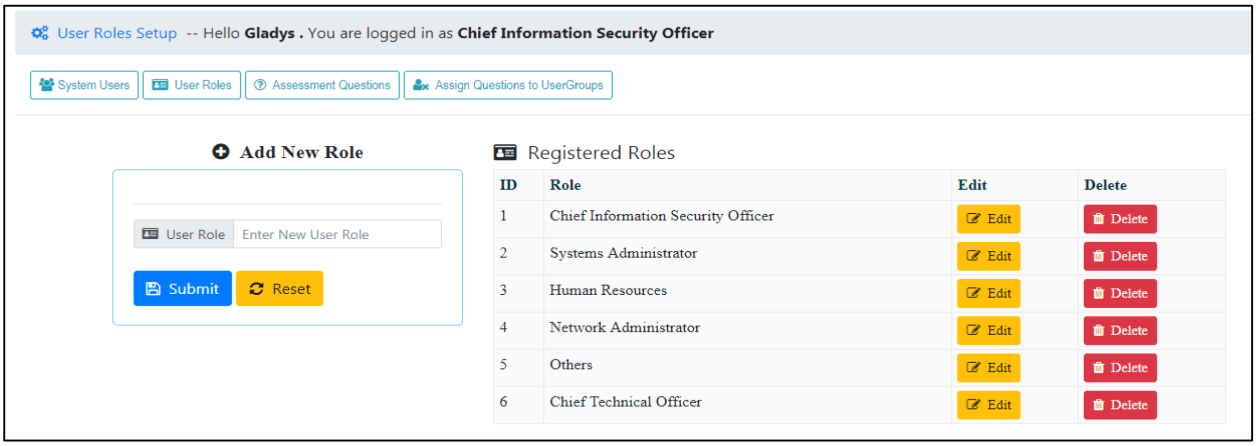


Figure 13: New Role registration GUI
Source: Researcher (2019)

c) Assessment questions

This sub-module allows the CISO to add more assessment questions to the information security assessment questions checklist. Figure 14 and 15 below shows the graphical user interface for this sub-module.

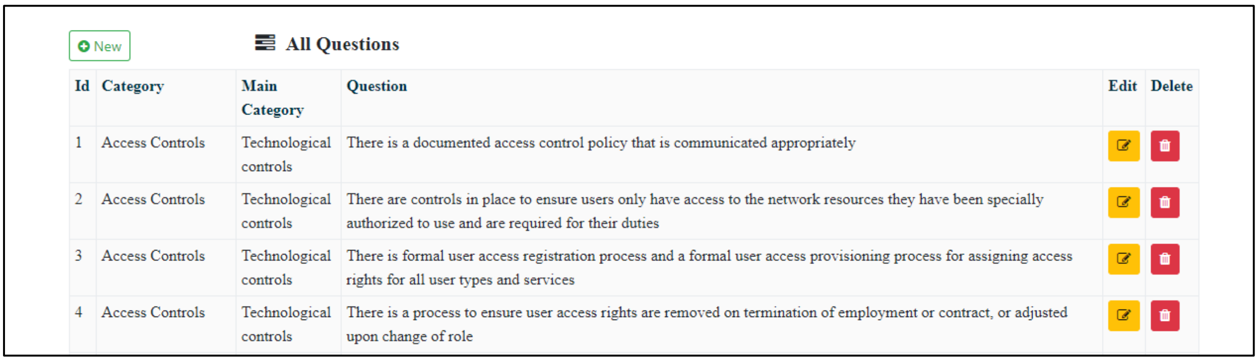


Figure 14: All questions list GUI
Source: Research (2019)

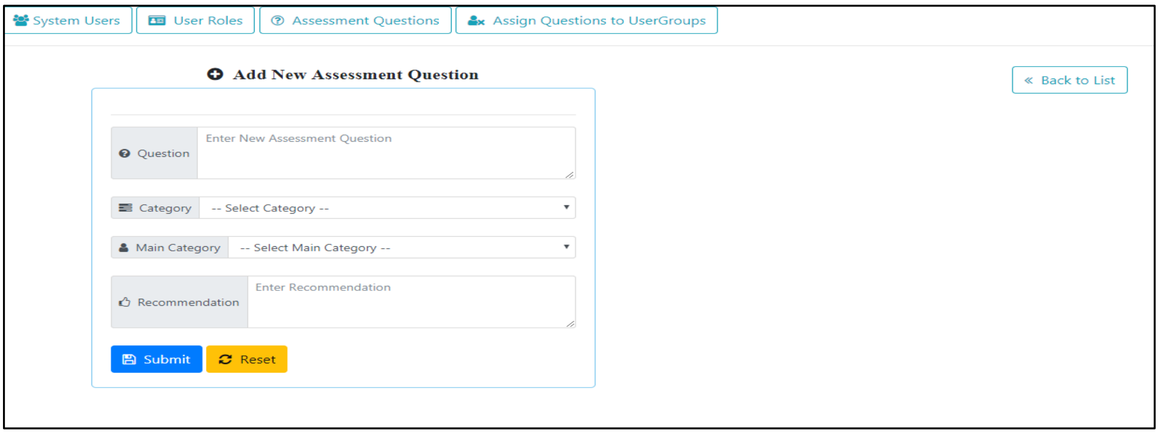


Figure 15: Add New assessment Question GUI

Source: Researcher (2019)

d) Assign questions to user groups

This sub-module allows the CISO to assign assessment questions to users with different roles in information security management. Figure 16 below shows the graphical user interface for this sub-module.

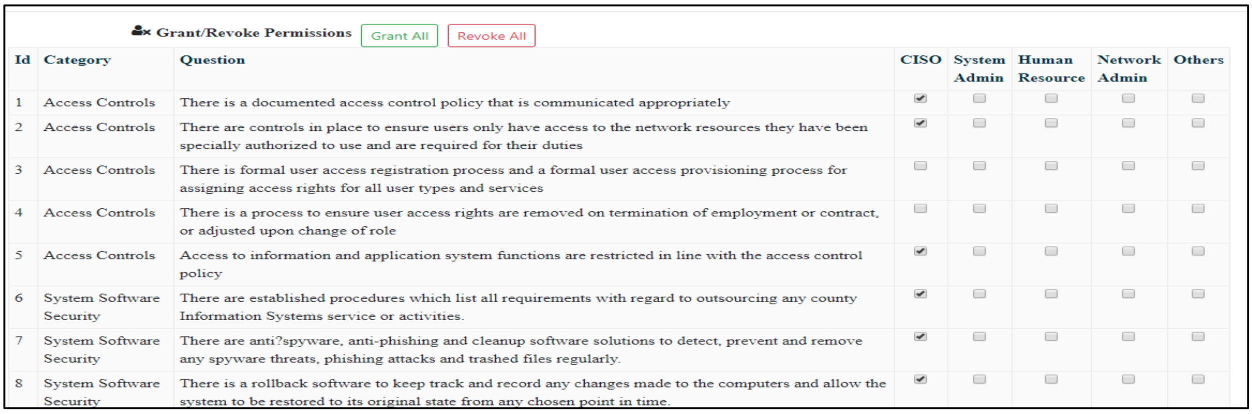


Figure 16: Assigning questions GUI

Source: Researcher (2019)

OISP system interface

The OISP system has a responsive user interface that once a user has successfully logged in to the system, one can easily interact with the system components and navigate the different modules. Figure 17 presents a graphical user interface layout of the home display component.

Figure 17: OISP dashboard

Source: researcher (2019)

Proof of Concept

As a proof of concept, the OISP platform was developed using PHP server-side scripting language for system logic controllers. Front end scripting was done using jQuery library to enhance front end responsiveness to the platform while styling was done using Cascading style sheets version 3 (CSS3). Visio studio code and notepad++ program editors were used to write and test code. Apache webserver was used to run the application locally, and MySQL was used as the backend database engine. The system was deployed online and can be accessed using the following URL; **www.gladysjebet.com.**

System evaluation

In order to determine how effective, the OISP system was in achieving its pre-set objectives, an evaluation was undertaken guided by a goal-based evaluation approach which determines the extent at which a system is achieving the pre-set objectives. Each functionality of the OISP system was tested with regards to its objectives as presented in table 5 below;

Table 5: Goal-based evaluation for the OISP system

	Objective	Evaluation Results
1.	**User login and Authentication:** The system was expected to prompt the user to provide login credentials before being allowed to access the system components.	**i.** The system prompted the user for login credentials and matches with the ones stored in the database. **ii.** The system allowed access to users who successfully provided a username or email and password that matches those stored in the database.
2.	**Information security assessment and submission:** The system was supposed to retrieve assessment questions from the database and present to the user in a Likert scale layout. It was also to allow the user to submit a duly filed assessment form to the database	**i.** The system was able to retrieve assessment questions and from the database and present them in an easy-to-use Likert scale format for the user. **ii.** It also allowed the user to submit a score from a duly filled assessment form into the database.
3.	**OISP calculation:** The system was expected to compute the preparedness level as per submitted user scores and present the results to the user in percentage	**i.** The system was able to read the user scores from the database and determine the preparedness level as per the user scores. **ii.** It provided the preparedness level as a percentage.
4	**Reports and recommendations:** The system was expected to retrieve reports on assessment scores and recommendations and allow the user to download the output into a portable and printable document format.	**i.** The system was able to retrieve the scores as well as recommendations from the database and present them to the user **ii.** It was also able to allow the user to download the output into a portable document format that can be printed.
5	**Registration of new users and the addition of new assessment questions:** The system was supposed to allow registration of new users as per their roles and responsibilities in information security management. Also, allow assignment of assessment questions as per their roles and responsibilities.	**i.** The system was able to allow registration of new users as per their roles and responsibilities in information security. **ii.** It also allowed assigning of different assessment questions to the new users as per their roles and responsibilities in information security management.

Source: Researcher (2019)

CONCLUSION

The premise upon which this research was based on is the lack of an information security self-assessment platform that information security personnel in county governments in Kenya can use to assess and review their information security practices. The proposed assessment tool is an organisation-wide assessment platform where key information security personnel in governments individually assess their department/organisation information security practices to determine their level of preparedness and their capability to reduce evolving information security risks.

The information security self-assessment tool for determining OISP was implemented as a web-based application using PHP as a server-side language, jQuery for frontend interactions, and MySQL as a database engine. The model has a database for storing assessment questions information, assessment scores information and system users' information. The model relies on the assessment information stored in the database to determine information security preparedness level of the assessor. The model provides the user with their level of preparedness and recommendation necessary to improve their information security practices.

RECOMMENDATIONS

The researcher recommends that the governments use the proposed tool to assess their information security preparedness levels periodically so that they can maintain the highest level of information security readiness at any time. Completed assessment reports should provide a basis for an action plan undertaken by county governments to upgrade their information security practices. Each department concerned with information security in e-governance should decide additional information security practices to be added to the system or customise the system to match their specific information security requirements.

It is also recommended that the government as a regulating agency impose compliance on periodic assessment of information security capabilities of their departments, counties and agencies. This process will motivate governments that are reluctant in reviewing and updating their information security practices to update their security practices regularly.

REFERENCES

1. Backus, M. (2001). E-Governance and Developing Countries: Introduction and examples. The Hague: IICD.
2. National Institute of Standards and Technology. (2019). Baldrige Cybersecurity Initiative. Retrieved from https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative
3. Bhatnagar, S. (2004). e-Government: From Vision to Implementation. Sage Publications.
4. Business Daily. (2014, December 1). 4. Kenya: Nation Media group.
5. Cisco. (2017). Cisco cyber security Anual report. Kenya: Cisco.
6. Common Criteria. (2018, August 23). Common Criteria, v3.1. Release 3. Retrieved from Common Criteria: http://www.commoncriteriaportal.org/cc/
7. Federal Financial Institutions Examination Council. (2017). FFIEC Cybersecurity Assessment Tool. USA: Federal Financial Institutions Examination Council.
8. ISO/IEC 27000. (2016). Information technology - Security techniques - Information security management systems - Overview and Vocabulary. ISO/IEC 27000. Switzerland: ISO/IEC 2016.
9. Karokola, G. R. (2012). A Framework for Securing e-Government services: A case of Tanzania. Sweden: Stockholm University.
10. Serianu Cyber Threat Intelligence Team. (2016). Kenya Cybersecurity Report. Nairobi: Serianu Cyber Threat Intelligence Team.
11. Luiza Fabisiak, T. H. (2012). Comparative Analysis of Information Security Assessment and Management Methods. Studies & Proceedings of the Polish Association for Knowledge Management, (pp. 56-70).
12. Maryland Health Care Commission. (2019). Cyber Security self-assessment tool. Maryland Health Care Commission.
13. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. USA: National Institute of Standards and Technology.
14. Ochara, N. M. (2008). The emergence of the eGovernment artefact in an environment of social exclusion in Kenya. The African Journal of Information Systems, 1(1) 18-43.
15. Otero, A. R. (2014). An Information Security Control Assessment for Organisation. Nova Southeastern University.
16. Scarfone, M. S. (2018). NIST Special Publication: Technical Guide to Information, Security Testing and Assessment. USA: Nationa Institute of Standards and Technology.
17. Serianu Cyber Threat Intelligence. (2016a). Africa Cyber Security Report, 2016. Nairobi: Serianu Cyber Threat Intelligence.
18. Sommervile, I. (2010). Software Engineering. New York: Addison Wesley.
19. The Information Commission Office. (2019, February 1). Data protection self-assessment. Retrieved from The Information Commission Office: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/
20. Wamoto, F. O. (2015). E-government Implementation in Kenya: An evaluation of Factors hindering or promoting e-government. International Journal of Computer Applications Technology and Research, 4(12), 906-915.