2017

A Web based information security skills assessment prototype

Regina Kagwiria Nkonge
Faculty of Information Technology (FIT)
Strathmore University

A Web Based Information Security Skills Assessment Prototype

Regina Kagwiria Nkonge

Dissertation Submitted in Partial Fulfilment of the Requirements for the Degree of Master of Science in Information Systems Security (MSc. ISS) at Strathmore University

Faculty of Information Technology
Strathmore University
Nairobi, Kenya

June, 2017

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

Regina Kagwiria Nkonge

…….

…….

Approval

The dissertation of Regina Kagwiria Nkonge was reviewed and approved by the following:

Dr. Humphrey Njogu,
Senior Lecturer, Faculty of Information Technology,
Strathmore University

Dr. Joseph Orero,
Dean, Faculty of Information Technology,
Strathmore University

Professor Ruth Kiraka,
Dean, School of Graduate Studies,
Strathmore University

Abstract

Cyber-attacks are continuously evolving to a great extent faster than cyber defences. The result is an ever-increasing frequency of attacks and the probability of success over time. To ensure employees are able to avoid or counter information security attacks directed at them and the organisation, it is necessary to carry out continuous security awareness and training, and, ensure this training is relevant to employees.

Existing tools to assess information security skills among employees generally require the expertise of technical persons and are often not well tailored to an organisations' specific needs. This study aims at developing a prototype which organisations can use to create information security skills assessments for their employees. Employees can then log in to the prototype at their convenient time and take the assessment. At the end of the assessment, each employee receives a percentage mark of their performance. Based on this percentage the employee is ranked as either beginner, intermediate or advanced and is also given a list of their weak areas based on questions they got wrong. The weak areas can be used to identify gaps and this information used to customise security awareness and training programs to meet employees' needs.

The research study adopted agile development methodology to design and develop a prototype to address identified gaps. The prototype was tested and validated to ensure it meets the intended goals and recorded impressive results.

Keywords: Information Security Skills, Information Security Awareness, Information Security Education, Information Security Training, Information Security Skills Assessment.

Table of Contents

Abbreviations/Acronyms

CIOs	-	Chief Information Officers
CISOs	-	Chief Information Security Officers
DDoS	-	Distributed Dos Attack
ENISA	-	European Network and Information Agency
HR	-	Human Resources
ICT	-	Information Communication Technology
IP	-	Internet Protocol
IT	-	Information Technology
NIST	-	National Institute of Standards and Technology
UI	-	User Interface
UK	-	United Kingdom

List of Figures

List of Tables

Acknowledgements

To list everyone I would want to thank for their contribution to this work would be a dissertation in itself. Few great things are accomplished by one person. The words that follow are not enough to describe my gratitude to all the people, including those not mentioned here, who have shaped this work. To my @iLabAfrica team, thank you. To Dr. Humphrey Njogu for holding my hand every step of the way, thank you. This work is as much yours as it is mine. To Dr. Stephen Ichatha, for your faith and high expectations of me, thank you. I have learned a lot from you. To mum and dad for your support and always encouraging creativity in me, thank you. To my brother Frank for always standing by my side, thank you. To Liz and Alice for your encouragement, thank you.

Dedication

To my parents Grace and George Nkonge. You did not lecture me on life…you simply lived and let me learn.

Chapter 1: Introduction

1.1 Background

Firms are facing numerous cyber threats and attacks (McCarthy, 2003). One of the reasons for this is that attackers are aware employees have access to sensitive information but are ignorant of information security (Whitman, 2003). They do not seem to understand the risks inherent in using the Internet (SecureWorks, 2012). They lack awareness and understanding of the value of information they hold and risks of exposing it to the wrong persons. Hence physical preventative measures such as antivirus software and firewalls are proving to solve only part of the problem as the employees using them lack adequate information security knowledge. This exposes organisations to risks (Gundu, T., 2013).

Physical and technical controls alone cannot solve the security problem (SANS, 2016). Taking the time to conduct security awareness and training to educate employees on acceptable and unacceptable behaviour is the next most effective way of reducing risk of information security breach (SecureWorks, 2012). It serves to keep information security at the forefront of employees' minds ensuring they realise its importance. It also prevents falling into attacks such as social engineering, phishing, malware installation and the like.

Close examination of organisations reveals that three main challenges exist that make it difficult to conduct effective information security awareness and training. A number of researchers and surveys (Hansche, 2001; Casmir & Yngstrom, 2005; Okenyi and Owens, 2007; Maeyer, 2007; CSI, 2008 & 2009; ENISA, 2008) identify the first challenge as lack of top management support and the second challenge as limited budgets. A third challenge which few researchers have addressed however is the lack of proper tools to analyse employees' information security skills so that gaps can be identified and this information used to customise awareness and training programs to address those gaps. Talib (2014) observes that current information security awareness strategies are arguably lacking in their ability to provide a robust and personalised approach to educating users, opting for a blanket, one-size-fits-all solution. Secondly, existing solutions that are

tailored or designed to conduct skills analysis may not be affordable by small or medium organisations, require technical skills such as those of penetration testers or are not tailored to meet the specific training needs of an organisation.

There is a clear need therefore for tools that help analyse employees' information security skills so that gaps can be identified. This information can be used in planning awareness and training programs ensuring their relevance. SAI Global (2012) holds the view that gap analysis can provide valuable insight by enabling organisations to evaluate current understanding, highlight knowledge gaps, customise training to actual organisation needs and compare awareness to previous results once training has been completed.

This study aims to develop a web based automated self-assessment prototype to help organisations analyse its employees' information security skills. The prototype will also point out an employees' areas of weakness and rank him/her as beginner, intermediate or advanced based on his/her percentage score. By identifying weak areas, gaps can be analysed and this information is in turn used to plan awareness and training programs making such programs more relevant, more effective and worth their cost.

1.2 Problem Statement

Information security awareness and training is one of the most important ingredients for achieving the goals of information security in an organisation (Thomson & von Solms, 1998; Siponen, 2000; D'Arcy et al., 2009). A security conscious workforce is best achieved through security awareness, education and training (SANS, 2009). Technology and processes therefore must combine with employee education (Howarth, F., 2014).

To be effective and relevant however, an internal skills analysis exercise should be conducted and gaps identified to ensure training programs cover the right content (Baker, J., 2012). However, this exercise is not always possible because existing solutions for analysing information security skills generally tend to focus on a single aspect of information security such as Phishing or Social Engineering and tend to be complex meaning they are meant for people with technical skills such as penetration testers.

Additionally, they are usually not tailored to meet the specific needs of an organisation. Therefore identifying training needs of employees has always been a big challenge. As a result, many organisations lack a global picture of their information security posture. When training opportunities arise, they have no idea who should be trained.

Based on the aforementioned challenges, this study aims at developing an automated web based prototype to help organisations analyse their employees' information security skills so that gaps can be identified and relevant awareness and training provided to address those gaps.

1.3 Research Objectives

i. To identify employees' information security weaknesses that are easily exploited by cyber attackers
ii. To identify and review the current approaches used to assess employees' information security skills
iii. To design, develop, test and validate a web based information security skills assessment prototype to improve the limitations of the current tools.

1.4 Research Questions

i. What information security weaknesses in employees do cyber attackers easily exploit?
ii. What are the current approaches to information security skills assessment?
iii. How can the proposed solution be designed, developed, tested and validated?

1.5 Justification of the Study

This research seeks to provide a web based automated information security skills assessment prototype to help organisations easily assess their employees' knowledge and level of information security awareness so that gaps can be identified and training programs customised to fill those gaps. On the one hand, reports provided by the prototype will serve to give a global picture on what kind of employee the organisation has. On the other hand, training can be prioritised, for example, financial resources for

security awareness and training can be allocated as a priority to members of staff who, after completing assessment using this tool, have been ranked as beginners. Most important, security awareness and training programs can be customised to address the identified gaps making these programs more personal, more relevant, effective and worth the resources allocated to them. Moreover, such reports would come in handy in the support of employee professional development and overall organisational cybersecurity strategy.

1.6 Scope and Limitations

The prototype will be web based for ease of access and use – no need to download and install. It will base a person's security level ranking on the individual's percentage score. The target population for testing this tool will be limited to one public university and one private university in Kenya.

Chapter 2: Literature Review

2.1 Overview

The section 2.2 of this chapter looks at the importance of information security. 2.3 to 2.5 analyses the rising threat sophistication and what organisations are doing about it. 2.6 addresses common types of threats faced by organisations today and the root causes of those threats. In 2.7 to 2.9 training needs and training needs analysis are defined and the importance of training needs analysis examined. 2.10 looks at common methods used by human resources departments to collect and analyse employees' training needs. Section 2.11 Looks at weaknesses that attackers easily exploit in employees while 2.12 identifies various perspectives of information security assessment that exist today. Current information security skills assessment tools are discussed in section 2.13. Finally 2.14 summarises the chapter and briefly describes the proposed solution.

2.2 Importance of Information Security

Companies are increasingly depending on computers and the Internet to conduct business. This means that almost all data processing, storage and transmission is done via computers and the Internet. As a result, a security incident that affects these systems can interrupt normal business, lessen revenue streams and cause customers to have poor confidence in the organisation. This dilemma makes information security an essential component to an effective overall business strategy (Pearson UK, 2015). Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure (Open University, 2016). Kruger & Keaney (2006) define the term as the protection of the confidentiality, integrity and access [availability] to information.

2.3 Increasing Threat Sophistication

Threats to information systems from criminals and cyber terrorists are increasing (Nigel Turnbull, 2003). Hackers are repeatedly probing networked computers for security weaknesses in order to gain access, wreak havoc or steal confidential information. Any computer hooked to the Internet is exposed to risks of malicious, or even just curious, visitors accessing the system and sniffing for information that was not intended to be

shared with anyone. Notably, incentives for hacking into an organisation and stealing its data are becoming ever more diverse and reflect the growing economic and social power of information (VMware, 2016). Traditional security products such as virus scanners and firewalls do not provide adequate protection against unknown threats and the thousands of mutations and variations of spyware and viruses available to hackers on the Internet.

2.4 Response by Organisations

Organisations are starting to understand how serious cybercrime is and the impact it can have on business from the data breach and reputation point of view. This realisation is partly because most of these organisations have faced threats themselves. As a consequence, CIOs and CISOs have realised the importance of protecting their information assets (Opil, B., 2016).

2.5 The Overlooked Factor

Despite the vast sums of money spent on information security, organisations remain inherently vulnerable to even the most basic of security, fraud weaknesses and vulnerabilities. This is because the focus has been mainly on technology while the most fragile element – people – has been neglected (Sârghe, P.D 2013). Employees use data in everyday activities to conduct the organisation's business; their mistakes represent a serious threat to the confidentiality, integrity and availability of data (Whitman, 2011).

Cyber criminals are constantly on the lookout trying to find employees' weaknesses to exploit. Deloitte Global Security Impact (2012) points out that human error is far more likely to cause serious information security breaches than technical vulnerabilities. For example simple configuration mistakes by careless employees can render network ports open, firewalls vulnerable and entire systems completely unprotected. IBM Index (2014) showed that 95 percent of all security incidents involve human error.

It is thus vital that organisations have security awareness and training programs in place to ensure employees are aware of the importance of protecting sensitive information, what they should do to handle information securely, and the risks of mishandling information.

2.6 Common Attacks Facing Organisations

Cisco (2006) gives and defines the following common attacks facing organisations today. These attacks may fall under two broader categories 1) Internal attacks which refer to attacks that originate from inside a local network 2) External attacks which refers to attacks originating from outside a local network.

2.6.1. Password Attacks

Password attacks refer to repeated attempts to identify a user account, password, or both. This can be achieved in various ways such as IP Spoofing, brute force attacks, Trojan horse programs, packet sniffers and so on.

2.6.2. Man-in-the-Middle Attacks

This is a common attack whose objective is theft of information or hijacking of an ongoing session in order to gain access to a private conversation or network resources, denial of service, corruption of data being transmitted, introduction of new information into the communication and so on. It can be done using packet sniffers, transport protocols among others.

2.6.3. Social Engineering

Here a criminal tricks an employee into disclosing valuable information such as passwords, emails, servers, file locations etcetera. This makes it easier for the criminal to hack the organisation.

2.6.4. Phishing

This is a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedure (Kenya Cybersecurity Strategy, 2014). It is a type of social engineering attack which entails a criminal masquerading as a trusted person uses email or other messaging platform to trick people into giving sensitive information such as passwords, credit card number. Messages sent tend to have a hyperlink that seemingly links to a legitimate website. However this website is setup by the criminal to capture the user's data. When a user enters their information it is captured and sent to the criminal.

2.6.5. Denial of Service (DoS) Attacks

A criminal sends a lot of data packets to a network with the aim of clogging it so that it is unavailable for use by the legitimate users. Examples of DoS are the Ping of Death and SYN flood attack. Distributed Denial of Service attacks (DDoS) are similar to DoS but operate at a much larger scale. Hundreds or thousands of attack points attempt to overwhelm an internet link causing legitimate traffic to be dropped.

2.6.6. Malicious Code

Viruses, worms, Trojan horses are all types of malicious codes. A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. A virus is a malicious software that is attached to another program to execute a particular unwanted function when that program is run. A Trojan horse is similar to a virus except that it is made to look like something that is harmless such as a game which when executed carries out some background commands that the user is not aware of.

2.6.7. IP Spoofing

An intruder falsifies an IP address thereby appearing to be another user. The intruder then assumes the identify of a valid user and gains that users access privileges, creates packets using the falsified IP address and sends them to the network of the person whose IP address has been spoofed, thus appearing to be a trusted user.

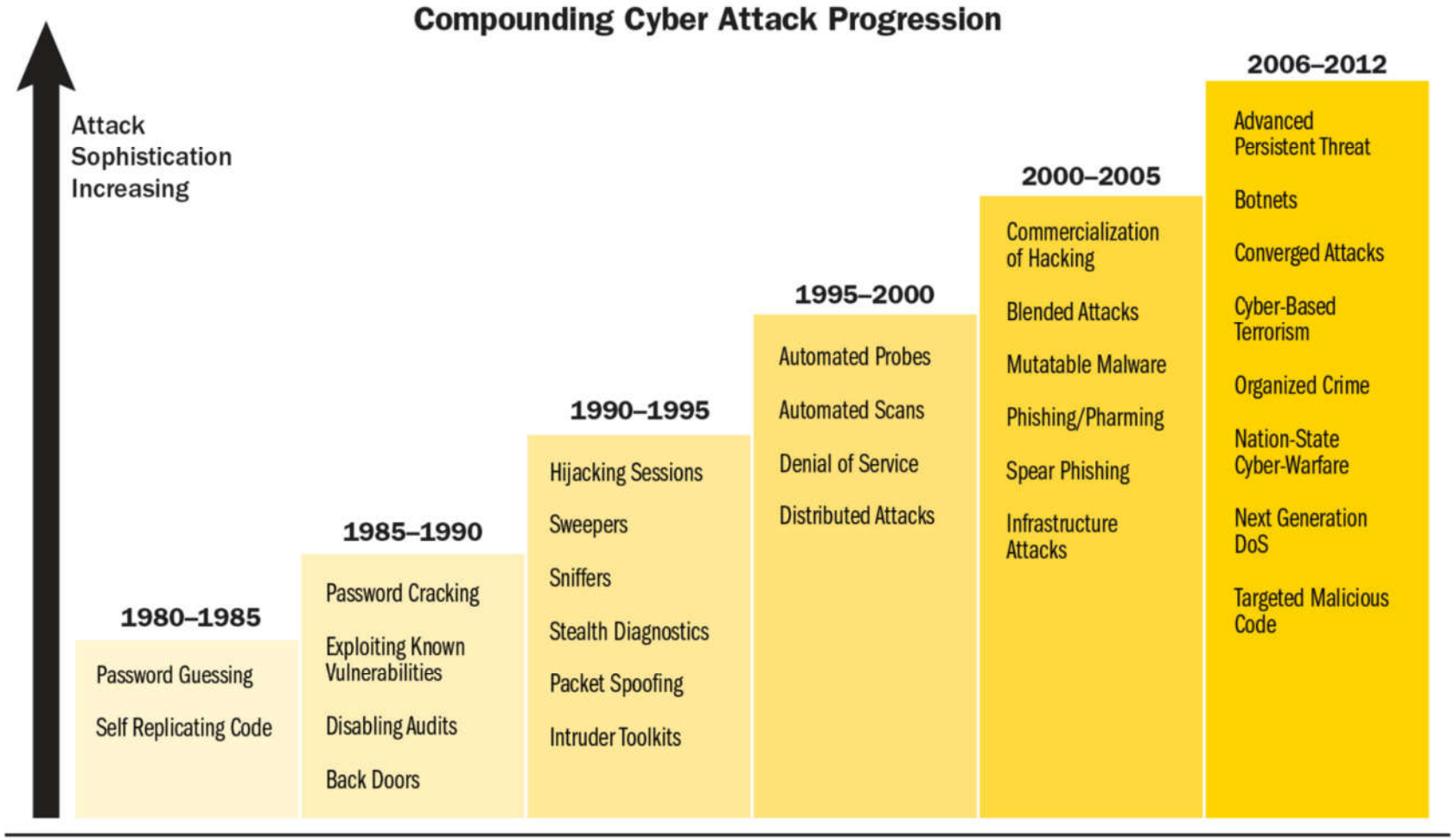


Figure 2.1 Sophistication of Cyber-attacks from 1980 – 2012 (Kenya Cybersecurity Strategy, 2014)

2.7 Training Needs

A training need is a shortage of skills or abilities, which could be reduced or eliminated by means of training and development. Training needs hamper employees in the execution of their job responsibilities or inhibit an organisation from attaining its objectives. They may be caused by a lack of skills, knowledge or understanding, or may arise from a change in the workplace (Chartered Management Institute, 2006).

2.8 Training Needs Analysis

Training Needs Analysis also known as Training Needs Assessment is the method of determining if a training need exists and, if it does, what training is required to fill the gap (JICA, 2007). Training Needs Assessment is also the process of collecting information about an expressed or implied organisational need that could be met by conducting training. The need can be a performance that does not meet the current standard. It means that there is a prescribed or best way of doing a task and that variance from it is creating a problem. Training Needs Analysis process helps the trainer and the person requesting training to specify the training need or performance deficiency (Jean Barbazette, 2006).

2.9 Importance of Training Needs Analysis

The goal of Training Needs Analysis is to make sure that training addresses existing problems, is tailored to organisational objectives, and is delivered in an effective and cost-efficient way (Chartered Management Institute, 2006). Training needs analysis encompasses monitoring current performance using techniques such as assessments, observation, interviews, surveys and questionnaires, identifying the type and level of training required and analysing how this can best be provided. Poorly conducted needs analyses can lead to training solutions that train: the wrong competencies; the wrong people; and employ the wrong learning methods (Carl Greenberg, 2016).

2.10 Common Methods used by HR to collect and Analyse Training Needs

METHOD	BENEFIT	WEAKNESS	WHEN TO USE
Review of References	Factual information Objective Can collect a lot if you have resources	May be out of date May be inaccurate or inconsistent Need cooperation of others to obtain information	When you need factual information about performance
Questionnaire Survey	Simple Quick Easy Can collate a lot of data	May not get important information People may not send back survey May be hard to understand responses	Have to know much about your topic first Combine with other processes to encourage response
Interviews	Obtain information about attitudes Obtain a lot of qualitative data Can have greater understanding of issues	Takes time of yourself and others More difficult to organize May be shy to respond depending on interviewer	When you know little about the topic or area When the training is about something complicated
Focus Group Discussion	Can be easy and quick Can understand responses more easily	People may be shy to be honest in group People may dominate discussion	When the training is impacted by team work When there is not much time for other methods
Observation	Does not interrupt work Can be more reliable than other sources	Can take observer a lot of time Need time to collate Need to know what you are looking for	When the training is about simple skills When you know about the topic yourself

(Source: MOI/DOLA, 2004, Training Needs Assessment, Phnom Penh)

Figure 2.2 Common Methods Used By Hr Departments to Collect and Analyse Training Needs: Their Benefits and Weaknesses

In addition to the weaknesses identified in Figure 2.2, traditional training needs collection and analysis tools somewhat lack automation hence require a certain level of human effort to analyse and produce reports.

2.11 Employees' Information Security Weaknesses that are Easily Exploited by Cyber Attackers

Through literature review the researcher identified some common information security weaknesses in employees that cyber attackers tend to easily exploit. These were useful in determining the kind of data required to assess information security skills in employees. Questions fed into the developed solution were mainly derived from these needs.

2.11.1. Weak Passwords and Reliance on Default Passwords

The Kenya Cyber Security Report (2015) points out that employees do not secure their gadgets or networks with strong passwords and often even rely on factory default passwords that are easy to hack. There is also the tendency to share passwords or to stick passwords under office desks. This is something that is overlooked due to poor information security training and awareness among employees.

2.11.2. Negligence

A study by Ponemon Institute (2011) shows that 39% of all data breached involved employee negligence while 37% of data breached involved malicious or criminal attack. The study explains that employee negligence whether deliberate or accidental, allows hackers to identify openings for a data breach or hack.

2.11.3. Lack of Compliance

Lack of compliance is also a big issue. Several employees do not follow organisational security policy or their IT security requirements especially on their mobile devices (iPass Mobile Workforce Report, 2012).

2.11.4. Ignorance of Social Engineering Techniques

Verizon (2016) observes that social engineering is one of the reasons why employee security awareness and training is necessary. Social engineering attacks have become increasingly common because of their relative ease of execution and lack of technical knowledge needed. Many employees however remain ignorant of social engineering attack methods and how to mitigate them.

2.11.5. Summary of Employees' Information Security Weaknesses

Information security awareness and training programs should aim at addressing the above identified weaknesses as well as any other weaknesses that the proposed system may identify. In a word, such programs should focus on a detailed understanding of information security threats, damage that could be caused by those threats and solutions to mitigate them. The programs should help employees become familiar with policies and procedures which help them to ensure their own security and that of the organisation. Common mistakes that users tend to make and which should be highlighted in training and awareness programs include: violation of security policy, opening unsolicited e-mail attachments, negligence and non-compliance, providing information without verifying that a caller is really who he says he is, installing software from unknown sources, visiting suspicious web sites and failure to report security incidents.

2.12 Various Approaches to Information Security Assessment

Most organisations do not know how they can go about conducting Information security awareness and training. They focus on technical solutions and ignore human based solutions which are more cost effective and have the potential to give higher returns on investment. To give organisations an idea of how to conduct effective information security awareness and training programs, various approaches have arisen over time. These are discussed below.

Amankwa, Loock and Kritzinger Approach

Amankwa, Loock and Kritzinger (2014) have studied the use of models to enhance information security education and awareness. They define a model as a framework that provides a step-by-step guide to a solution of a known problem. Their paper categorises information security education and awareness models into three stakeholder domains: End-users, Industry and Institutions. The Institution domain, which is the main focus of the study, is made up of educational institutions, government agencies, and, small and medium businesses with limited resources and semi structured IT setup. Characteristics of the Institutions domain is that information security professionals in senior management are rare and there are limited resources. By analysing previous literature, the paper points out to the lack of models in the institutions domain for enhancing information security

knowledge of employees through awareness and education so as to build a security conscious workforce.

Table 2.1 Categorisation of Existing Models of Information Security Awareness and Training (Amankwa, E., Loock, M. & Kritzinger, E., 2014)

Existing model & source article	End User Domain	Organisations Domain	Industry Domain
The **National Institute of Standards and Technology (NIST)** special publication 800-50 [18]	☑	☒	☑
Smith, E., Kritzinger, E., Oosthuizen, H.J., & Von Solms, S.H. (2005), "Information Security Education: Bridging the gap between academic institutions and industry", UNISA Institutional Repository.	☒	☒	☑
Sharma, S.K. & Sefchek, J. (2007), "Teaching information systems security courses: A hands-on approach", Computers & Security, pp.290– 299.	☑	☒	☒
Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007), "A video game for cyber security training and awareness", Computers & Security, 26(1), 63-72.	☑	☒	☑
Kritzinger, E. & Smith, E. (2008), "Information security management: An information security retrieval and awareness model for industry", Computers & Security, 27(5-6), pp. 224–231.	☑	☒	☑
Boujettif, M. & Wang, Y. (2010), "Constructivist Approach to Information Security Awareness in the Middle East", In International Conference on Broadband, Wireless Computing, Communication and Applications, pp.192–199.	☒	☒	☑
Monk, T., van Niekerk, J., & von Solms, R. (2010), "Sweetening the medicine : educating users about information security by means of game play", In Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists. Bela Bela, South Africa.: ACM New York, NY, USA, pp. 193–200.	☑	☒	☒
Kritzinger, E. & von Solms, S.H. (2010), "Cyber security for home users: A new way of protection through awareness enforcement", Computers & Security, 29(8), pp.840–847.	☑	☒	☒
The Information Technology Infrastructure Library (ITIL), (2011), "Best practice solutions: ITIL".	☒	☒	☑
ISACA, (2012), "Cobit 5", Cobit Publications Directory.	☒	☒	☑
Stewart, G. & Lacey, D. (2012), "Death by a thousand facts: Criticising the technocratic approach to	☒	☒	☑

information security awareness", Information Management & Computer Security, 20(1), pp. 29–38.			
Mugo, A.E.K., (2012), "A Model to Measure Information Security Awareness Level in an Organization: Case Study of Kenya Commercial Bank", Masters Thesis, Strathmore University, Nairobi Kenya.	☒	☒	☑
The International Organisation for Standardization (ISO 27002), (2013), "Introduction to ISO 27002 (ISO27002)".	☒	☒	☑
Jama, A.Y., Siraj, M. & Kadir, R. (2014), "Towards Metamodel - based Approach for Information Security Awareness Management", In 2014 International symposium on biometrics and security technologies (ISBAST). pp. 316–321.	☒	☒	☑
Mogale, M. Gerber, M. Carroll, M. & von Solms, R. (2014), "Information Security Assurance Model (ISAM) for an Examination Paper Preparation Process". IEEE transaction.	☒	☑	☒

From Table 2.1 there is a clear lack of information security education and awareness models in the organisations domain. Amankwa, Loock and Kritzinger (2014 recommend that this lack be addressed. They also propose that models developed for the organisation domain should focus on drawing attention of employees of an organisation to relevant security issues and the importance of complying with corporate policies and enforcement. The models should also aim at identifying employees' information security needs and gaps and should take into account different positions in the organisation ensuring employees are not overburdened with security issues that may not be relevant for their area of work. Finally the models should be structured into three layers namely novice, intermediate and advanced in order to best serve the different user groups.

NIST Approach

NIST 800-50 (2003) proposes conducting needs assessment before training programs are planned. The assessment can then be used to make training programs more specific and provide justification to convince management to allocate adequate resources to meet the identified awareness and training needs. NIST further proposes that employees be given training based on their roles and regularly updated on changes in policy and procedures. To achieve role based training a needs assessment would be necessary in order to identify the needs of the specific role.

Jason Baker Approach

Jason Baker (2016) recommends that security-training programs should be customised to address employees' actual security gaps. He further observes that majority of medium to large companies have had some form of information security awareness training in place for a number of years. ELearning is an established medium for training large numbers of people cost-effectively, however, unless done well and tailor made to meet actual needs of those being trained, this method can have limited success. Dull, uninspiring eLearning which fails to engage learners, address their needs and challenge their attitude toward information security, is unlikely to actually make them change the way they do things and make them behave in a more secure way.

SAI Global Approach

SAI Global (2016) points out that due to lack of proper and affordable tools, many organisations do not assess their employees' level of security knowledge before planning security-training programs. They therefore propose that organisations should determine the level of security awareness their employees have. This sort of benchmarking can enable the organisation to evaluate current understanding, highlight knowledge gaps and attitudes that could lead to insecure working practices, customise security awareness training to meet those gaps, and, compare awareness to previous results once training has been completed. Training must meet the needs of today's employees in order to be effective and deliver positive and sustained behavioural development. An effective information security awareness strategy is one that takes into account the requirements of the business and learner.

SANS Institute Approach

SANS Institute (2005) proposes customising contents of security awareness and training as per audience profiles. The first audience profile is the management which is the ultimate and most important sponsor of the awareness program. Managers have a very specific need to understand the goals of awareness and training programs and the role security plays in achieving their business objectives. The presentation to the management should focus on security threats which organization may encounter in the shorter or longer

run. It should be clearly communicated to the management that without its support the organisation and the employees would not be able to protect information assets.

The second audience profile is the users. Users are usually not responsible for overall protection of the information. However, they must secure the work environment and the information they handle. End users use data to perform their day-to-day tasks. This type of audience requires a detailed understanding of the information security threats, damage by those threats and solutions to mitigate the damage. They should also be familiar with the policies and procedures, which will help them to ensure performance and security. Common mistakes that users tend to make and which should be highlighted in training and awareness include: violation of security policy, opening unsolicited e-mail attachments, installing software from unknown sources, visiting suspicious web sites and failure to report security incidents.

The third audience profile is the technical people. It is generally thought that technical people do not require basic security awareness, as they are the ones who design the systems. However, the purpose of security awareness and training session for technical people is to bring out how technology helps the organisation and what is needed to protect the information assets of the organisation. Awareness session for technical people should be centred on technology is not driving the business, but vice versa. It is always the organisation that decides the need of technology. A security awareness and training program does not mean one-size fits for all. Topics have to be customized according to profile of the audience.

2.13. Existing Information Security Skills Assessment Tools That Support Information Skills Assessment

Gophish (https://getgophish.com) is an open source phishing toolkit built by MIT that to help penetration testers and organisations conduct real-world phishing simulations. It provides the ability to provide security awareness training by easily and quickly setting up and executing phishing campaigns on employees. It is compatible with Linux, Windows and OS X operating systems and has the advantage of being open source thus

making it accessible to small organisations. It also makes phishing training available to everyone. Its disadvantage is that it has to be installed on a machine and is restricted to phishing training only (Gophish, 2013).

Social Engineering Toolkit (SET) is an open source python-driven social engineering toolkit for social engineering focused penetration testing. The tool provides readymade templates that can be sent via email to people. Custom made templates can also be made and saved. The attacks built into the toolkit are designed to be targeted and focused against a person or organization. The tool has the advantage is that it is open source and incorporates many social engineering attacks in one interface. Results can be used by an organisation to prepare training programs for its employees. A major drawback is that to use it one requires a certain level of technological skills such as penetration testers and those with proficiency in Linux (PrimalSecurity, 2016).

King Phisher is an open source tool for testing and promoting user awareness by simulating real world phishing attacks. Like Gophish, Kingphisher can be used to run phishing campaigns ranging from simple awareness training to more complicated scenarios in which user aware content is served for harvesting credentials. The tool is meant for legal use only when explicit permission of the targeted organization has been obtained. It uses the packaged web server that comes standard with python making configuring a separate instance unnecessary. This tool has the same drawbacks of Gophish that is; it is restricted to phishing training only. It therefore does not assess the overall cyber skills proficiencies and gaps of each individual.

Alert Online (www.alertonline.nl/cyberskillstest) is a web based simple cyber skills assessment tool developed to create cyber security awareness in the Netherlands. The tool presents questions in various categories of critical areas in cybersecurity. The user selects a category and answers the question. Feedback is provided after each question. The feedback is not only right or wrong but contains information to help enlighten the user more on the topic. The drawback of the tool is that it does not provide a comprehensive analysis and reporting of the user's proficiencies nor does it analyse their gaps.

Think. Check. Share is tool aimed at communicating the importance of information security to staff. The tool is not automated. Rather it comes as a document such as pdf or word and covers some of the most common mistakes at the work place including sending information to the wrong recipient, leaving work documents in public view or not appropriately disposing of information. It also covers phishing email awareness, importance of using authorised software, encryption of information, not leaving information unattended and acceptance use. All this information is presented in the form of printable posters to create awareness.

2.14. Summary

Reviewed literature points to the need for tools to help organisations assess employees' security skills so that gaps can be analysed and awareness and training programs customised to address those gaps. Some existing applications that support information security skills assessment have been reviewed. What is common about them is that they are mainly aimed at addressing a single area of information security skills assessment such as social engineering or phishing and require a certain level of technical skills. In addition, they are not customised or customizable to address the specific needs of an organisation.

The proposed application will therefore be adding some characteristic features that none of the existing applications have. These are 1) simplicity of use in the sense that users will require basic level of literacy to understand the information at the front-end and back-end dashboard and to respond to questions of the assessment. Users will not need to have any technical skills. 2) The application will take the form of an examination and will try to test all areas of information security that are relevant to employees. These areas include phishing, email security, social engineering, password security, malware, security policies and so on. As the employee goes through these questions the process helps him familiarise with various security terminologies and issues. 3) The application will give a report to the organisation on employees who have been assessed, their proficiencies and weak areas. The weak areas point to gaps which should be addressed through awareness and training.

2.15. A Conceptual Framework of the Proposed Solution

The aim of this study was to develop a web based information security self-assessment prototype to help organisations assess information security skills of their employees so that gaps can be analysed and security awareness and training programs customised to address those gaps. By a review of existing tools and approaches for information security skills assessment and knowledge enhancement, a conceptual framework for the proposed prototype was constructed. Figure 2.3 shows that framework.

The application was implemented in the following manner: questions that address common employees' weaknesses which attackers tend to easily exploit are created. These are then stored in a database in multiple choice format. Once a user initiates assessment, the questions are fed to his UI display using an html form. Questions are selected based on the department a particular user is registered under. If his department is ICT Management or ICT Support then technical security questions are selected. If he is not in an ICT department then only general information security questions are selected for him. Questions have multiple answers with a pre-determined best answer. The user can only choose one answer per question. Once the user completes the assessment and submits the answers, the results are processed using a PHP script in the application controller and the resulting values stored in the same database but in a different table. The analysis is achieved by using a basic JavaScript algorithm to first calculate the percentage from the points earned and then map this percentage onto a chart/graph. After analysis, the user is assigned a percentage score and ranked either as beginner (<=50%), intermediate (>50 & <70%) or advanced (=>70%).

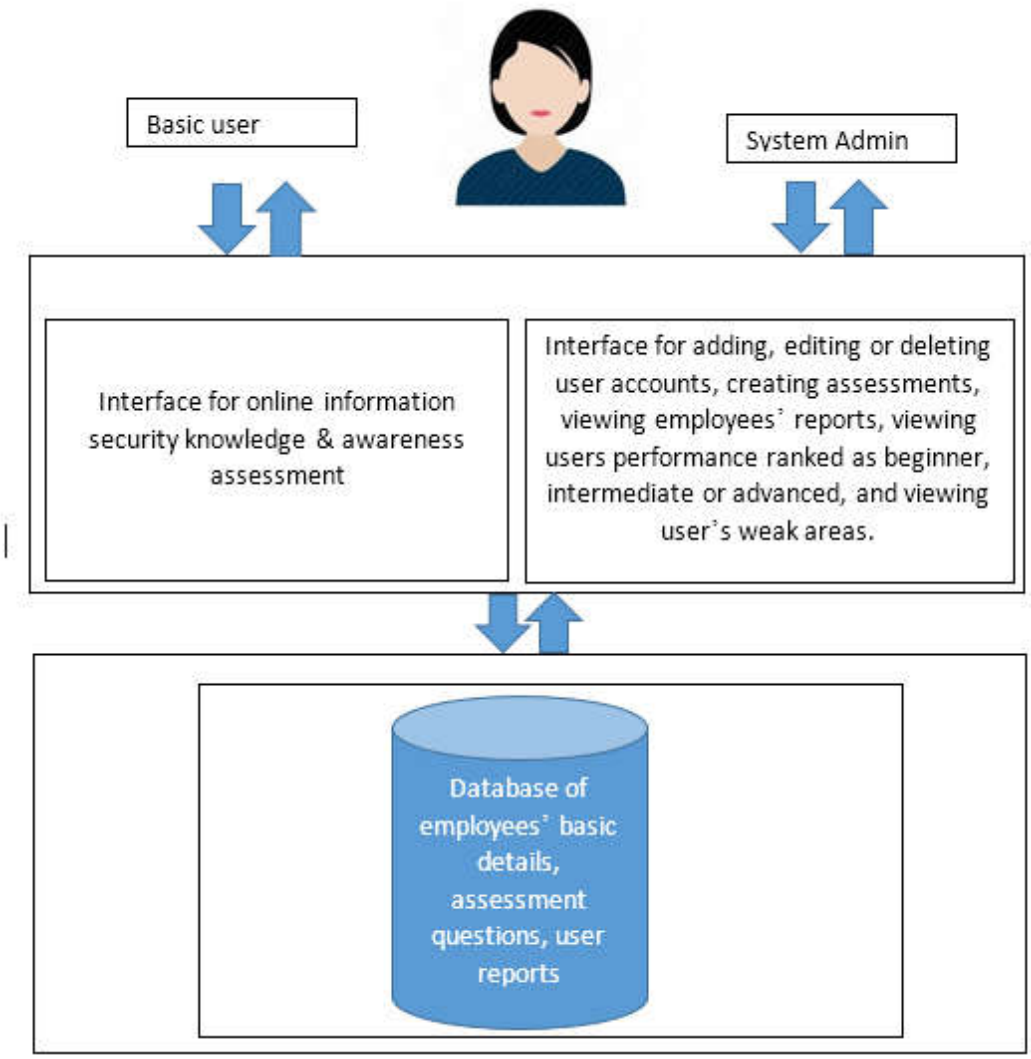


Figure 2.3 Conceptual Framework of the Proposed Solution

Chapter 3: Research Methodology

3.1. Overview

This chapter describes the methodology that was used to enable the researcher to answer research questions outlined in Chapter 1. The methods used for conducting the research and their viability are described in this chapter. Data collection procedures, approaches applied in system analysis, system design, system development and implementation and testing are discussed.

3.2. Research Design

A research design is basically a detailed outline of how an investigation will take place. It helps the researcher in addressing the problem statement and answering the research questions (Chilisa, 2012).

3.2.1. Collection of Data

Review of relevant scholarly articles, books, journals and surveys was used to illuminate the need for, approaches and challenges to information security in organisations. It also served to identify common employees' weaknesses that are easily exploited by attackers.

Given the lack of ample literature on information security in Kenya, research and surveys by various scholars and organisations across different countries were used. The quality of a literature review strongly depends on the search process (Brocke et al, 2009; Lebek et al, 2013a; 2014). Therefore the process of identifying literature that is relevant to the research objectives was paramount. This study followed the structure proposed by Webster and Watson (2002) to identify relevant literature. The search was limited to publications written in the English language. Publications, which are not accessible to the broad public, were excluded.

3.2.2. Software Development Methodology

The study adopted agile development methodology (Shore, J & Warden S, 2007), which comprises of 4 steps as shown in figure 3. Agile development was chosen for its short life cycle and ability to incorporate user feedback for future improvement of the prototype. The methodology is also useful in that it makes it possible to assess the direction of a project throughout its development life cycle (Harvin, 2016).

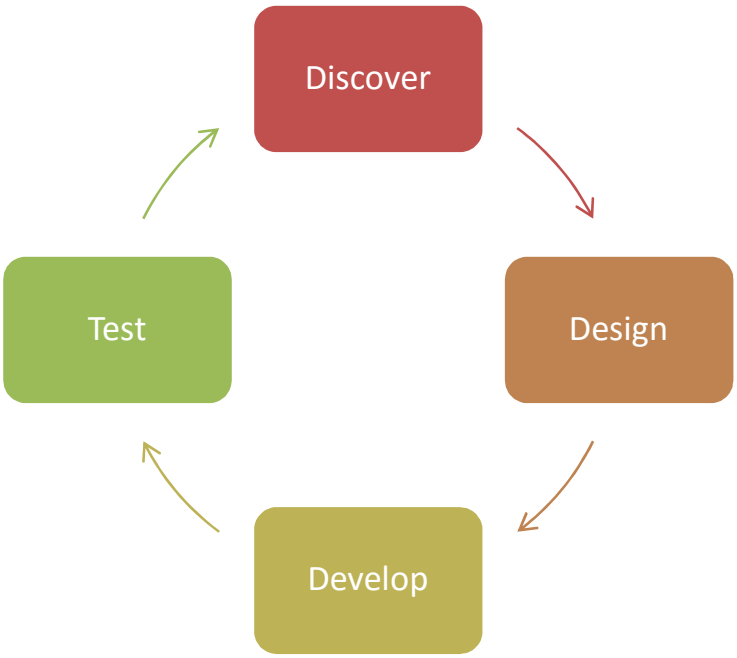


Figure 3.1 Agile Development Method

3.2.3. Analysis and Design

This study adopted object-oriented analysis and design (OOAD) approach. OOAD is a technical approach used in the analysis and design of a system through the application of the object-oriented concepts including visual modelling. This is applied throughout the development life cycle, fostering better product quality and even encouraging stakeholder participation and communication. In OOAD, objects are grouped into classes, which share structural and behavioural characteristics (University of Missouri, 2001).

In OOAD, the analysis phase entails using Unified Modelling Language (UML) to build a model of the real-world application and show its important properties. The UML is a

visual modelling language and is useful for graphically depicting object-oriented analysis and design models. The UML diagrams used in this study were use-case, class and sequence diagrams. These helped to visualise the proposed system in different ways and facilitate better understanding and communication of requirements. Object-oriented design (OOD) was used to refine the requirements identified during system analysis phase and to define design specific objects. The following is a further description of the UML diagrams that were adopted:

3.2.3.1. Use Case Diagram

A use case diagram was used to identify and partition the application into different functionality. This helps gain a clear understanding of the functional requirements of the system without worrying about how those requirements will be applied (University of Missouri, 2001). The application was divided into actors and use cases. An actor is an external entity that interacts with the system and a use case denotes a sequence of interrelated activities initiated by an actor to achieve a precise objective (Hoffer, 2001). In the case of the developed solution, actors are employees (as basic system user) and manager (as system administrator). A use case is normally presented as a text that describes the action an actor is effecting on the system.

3.2.3.2. Sequence Diagram

A sequence diagram was used to model, in a visual manner, the flow of logic within the application making it possible to document and validate application logic. Sequence diagrams are commonly used for both analysis and design purposes. They are the most popular UML artefact for dynamic modelling, which focuses on identifying the behaviour within your system (Rumbaugh, J. et al, 2005).

3.2.3.3. Design Class Diagram

A design class diagram was used for general conceptual forming of the application. It represented all the classes used in the system and how they are defined. A class is defined using its attributes and methods (IBM Developer Works, 2004).

3.2.3.4. System Architecture Design Diagram

A system architecture design was used to enable the researcher to breakdown the system into different main components and illustrate their relationship to each other. The main

components of the developed solution are a front-end accessible via a web browser and a back-end that comprises of a web server with a database that stores general user information, security questions used for assessment, assessment results and reports (Tutorial Point, 2017).

3.2.4. Implementation

The developed solution is a web-based application consisting of a front-end and a back-end. The backend dashboard was implemented using PhP. HTML 5 was the mark-up language used to layout the front end and to structure and present content in the back-end. MySQL was the relational database management system adopted. MySQL was preferred because it is open source and cross platform. PHP was selected because it is fast and platform independent (Sakshay, 2013). HTML 5 is dynamic and can be used to produce neat websites with less code than HTML its predecessor. JavaScript was used to create a basic algorithm, which calculates the percentage from the points earned by an employee after assessment, and then maps this percentage onto a chart/graph.

3.2.5. Testing

The aim of this stage was to demonstrate that the developed solution accurately satisfies its specified requirements and objectives (Guru99, 2017). Agile testing methodology was employed. Agile testing allows for continuous testing from start to end of development as well as after deployment. More specifically, individual components of the prototype were identified and independently tested. Menu buttons were also tested to ascertain that they function as intended. After testing individual components, the system was tested as a whole whereby sample data was loaded into the application and results observed. Finally, once all individual components were ascertained to work as intended, the prototype was deployed via the web to allow users to test its usability. Questionnaires were used to collect usability feedback from respondents. The feedback was analysed against specified requirements of the prototype to ascertain that these requirements were actually met and to what degree.

3.2.6. Validation

Software validation generally is a process to show that a system conforms to its specifications and meets the expectations of the requirement definition and program development (Sommerville, 2004). In this study, questionnaires issued to users during testing phase were studied. Positive responses to the questions were used to determine whether the prototype functioned as intended and was of value to the users. Negative responses were used to determine usability and functionality problems in the system so that improvements can be made.

Chapter 4: Design and Architecture

4.1. Overview

The developed prototype called Mambo Analytics enables organisations to assess its employees' information security skills. Information security questions covering general areas that tend to be easily exploited by attackers are created by the system administrator. These are then stored in a database. These questions fall under two main categories namely Apprentice and Master. Apprentice questions cover general information security topics that are applicable to all information systems users. Master category of questions cover advanced information security topics mainly focusing on technical personnel such as ICT support department. A staff member in the ICT department is given access to the Master category while a member of staff from any other department is directed to the Apprentice category. Agile development methodology was used to develop the prototype.

4.2. System Architecture

The main components of the developed solution are a front-end accessible via a web browser and a back-end that comprises of a web server with a database that stores general user information, security questions used for assessment and assessment results of each user. The system has the following main actors: system administrator with unlimited organisation specific data access. He/she has to be a trusted person in the organisation because he can create user accounts and view reports of all staff members. The second actor is the basic user with unlimited access to his own profile, assessments appropriate for his department and his own assessment report and certificate of completion. The basic architecture

of the prototype is depicted in Figure 4.1.

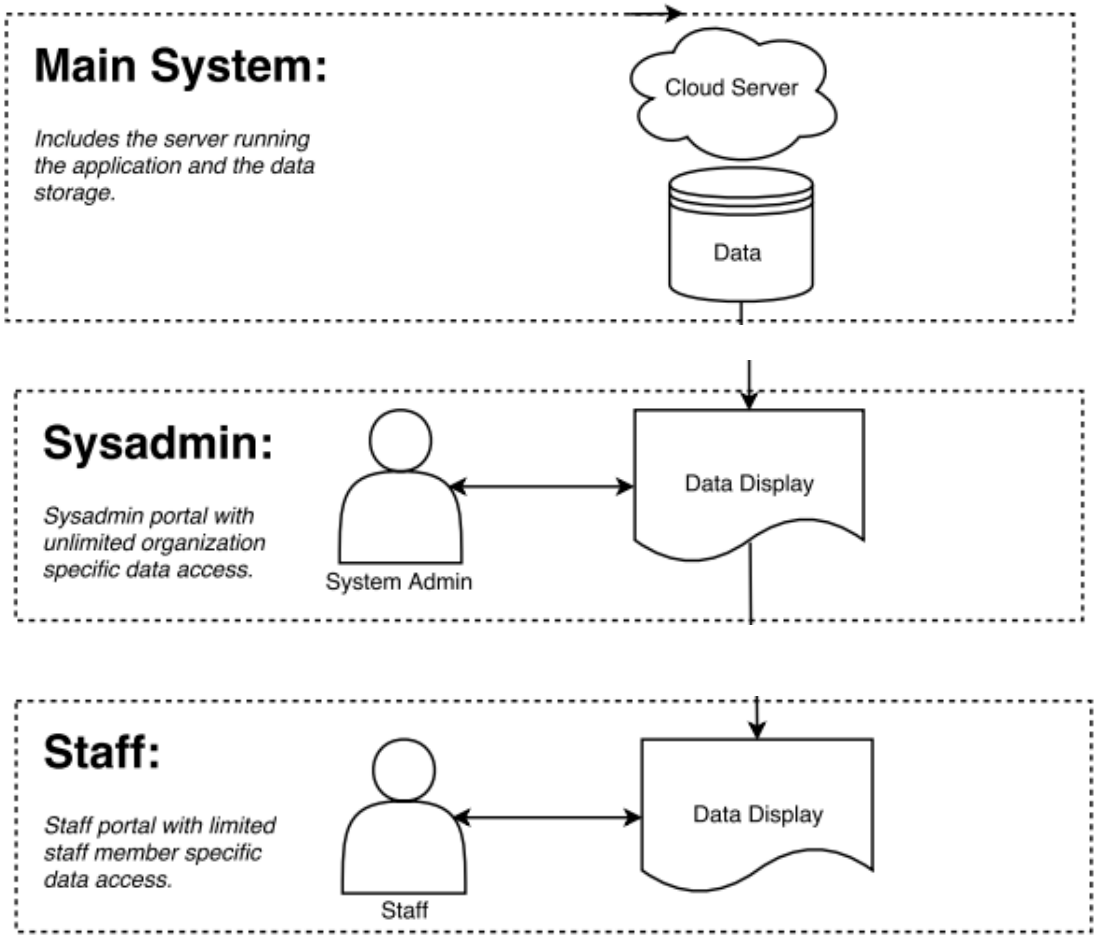


Figure 4.1 System Architecture

4.2.1. Question Database

The system is an automated web-based self-assessment prototype. Information security questions are created by the system administrator and stored in a MySQL database in text format and are categorised into two groups namely Apprentice and Master. Apprentice questions cover general information security topics such as social engineering, phishing, password security and so on. Apprentice questions cover technical information security topics such as firewalls, intrusion detection systems, operating system hardening and so on. A system administrator can create more categories according to the organisation's needs. Questions have multiple choices with a predetermined correct answer stored in the database. A key field in the user profiles is the department because it determines which

category of questions is available to a user. Apprentice category of questions is made available to all departments while the Master category is availed only to ICT department because of its technical nature. Questions are retrieved from the database, depending on the particular member of staff's department, and fed to his UI.

4.2.2. Scoring Engine

The user gets to respond to the questions by selecting what he thinks is the correct answer to each question. The system analyses the answer provided by the user and marks them either as correct or wrong depending on whether they tally with a predetermined correct answer stored in the database. Each question has a pre-allocated mark. The marks for every correct question are added up and a percentage score automatically calculated.

4.2.3. Reporting

A report is produced which shows the respondent an overall percentage score and questions that were marked wrong. If the percentage score of the user is 50% or less he is ranked as beginner, above 50% but less than 70% intermediate, above 70% is ranked as advanced. The questions marked wrong point the staff member to areas that he needs to improve. The system administrator can view all user reports individually or aggregated.

When a system user later on requests for a given report, the corresponding variable values (i.e. staff id, assessment id) are passed to the 'Reports Controller' under the 'Reports Function'. These variables are then used in the corresponding SQL queries to the database to obtain the basic data sets required for report processing (i.e. question id, number of questions attempted, number of questions completed, number of questions failed and so on). Once this data is returned from the database into the report script, the 'Performance generation' algorithm then computes out all the raw data into meaningful data sets which can be appended onto the display pages. The processed data is then appended onto the 'Reports' module, either directly via html tags, or via JavaScript onto visualization charts and graphs. The reports generated are session specific, and hence they are only available upon request by the system user and are terminated once a session is terminated.

4.2.4. Analytics

The system administrator can view summary of reports such as ranking of staff members as beginner, intermediate or advanced. He can also view a staff recap report showing the Apprentice and Master level total number of users who attempted each assessment, number that passed and number of staff that failed. In addition, the system administrator is able to view each user's reports such as percentage score, ranking, number of questions attempted, number of questions answered correctly, number of questions failed and the specific questions that were failed. The failed questions known in the system as 'weak areas' are a pointer to areas that the particular member of staff needs to improve on.

4.3. System Design Tools

4.3.1. Use Case Diagram

The Use Case diagram illustrates the major interactions that take place between the various subsystems and actors in the developed prototype.

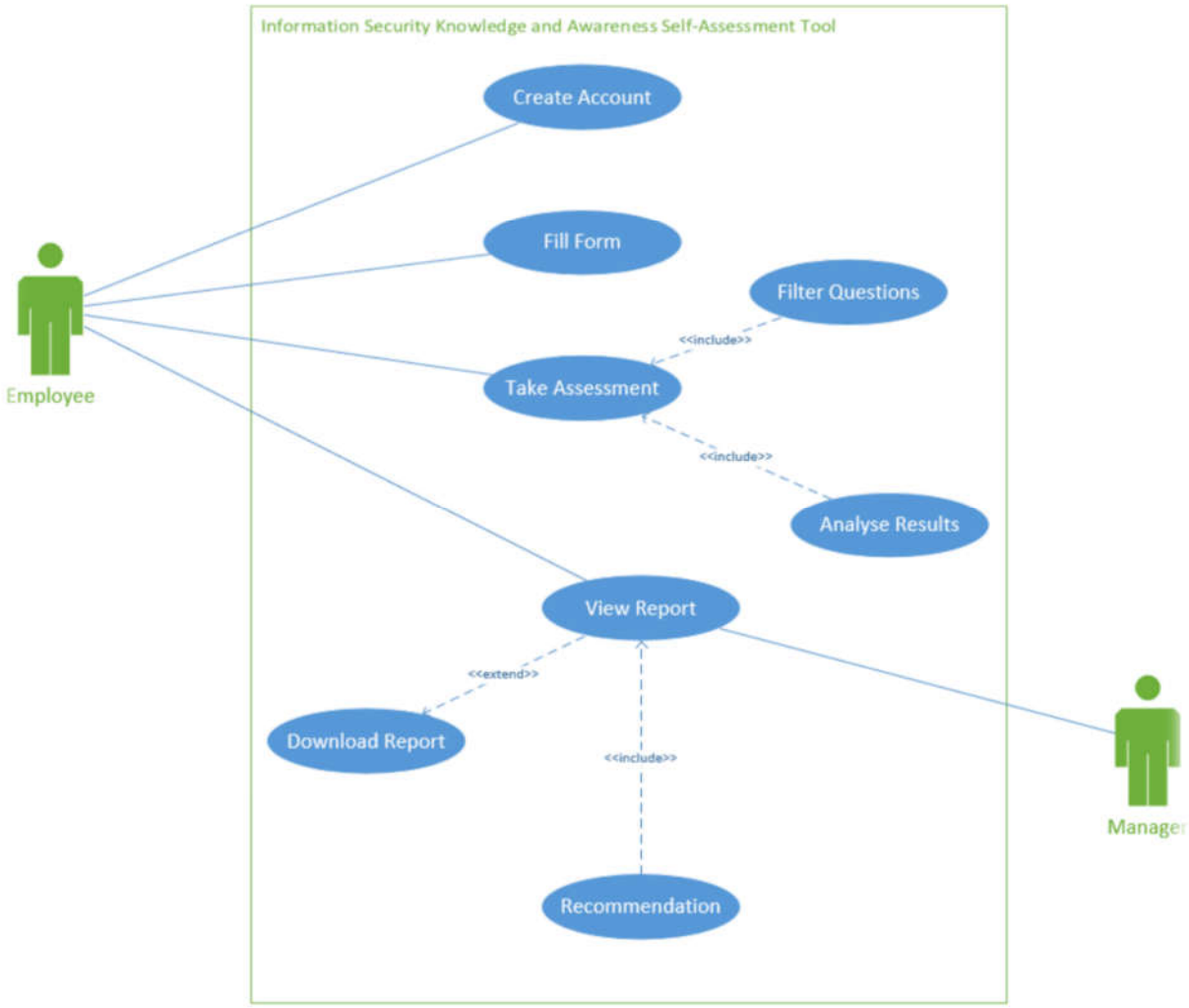


Figure 4.2 Use Case Diagram

4.3.2. Class Diagram

Figure 4.3 shows a class diagram, which is basically a static representation of the system. It describes the attributes and operations of each class and the constraints imposed on the system.

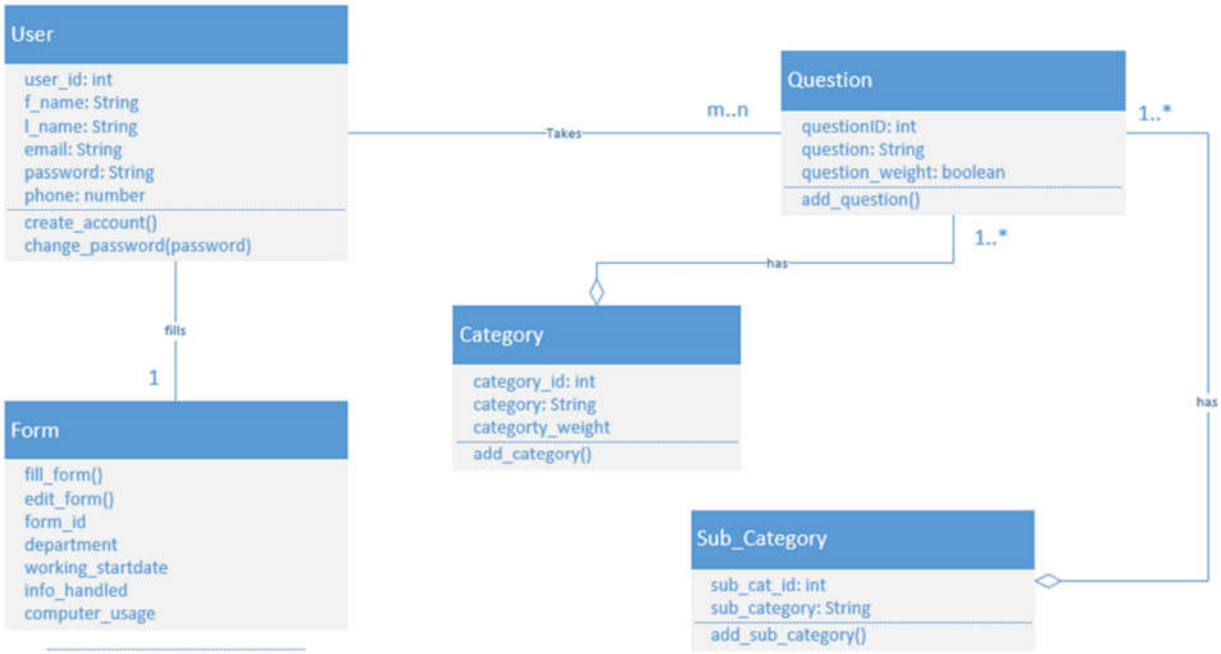


Figure 4.3 Class diagram

4.3.3. Sequence Diagram

The purpose of a sequence diagram is to illustrate the sequential flow of information passing through the key entities of the system. Figure 4.4 shows a sequence diagram for the developed solution showing how a user is authenticated into the system to allow access to the assessment.

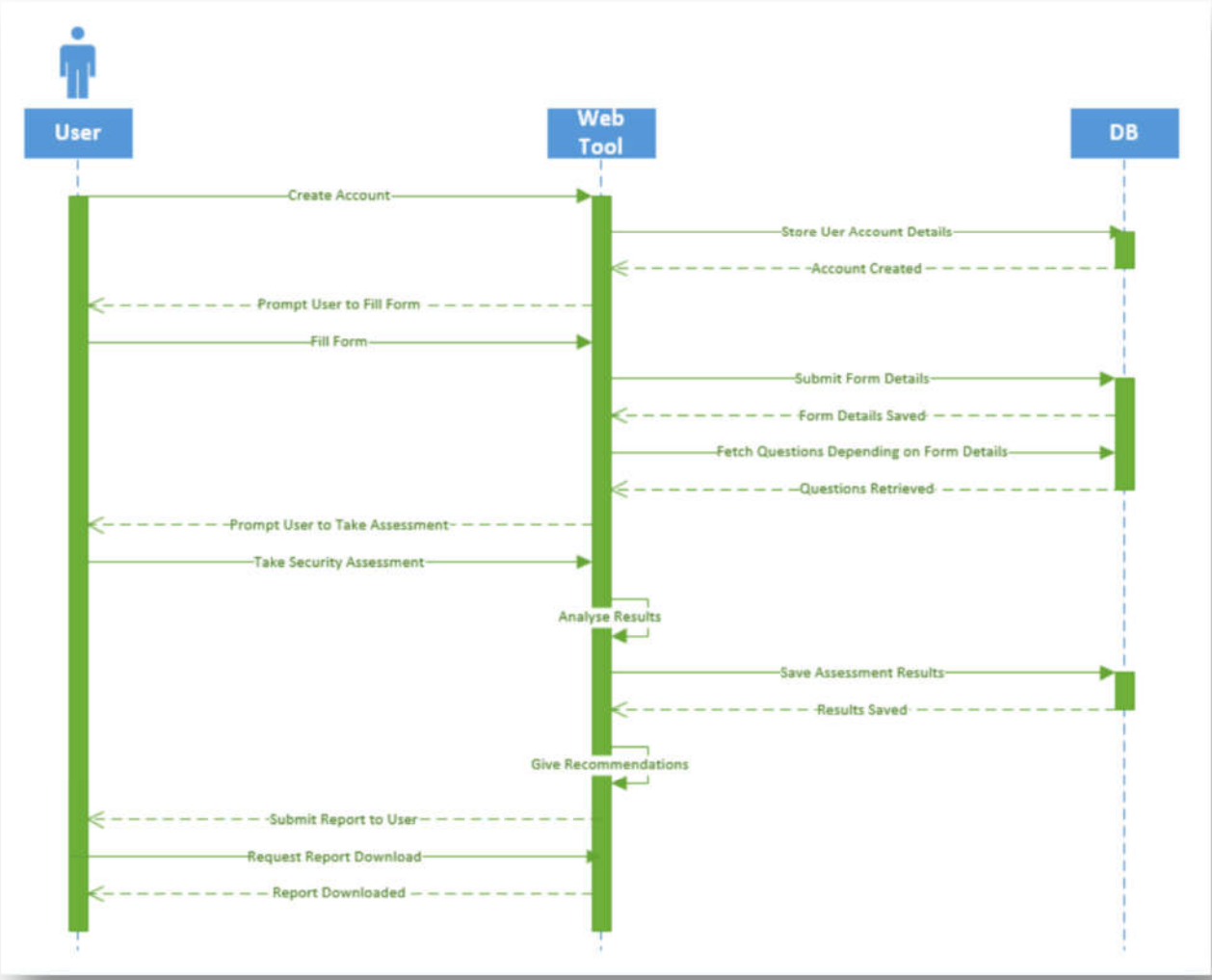


Figure 4.4 Sequence diagram

4.4. Database Design

4.4.1. Entity Relationship Diagram

The database uses a number of entities to collect, save and retrieve data. These entities are represented in Figure 4.5. An Entity Relationship Diagram is a type of flowchart that shows how "entities" such as people, objects or concepts communicate with each other within a system. In this system, a basic user can only take the assessment appropriate for his department. For example a member of staff in the ICT department can access and attempt the Master category of questions while a member of staff from any other

department can only attempt the Apprentice category of questions which cover general information security questions applicable to all information systems users. Additionally, a user can attempt only one assessment at a time. A basic user can edit his own profile, change his password, view his own assessment report, and print his own certificate of completion. The system administrator can create user accounts, create new categories of assessment, and populate an assessment with questions, view individual users' reports, and view aggregate reports.

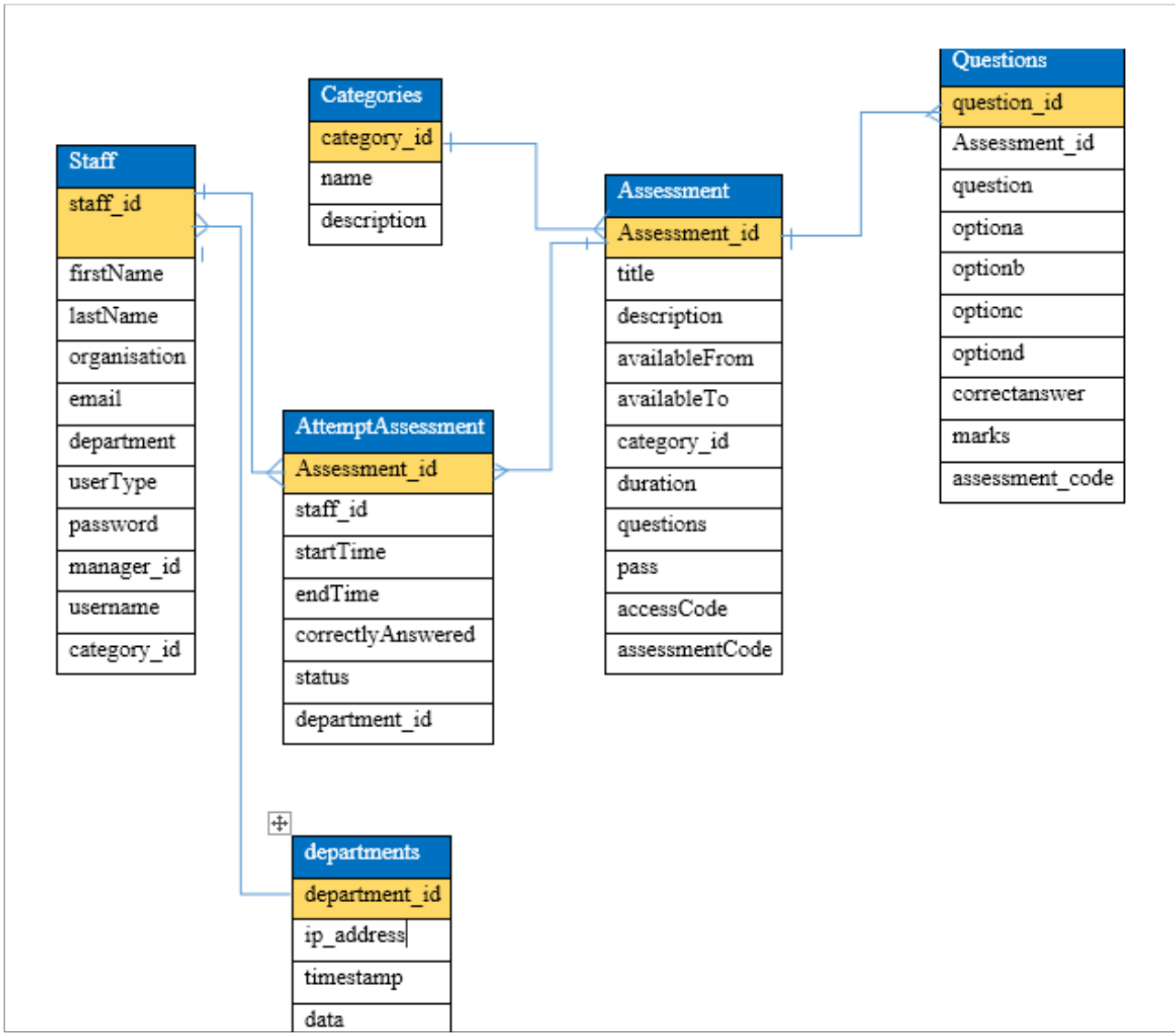


Figure 4.5 Entity Relationship Diagram

After identifying main functions of the prototype, the database schema was designed. A top-down design approach was used to design the schema whereby logical groupings of attributes into relations were identified such as user registration and user management, creating an assessment, taking assessment, results analysis and reporting. Database tables are shown in Appendix H.

4.5. Security Design

Principles adopted to design the solution were: (1) least privilege, which ensures a user, is assigned minimum privileges needed to carry out his responsibilities, (2) Separation of privilege - there is a system administrator account and basic user account whereby the administrator account is granted the privilege to edit user records and view all reports. A basic user account is only able to view own profile, take assessment and view own report. To ensure confidentiality and availability, the web application authenticates all users to ensure authorised access to the system and its various modules and to determine their level of privilege.

To safe guard system integrity, internal security was implemented to restrict access of critical data items to only those access types required by users, audit procedures were used to meet control, reporting, and retention period requirements for operational and management reports, application audit trails were implemented to dynamically audit retrieval access to designated critical data. Verification processes for additions, deletions, or updates of critical data were also implemented.

4.6. User Interface Design

Figure 4.6 shows the system architecture flow chart.

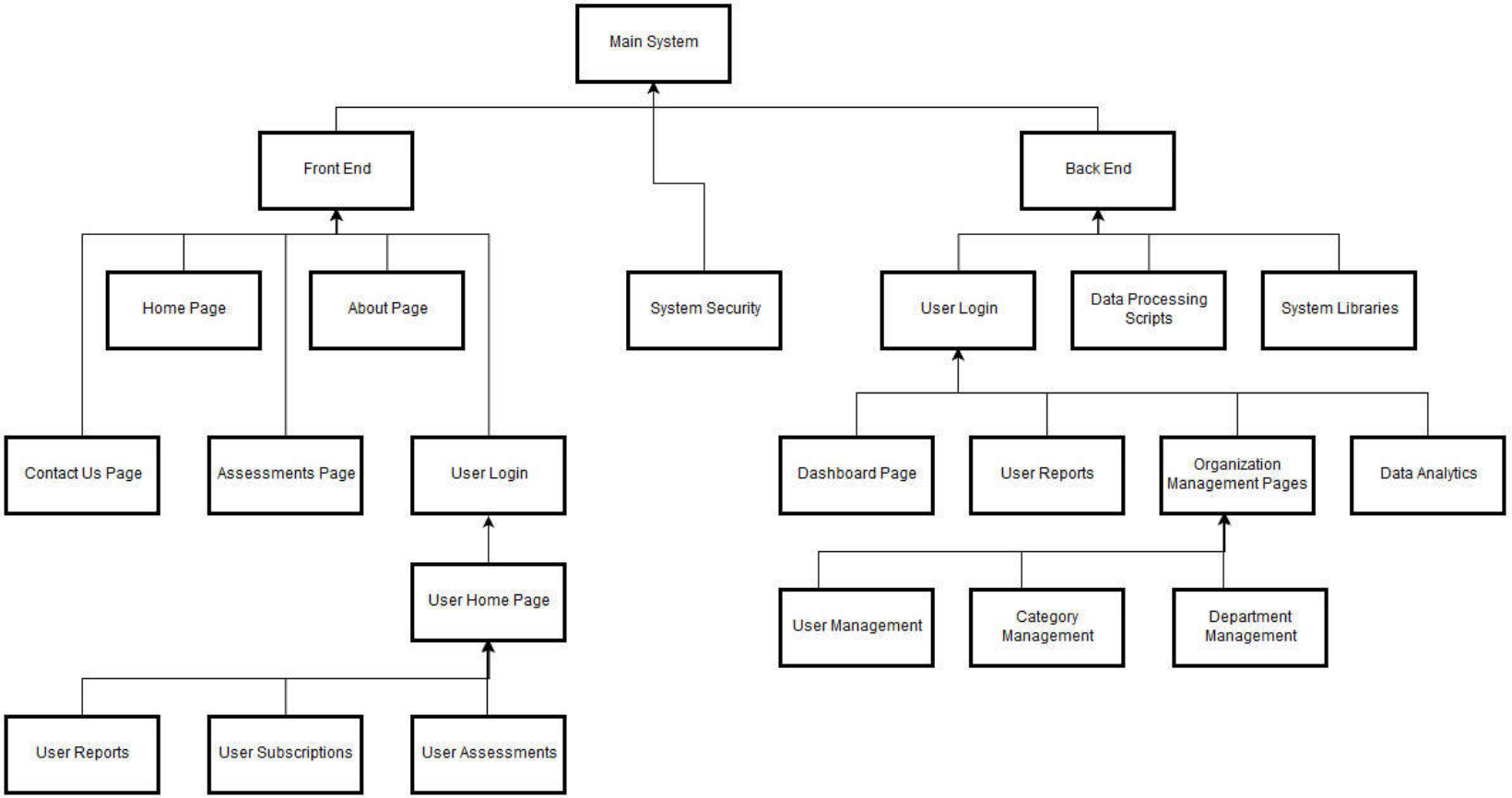


Figure 4.6 System Architecture Flow Chart

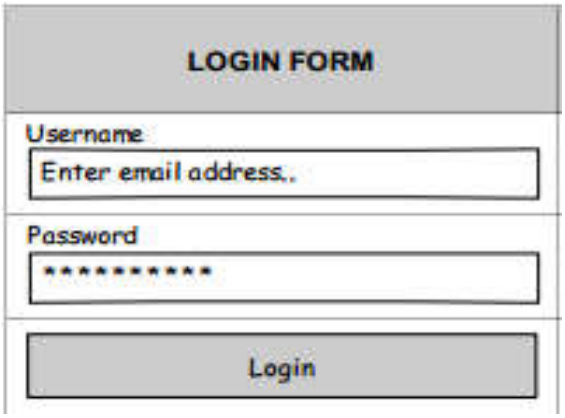


Figure 4.7 Login Form

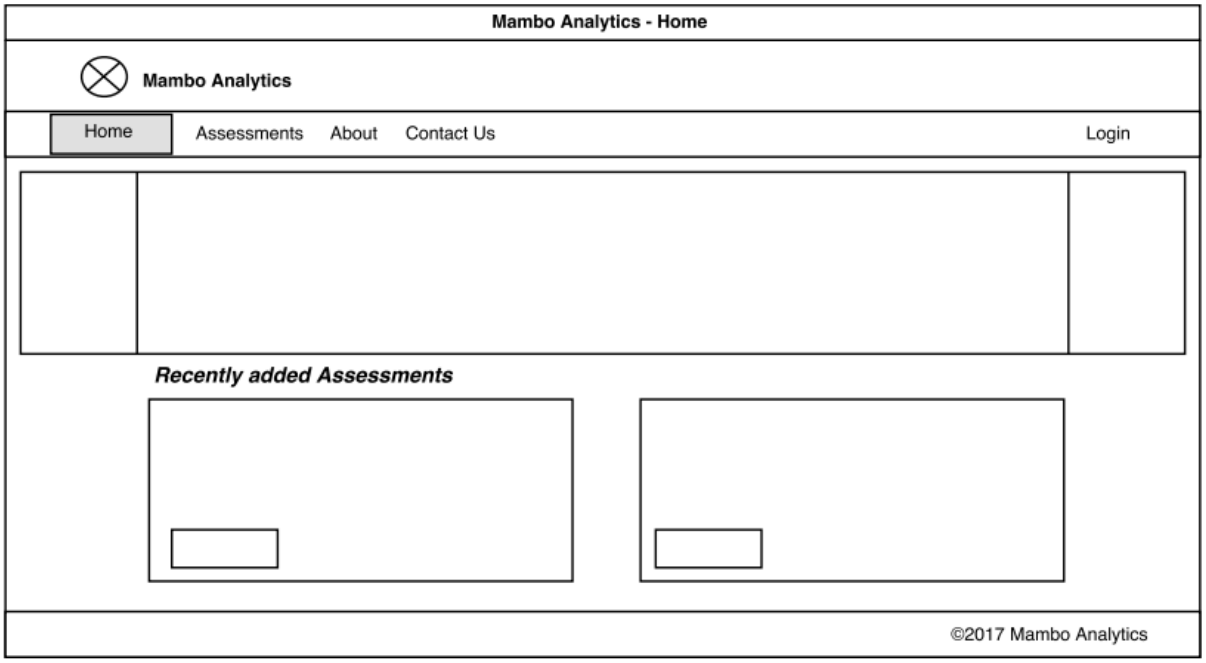


Figure 4.8 Home Page

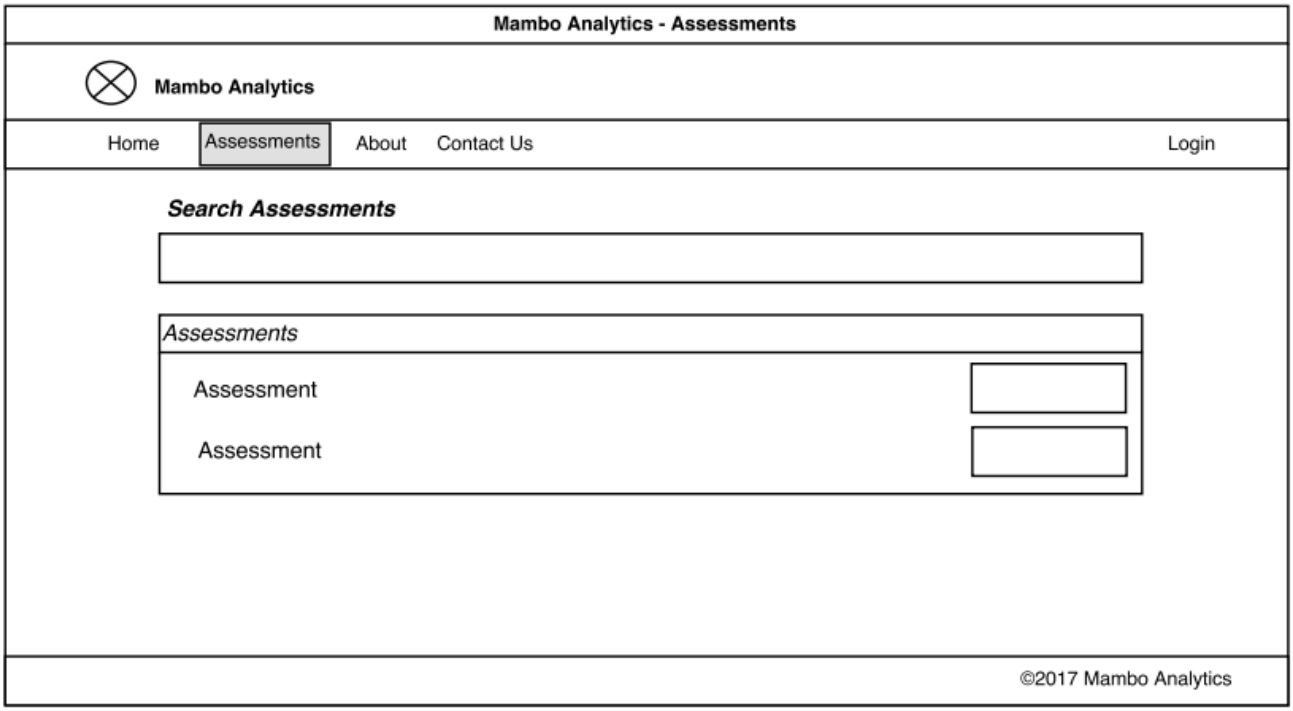


Figure 4.9 Assessments Page

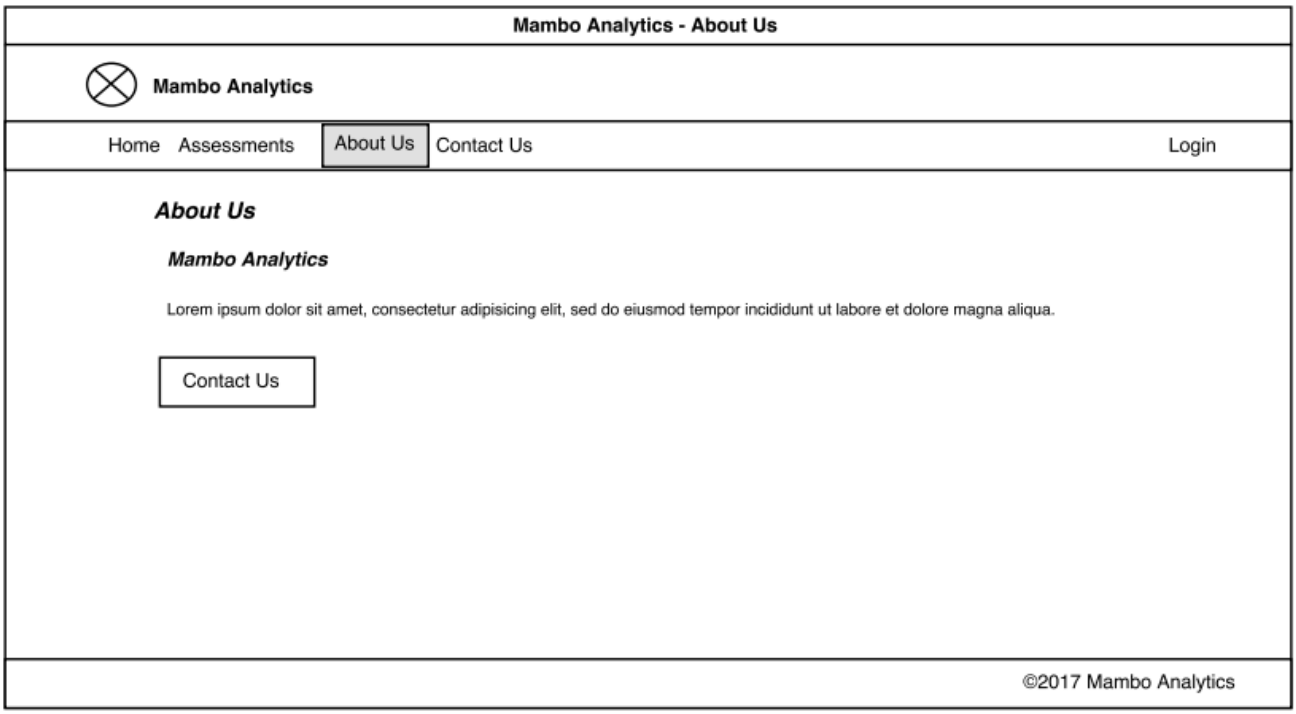


Figure 4.10 About Us Page

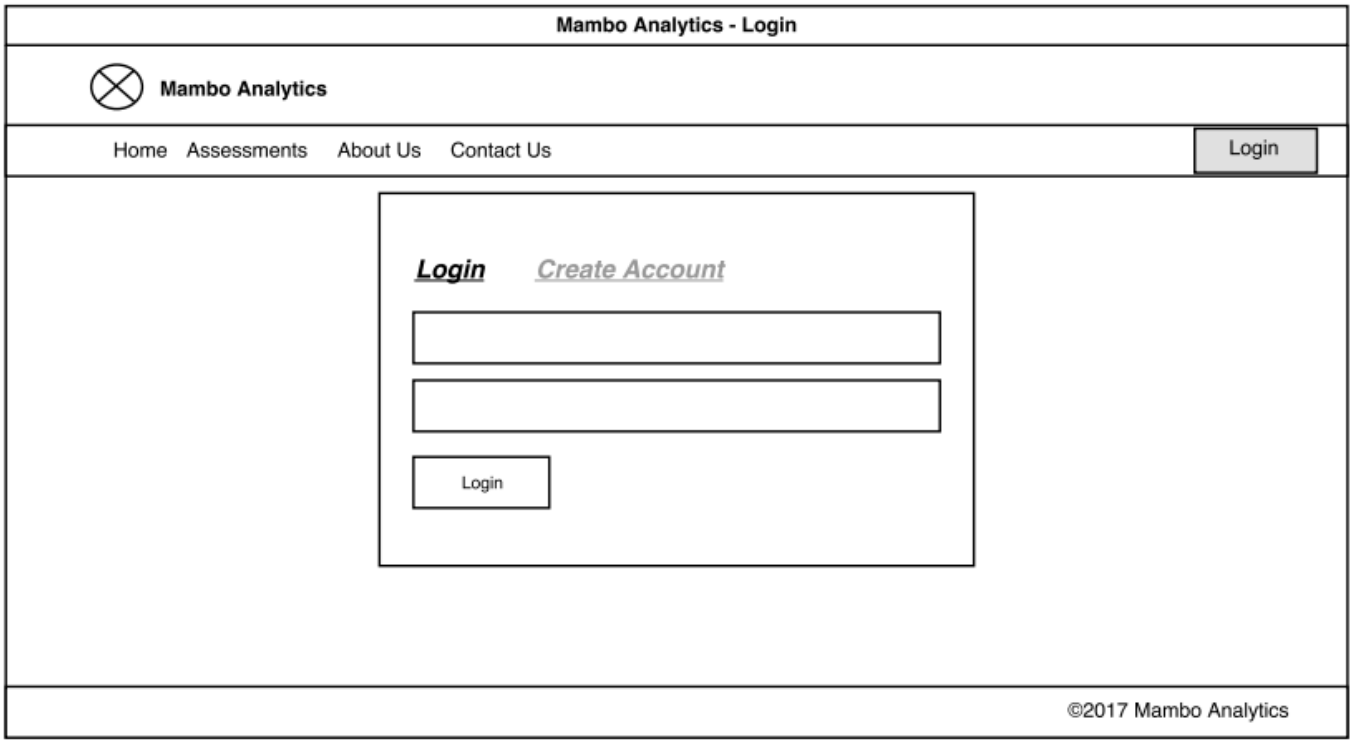


Figure 4.11 Create New User Account Page

Chapter 5: System Implementation and Testing

5.1. Overview

This chapter discusses the system implementation procedures. 5.2 Software implementation environment. 5.3 Hardware environment. 5.4 Main functions of the prototype. 5.5 Testing which describes the kind of tests carried out and the intended results. It includes the relevant screenshots of the web application. Lastly 5.6 Provides a summary of the chapter.

5.2. Implementation Environment

The developed solution known as Mambo Analytics is a web-based application whose backend dashboard was implemented using PhP. PHP was selected because it is fast and platform independent (Sakshay, 2013). HTML 5 mark-up language was used to layout the frontend and to structure and present content in the back-end. HTML 5 was chosen because it is dynamic and can be used to produce neat websites with less code than HTML its predecessor. MySQL version 5.1.73 relational database management system was adopted. MySQL was preferred because it is open source and cross platform. JavaScript was used to create a basic algorithm, which calculates the percentage from the points earned by an employee after assessment, and then maps this percentage onto a chart/graph.

Mambo Analytics was developed using the Model View Controller (MVC) architecture and on the open-source Code Igniter platform. Overall, the system is divided into several modules which include user authentication, user management, assessments, analytics and reports. The data received from the input forms is processed by a Controller in the application folder. The processed data is displayed to the user via dynamically generated charts and graphs using Ajax and JavaScript. Mambo Analytics can run on any PHP enabled web server that can connect to a MySQL database. This includes shared servers, dedicated servers, and local installations running on Linux, UNIX, BSD, Mac OS X, and Microsoft Windows operating systems. The requirements to have Mambo Analytics system up and running are: web Server, PHP version 4.5+, MySQL Database Server.

Mambo Analytics consists of a front-end and back-end: Both can be accessed through a web browser. PhP programming language was used to develop the web application – back end, while HTML 5 was used to develop the user interface. Both front-end and back-end are further explained below.

Mambo Analytics Front-end

Figure 5.1 shows a screenshot of Mambo Analytics front-end while Figure 5.2 shows the assessment page. To take an assessment a user must login first.

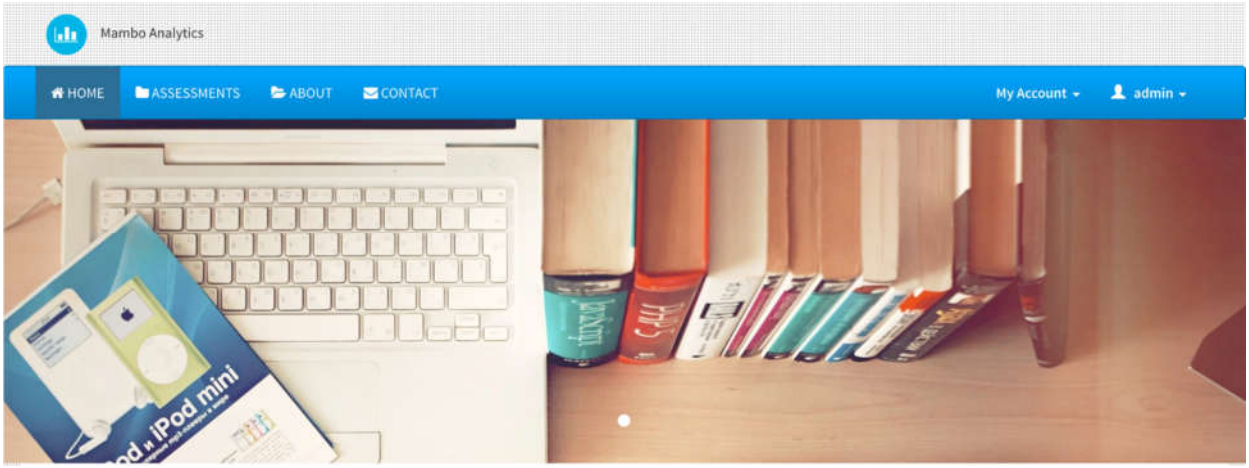


Figure 5.1 Mambo Analytics Home Page

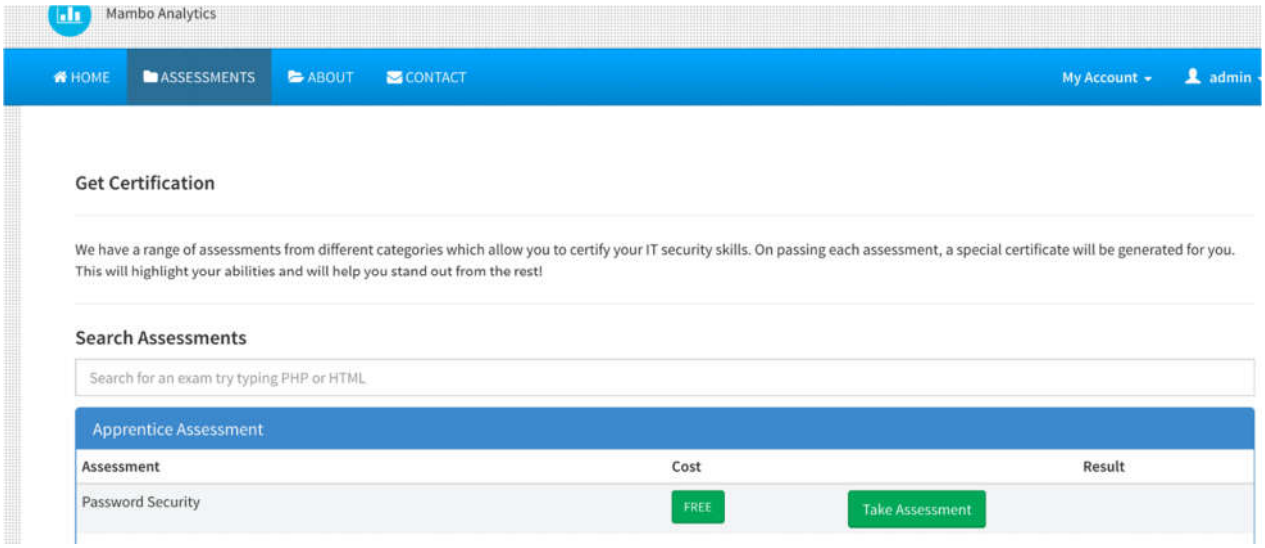


Figure 5.2 Mambo Analytics Assessments Page

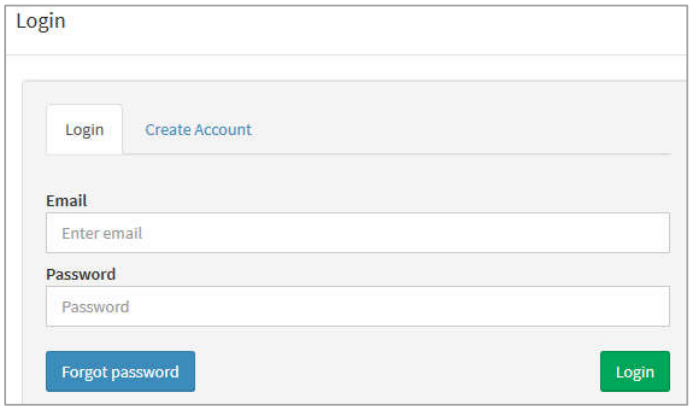


Figure 5.3 Mambo Analytics User Login Page

Mambo Analytics Back-end

Once logged in, a basic user can only view his profile and attempt the assessments available for his department. There are two categories of assessments namely apprentice and master. Apprentice assessment covers general information security topics and is meant for non-technical personnel. This category can have many sub categories such as password security assessment, general information security assessment, social engineering assessment and so on. The Master category on the other hand covers mainly technical information security topics and is meant for technical personnel such as ICT managers and ICT support staff. Assessment categories screenshots are shown in Appendix A.

Generation and Storage of questions

Questions are generated from normal text data input into an html form in the application. This form-data is first filtered and cleaned to avoid SQL injection and cross site scripting (XSS). Once checked, the 'Questions Controller' then binds it into an array and sends it for storage in the database under the table 'Questions'. For every question, a predetermined best answer is set and stored in the database under the table 'Answers', this also includes the allocated mark/points. Once a user answers a question, the answer he/she chooses is stored together with the question_id and assessment_id into the database under the table 'User assessments'. Figure 5.4 shows sample questions with points allocation. Figure 5.5 shows a sample question and its predetermined answer.

My personal security and that of my organisation is first and foremost my responsibility.	2
What is the most common delivery method for viruses?	2
If you're not careful which websites you visit, which of the following can result?	2
What should everyone know about information security? (Select the best answer)	2
What is the biggest vulnerability to the security of your organisation's sensitive information?	2
Which of these is not a good physical security practice?	2
The first step in Security Awareness is being able to _____ a security threat.	2
Which of the following is NOT a best practice for ensuring security of your organisation building?	2

Figure 5.4 Sample Questions and Points Allocated

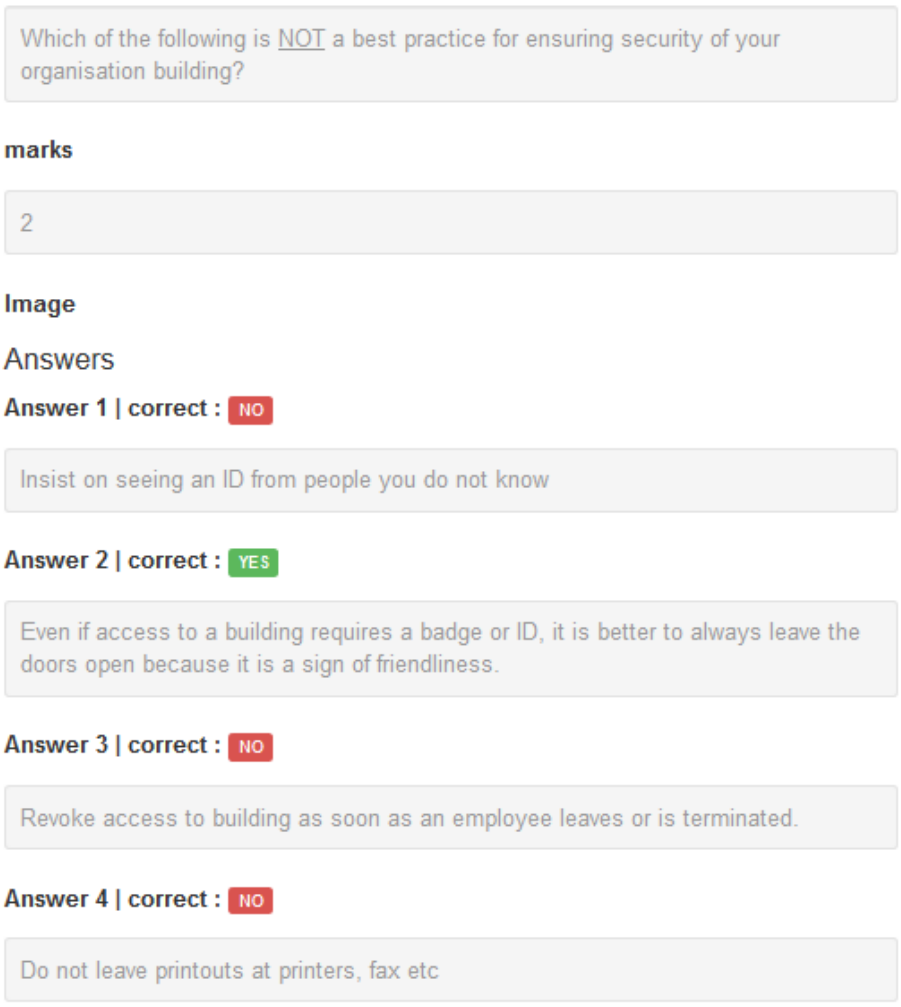


Figure 5.5 A Sample Question and its Predetermined Answer

Marking and Scoring

Questions are retrieved from the database, depending on the particular member of staff's department, and fed to his UI. The employee gets to respond to the questions by selecting what he thinks is the correct answer to each question. The system analyses the answer provided by the user and marks them either as correct or wrong depending on whether they tally with a predetermined correct answer stored in the database. Scores for the user are calculated by a script in the 'Assessments Controller'. This script computes all total questions attempted, correctly answered questions, wrongly answered questions, time taken to complete assessment and their corresponding percentages. Figure 5.6 shows an assessment report showing user's score.

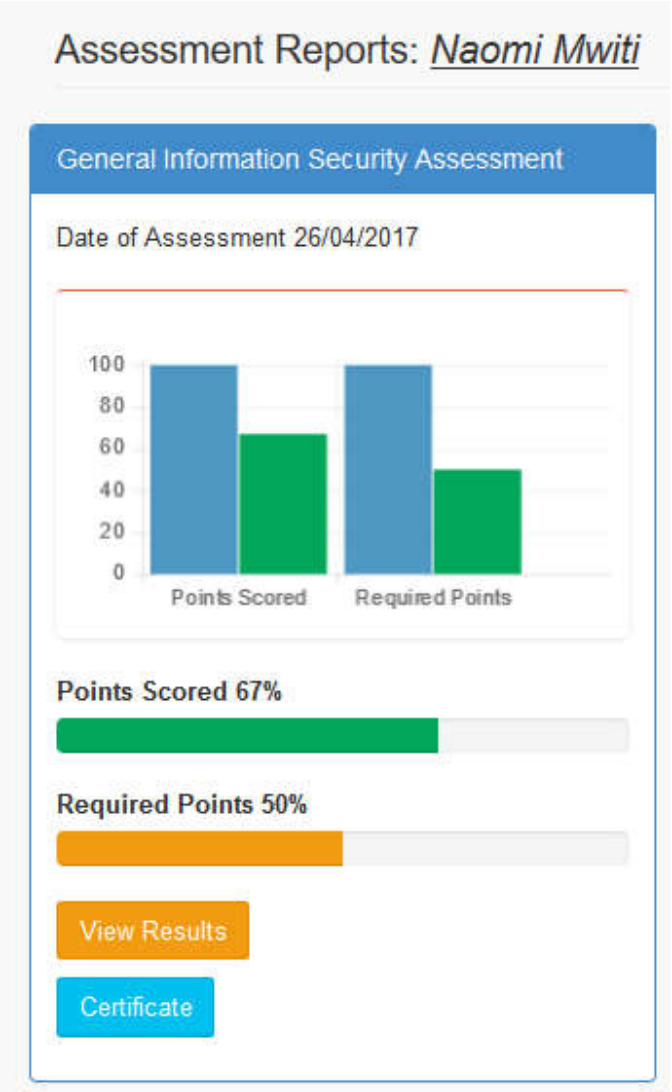
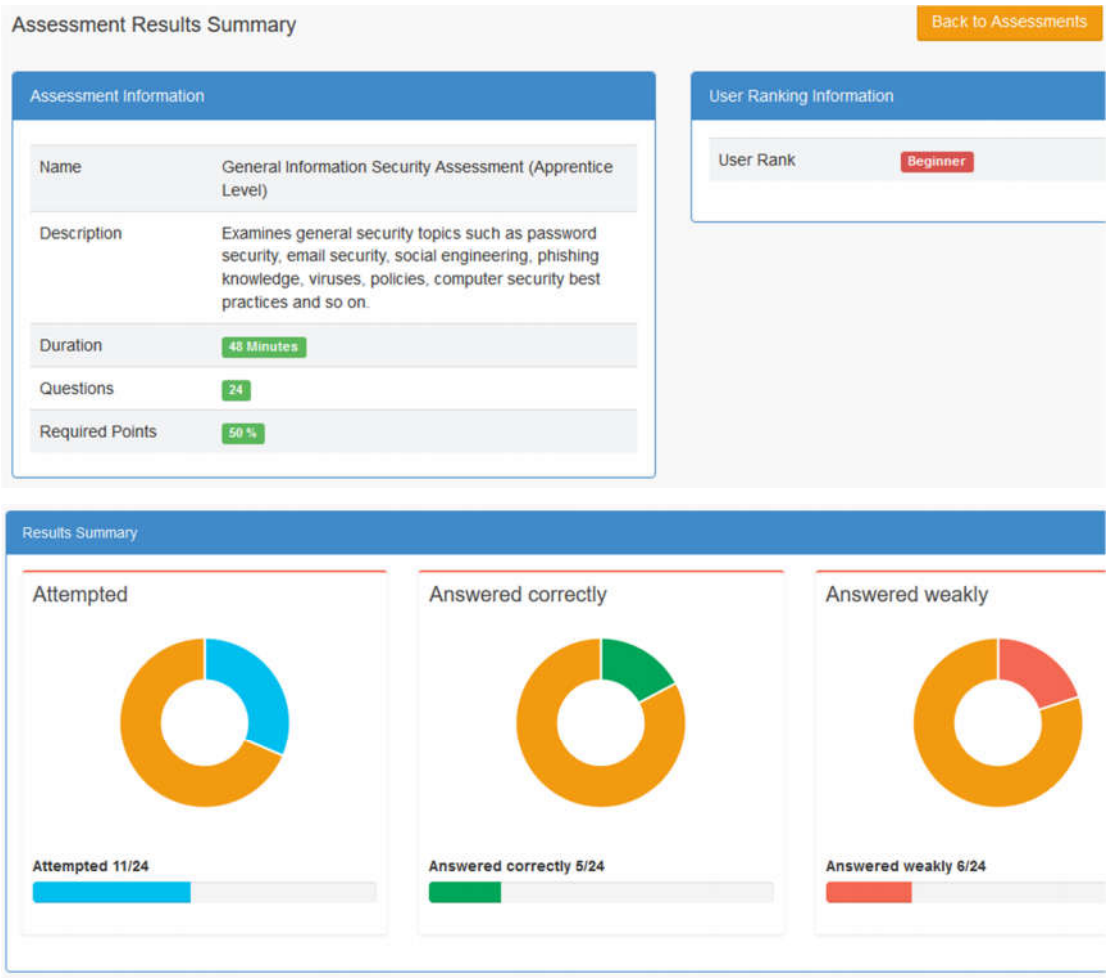


Figure 5.6 Assessment Report Showing User's Score

Reporting

The computed data is then appended into JavaScript charts and graphs for reporting and analytic visualisations. This is done entirely from JS scripts in the corresponding modules. Figure 5.7 shows a sample assessment summary for an individual user while figure 5.8 shows a sample certificate of completion generated for a user after an assessment.



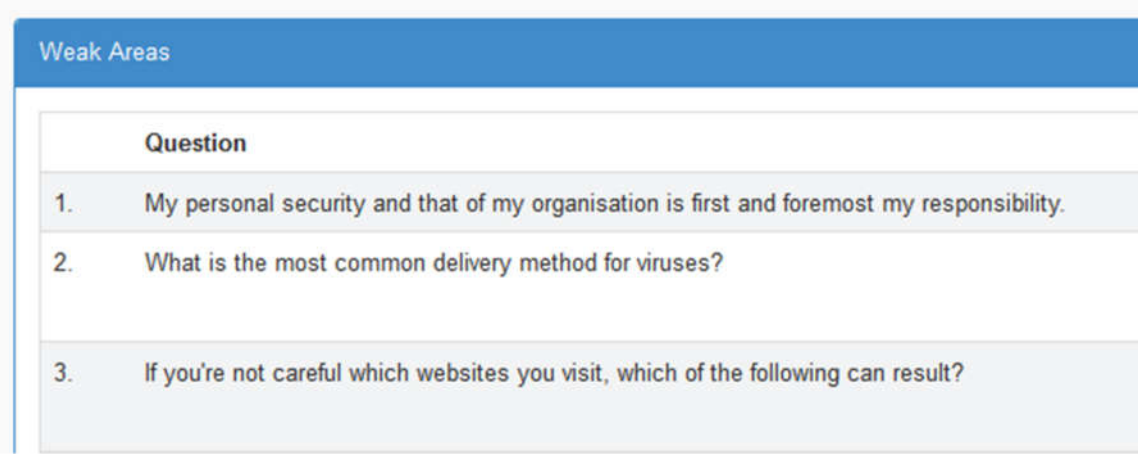


Figure 5.7 Sample User Assessment Summary

Figure 5.8 Sample Certificate of Completion

5.3. System Testing

An application must be thoroughly tested to ensure that it accurately and completely satisfies requirements. Agile testing methodology was employed which means testing was conducted continuously from the start to end of development as well as after prototype deployment. For example, individual components of the Mambo Analytics prototype were independently tested, then tested as a whole system. Additionally, the

application was deployed via the web to allow employees of Strathmore University and the University of Nairobi to test its usability. The researcher selected some key departments with consultation with HR units from which to randomly identify staff who could participate in the testing.

5.3.1. Individual Component Testing

The main pages of Mambo Analytics prototype are login page, dashboard page, users management page, create new assessment page, manage assessment page, add assessment questions page, view assessment page, questions management page, edit assessments page, system reports page. Each of these were tested and ascertained to be functioning as intended.

5.3.2. Whole System Testing

After testing the individual components, the system was tested as a whole from the time an organisation creates an account to the time a user takes assessment and reports generated. This was to check on functionality, robustness, performance speed and security. All pages and reports loaded in less than 3 seconds. All modules were ascertained to be working as intended. Sample screenshots are shown in appendix C.

5.3.3. Usability Testing

Once the above testing was completed, the application was deployed to the internet via URL http://www.demo.genericgroup.co.ke/mamboanalytics/. Strathmore and University of Nairobi personnel were invited to test the application. The researcher selected some key departments with consultation with HR units from which to randomly identify staff who could participate in the testing. The feedback was generally positive. Appendix D shows a questionnaire that was used to collect feedback from users.

5.4 Usability Testing Results

Questionnaires were used to collect feedback from 10 respondents who volunteered to test the application. This feedback is shown in Appendix E and is further discussed below.

5.4.1. User Friendliness

By use of the usability testing questionnaire, the researcher was able to collect the number of respondents who work as ICT support staff and those who consider themselves tech

survey. This was important in determining whether the application is suitable for non-technical people based on their usability feedback. Out of the 10 respondents, 50% considered themselves tech survey while the other 50% did not. 20% of the respondents work as ICT support while 80% are not. 60% of respondents were teaching staff while 40% were not.

The above notwithstanding, 100% of respondents were able to login to the application. 20% however indicated that they had trouble logging in at the start. They however indicated incorrectly typed password and poor internet connectivity as the cause. Out of the 10 respondents who tested the application, 60% rated ease of navigation and clarity of questions good while 40% rated it excellent. Clarity of assessment reports was rated good by 50% of respondents and excellent by the other 50%. Usefulness of assessment report was rated excellent by 90% of respondents. 50% respondents strongly agreed that the system was easy to use. 70% of respondents strongly disagreed with the statement that they would need support of a technical person to be able to use the system, 20% disagreed and 10% were neutral.

5.4.2. Usefulness of the System

90% respondents strongly agreed that the system was useful and 80% respondents strongly agreed that they would recommend it to their friends. When asked what they liked most about the application, many respondents responded that they did not know that security skills could be tested and that the application was a novel and very important idea. Figure shows their responses.

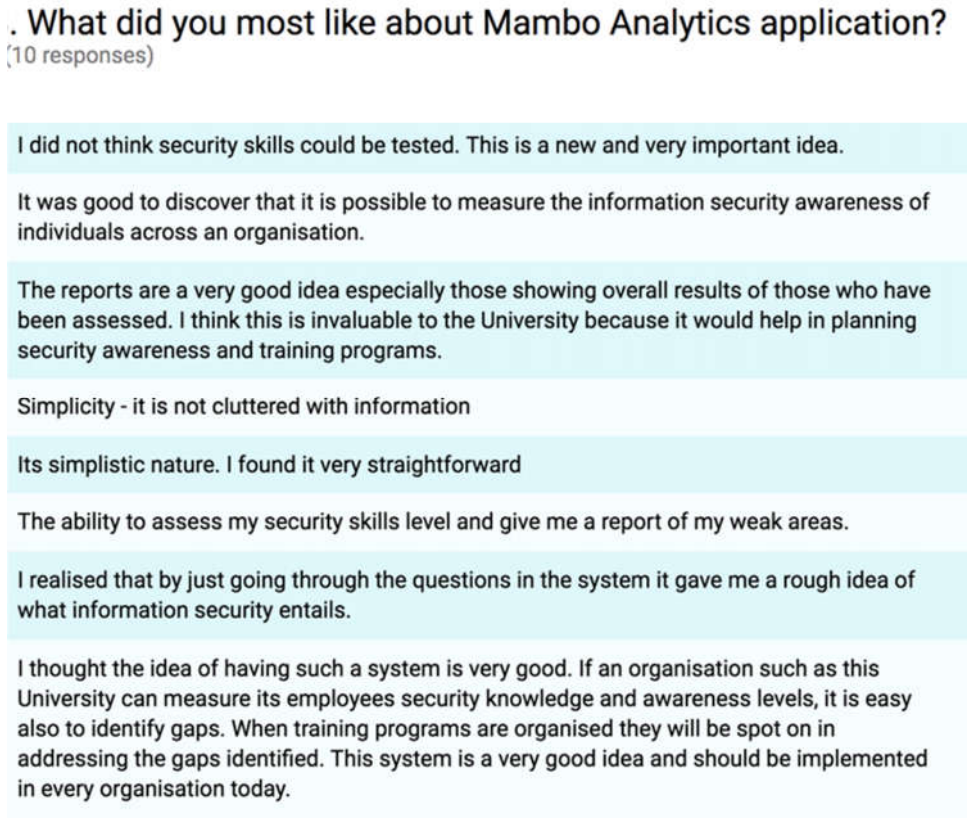


Figure 5.9 What Respondents Liked Most about Mambo Analytics

5.4.3. Hurdles of Implementing the Application in Organisations

When asked what they thought would be hurdles of implementing the system in their organisations, 100% respondents thought that fear of technology and online assessments would be a hurdle in implementing the system. 70% respondents thought that for successful implementation of the system there is need to overcome organisation culture. 50% thought that lack of understanding of the importance of information security assessment by university Management would be a hurdle in implementing the system. Finally, 50% thought that university personnel do not understand the role they play in strengthening information security in the organisation. This would need to be explained clearly to ensure all employees understand the need to use this system.

Chapter 6: Discussion of Key Findings

6.1. Overview

Findings obtained during the study formed the basis on which the information security skills assessment prototype was developed. The prototype was tested to ascertain that it met all its requirements. This chapter analyses the findings in relation to the research objectives and extent to which the findings agree with the literature review.

6.2. To Identify Employees' Information Security Weaknesses that are Easily Exploited by Cyber Attackers

Employees are the most fragile element in the security chain. They use data in their everyday activities to conduct the organisation's business, yet remain ignorant of information security threats and how to mitigate them. This is in harmony with study findings in section 2.5.

Section 2.11 identified employees' information security weaknesses which are easily exploited by cyber attackers. These are reliance on weak or default passwords, lack of password privacy, ignorance of social engineering, lack of knowledge on information security threats and the damage that could arise by those threats, lack of knowledge of solutions to mitigate threats, lack of awareness on organisation security policies and procedures which are meant to help employees ensure their own security and that of the organisation, not knowing how to deal with unsolicited e-mail attachments, negligence and non-compliance, lack of awareness on the dangers of installing software from unknown sources and the danger of visiting suspicious web sites. Finally, not reporting security incidents. These weaknesses guided the researcher in determining the kind of questions to feed into Mambo Analytics prototype for the purpose of assessing employees' information security skills.

6.3. To Identify and Review the Current Approaches Used to Assess Employees' Information Security Skills

The second research objective was to identify and review the current approaches used to assess employees' information security skills. Many scholars and international surveys recommend taking the skills analysis approach before awareness and training programs are planned. Once skills are identified, gaps can be analysed so that security awareness

and training programs are customised to address those gaps. This is in harmony with literature review section 2.12 which stresses on the necessity of security skills assessment and proposes finding ways of conducting needs assessment so that this data can inform security awareness and training programs. Definition of training needs and the importance of training needs analysis were discussed in section 2.7 to 2.9.

The study also points to a lack of models for enhancing information security knowledge of employees through awareness and education so as to build a security conscious workforce. This was noted to be the case mainly in the organisations domain. These findings were covered in section 2.12. Characteristics for developing models which will act as a blue print for organisations to enhance information security knowledge of their employees, were identified in the same section. These characteristics were invaluable in developing this prototype.

6.4. To Design, Develop, Test And Validate A Web Based Information Security Skills Assessment Prototype To Improve The Limitations Of The Current Tools.

The third research objective was to design, develop, test and validate a web based information security skills assessment prototype to improve the limitations of the current tools. Research findings section 2.12 indicate that information security skills assessment and tools for achieving the same are important to organisations. Section 2.10 and 2.13 looked at existing tools for information security assessment and established that few tools exist and even then, they fall short in that their target user requires technical skills such as those of penetration testers. In addition, the tools are not customizable which would come in handy in helping organisations create information security assessments that address their actual needs. Finally, the few existing tools for information security skills assessment are quite specialised addressing only a single aspect of information security such as social engineering or phishing.

The researcher developed a prototype called Mambo Analytics. The prototype is web based for ease of access and so that it requires no hardware specifications. The tool allows for self-assessment, a function that was found to be lacking in the existing tools. When

an individual completes an assessment and submits answers, the application is able to show a percentage score. The individual passes if the score is equal to or above50%. The individual can also view what was marked wrong, a pointer to what the individual needs to improve. Literature review identified characteristics for developing new models for enhancing employees' information security knowledge and skills. These characteristics were taken into account when developing this prototype.

The system allows a basic user to view and edit his own profile, view his assessment report and certificate of completion. A system administrator on the other hand can view individual user reports as well as overall organisation reports. Appendix F shows screenshots of assessment reports as viewed by a system administrator. Such reports help the individual identify areas of improvement. They also give a picture of the kind of employee an organisation has with regard to information security posture. Performance ranking as beginner, intermediate or advanced allows for training needs to be prioritised. Finally this information can be used to customise awareness and training programs so that actual employees' gaps can be addressed.

Testing was carried out with the aim of demonstrating that the developed solution accurately satisfies its specified requirements and objectives. Agile testing methodology was employed. Agile testing allowed for continuous testing from start to end of development as well as after deployment. More specifically, individual components of the prototype were identified and independently tested. Menu buttons were also tested to ascertain that they function as intended. After testing individual components, the system was tested as a whole whereby sample data was loaded into the application and results observed. Finally, once all individual components were ascertained to function as intended, the prototype was deployed via the web to allow users to test its usability. Questionnaires were used to collect usability feedback from respondents.

During usability testing, questionnaires were used to collect feedback from respondents. This feedback was analysed to demonstrate that the solution fulfils its intended purpose. None of the respondents who participated in testing experienced login problems. All

respondents were able to complete assessment and received their performance report and a certificate of completion. Appendix G shows sample questions and their predetermined answer. Appendix C shows a step by step assessment until results and certificate is generated. The application was therefore ascertained to be reliable. Out of 10 respondents who tested the system, 60% rated ease of navigation and clarity of questions good while 40% rated it excellent. 50% respondents rated clarity of assessment reports excellent. Usefulness of assessment report was rated excellent by 90% respondents. 80% of the respondents strongly agreed that they would recommend the system to their friends.

6.5. Advantages of the Developed Solution Compared To Existing Tools

The developed solution is a web based self-assessment tool. It is simple enough for use by employees with little or no information security skills. As a matter of fact, 80% respondents who tested the system were non ICT support staff, while 50% respondents did not consider themselves tech survey, yet all were able to login, complete the assessment and view their reports.

The tool marks a respondents answers and gives an overall percentage. Those who complete the assessment are also ranked as beginner, intermediate or advanced based on their overall percentage. This kind of ranking is useful to the Management because it can help prioritise training needs. Respondents also receive a report on their strength and weak areas. The weak areas point to what the respondent should focus on improving. This information can help the Management customise awareness and training programs so that employees' actual gaps are addressed.

Chapter 7: Conclusions, Recommendations and Future Work

7.1. Conclusions

The study reveals that employees are the weakest link in the security chain because they handle sensitive data in their day to day activities yet remain ignorant of information security threats and how to mitigate them. Common attacks faced by organisations are also identified as well as common employees' weaknesses that are easily exploited by attackers. Research findings reveal the importance of information security skills assessment prior to planning any security awareness and training. Once skills are identified gaps can be analysed and this information can feed to security awareness and training programs planning, so that these programs are customised to address the identified gaps.

The research shows that some tools do actually exist that have tried to address this problem. However, these tools require technical skills such as those of penetration testers and, they are specialised addressing a single aspect of information security such as social engineering or phishing. Using the development tools discussed in chapter 4, Mambo Analytics prototype was developed. During system development agile methodology was used. This allowed for more frequent release with subsequent user feedback which led to development of a usable and reliable prototype. Usability testing and system validation was performed and respondents generally found the tool valuable and satisfying.

The aim of the developed tool is to help organisations easily assess their employees' information security skills so that gaps can be analysed and training programs customised to fill those gaps. In a word, the tool provides the following advantages: 1) Reports serve to give a global picture on what kind of employee the organisation has. 2) Training can be prioritised. 3) Makes it possible for security awareness and training programs can be customised to address employees' areas of weakness making these programs more personal, more relevant and effective and worth the resources allocated to them. 4) The reports support employee professional development and overall organisational information security strategy.

7.2. Recommendations

The web based information security self-assessment prototype was of great importance to employees both technical and non-technical. The researcher noted however, that there was still a lot more that can be done. The following recommendations are thus given:

Public awareness is necessary to increase adoption of this tool. The tool can be advanced by collaborating with private and public organisations in order to create more security assessments so as to cater for all types of organisations and so that those assessments address all industries. It is worth noting that the developed prototype allows a system administrator to create new assessments and to edit old ones depending on the needs of the organisation. Finally, integration with some already existing tools such as Gophish would strengthen it because reports produced by both tools can complement each other. 100% of respondents who tested the system thought it was absolutely important to integrate it with relevant information security material so that employees know where to get the information they need to enhance their information security skills.

7.3. Future Work

The main focus of this study was to develop a web-based self-assessment tool to help organisations identify employees' information security knowledge and awareness levels so that gaps can be analysed and training/awareness programs customised to address those gaps. Future work will concern prioritising skills that staff should get so that an organisation can estimate how much budget they are likely to require for training, using data mining algorithms to analyse an individual's assessment results and intelligently determine areas of training for the individual, integrating the system with existing penetration testing tools such as Gophish so that the power of both tools can be harnessed for better decision making and planning. Developing other versions of the system such as android and IOS is key. It will be of great importance to integrate the application with relevant information security material to help employees know where to acquire such information in order to enhance their skills. Additionally, other categories of assessment should be created for example to assess top management's understand of information security from the point of view of organisational goals and objectives as well as overall organisation strategy.

References

Amankwa, E., Loock, M. & Kritzinger, E. (2014). *A Conceptual Analysis of Information Security Education, Information Security Training and Information Security Awareness Definitions*. Paper presented at 9th International Conference for Internet Technology and Secured Transactions (ICITST -2014), London. IEEE.

Boujettif, M and Wang, Y. (2010*). Constructivist Approach to Information Security Awareness in the Middle East.* Presented at the International Conference on Broadband, Wireless Computing, Communication and Applications, pp.192–199. IEEE Press

Casmir, R. and Yngstrom, L. (2005). *Towards a dynamic and adaptive information security awareness approach*. Presented in the proceedings of the IFIP TC11 WG11.8 Fourth World Conference on Information Security.

Cisco (2003). *Economic Impact of Network Security Threats*. Retrieved from http://www.cisco.com/warp/public/cc/so/neso/sqso/roi1_wp.html

Cisco (2006). *What Is the Difference: Viruses, Worms, Trojans, and Bots?* Retrieved from http://www.cisco.com/c/en/us/about/security-center/virus-differences.html

D'arcy, J., and Hovav, A. (2009). *Does one size fit all? Examining the differential effects of IS security countermeasures*. Journal of Business Ethics 89(1), 59–71.

Deloitte (2008). *Global Financial Services Industry (GFSI) Security Survey*. Retrieved from https://www2.deloitte.com/ie/en/pages/financial-services/articles/global-fs-industry-security-study-2012.html.

European Network and Information Agency (2010). *A new Users' Guide: How to Raise Information Security Awareness*. European Network and Information Security Agency.

European Network and Information Agency (2008). *Measuring Awareness*. Retrieved from http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf.

European Network and Information Security Agency (2007). *Information Security Awareness Initiatives: Current Practice and the Measurement of Success.* ENISA.

Global Information Security Survey (2017). *Path to Cyber Resilience: Sense, Resist, React*. India Report.

Government of Kenya (2014). *Kenya National Cybersecurity Strategy*. Government Press.

Government of Kenya (2015). *The Kenya Cyber Security Report*. Government Press.

Gundu, T., & Flowerday, S.V. (2013). Ignorance to Awareness: Towards an Information Security Awareness Process. South African Institute of Electrical Engineers.

Guru99 (2017). *Agile Testing Course*. Retrieved 4th April, 2017 from http://www.guru99.com/agile-testing-course.html

Howarth, F (2014). *The role of human error in successful security attacks.* Retrieved December 16, 2016 from https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/ .

IBM Developer Works (2004). *UML basics*. Retrieved from

https://www.ibm.com/developerworks/rational/library/content/RationalEdge/sep04/bell/

ISACA (2012). *Cobit 5: A Business Framework for the Governance and Management of Enterprise IT*. Cobit Publications Directory.

Jama, A.Y., Siraj, M. & Kadir, R. (2014). *Towards Metamodel - based Approach for Information Security Awareness Management*. Presented in 2014 International symposium on biometrics and security technologies (ISBAST). pp. 316–321.

Kabugu, E.A (2012). *A Model to Measure Information Security Awareness Level in an Organization: Case Study of Kenya Commercial Bank* (master's thesis). Retrieved from Strathmore Digital Repository.

Khan, B et al. (October 2011). *Effectiveness of Information Security Awareness Methods Based on Psychological Theories*. African Journal of Business Management.

Kritzinger, E. & Smith, E. (2008). *Information security management: An information security retrieval and awareness model for industry*. Computers & Security, 27(5-6), pp. 224–231.

Kritzinger, E. & Von Solms, S.H. (2010). *Cyber security for home users: A new way of protection through awareness enforcement*. Computers & Security, 29(8), pp.840–847.

Kruger, H. A., & Kearney, W. D. (2006). *A prototype for assessing information security awareness*. Computers and Security, 25, 289-29. Retrieved February 2, 2017, from Science Direct.

Kruger, H., Drevin, L., & Steyn, T. (2010). *A vocabulary test to assess information security awareness.* Information Management and Computer Security, 18,316-327.

Luo, X., & Liao, Q. (2007). *Awareness Education as the Key to Ransomware Prevention.* Retrieved from http://www.unm.edu/~xinluo/papers/ISS2007.pdf.

Maeyer, D. D. (2007). *Setting up an Effective Information Security Awareness Programme.* Presented in ISSE/SECURE 2007 Conference. Information Systems Security, 9(6), 14-23.

Native Intelligence (2016). *Measure What Matters.* Retrieved December 12, 2016 from http://www.nativeintelligence.com/ni-programs/metrics-01.asp.

Mogale, M., Gerber, M., Carroll, M., & von Solms, R. (2014). *Information Security Assurance Model (ISAM) for an Examination Paper Preparation Process*. IEEE transaction.

Monk, T., Van Niekerk, J., & Von Solms, R. (2010). *Sweetening the medicine: educating users about information security by means of game play*. Presented in proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists.

Mugo, A.E.K. (2012). *A Model to Measure Information Security Awareness Level in an Organization: Case Study of Kenya Commercial Bank*. Master's Thesis, Strathmore University, Nairobi Kenya.

Okenyi, P. O., & Owens, T. J. (2007). *On the Anatomy of Human Hacking*. Information Systems Security, 16:6, 302-314, DOI: M10.1080/10658980701747237

Parsons, Kathryn & Defence Science and Technology Organisation (Australia). Command, Control, Communications and Intelligence Division (2010). *Human factors and information security: individual, culture and security environment*. Command, Control, Communications and Intelligence Division, Defence Science and Technology Organisation, Edinburgh, S. Aust

Peltier, T. R. (2005). *Implementing an Information Security Awareness Program*. Information Systems Security, 14 (2), 37- 48.

Puhakainen P., & Siponen T.M. (2010). *Improving employees' compliance through information systems security training: An Action Research Study*. MIS Quarterly, 34(4), 757-778.

Rumbaugh, J.; Jacobson, I.; Booch, G. (2005): *The Unified Modeling Language User Guide* 2nd Edition, Addison Wesley, Boston.

Russell, S., & Norvig, P. (2009). *Artificial Intelligence: A Modern Approach*, 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall Press.

SAI Global (2008). *Information Security Awareness Survey*. SAI Global.

Sârghe, P.D (2013*). The Human Factor in Information Security*. Presented in the 8th International Scientific Conference "Defense Resources Management in the 21st Century" Braşov, November 14th 2013.

Secure Works (2012). *Human error information security risk organisation.* Retrieved January 5, 2017 from https://www.secureworks.com/blog/general-human_error_information_security_risk_organization

Sharma, S.K., & Sefchek, J. (2007). *Teaching information systems security courses: A hands-on approach*. Computers & Security, pp.290– 299.

Siponen M. T. (2000). *A conceptual foundation for organizational information security awareness.* Information Management & Computer Security. Education (WISE4), May 2005, Moscow, Russia.

Smith, E., Kritzinger, E., Oosthuizen, H.J., & Von Solms, S.H. (2005). *Information Security Education: Bridging the gap between academic institutions and industry.* UNISA Institutional Repository.

Stewart, G., & Lacey, D. (2012). *Death by a thousand facts: Criticising the technocratic approach to information security awareness*. Information Management & Computer Security, 20 (1), pp. 29–38.

Talib, S. (2014). Personalising Information Security Education. Master's dissertation, University of Plymouth, Malaysia.

The Information Technology Infrastructure Library (2011). *Best practice solutions*. ITIL.

The International Organisation for Standardization (ISO 27002), (2013). *Introduction to ISO 27002.* ISO

The National Institute of Standards and Technology (NIST) special publication 800-50 [18] Vol.104 (2), (June 2013).

The Open University (2016). *Introduction to information security.* Retrieved on January 8, 2017 from http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-1.

Thomson, K., Von Solms, R., Louw, L. (2006). *Cultivating an organizational information security culture*. Computer Fraud & Security. Vol. 2006, Issue 10, Pages 7-11.

Tutorial Point (2007). *Software Architecture and Design.* Retrieved 4th April, 2017 from https://www.tutorialspoint.com/software_architecture_design/quick_guide.htm

VMware (2016). *University Challenge: Cyber Attacks in Higher Education.* A report exploring the evolving threat for UK universities and how they can guard against cyber-attacks to preserve their intellectual property. VMware.

Werlinger, R., Hawkey, K., & Beznosov, K (2008). *Human, Organizational and Technological Challenges of Implementing Information Security in Organizations*. Presented in the proceedings of the second international symposium on human aspects of information security assurance.

Whitman, E.M and Mattord, H. J (2012). *Principles of Information Security*, 4th Edition. Cengage Learning.

Appendices

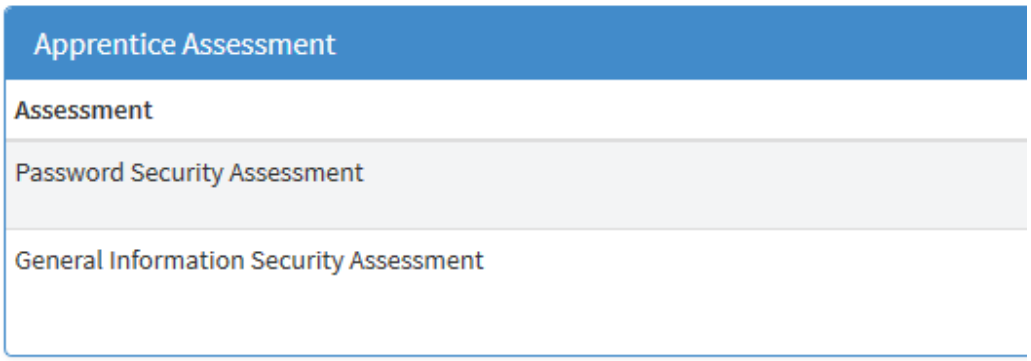
Appendix A: Assessment Categories

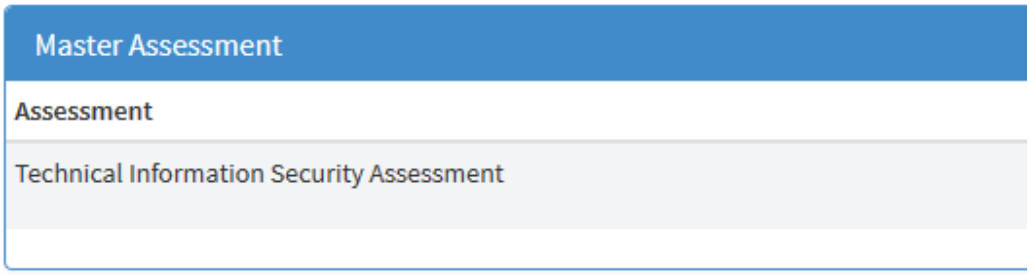
Categories

Search:

#	Name	Description
1.	Master Assessment	Covers advanced information security with a technical aspect. This assessment is meant mainly for ICT Managers and ICT support personnel.
2.	Apprentice Assessment	General information security questions applicable to all information systems users.

Showing 1 to 2 of 2 entries





Appendix B: Generation and Storage of Questions

Assessment

Search:

	Name	Description	Available From	Available To	Questions
1.	Technical Information Security Assessment	Assesses mainly technical topics of information security	24/04/2018	24/04/2017	20 Manage
2.	General Information Security Assessment	Examines general security topics such as viruses, security policy, computer sec ...	24/04/2017	24/04/2018	11 Manage
3.	Password Security Assessment	Examines knowledge and awareness of password security.	13/04/2017	15/04/2017	5 Manage

Showing 1 to 3 of 3 entries

Assessment :: Technical Information Security Assessment

Questions | Add Question

	Question	Points
1.	Are all the software you use supported by the manufacturer?	2
2.	Have you ever changed any of the default settings in firewalls either on your personal or organisation's PC or router?	2
3.	Your company wants to prevent SQL and script injection attacks on its Internet web application. The company should implement:	2
4.	A system administrator needs to harden a server. The most effective approach is:	2
5.	The most effective countermeasures against input attacks are:	2

Assessment :: General Information Security Assessment

Questions | Add Question

	Question	Points
1.	Which of the following is a good practice to avoid email viruses?	2
2.	I know my organisation's Personal Use Policy	1
3.	My personal security and that of my organisation is first and foremost my responsibility.	2
4.	What is the most common delivery method for viruses?	2
5.	If you're not careful which websites you visit, which of the following can result?	2
6.	What should everyone know about information security? (Select the best answer)	2
7.	What is the biggest vulnerability to the security of your organisation's sensitive information?	2

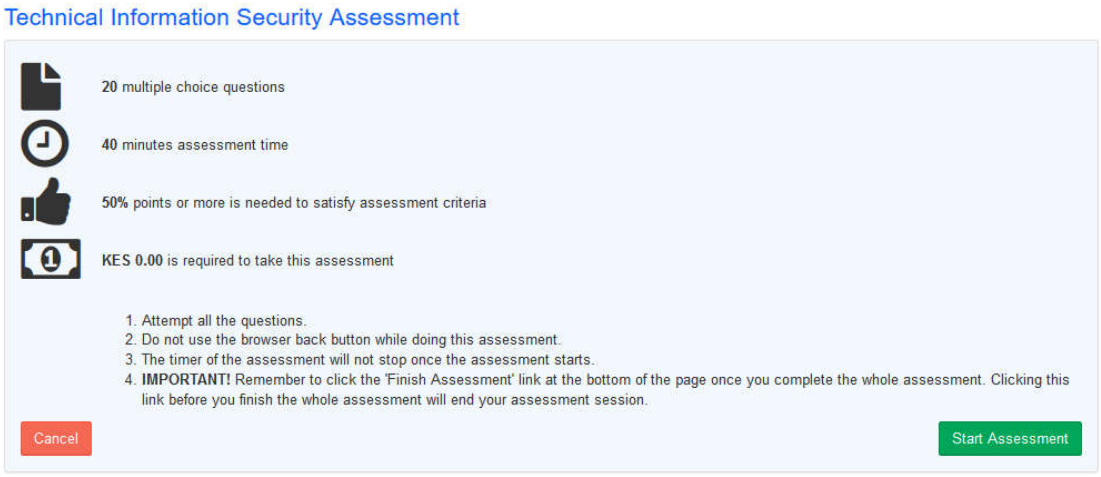
Assessment :: Password Security Assessment

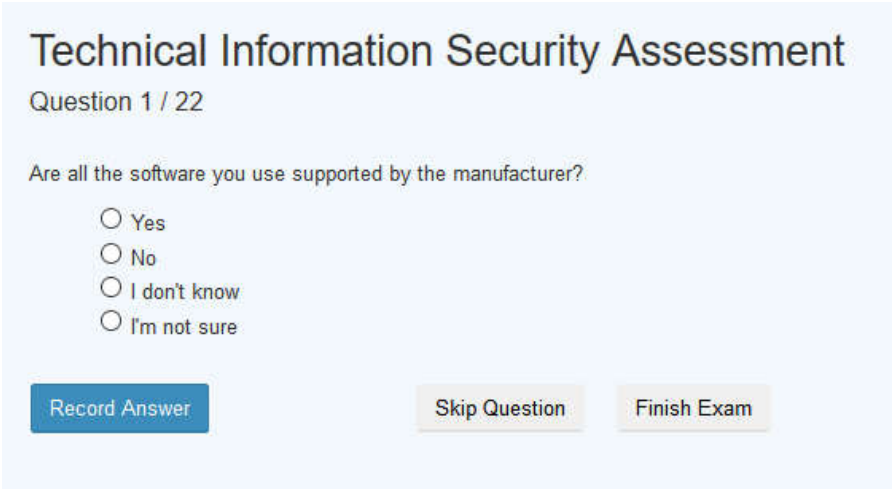
Questions | Add Question

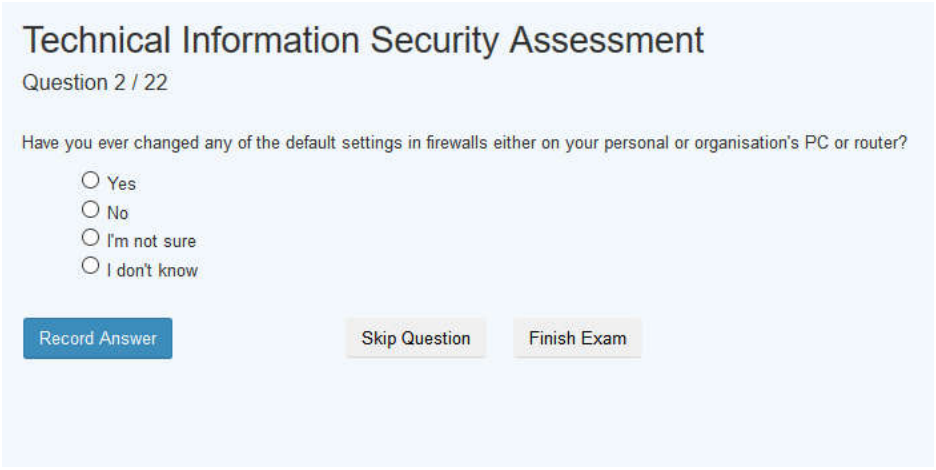
	Question	Points
1.	Which of the following is a good way to create a password?	2
2.	Which of the following would be the strongest password?	2
3.	Factory set passwords in your PC, laptop or smart phone should be changed as soon as the device is purchased.	2
4.	What should you do if you think your password has been compromised? (pick the best answer).	2
5.	Which of the following is the best way to store your password?	2

Showing 1 to 5 of 5 entries

Appendix C: Mambo Analytics Testing and Validation Screenshots







Technical Information Security Assessment

Question 4 / 22

A system administrator needs to harden a server. The most effective approach is:

- ○ Install security patches and install a firewall
- ○ Remove unneeded services, remove unneeded accounts, and configure a firewall
- ○ Remove unneeded services, disable unused ports, and remove unneeded accounts
- ○ Install security patches and remove unneeded services

Record Answer | Skip Question | Finish Exam

Technical Information Security Assessment

Question 7 / 22

The following are valid reasons to reduce the level of privilege for workstation users EXCEPT:

- ○ Decreased support costs because users are unable to change system configurations
- ○ Decreased need for whole disk encryption
- ○ Decreased impact from malware
- ○ Increased security because users are unable to tamper with security controls

Record Answer | Skip Question | Finish Exam

Technical Information Security Assessment

Question 11 / 22

The purpose of off-site media storage is:

- ○ To protect media from damage in the event of a disaster
- ○ To protect media from theft
- ○ To provide additional storage not available on-site
- ○ To meet regulatory requirements for media protection

Record Answer | Skip Question | Finish Exam

Technical Information Security Assessment

Question 13 / 22

The purpose of a periodic review of user access rights is:

- ○ To check whether employees have logged in to the system
- ○ To check for active accounts that belong to terminated employees
- ○ To determine password quality and expiration
- ○ To determine whether access control systems still function properly

Record Answer | Skip Question | Finish Exam

Technical Information Security Assessment

Question 14 / 22

The purpose of a password policy that requires a minimum number of days between password changes is:

- ○ To prevent a brute force attack against a password
- ○ To prevent an intruder from carrying out a dictionary attack against a password
- ○ To prevent someone from quickly cycling back to their familiar password
- ○ To prevent a second user from changing the password

Record Answer | Skip Question | Finish Exam

Technical Information Security Assessment

Question 16 / 22

Your organization is discarding its old desktop computers. Being concerned with data security, what measures should the organization take first?

- ○ Erase the hard drives
- ○ Format the hard drives
- ○ Activate its TEMPEST shielding
- ○ Clear the computers' RAM

Record Answer | Skip Question | Finish Exam

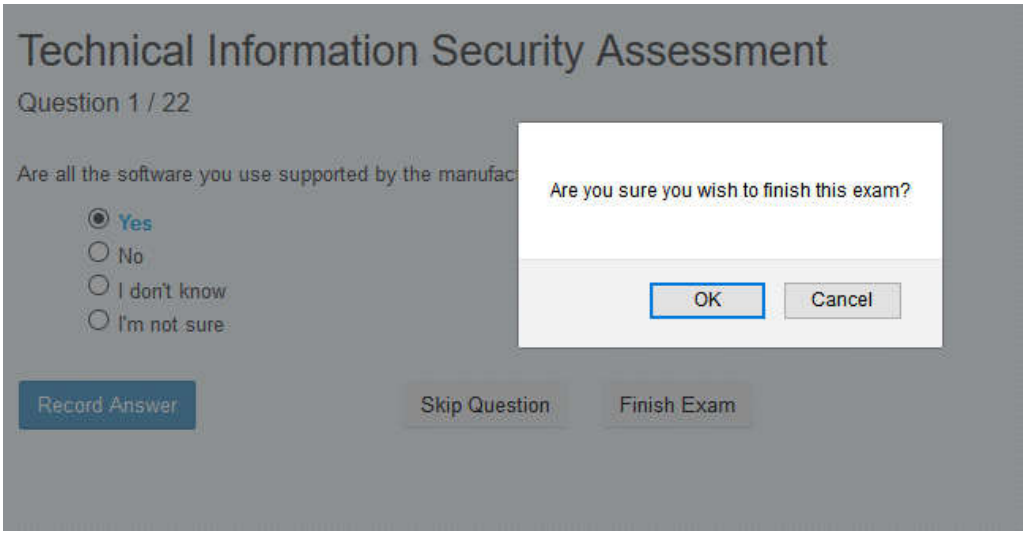
Technical Information Security Assessment

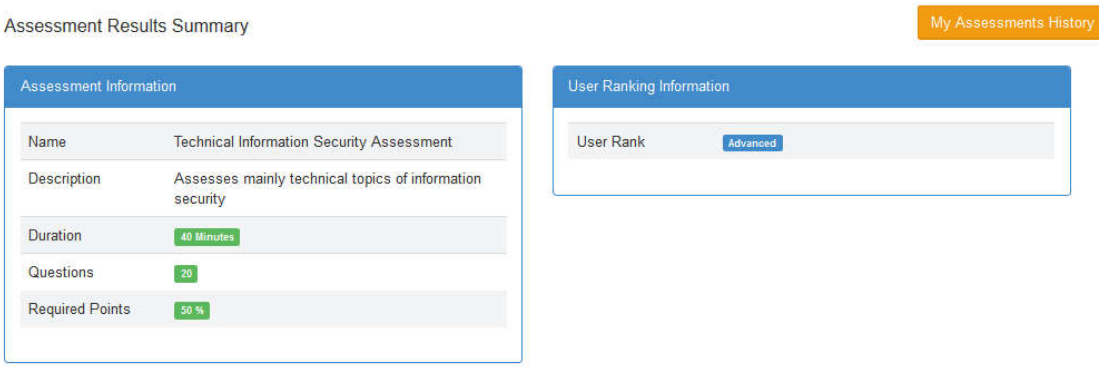
Question 22 / 22

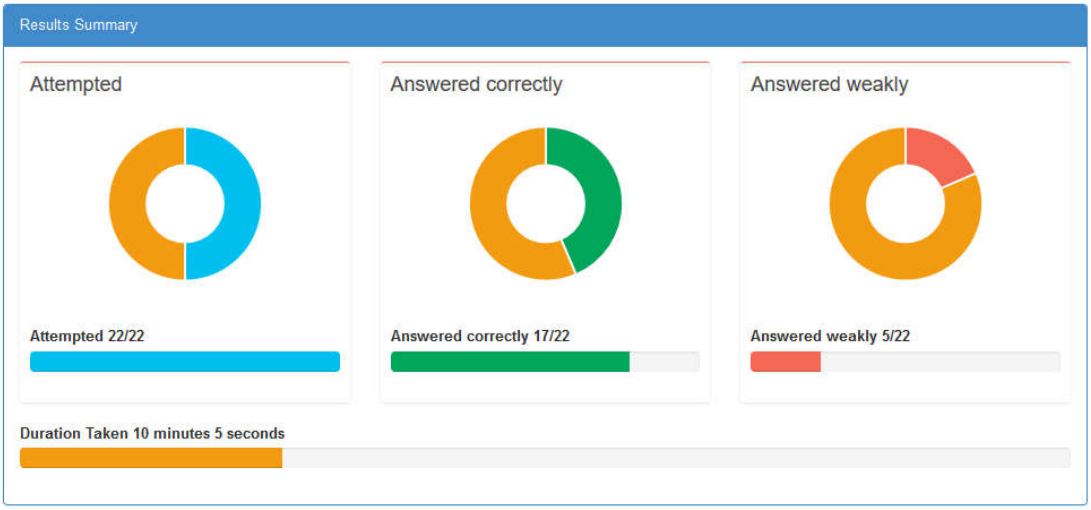
An employee with a previous criminal history was terminated. The former employee leaked several sensitive documents to the news media. To prevent this, the organization should have:

- ○ Reviewed access logs
- ○ Restricted the employee's access to sensitive information
- ○ Obtained a signed non-disclosure statement
- ○ Performed a background verification prior to hiring the employee

Record Answer | Finish Exam

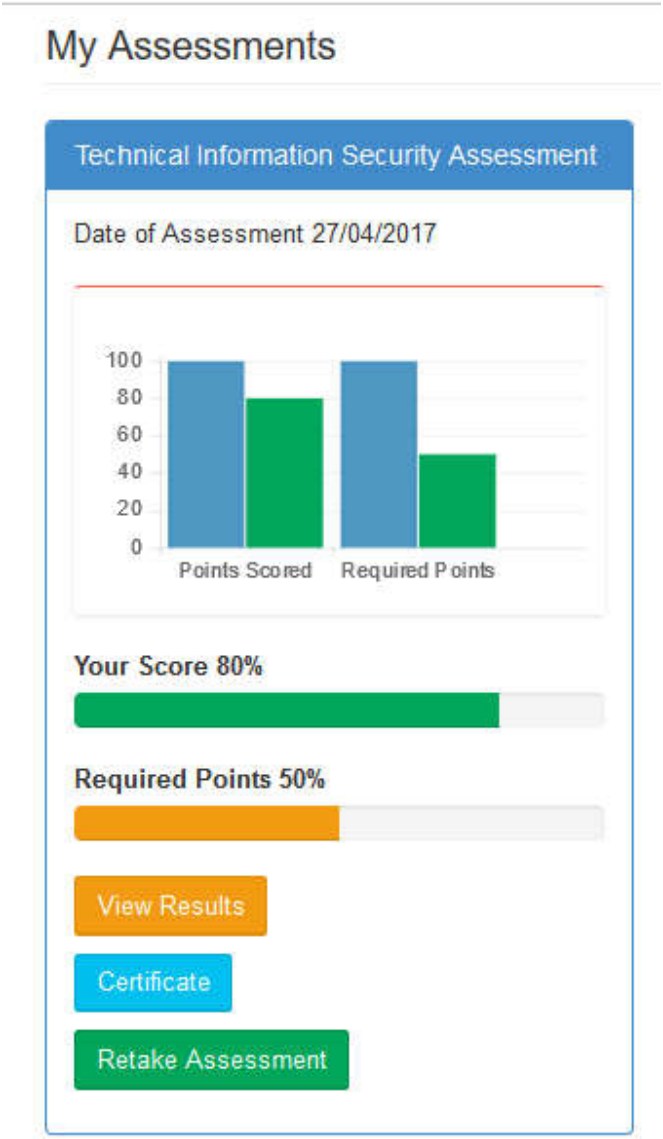

Technical Information Security Assessment
Question 1 / 22
Are all the software you use supported by the manufac
Yes
No
I don't know
I'm not sure
Are you sure you wish to finish this exam?
OK
Cancel
Record Answer
Skip Question
Finish Exam


Assessment Results Summary
My Assessments History
Assessment Information
Name
Technical Information Security Assessment
Description
Assesses mainly technical topics of information security
Duration
40 Minutes
Questions
20
Required Points
50 %
User Ranking Information
User Rank
Advanced


Results Summary
Attempted
Attempted 22/22
Answered correctly
Answered correctly 17/22
Answered weakly
Answered weakly 5/22
Duration Taken 10 minutes 5 seconds

Weak Areas

	Question	Points
1.	The following are valid reasons to reduce the level of privilege for workstation users EXCEPT:	2
2.	A system administrator needs to harden a server. The most effective approach is:	2
3.	The purpose of a periodic review of user access rights is:	2
4.	The options for risk treatment are:	1
5.	An employee with a previous criminal history was terminated. The former employee leaked several sensitive documents to the news media. To prevent this, the organization should have:	1



Certificate of Completion

This is to certify that

admin admin.

has completed the assessment

Technical Information Security Assessment

with score of **77.27%** from our Online Security Assessment System.

Dated **27/04/2017**

Head of Assessments

Appendix D: Usability Testing Questionnaire

1. Teaching staff

- Yes
- No

2. ICT Support Staff? *

- Yes
- No

3. Do you consider yourself tech survey? *

- Yes
- No

4. Were you able to login to Mambo Analytics application? *

- ○ Yes
- ○ No

5. If the above answer is No, please list the difficulties you encountered

Long answer text

6. Please rate Mambo Analytics application on the following (Pick one option for each row)

Row 1. Ease of Navigation	Column 1. 1=Poor
Row 2. Clarity of Questions	Column 2. 2=Fair
Row 3. Clarity of Assessment Report	Column 3. 3=Average
Row 4. Usefulness of Assessment Report	Column 4. 4=Good
	Column 5. 5=Excellent

7. Please rate Mambo Analytics application on the following (Pick one option for each row)

Row 1. I thought the system was easy to us	Column 1. 1=Strongly Disagree
Row 2. I would need the support of a techni	Column 2. 2= Disagree
Row 3. I think the system is very useful	Column 3. 3= Neutral
Row 4. I would recommend the system to n	Column 4. 4=Agree
	Column 5. 5=Strongly agree

8. What did you most like about Mambo Analytics application? *

Long answer text

9. When looking at using Mambo Analytics application to assess your skills in the future, what importance would you attach to the following considerations? *

Row 1. Security of data held in the applicati	Column 1. Unimportant
Row 2. Scalability	Column 2. Important
Row 3. Integration with existing IT systems	Column 3. Very important
Row 4. Having an android version of the apı	Column 4. Absolutely important
Row 5. Having an Intranet version of the apı	
Row 6. Having an IOS version of the applica	
Row 7. Integrating system with relevant infc	

10. Do you think your organisation would consider using Mambo Analytics for information security skills assessment? *

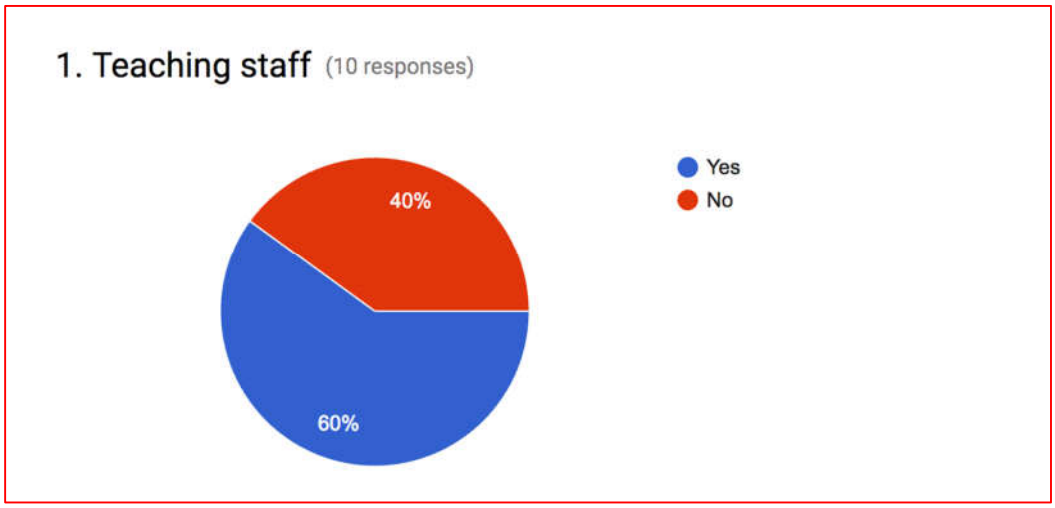
- ○ Yes
- ○ No

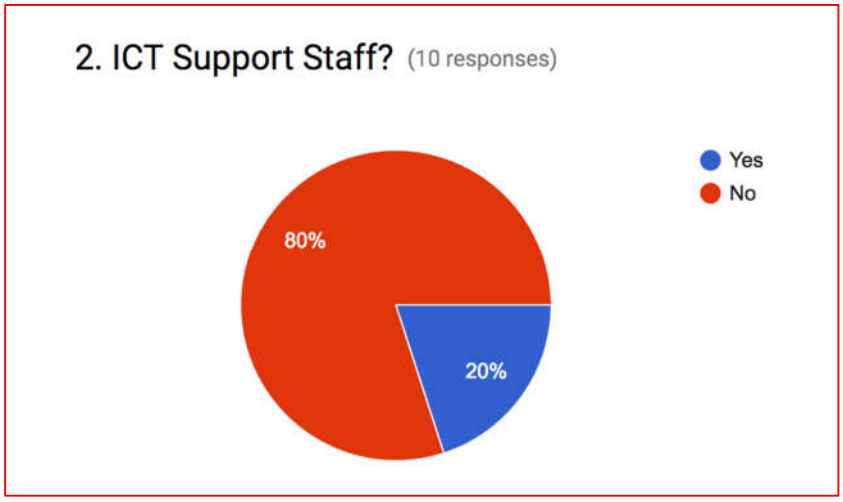
11. If yes above, what are the key hurdles that your organisation might face in implementing the system?

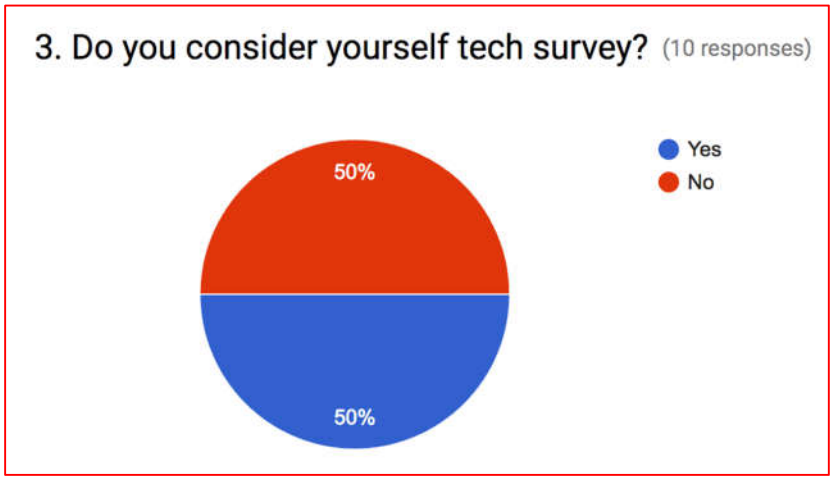
select all applicable

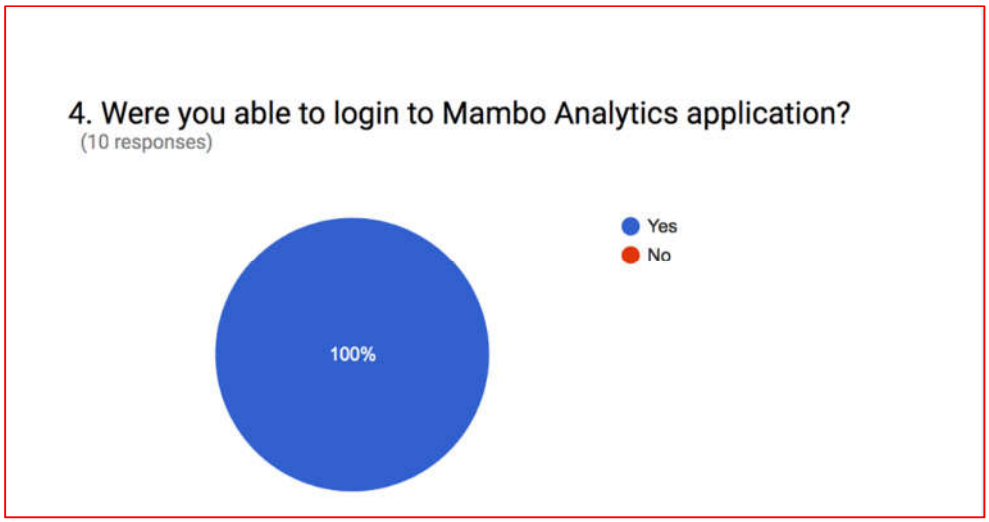
- [ ] Overcoming organizational culture
- [ ] University decision makers are not aware of the benefits of information security skills assessment
- [ ] University personnel not aware of the role they play in information security strengthening
- [ ] Fear of online assessments and technology
- [ ] Other...

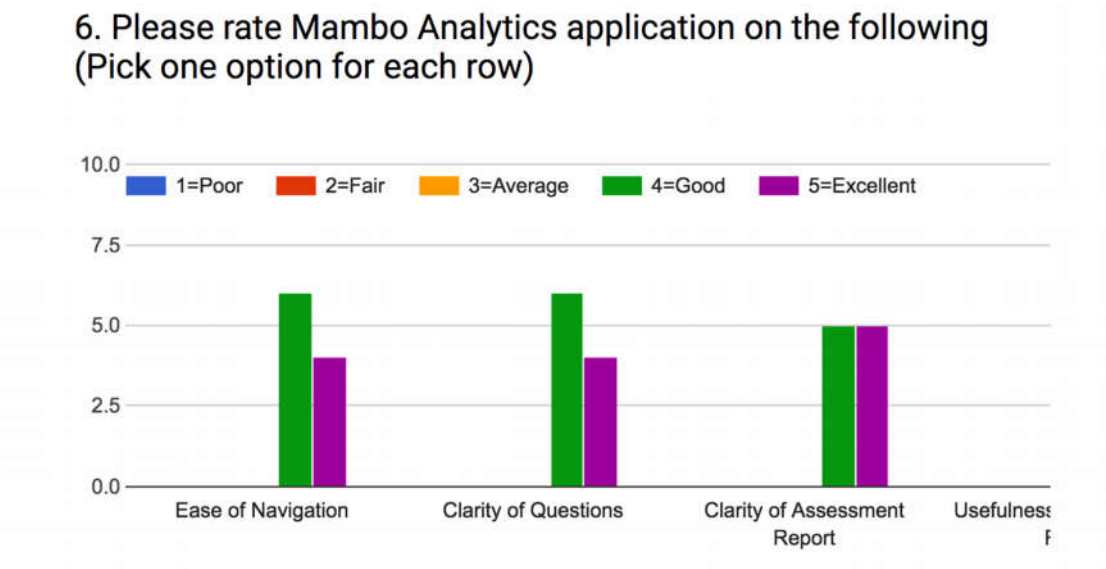
Appendix E: Usability Testing Feedback



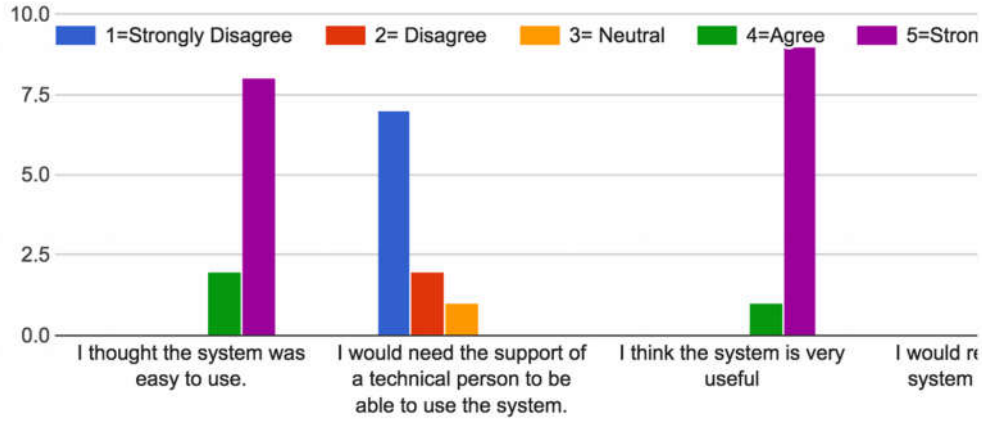



3. Do you consider yourself tech survey? (10 responses)
50%
50%
Yes
No


4. Were you able to login to Mambo Analytics application?
(10 responses)
100%
Yes
No


6. Please rate Mambo Analytics application on the following (Pick one option for each row)
10.0
7.5
5.0
2.5
0.0
1=Poor
2=Fair
3=Average
4=Good
5=Excellent
Ease of Navigation
Clarity of Questions
Clarity of Assessment Report
Usefulness

7. Please rate Mambo Analytics application on the following (Pick one option for each row)



8. What did you most like about Mambo Analytics application?

(10 responses)

I did not think security skills could be tested. This is a new and very important idea.

It was good to discover that it is possible to measure the information security awareness of individuals across an organisation.

The reports are a very good idea especially those showing overall results of those who have been assessed. I think this is invaluable to the University because it would help in planning security awareness and training programs.

Simplicity - it is not cluttered with information

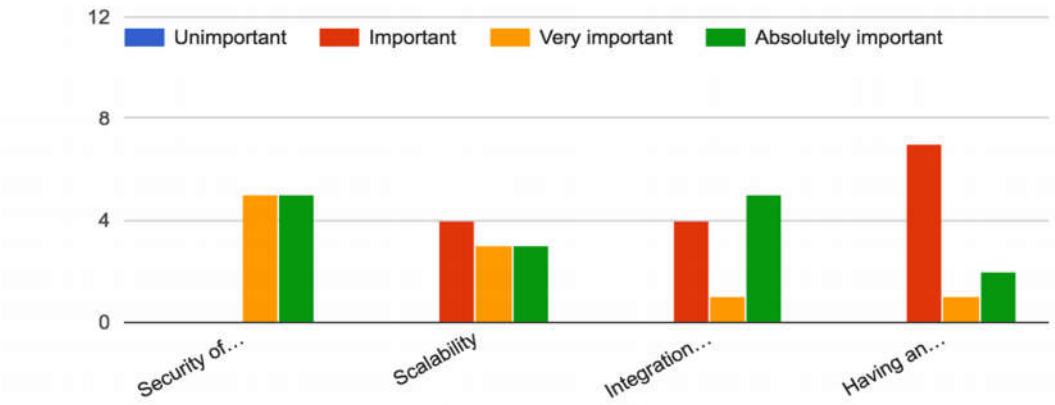
Its simplistic nature. I found it very straightforward

The ability to assess my security skills level and give me a report of my weak areas.

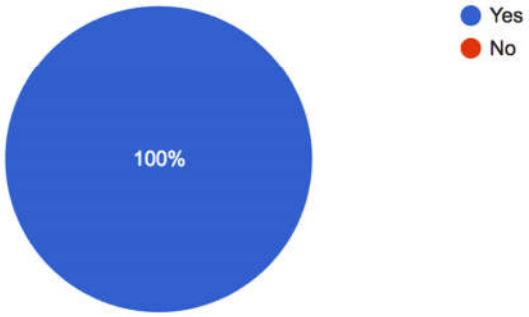
I realised that by just going through the questions in the system it gave me a rough idea of what information security entails.

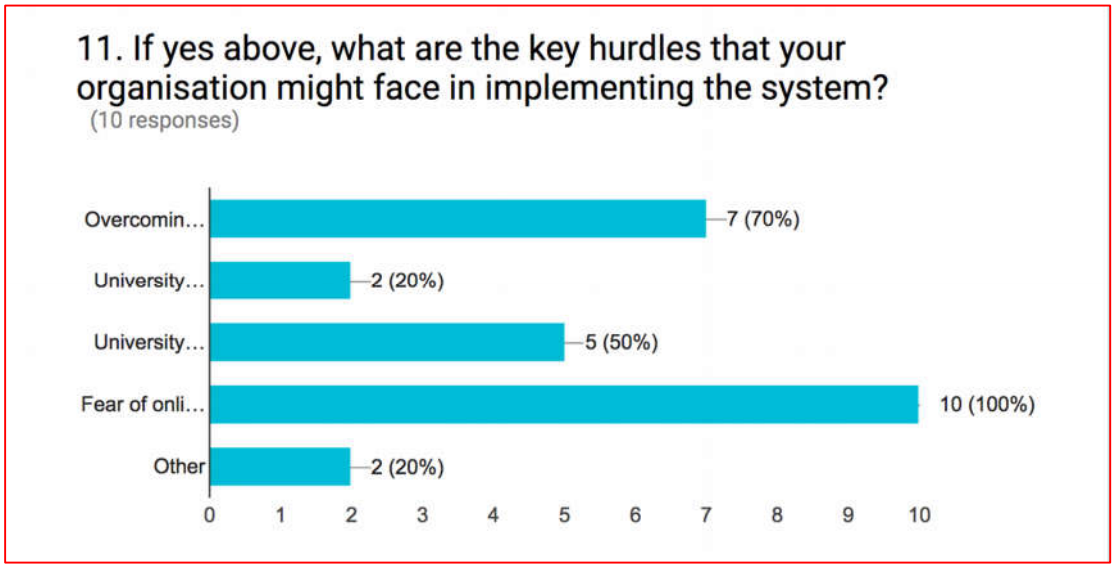
I thought the idea of having such a system is very good. If an organisation such as this University can measure its employees security knowledge and awareness levels, it is easy also to identify gaps. When training programs are organised they will be spot on in addressing the gaps identified. This system is a very good idea and should be implemented in every organisation today.

9. When looking at using Mambo Analytics application to assess your skills in the future, what importance would you attach to the following considerations?

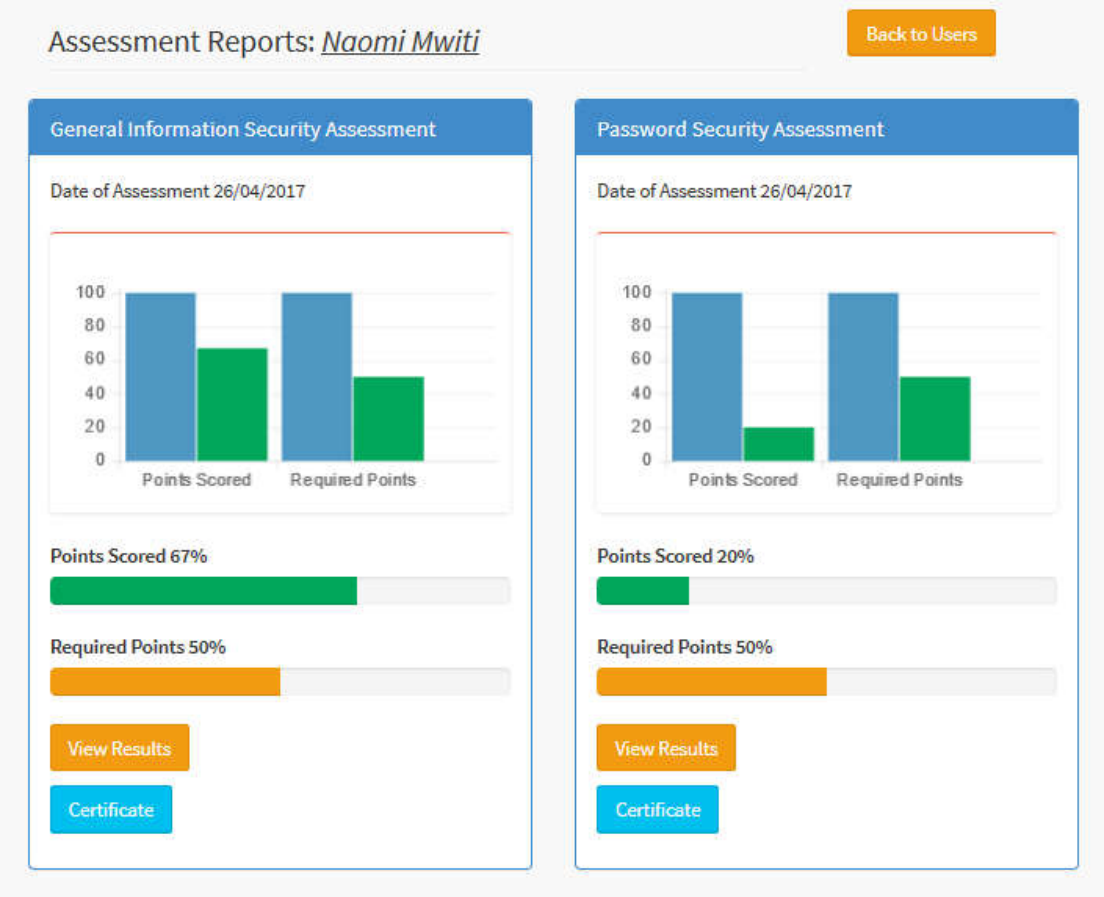


10. Do you think your organisation would consider using Mambo Analytics for information security skills assessment?
(10 responses)

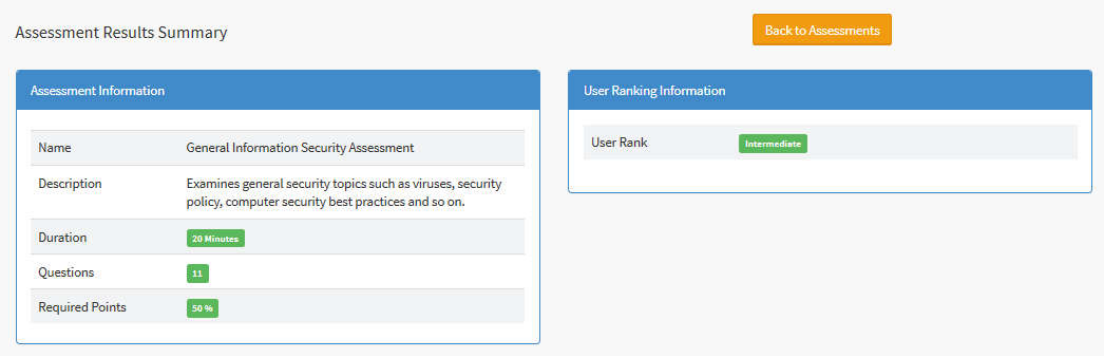


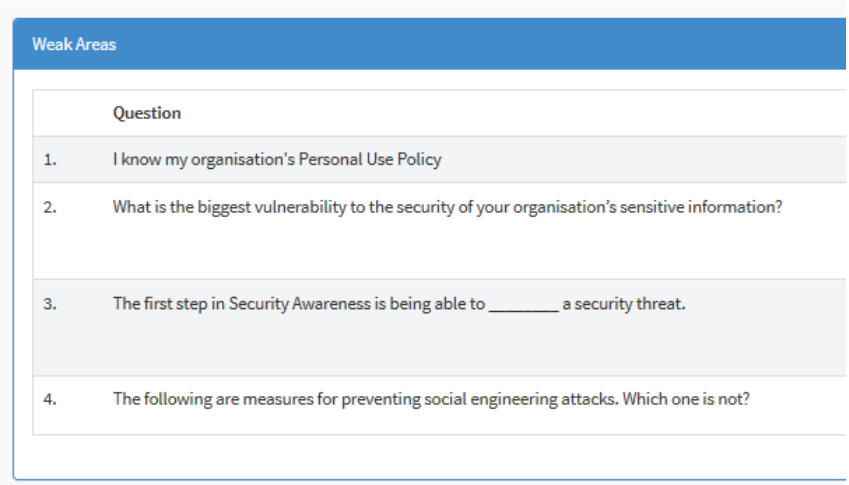

11. If yes above, what are the key hurdles that your organisation might face in implementing the system?
(10 responses)
Overcomin...
University...
University...
Fear of onli...
Other
7 (70%)
2 (20%)
5 (50%)
10 (100%)
2 (20%)
0
1
2
3
4
5
6
7
8
9
10

Appendix F: Assessment Reports as viewed by System Administrator



Beginner	Naomi	Mwiti	nmwiti@strathmore.edu
Beginner	Anne	Betty	abetty@strathmore.edu
Beginner	Esther	Gathenya	egathenya@strathmore.edu
Beginner	Mercy	Chepchichir	mchepchichir@gmail.com
Beginner	Charles	K	ckiilur@strathmore.edu
Beginner	Regina	Nkonge	rnkonge@strathmore.edu
Beginner	Joan	Munasia	ynkmee@aim.com
Beginner	Ken	Mbogo	useraes@bigdatainc.co.ke


Assessment Results Summary
Back to Assessments
Assessment Information
Name
General Information Security Assessment
Description
Examines general security topics such as viruses, security policy, computer security best practices and so on.
Duration
20 Minutes
Questions
11
Required Points
50 %
User Ranking Information
User Rank
Intermediate


Weak Areas
Question
1. I know my organisation's Personal Use Policy
2. What is the biggest vulnerability to the security of your organisation's sensitive information?
3. The first step in Security Awareness is being able to _____ a security threat.
4. The following are measures for preventing social engineering attacks. Which one is not?


Dashboard
1
Assessments
0
User Reports
8
User Registrations
3
Total questions
Organization Staff Chart
Organization Performance Chart
Assessment Data Chart
Assessment Performance Chart

Appendix G: Sample Questions Showing Predetermined Answer

Which of the following is a good practice to avoid email viruses?

marks

2

Image

Answers

Answer 1 | correct : NO

Delete unexpected or unsolicited emails

Answer 2 | correct : NO

Use anti-virus software to scan attachments before opening

Answer 3 | correct : NO

Delete similar messages that appears more than once in your Inbox

Answer 4 | correct : YES

All the above

My personal security and that of my organisation is first and foremost my responsibility.

marks

2

Image

Answers

Answer 1 | correct : YES

I strongly agree

Answer 2 | correct : NO

I disagree

Answer 3 | correct : NO

I agree

Answer 4 | correct : NO

I strongly disagree

If you're not careful which websites you visit, which of the following can result?

marks

2

Image

Answers

Answer 1 | correct : NO

Spyware or Adware installation

Answer 2 | correct : NO

Someone may hijack your browser

Answer 3 | correct : NO

Information or identity theft

Answer 4 | correct : YES

All of the above

Which of these is not a good physical security practice?

marks

2

Image

Answers

Answer 1 | correct : YES

Always wear your security badge when leaving work, even if just for a break. They should be worn outside of the office in public so other people know where you work.

Answer 2 | correct : NO

When working in a public setting, prevent people from reading your work by shielding your paperwork, screen, and, keyboard when typing passwords.

Answer 3 | correct : NO

Control access to your office by ensuring the door closes completely behind when entering and exiting. Ensure that no one slips in behind you.

Answer 4 | correct : NO

Store confidential and sensitive items in a secure place

Appendix H: Database Tables

1 answers

Creation: Apr 24, 2017 at 03:21 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	int(11)	UNSIGNED	No		auto_increment			
question_id	int(11)		No					
answer	text		No					
correct	enum('0', '1')		No					
created_at	datetime		No					
updated_at	datetime		No					

2 assessments

Creation: Apr 24, 2017 at 03:21 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	int(11)	UNSIGNED	No		auto_increment			
name	varchar(100)		No					
description	text		No					
category_id	int(11)		No					
available_from	date		No					
available_to	date		No					
duration	bigint(20)		No					
questions	int(11)		No					
pass_mark	int(11)		No					
type	enum('paid', 'free')		No	free				
cost	int(50)		No					
active	enum('0', '1')		No	1				
created_at	datetime		No					
updated_at	datetime		No					

3 categories

Creation: Apr 24, 2017 at 03:21 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	int(11)	UNSIGNED	No		auto_increment			
name	varchar(100)		No					
description	text		No					
created_at	datetime		No					
updated_at	datetime		No					

4 departments

Creation: Apr 24, 2017 at 03:21 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	int(11)	UNSIGNED	No		auto_increment			
name	varchar(100)		No					
description	text		No					
created_at	datetime		No					
updated_at	datetime		No					

5 groups

Creation: Apr 24, 2017 at 03:21 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
name	varchar(20)		No					
description	varchar(100)		No					

6 login_attempts

Creation: Apr 24, 2017 at 03:21 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
ip_address	varbinary(16)		No					
login	varchar(100)		No					
time	int(11)	UNSIGNED	Yes	NULL				

7 migrations

Creation: Apr 24, 2017 at 03:21 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
version	int(3)		No					

8 questions

Creation: Apr 24, 2017 at 03:29 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	int(11)	UNSIGNED	No		auto_increment			
assessment_id	varchar(100)		No					
question	text		No					
image	varchar(100)		No					
marks	int(11)		No					
created_at	datetime		No					
updated_at	datetime		No					

10 subscriptions

Creation: Apr 24, 2017 at 03:28 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	int(11)	UNSIGNED	No		auto_increment			
user_id	int(11)		No					
assessment_id	int(11)		No					
amount	double		No					
payer_name	varchar(255)		No					
payer_email	varchar(255)		No					
paypal_transaction_id	varchar(255)		No					
payment_status	enum('Pending', 'Completed')		No	Pending				
created_at	datetime		No					
updated_at	datetime		No					

11 user_assessments

Creation: Apr 24, 2017 at 03:21 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	int(11)	UNSIGNED	No		auto_increment			
user_id	int(11)		No					
exam_id	int(11)		No					
start	datetime		No					
end	datetime		No					
status	enum('completed', 'inprogress')		No					

12 user_questions

Creation: Apr 24, 2017 at 03:28 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	int(11)	UNSIGNED	No		auto_increment			
user_id	int(11)		No					
question_id	int(11)		No					
assessment_id	int(11)		No					
filled	enum('yes', 'no')		No					
answer	int(11)		No					

13 users

Creation: Apr 24, 2017 at 03:21 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
ip_address	varbinary(16)		No					
username	varchar(100)		No					
password	varchar(80)		No					
salt	varchar(40)		No					
email	varchar(100)		No					
activation_code	varchar(40)		Yes	NULL				
forgotten_password_code	varchar(40)		Yes	NULL				
forgotten_password_time	int(11)	UNSIGNED	Yes	NULL				
remember_code	varchar(40)		Yes	NULL				
created_on	int(11)	UNSIGNED	No					
last_login	int(11)	UNSIGNED	Yes	NULL				
active	tinyint(1)	UNSIGNED	Yes	NULL				
first_name	varchar(50)		Yes	NULL				
last_name	varchar(50)		Yes	NULL				
company	varchar(100)		Yes	NULL				
phone	varchar(20)		Yes	NULL				
photo	varchar(100)		No					

14 users_groups

Creation: Apr 24, 2017 at 03:21 PM

Column	Type	Attributes	Null	Default	Extra	Links to	Comments	MIME
id	mediumint(8)	UNSIGNED	No		auto_increment			
user_id	mediumint(8)	UNSIGNED	No					
group_id	mediumint(8)	UNSIGNED	No					