UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES

SCHOOL OF COMPUTING AND INFORMATICS

CYBER SECURITY PREPAREDNESS ASSESSMENT TOOLKIT

PRESENTED

BY

VINCENT NGUNDI IKOVO

REG-NO: P58/9170/2006

A PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF MASTERS OF SCIENCE IN COMPUTER SCIENCE

OCTOBER 2018

DECLARATION

This project, as it is, is my original work and has not been presented for the award of any degree in any other University.

Signature: …… Date: ……

Ngundi Vincent Ikovo

This project has been submitted with my approval as University supervisor.

Signature: …… Date: ……

Dr. Abade Elisha Odira

School of Computing and Informatics

ABSTRACT

The internet is becoming an important thing in people's daily life and has grown at an explosive rate. According to GlobalWebIndex (2018), internet users (population) around the world are over 4 billion, which corresponds to almost 53% of the world's population. In the developing countries, people who use internet is around 31% of the population, compared with 77% in the developed countries. Nonetheless, in Kenya, Internet usage is at 52%, well above the ITU average for developing countries. This can be explained by high mobile penetration in Kenya which stands at 90.4% according to the Communication Authority of Kenya (CA). The Internet usage purposes bring both advantages and disadvantages for people and their community. In this research we focus on the downside which includes illegal content, online fraud, identity theft, espionage, sabotage, cyber terrorism, and cyber stalking. While many organizations would not wish to have their information exposed to unauthorized audiences, they also face the challenge that they cannot do meaningful business today without automation of their services. This therefore underscores the position of ensuring that while they go online, they are also guaranteed that their data is secure, which leads to the fact that organizations should take the concept of cyber security seriously. To deal with this predicament, advisory organizations are promoting a more proactive and adaptive approach. This has necessitated recommendation of various frameworks such as National Institute of Standards and Technology (NIST) and Control Objectives for Information and Related Technologies (COBIT) that can help organizations navigate through the complex landscape of cyber security with a shift toward continuous monitoring and real-time assessments. The challenge then comes on how organizations can apply these standards in a cost-effective manner that allows them to be guaranteed of being cyber security ready.

DEDICATION

To my loving family for your support and encouragement.

To my parents for encouraging me to pursue education to the highest.

To my daughters, as an inspiration to you.

ACKNOWLEDGEMENT

I thank the Almighty God for His grace and mercies.

I thank Dr. Abade Elisha Odira for his continued guidance throughout the project cycle.

I thank Dr. Andrew Mwaura Kahonge for finding time to positively review the project.

I thank Prof. Omwenga for his constructive critiques which helped in re-shaping this project.

I thank Prof. Waema Timothy. He has a unique way of simplifying complex concepts for his students.

I thank the entire School of Computing fraternity for their support during the time of my study.

LIST OF ABBREVIATIONS AND ACCRONYMS

BYOD	Bring Your Own Device
CA	Communication Authority of Kenya
CEOs	Chief Executive Officer
CERT	Chief Information Officer
CIOs	Chief Information Officer
CISOs	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technologies
CSF	Cybersecurity Framework
IMDB	Internet Movie Database
ITIL	Information Technology Infrastructure Library
MILs	Maturity Indicator Levels
MITM	Man in the middle
NIST	Cybersecurity Framework
NoSQL	Non-Relational Structured Query Language
PCI DSS	Payment Card Industry Data Security Standard
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management System
SME's	Small and Medium Enterprises
UI	User Interface
WIMP	Windows, Icons, Mouse, and Pull-down menus

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

1.1 Background of the study

The internet is becoming an important thing in people's daily life and has grown at an explosive rate (Greitzer & Frincke, 2010). According to GlobalWebIndex (2018), internet users (population) around the world are over 4 billion, which corresponds to almost 53% of the world's population. In the developing countries, people who use internet is around 31% of the population, compared with 77% in the developed countries (ITU, 2013). Nonetheless, in Kenya, Internet usage is at 52%, well above the ITU average for developing countries (Research ICT Africa, 2018). This can be explained by high mobile penetration in Kenya which stands at 90.4% according to the Communication Authority of Kenya (CA).

Traditionally, the Internet was used for military, defense contractors, and a university research purpose. However, in recent years, it has been developed to multi-purposes including information, communication, leisure, shopping, education, e-social activities, financial, job seek, homepage, file share service, and download (Kisa, 2011). These internet usage purposes bring both advantages and disadvantages for people and their community. In this research we focus on the downside which include illegal contents, online fraud, identity theft, espionage, sabotage, cyber terrorism, and cyberstalking (Boateng, 2011; Department of Economic and Social affairs, 2012; Greitzer & Frincke, 2010; Arif & Gultom, 2005) among others hence the need for cyber security.

Theoretically, cyber security has to fulfill 3 (three) critical points: Measures to protect Information Technology; the degree of protection resulting from application of those measures; and the associated field of professional endeavor (Fisher, 2009). These three

critical aspects of cyber security play an important role to protect personal, institutional and even government data, which if not protected, can be exposed to misuse or undue manipulation (IBM X-Force Research, 2015; Geer & Pareek, 2012).

While many organizations would not wish to have their information exposed to unauthorized audiences, they also face the challenge that they cannot do meaningful businesses today without automation of their services (PwC & Iron Mountain, 2012). This therefore underscores the position of ensuring that while they go online, they are also guaranteed that their data is secure, which leads to the fact that organizations should take seriously, the concept of Cyber Security (McKinsey & Company, 2014).

Interestingly, it is not easy to define the phrase "Cyber Security". According to Eric A. Fisher, "there are many components of cyberspace and many potential components of cyberspace" to be used in order to determine the cyberspace's meanings (Fisher, 2009). However, in the context of our study, we shall take cyber security to mean the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. This comprises of the following elements:

(i) Application security

(ii) Information security

(iii) Network security

(iv) Disaster recovery / business continuity planning

(v) Operational security

(vi) End-user education

One of the most problematic elements of cyber security is the quickly and constantly evolving nature of security risks. The traditional approach has been to focus most

resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment (Booz, 2011).

To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach (GCSCC, 2014). This has necessitated recommendation of various frameworks such as NIST and COBIT that can help organizations navigate through the complex landscape of cyber security with a shift toward continuous monitoring and real-time assessments (HLEG, 2008). The challenge then comes on how organizations can apply these standards in a manner that allows them to be guaranteed of being Cyber security ready.

1.2 Problem Statement

Today, many organizations have invested heavily in computer technology so as to enjoy the gains that come with automation such as cost effectiveness, efficiency and timely production (Such *et al.,* 2015). However, cyber security issues are on the rise, in multiple forms, ranging from simple techniques to sophisticated malwares and other threats thereby threatening to erode the very gains for which the organization invested in computer technology (Such *et al.,* 2015). Organizations therefore find it very important to prepare themselves against any incidences of cyber security threats (ITU, 2014a).

Aho and Nevala (2016) evaluated cyber security preparedness of SME's and found that less than 3% of the organisations knew they had suffered a security breach and less than 13% of them taught their employees about their information security policies. Suihkonen (2016) also found that the biggest challenge with cyber security in SME organizations is the preparedness for network incidents.

To this effect, it is important that such organizations can have mechanisms to help them determine, how prepared they are to combat cybercrimes aimed at their computing systems. While Frameworks such as NIST (2018) and COBIT (2011) exist that can help organizations to assess their readiness, it is a fact that implementing them has not been easy. Therefore, this research project aims at implementing a voluntary, non-technical assessment toolkit to help an organization evaluate its operational resilience and cyber security practices. The toolkit is intended to be simple so that the readiness assessment can be conducted as a self-assessment or as an on-site assessment facilitated by a cyber-security professional.

1.3 Research Objectives

The overall objective of the research was to investigate how organizations currently determine their level of preparedness to combat cybercrimes and to come up with a simple to toolkit that would simplify the process of cyber security readiness assessment.

The specific objectives of the research were postulated as follows:

i. To investigate how organizations determine or assess their level of preparedness against cyber security threats.
ii. To determine the frameworks available for Cyber security readiness assessment.
iii. To determine which of these frameworks are utilized and reasons for their utilization or lack of it among key business organizations in Kenya.
iv. To design and implement a simple toolkit for cyber security assessment
v. To demonstrate effectiveness of proactive self-assessment using the developed toolkit.

1.4 Research Questions

This research was guided by the following questions:

i. How do organizations in Kenya determine their own level of preparedness against cyber security threats?
ii. What are the main frameworks available for assessing levels of cyber security preparedness?
iii. Which of these cyber security frameworks are implemented by Kenyan enterprises and why?
iv. Are there any challenges Kenyan businesses faces when it comes to determining their own levels of cyber security preparedness?
v. Can a toolkit be used to assist more Kenyan businesses understand their own level of cyber Security preparedness?
vi. What are the perceived benefits of using an automated toolkit for assessing levels of cyber security preparedness?

1.5 Justification and Significance of the Study

The study indicated that most organizations avoid using external consultants to conduct cyber security capability assessments mainly due to the related costs and the need for privacy. Respondents further indicated that some of the challenges with their internal assessments methods included difficulty in assessing, measuring and analyzing the level of capability or preparedness. A large majority of the organizations also indicated that they use a manual system of assessment and that an automated system would be important in assessing their organization's cyber security preparedness especially because it would ease the adoption of cyber security capability assessment frameworks; ease the

complexity of assessment and the time it takes to conduct such; enhance the objectivity of the assessment process and reduce related costs.

The automated cyber security preparedness assessment toolkit will significantly reduce the costs of assessment as it is a tool mainly meant for proactive self-assessment using facilitators that are internal to the organization. This is particularly useful for Small and Medium Enterprises (SME's) which form a majority of Kenyan enterprises. Having an internal self-assessment tool will also address the need for privacy. The automated toolkit will also ease the difficulty in assessing, measuring and analyzing the level of capability or preparedness, while enhancing the objectivity of the assessment process and reduce related costs.

The cyber security preparedness assessment toolkit may also go a long way in enhancing organizational planning by facilitating the creation of an action plan for addressing weaknesses and leveraging strengths identified in the assessment. The toolkit may also be used to enhance resource optimization through the performance summary which may give some initial insights into where to invest in cyber security improvements. Indeed, the toolkit may contribute to overall organizational process improvement given the toolkit provides an organization with information on its current level of cyber security capabilities as a baseline for initiating a data-driven process improvement.

1.6 Deliverables

The study delivered the following;

i. A functional VART-prototype which was can be used to assess the level or cybersecurity preparedness in an organization.
ii. A project report, which described the functionalities of the VART-prototype.

CHAPTER TWO

REVIEW OF THE RELATED LITERATURE

2.1 Introduction

This chapter covered a review of related literature that had similarities or were related to the problem under study. The reviews included studies done by prominent researchers on problems revolving around the Cyber security.

The reviews provided the researcher with a clear picture of how similar research problems were best solved elsewhere in the World. It must be noted that there was no guarantee that a specific approach used to solve a research problem elsewhere, could be implemented to solve a similar research problem and work effectively on a different environment. The researcher borrowed ideas from similar research and contextualized them to fit the current local context.

With respect to the statement that, a researcher must examine all available literature to familiarize himself /herself with the problem at hand, and that he/she may adopt any or both two types of literatures namely;

i. The conceptual literature-which concerns concepts and theories, and/or
ii. The empirical literature-which consist of studies done in the past and related to the proposed study. The following literatures were reviewed;

2.2 Cyber Security

Cyber security consists of technologies, processes and measures that are designed to protect systems, networks and data from cybercrimes. Effective cyber security reduces the risk of a cyber-attack and protects entities, organizations and individuals from the deliberate exploitation of systems, networks and technologies (Ponemon Institute, 2013).

A cyber-attack is usually intended to inflict damage or expropriate information from an individual, organization or public entity, for the purpose of theft (of payment card data, customer details, company secrets or intellectual property), unauthorized access to networks, and compromise of official records or financial and/or reputational damage.

Reasons for increase in cyber crimes

1. **Cyber criminals are indiscriminate**. Where there is a weakness, they will try to exploit it. Due to the massive financial gains being made, cyber-crime has become a multibillion pound industry.
2. **Cyber-crimes are constantly evolving**. Cyber-attacks are becoming more complex and organisations are struggling to keep up with the pace of change.
3. **Cyber-attacks come in various forms** and are designed to not only target technological weaknesses (for instance, outdated software) but also exploit people (for instance, uninformed employees who click on malicious links) and a lack of effective organisational processes and procedures (Nykodym, Taylor & Vilela, 2005).

2.3 Attack techniques

Cyber criminals use a variety of malware and vectors to attack their targets:

- **Malware**

  It refers to software programs designed to damage or do other unwanted actions on a computer system (Christensson, 2006).

- **Ransomware**

  It is a type of malware that prevents you from using your computer or accessing certain files unless you pay a ransom (Christensson, 2017).

- **Virus**

  it is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions (Christensson, 2017).

- **Worms**

  It is a type of malicious software program whose primary function is to infect other *computers* while remaining active on infected systems (Barwise, 2010)

- **Spyware/adware**

  A software that's designed to gather data from a computer or other device and forward it to a third party without the consent or knowledge of the user (Barwise, 2010)

- **Trojans**

  It is any malicious computer program which misleads users of its true intent (Vincentas, 2013)

Attack vectors

There are also a number of attack vectors available to cyber criminals that allow them to infect computers with malware or harvest stolen data, such as:

- **Social engineering** – refers to tricking people into divulging personal information or other confidential data (Christensson, 2016)

- **Phishing** – is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication (Ramzan, 2010)
- **Pharming** – refers to redirecting website traffic through hacking, whereby the hacker implements tools that redirect a search to a fake website (Ramzan, 2010)
- **Drive-by** – refers to potentially harmful software code that is installed on a person's computer without the user needing to first accept or even be made aware of the software installation.
- **Man in the middle (MITM)** – is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other (Callegati, Cerroni & Ramilli, 2009)

2.4 Key Cyber security Challenges in Todays Networked Environment

2.4.1 Secure Computations in Distributed Programming Frameworks

Distributed programming frameworks utilize parallel computation and storage to process massive amounts of data. For example, the MapReduce framework splits an input file into multiple chunks (Apache Software Foundation, 2016). In the first phase of MapReduce, a Mapper for each chunk reads the data, performs some computation, and outputs a list of key/value pairs. In the next phase, a Reducer combines the values belonging to each distinct key and outputs the result. There are two major attack prevention measures: securing the mappers and securing the data in the presence of an untrusted mapper (Priya *et al.,* 2014; Madhusudhan *et al.,* 2017).

2.4.2 Security Best Practices for Non-Relational Data Stores.

The security infrastructures of non-relational data stores popularized by NoSQL databases are still evolving. For instance, robust solutions to NoSQL injection are still not mature. Each NoSQL database was built to tackle different challenges posed by the analytics world, and security was never addressed during the design stage (Lior, 2011). Developers using NoSQL databases usually embed security in the middleware. NoSQL databases do not provide any support for explicitly enforcing security in the database. However, clustering aspects of NoSQL databases pose additional challenges to the robustness of such security practices (Padhy et al., 2011).

2.4.3 Secure Data Storage and Transactions Logs

Data and transaction logs are stored in multi-tiered storage media. Manually moving data between tiers gives the IT manager direct control over exactly what data is moved and when (Katal *et al.,* 2013) However, as the size of data set continues to grow exponentially, scalability and availability have necessitated auto-tiering for Big Data storage management. Auto-tiering solutions do not keep track of where the data is stored, which poses new challenges to secure data storage (Amanatullah *et al.,* 2013) New mechanisms are imperative to thwart unauthorized access and maintain constant availability.

2.4.4 End-Point Input Validation/Filtering

Many Big Data uses in enterprise settings require data collection from a variety of sources, including end-point devices. For example, a security information and event management system (SIEM) may collect event logs from millions of hardware devices and software applications in an enterprise network (Cloud Security Alliance, 2013). A key challenge in the data collection process is input validation: how can we trust the data?

How can we validate that a source of input data is not malicious? And how can we filter malicious input from our collection? Input validation and filtering is a daunting challenge posed by untrusted input sources, especially with the bring-your-own-device (BYOD) model (Cloud Security Alliance, 2013).

2.4.5 Real-Time Security Monitoring.

Big Data and security do not only intersect at the protection of Big Data infrastructures, but also at the leveraging of Big Data analytics to help improve the security of other systems. One of the most challenging Big Data analytics problems is real-time security monitoring, which consists of two main angles:

i. Monitoring the Big Data infrastructure itself and
ii. Using the same infrastructure for data analytics.

An example of (a) is the monitoring of the performance and health of all the nodes that make up the Big Data infrastructure. An example of (b) would be a health care provider using monitoring tools to look for fraudulent claims or a cloud provider using similar Big Data tools to get better real-time alert and compliance monitoring. These improvements could provide a reduction in the number of false positives and/or an increase in the quality of the true positives (Cloud Security Alliance, 2013).

Real-time security monitoring is a challenge because of the number of alerts generated by security devices. These alerts (correlated or not) lead to a massive number of false positives, which are often ignored due to limited human capacity for analysis. This problem might even increase with Big Data, given the volume and velocity of data streams. However, Big Data technologies may provide an opportunity to rapidly process and analyze different types of data. These technologies can be used to provide, for

instance, real-time anomaly detection based on scalable security analytics (Cloud Security Alliance, 2013)..

2.4.6 Scalable and Composable Privacy-Preserving Data Mining and Analytics

Big Data can potentially enable invasions of privacy, invasive marketing, decreased civil liberties, and increased state and corporate control (Boyd & Crawford, 2012).

A recent analysis of how companies are leveraging data analytics for marketing purposes included an example of how a retailer was able to identify a teen's pregnancy before her father learned of it. Similarly, anonymizing data for analytics is not enough to maintain user privacy (Boyd & Crawford, 2012). For example, AOL released anonymized search logs for academic purposes, but users were easily identified by their searches. Netflix faced a similar problem when anonymized users in their data set were identified by correlating Netflix movie scores with IMDB scores. Therefore, it is important to establish guidelines and recommendations for preventing inadvertent privacy disclosures.

2.4.7 Cryptographically Enforced Data-Centric Security

There are two fundamentally different approaches to controlling the visibility of data to different entities, such as individuals, organizations and systems. The first approach controls the visibility of data by limiting access to the underlying system, such as the operating system or the hypervisor (Bethencourt, Sahai & Waters, 2007). The second approach encapsulates the data itself in a protective shell using cryptography. Both approaches have their benefits and detriments. Historically, the first approach has been simpler to implement and, when combined with cryptographically-protected communication, is the standard for the majority of computing and communication infrastructure (Goyal *et al.,* 2008).

However, the system-based approach arguably exposes a much larger attack surface. The literature on system security is replete with attacks on the underlying systems to circumvent access control implementations (such as buffer overflow and privilege escalation) and access the data directly (Goyal *et al.,* 2006). On the other hand, protecting data end-to-end through encryption exposes a smaller, more well-defined attack surface. Although covert side-channel attacks are possible to extract secret keys, these attacks are far more difficult to mount and require sanitized environments.

2.4.8 Granular Access Control

The security property that matters from the perspective of access control is secrecy – preventing access to data by people that should not have access. The problem with course-grained access mechanisms is that data that could otherwise be shared is often swept into a more restrictive category to guarantee sound security. Granular access control gives data managers more precision when sharing data, without compromising secrecy (Li, Wang, Ma, Liang, 2008; Elliott & Knight, 2010).

2.4.9 Granular Audits

With real-time security monitoring, notification at the moment an attack takes place is the goal. In reality, this will not always be the case (e.g., new attacks, missed true positives). In order to discover a missed attack, audit information is necessary. Audit information is crucial to understand what happened and what went wrong. It is also necessary due to compliance, regulation and forensic investigation. Auditing is not something new, but the scope and granularity might be different in real-time security contexts. For example, in these contexts there are more data objects, which are probably (but not necessarily) distributed (Sunderland, 2017).

2.4.10 Data Provenance

Provenance metadata will grow in complexity due to large provenance graphs generated from provenance-enabled programming environments in Big Data applications. Analysis of such large provenance graphs to detect metadata dependencies for security and/or confidentiality applications is computationally intensive (McDaniel, 2011).

2.5 Key Security Frameworks used

2.6 NIST Framework

President Obama signed Executive Order 13636 in 2013, titled Improving Critical Infrastructure Cyber security, which set the stage for the NIST Cyber security Framework (US Federal Register, 2013). The CSF's goal is to create a common language, set of standards, and easily executable series of goals for improving cyber security.

The CSF standards are completely optional-there's no penalty to organizations that don't wish to follow its standards. That doesn't mean it isn't an ideal jumping off point though-it was created with scalability and gradual implementation so any business can benefit (Joint Task Force Transformation Initiative, 2013). The framework itself is divided into three components: core, implementation tiers, and profiles.

Framework Core

The core is "a set of activities to achieve specific cyber security outcomes, and references examples of guidance to achieve those outcomes." It is further broken down into four elements: functions, categories, subcategories, and informative references.

- **Functions**: There are five functions used to organize cyber security efforts at the most basic level: identify, protect, detect, respond, and recover. Together these

five functions form a top-level approach to securing systems and responding to threats—think of them as your basic incident management tasks.

- **Categories**: Each function contains categories used to identify specific tasks or challenges within it. For example, the protect function could include access control, regular software updates, and anti-malware programs.
- **Subcategories**: These are further divisions of categories with specific objectives. The regular software updates category could be divided into tasks like making sure wake on LAN is active, that Windows updates are configured properly and manually updating machines that are missed.
- **Informative references:** Documentation, steps for execution, standards, and other guidelines would fall into this category. A prime example in the manual Windows update category would be a document outlining steps to manually update Windows PCs (Stouffer *et al.,* 2017)

Implementation Tiers

There are four tiers of implementation, and while CSF documents don't consider them maturity levels, the higher tiers are considered more complete implementation of CSF standards.

- **Tier 1**: Called partial implementation, organizations at Tier 1 have an ad-hoc and reactive cyber security posture. They have little awareness of organizational risk and any plans implemented are often done inconsistently.
- **Tier 2**: Risk informed organizations may be approving cyber security measures, but implementation is still piecemeal. They are aware of risks, have plans, and

have the proper resources to protect themselves but haven't quite gotten to a proactive point.

- **Tier 3**: The third tier is called repeatable, meaning that an organization has implemented CSF standards company-wide and are able to repeatedly respond to crises. Policy is consistently applied, and employees are informed of risks.
- **Tier 4**: Called adaptive, this tier indicates total adoption of the CSF. Adaptive organizations aren't just prepared to respond to threats - they proactively detect threats and predict issues based on current trends and their IT architecture (Stouffer *et al.,* 2017).

Profiles

Profiles are both outlines of an organization's current cybersecurity status and roadmaps toward CSF goals. NIST said having multiple profiles - both current and goal - can help an organization find weak spots in its cybersecurity implementations and make moving from lower to higher tiers easier.

Profiles also help connect the functions, categories, and subcategories to business requirements, risk tolerance, and resources of the larger organization it serves. Think of profiles as an executive summary of everything done with the previous three elements of the CSF (Stouffer *et al.,* 2017).

Why does the NIST Cybersecurity Framework matter?

The cybersecurity world has a problem: It's incredibly fragmented despite its ever-growing importance to daily business operations. Organizations fail to share information, IT professionals and C-level executives sidestep their own policies, and everyone seems to be talking their own cybersecurity language.

NIST's goal with the creation of the CSF is to help eliminate the utterly fragmented cybersecurity landscape we find ourselves in, and it couldn't matter more at this point in the history of the digital world.

Cybersecurity threats continue to increase, and the latest disasters seemingly come out of nowhere and the reason why we're constantly caught off guard is simple: There's no cohesive framework tying the cybersecurity world together (Stouffer *et al.,* 2017).

Who does the NIST Cybersecurity Framework affect?

The CSF affects literally everyone who touches a computer for business. IT teams and CXOs are responsible for implementing it; regular employees are responsible for following their organization's security standards; and business leaders are responsible for empowering their security teams to get the job done.

The degree to which the CSF will affect the average person won't lessen with time either, at least not until it sees widespread implementation and becomes the new standard in cybersecurity planning.

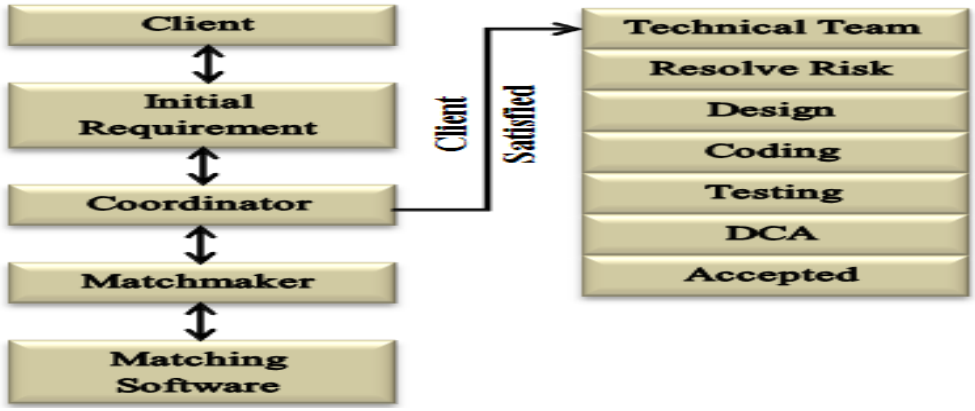
If it seems like a headache it's best to confront it now: Ignoring the NIST's recommendations will only lead to liability down the road that could have easily been avoided. Embrace the growing pains as a positive step in the future of your organization (Stouffer *et al.,* 2017).

2.7 Software Development Models

The Software Development Life Cycle (SDLC) model has continued to evolve (Jamwal, 2010). Comparison was done relating to three previous models namely; Waterfall Model, Prototype Model, and Incremental Model with regards to their advantages, disadvantages,

how they work, deployment method, client satisfaction, quality, budgetary allocation and completion time. From the findings, a new software development model named the New SDLC-2013 Model was developed (Kumar, *et al.,* 2013).

Figure 2.1: SDLC-2013Model



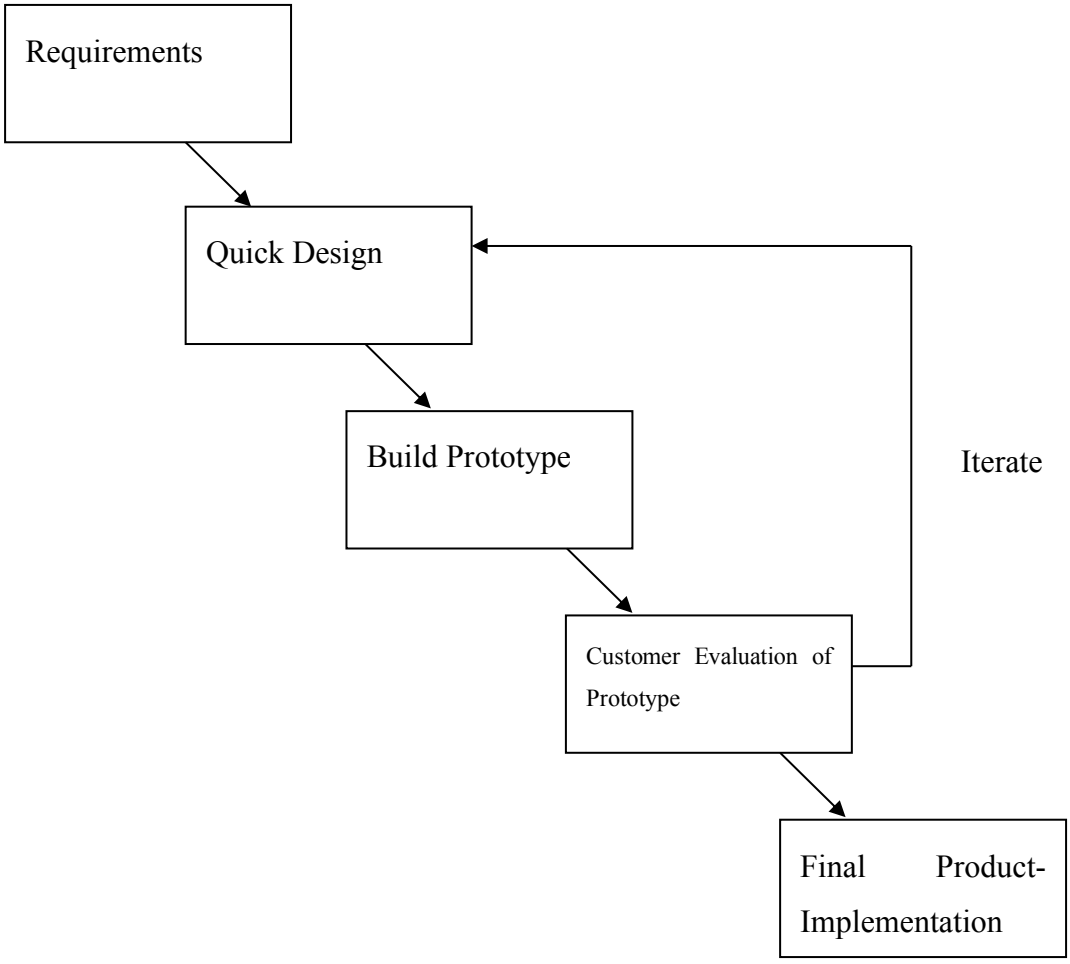
Source: Kumar *et al.*, (2013)

2.8 Theoretical Framework

2.8.1 The Prototyping Software Development Model

Many approaches of software development models do exist and most of them share a combination of stages such as; market research, problem analysis, software implementation, software testing, software deployment, and maintenance. Analysis was done on Waterfall, Prototype, Spiral, Iterative, and Agile models (Jamwal, 2010). The phases involved in prototyping are clearly depicted in the model diagram below:

Figure 2.2: Prototyping Model Approach



Source: Nguyen and Vai (2010)

2.8.2 Software Architecture Models

Software architecture refers to a structured solution aimed at achieving the technical and operational requirements of a system and optimizing common quality attributes like security, performance, and manageability. The choice of software architecture style greatly determines how data can be shared.

Figure 2.3: A 3-Tier Architecture

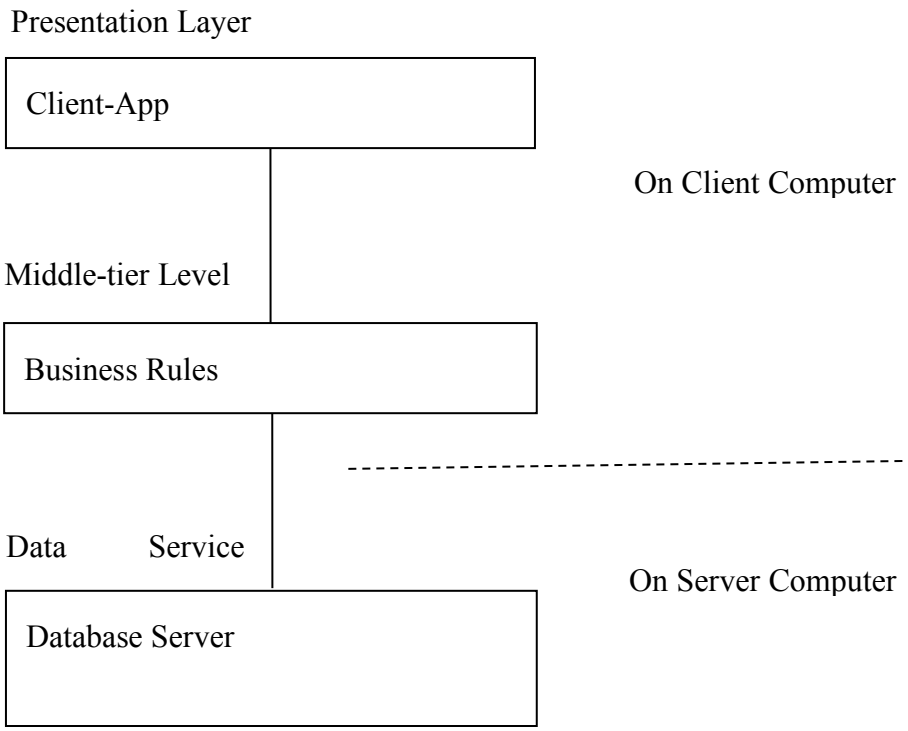
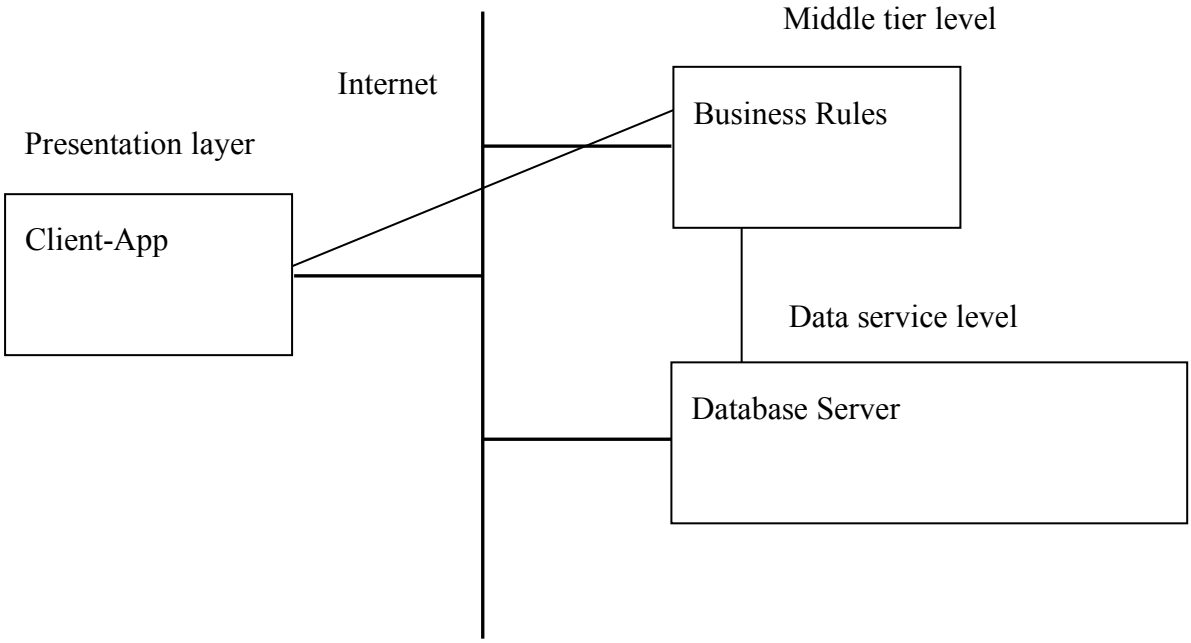


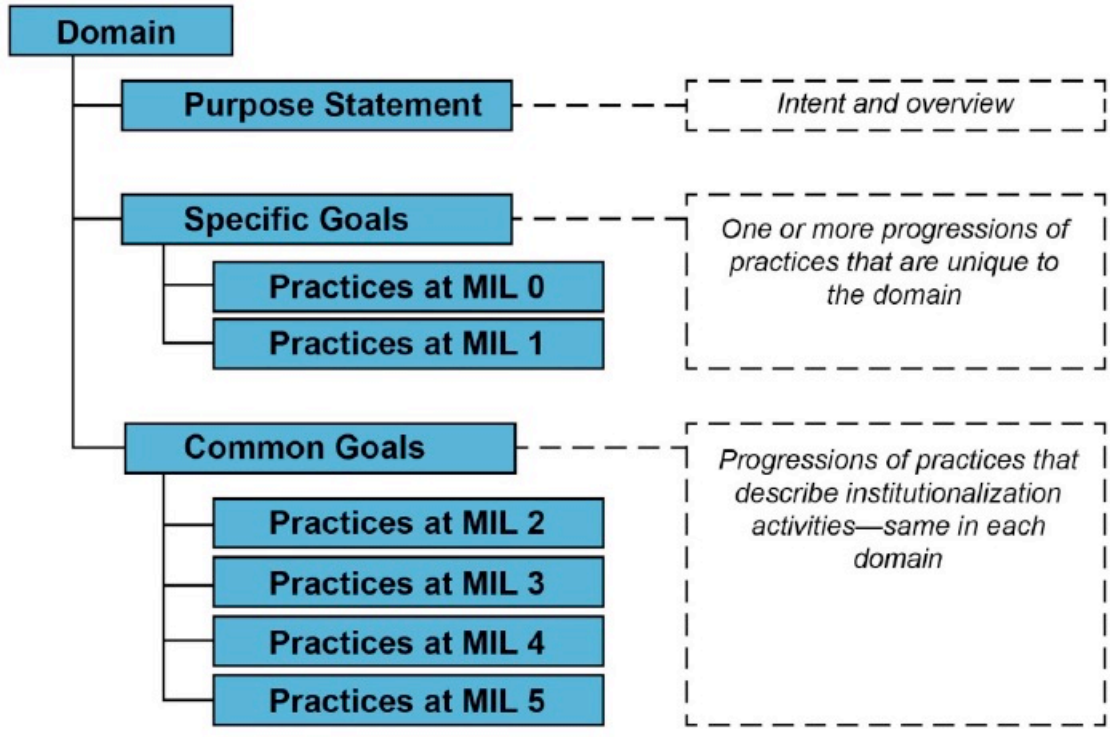
Figure 2.4: An Internet-Based 3 Tier Architecture



2.9 The Proposed Conceptual Model

The conceptual model structure for the VART prototype was based on key aspects from the NIST Framework. It is organized into a set of 10 domains, each domain is further subdivided into Goals and within each goal there are a number of questions referred to as "practices" which seek to determine what the organization does to manage security. Each domain is composed of a purpose statement, a set of specific goals and associated practice questions unique to the domain, and a standard set of Maturity Indicator Level (MIL) questions. The MIL questions examine the institutionalization of practices within an organization. Figure 1 graphically presents the VART domain architecture.

Figure 2.5: Proposed Conceptual Model



All VART questions have three possible responses: "Yes," "No," and "Incomplete." The number of goals and practice questions varies by domain, but the set of MIL questions and the concepts they encompass are the same for all domains.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

According to (Kothari, 2004), it is important for a researcher to know not only the research methods and techniques, but also the methodologies and how to go about designing a research methodology befitting the research problem at hand. He elaborated with relevant examples on how, why, and which methodologies to implement in different situations. This chapter explains who is the target group, how data was collected from the target group, and procedural activities involved during the development of the VART.

3.2 Methods of Data Collection and Sources

3.2.1 The Target Group

The study focused on managers whose duties revolve around ensuring that the information assets are secure. Majority of the respondents were also at senior management level.

3.2.2 Questionnaire Forms

The use of questionnaire forms is said to be best suited for acquiring data from literate people (Kothari, 2004). In this case, we targeted an array of professionals in the management of several SMEs. These included:

i. CEOs

ii. CIOs

iii. CISOs

iv. Information Security Managers

v. IT Managers

vi. Risk Managers

vii. Audit Managers

The questionnaire forms were designed to have closed ended questions, and to get information from respondents on how they manage Information Security in their workplaces.

3.2.3 Administration of the Questionnaires

The questionnaire was administered online to the various respondents via Survey Monkey online survey development software.

3.3 The Development Methodology

The prototyping software development methodology was used for the development of the VART prototype.

3.1 Justification

The justification for using prototyping approach was based on Jamwal's analysis, where prototyping software development model stood out as a model with no risk analysis, high user involvement, good guaranteed success, simple, and was found to be more flexible (Jamwal, 2010). Also Nguyen and Vai (2010) shared a similar perspective, where they stated that a Rapid Prototyping is customer oriented and puts emphasis on validation, and strong advantages such as; very low risk of inappropriate user requirements, uncommitted and accommodates new changes during development, and has a good support for market.

3.4 Design

The researcher used his knowledge and the information collected from the various respondents to come up with a blueprint design for the VART prototype. Some of the phases involved during design were; User Interface (UI) design and the Database design. The architecture of the VART prototype was defined during the design phase, and the preferred development platform was chosen. Java Suite of applications including Java Development Kit, Spring Framework and Maven were used because of their being open source and ability to run across multiple architectures. The VART prototype architecture is as explained below;

a) The User Interface (UI).

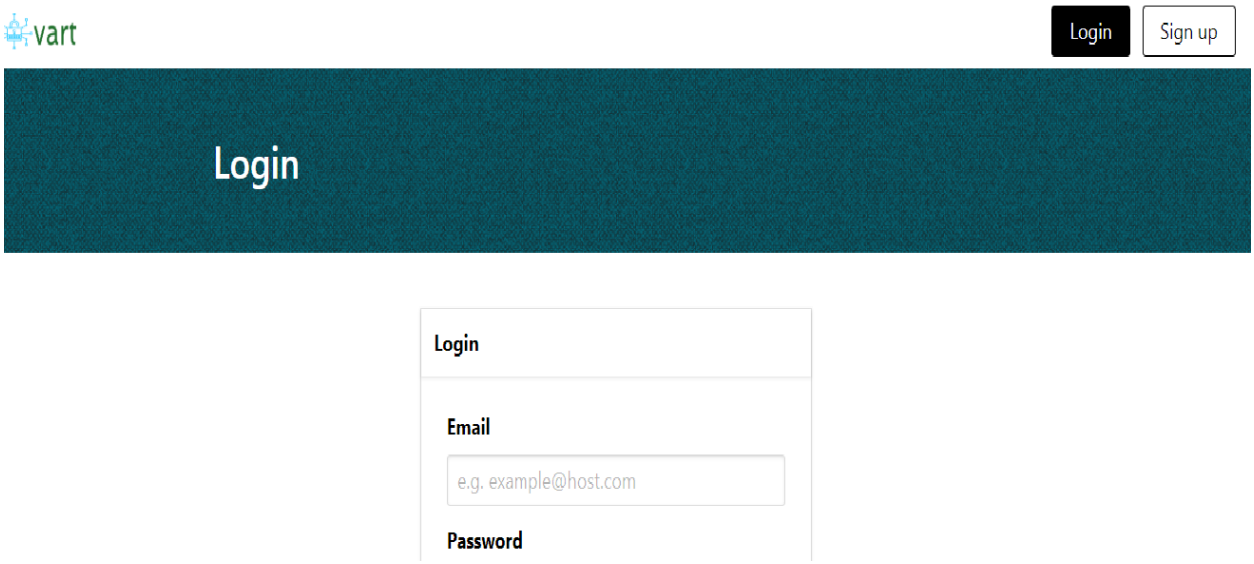
b) The database layer.

c) Logical operations.

The User Interface (UI)

The UI was designed to be as simple as possible, strategically positioning screen elements for the user to easily locate them, re-enforced clarity, user-centered, and with a high degree of better results. Objects like, Menus, Buttons, Scrollbars, and such like were used to increase the ease of use. Sense of security was provided by the provision for user login authentication. It was included to ensure some level of security and integrity of the stored data. It made sure that only a legitimate user gained access to the system and rights to other system modules via the UI.

Figure 3.1: The Login Interface for the VART

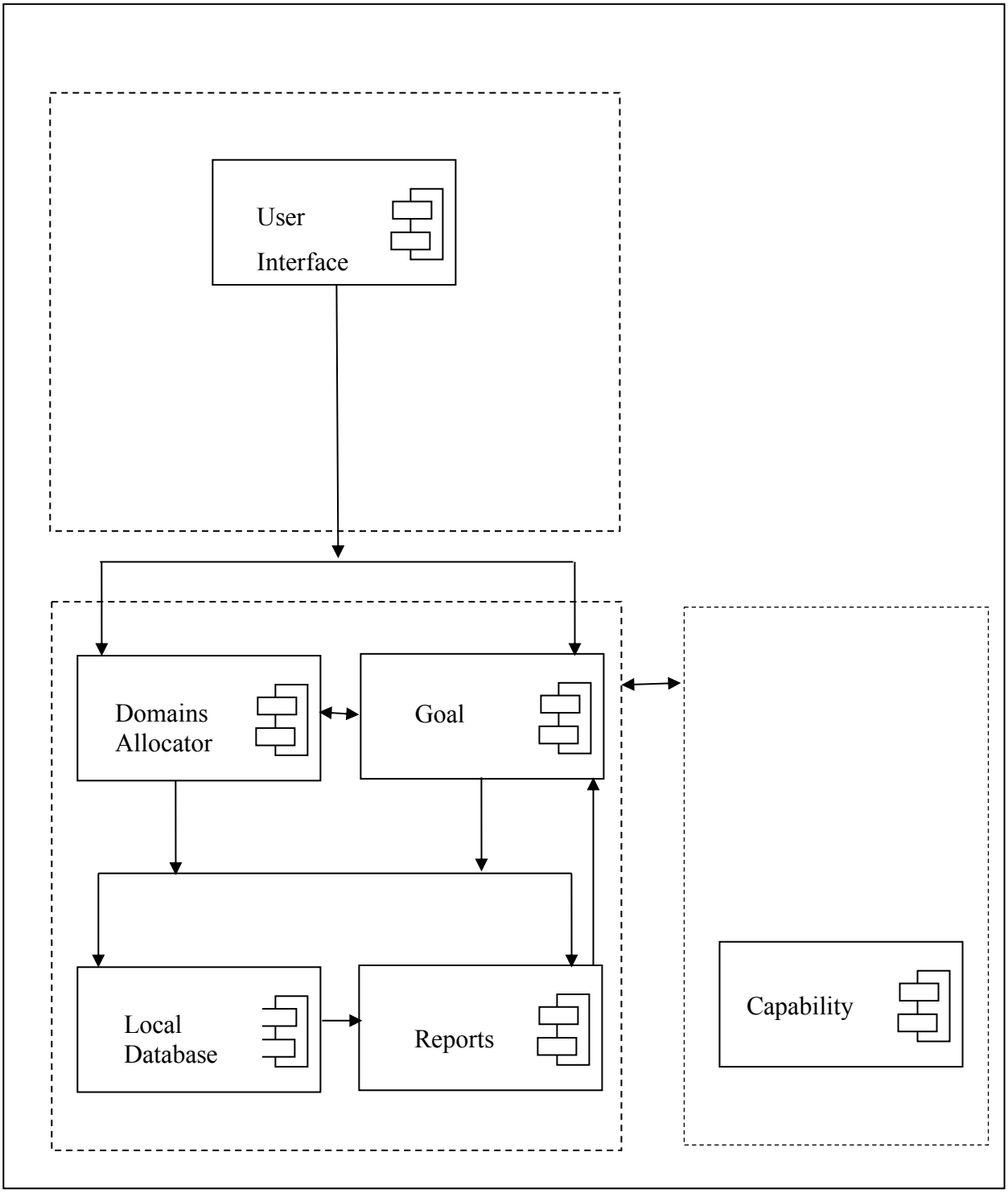


The Databases

The VART was designed to have a local database implemented later on in MySQL. The data model captured the relationship between Domains, Goals and Practices as outlined earlier in our proposed conceptual architecture. The entire system comprised of 14 tables as explained in the section on schema.

The System Architecture

Figure 3.2: The System Architecture



The system architecture is used to show specific components of a system, how they are structured and interconnected (Coulouris *et al.,* 2011). The system architecture for the VART was arrived at after a scrutiny of the current system and preliminary requirements collection from the respondents. The VART architecture is as depicted Figure12. The VART architecture has 6 components namely; UI (User Interface)-responsible for interacting with the user, Domain Allocator-responsible for assigning security domains, Goal Checker-responsible for defining a security goal to a domain, Local Database-responsible for holding data on practices per goal or domain, Reports-responsible for returning various reports using certain defined criteria, and lastly the Assessments repository- which is part of the local database but can be used for tracking the areas of improvement based on a series of vulnerability evaluations.

The Scale and Scoring based on MILs

The VART uses Maturity Indicator Levels (MILs) to provide organizations with an approximation of the maturity of their practices in the 10 cybersecurity domains. The VART's approach to maturity is based on an underlying capability maturity model, the CERT Resilience Management Model. In this approach, the organization's maturity is based on how completely the cybersecurity practices in each of the domains are institutionalized within the organization.

Institutionalization means that cybersecurity practices become a deeper, more lasting part of the organization because they are managed and supported in meaningful ways. When cybersecurity practices become more institutionalized—or "embedded"—managers can have more confidence in the practices' predictability and reliability. The practices also become more likely to be sustained during times of disruption or stress to the

organization. Maturity can also lead to a tighter alignment between cybersecurity activities and the organization's business drivers.

The MIL scale itself uses six maturity levels, each with rigorous, defined components:

(i) Incomplete

(ii) Performed

(iii) Planned

(iv) Managed

(v) Measured

(vi) Defined

MIL0 Incomplete

Practices in the domain are not being performed as measured by responses to the relevant VART questions in the domain.

MIL1 Performed

All practices that support the goals in a domain are being performed as measured by responses to the relevant VART questions.

MIL2 Planned

A specific practice in the VART domain is not only performed but is also supported by planning, stakeholders, and relevant standards and guidelines. A planned process or practice is:

- Established by the organization through policy and a documented plan
- Supported by stakeholders

- Supported by relevant standards and guidelines

MIL3 Managed

All practices in a domain are performed, planned, and have the basic governance infrastructure in place to support the process. A managed process or practice is:

- Governed by the organization
- Appropriately staffed with qualified people
- Adequately funded
- Managed for risk

MIL4 Measured

All practices in a domain are performed, planned, managed, monitored, and controlled. A measured process or practice is:

- Periodically evaluated for effectiveness
- Objectively evaluated against its practice description and plan
- Periodically reviewed with higher level management

MIL5 Defined

All practices in a domain are performed, planned, managed, measured, and consistent across all constituencies within an organization who have a vested interest in the performance of the practice. At MIL5, a process or practice is:

- Defined by the organization and tailored by individual operating units within the organization for their use

- Supported by improvement information that is collected by and shared among operating units for the overall benefit of the organization.

Scoring of the Maturity Indicator Levels (MILs)

In the above progression, an organization can only attain a given MIL if it has attained all lower MILs. In other words, an organization that fails to perform all of the cybersecurity practices at MIL1 in a domain would also fail to reach MIL2 in that domain, even if it would have satisfied all the requirements at MIL2.

The scores for practice performance determine the scores for goal performance, which in turn determine the final scoring result for each domain, expressed in the MIL scale. Scores of MIL0 and MIL1 indicate base practice performance. Scores of MIL2 through MIL5 indicate institutionalization of practices.

Basic rules

1. Practices are either performed (answer = “Yes”), incompletely performed (answer = “Incomplete”), or not performed (answer = “No”).

2. A goal is achieved only if all practices are performed.

3. A domain is achieved at MIL1 if all the goals in the domain are achieved.

4. A domain can be achieved at higher levels if the MIL questions for each level (MIL2 through MIL5) are answered “Yes.”

Coding and Development

The choice of the Java Suite of technologies for the development of the VART prototype was informed by the fact that these are open source tools and are widely supported. Being

free and open source, there would be no restrictions on licensing, improvement and deployment of the prototype.

There were key phases which the researcher had to perform according to the demands of the Prototyping model design. These phases were; Requirements, Design, Prototype Development, Customer evaluation of prototype, and finally the Final product implementation phase (Nguyen & Vai, 2010). During coding, each module/component was repeatedly subjected to the user and recommended changes were included, in line with the Prototyping requirements which dictate that the three middle phases namely; Design, Prototype Development, and Customer evaluation phases must iterate to improve acceptance by customer. This approach was a plus for the proposed VART as it went a long way to deliver the expected results.

Testing

The researcher adopted two types of testing namely; Usability testing and Functionality testing.

Usability Testing

This testing focused on the ease of use where users were invited to participate in using the VART and thereafter, they were asked questions targeting to find out the usability issues/challenges. The issues/challenges that were reported in the questionnaire forms were addressed in the prototype and then the prototype was subjected repeatedly to the testing by users until they were satisfied on the ease of use. Features and objects such as; Windows, Icons, Mouse, and Pull-down menus (WIMP) were strategically included to address the ease of use issues/challenges, see appendices C, and D summary test results respectively.

Functionality Testing

The functionality test helped the researcher to address objective (b). A user could use the system to capture details of how they are currently managing vulnerability assessment in their organization, the system then applies the scoring rubric to come up with the overall rating. This could be compared with what the author manually computes to determine that the system meets the required functionality.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

This chapter discussed the results of the study based on findings of the research with regards to the research objectives, and the functionality of the VART prototype.

4.2 Current practices in Cybersecurity assessment

The researcher sought to establish the current landscape of vulnerability management within the various institutions. This was made possible in two ways namely; through the analysis of questionnaire form data collected and the use of the VART system. The results from analysis and available records are as discussed;

4.2.1 Profile of Cybersecurity Personnel

Figure 4.1: Profile of Cybersecurity Personnel

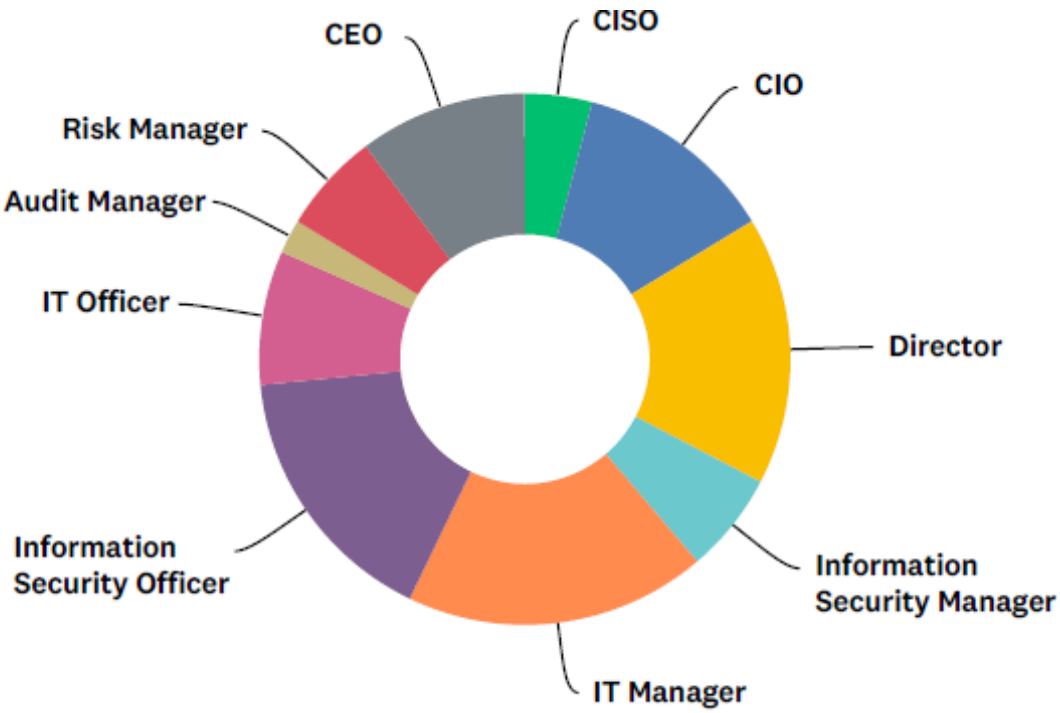
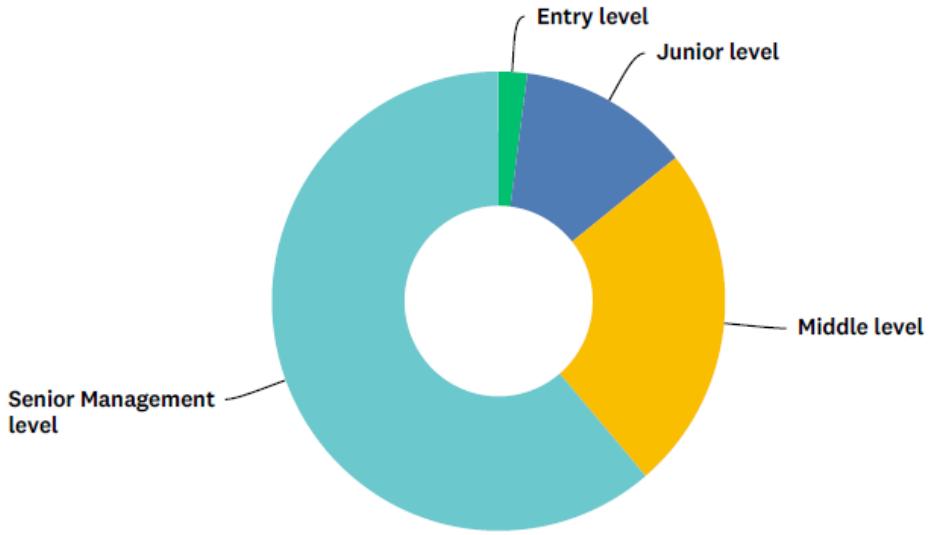


Table 4.1: Profile of Cybersecurity Personnel

Answer Choices	Response Percent	Responses
CISO	4.08%	2
CIO	12.24%	6
Director	16.33%	8
Information Security Manager	6.12%	3
IT Manager	18.37%	9
Information Security Officer	16.33%	8
IT Officer	8.16%	4
Audit Manager	2.04%	1
Risk Manager	6.12%	3
CEO	10.2%	5
TOTAL		49

The respondents comprised information security managers (18.3%), information security officers (16.3%), directors (16.3%), CIO's (12.2%), CEO's (10.2%), IT officers (8.2%), risk managers (6%) and audit managers (2%) as shown in Table 4.1

Figure 4.2: Respondents Managerial Level



Answer Choices	Response Percent	Responses
Entry level	2.04%	1
Junior level	12.24%	6
Middle level	24.49%	12
Senior Management level	61.22%	30
TOTAL		49

The study sought to determine the managerial levels of the respondents. The respondents were mainly from the middle level and senior management levels. They were therefore decision makers in the organisations.

4.3 Adoption of Cybersecurity Management Framework

In this section, the study sought to know from the respondents whether their organizations have adopted any mechanism for measuring cybersecurity preparedness. The responses were as follows:

Figure 4.3: Adoption of Cybersecurity Management Framework

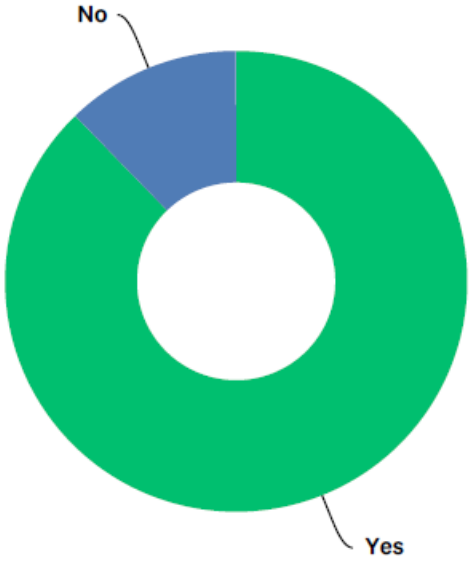


Table 4.2: Adoption of Cybersecurity Management Framework

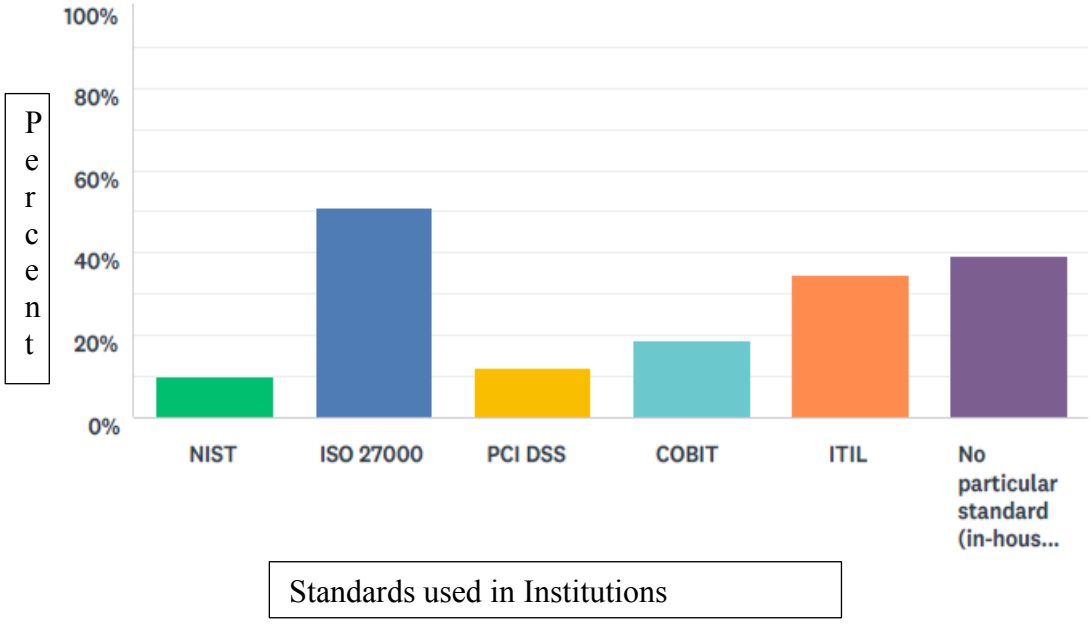
Answer Choices	Response Percent	Responses
Yes	87.76%	43
No	12.24%	6
TOTAL		49

The findings indicate that most of the organizations had adopted a cyber-security management framework with a few exceptions being in the minority.

4.3.1 The Standards Used

The study sought to find out the standards used by the respondents in their institutions. The results are as follows:

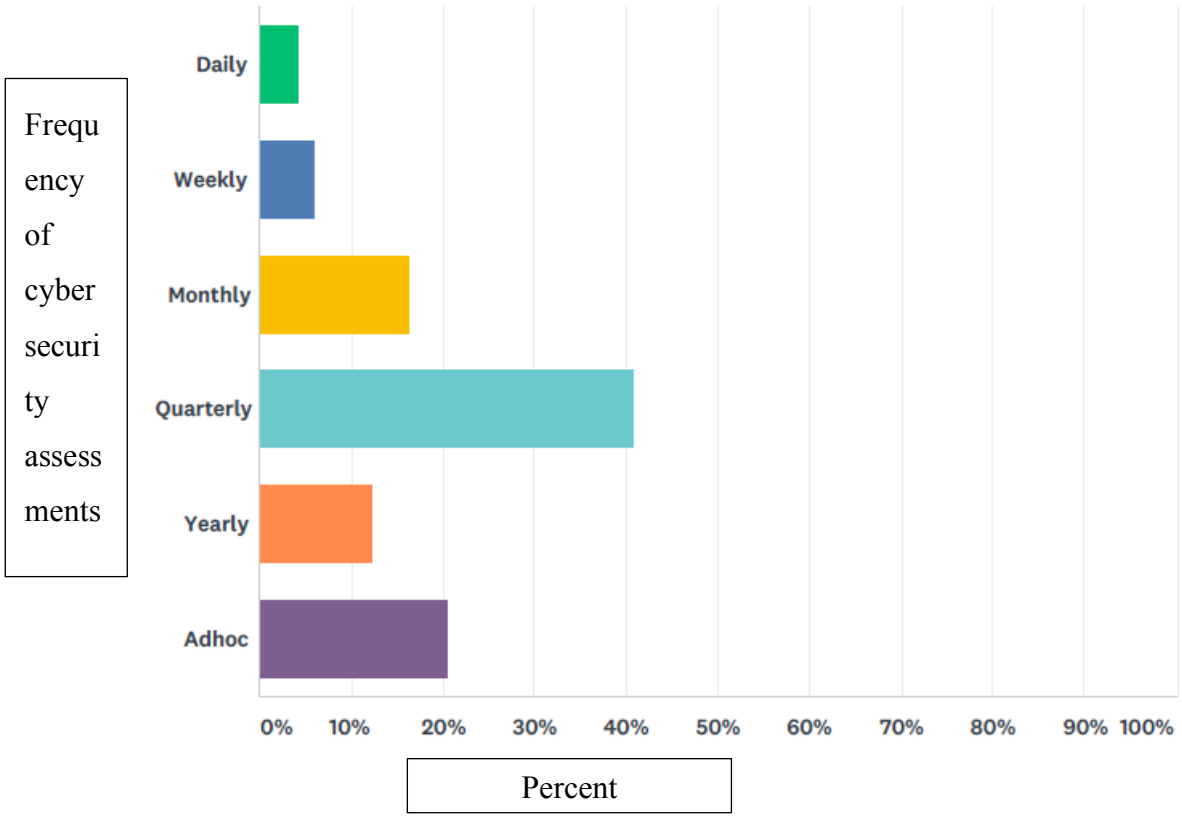
Figure 4.4: Standards Used



The most adopted framework was ISO 27000 (51%), followed by ITIL (34.6%), COBIT (18.3%) and NIST (10.2%). In-house/internally developed cybersecurity assessment framework also comprised a significant framework in the organisations at 38.7%

4.3.2 Frequency of Cybersecurity assessments

Figure 4.5: Frequency of Cybersecurity assessments



The findings in figure 4.5 indicate that most of the organizations did Cybersecurity assessments on a quarterly basis with some doing it on a monthly and ad-hoc basis.

4.3.3 Resources used in assessing Cybersecurity preparedness

Figure 4.6: Resources used in assessing Cybersecurity preparedness

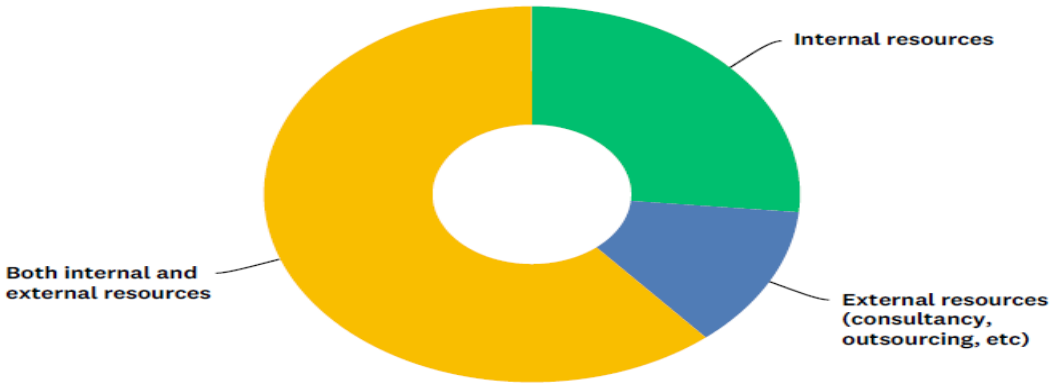


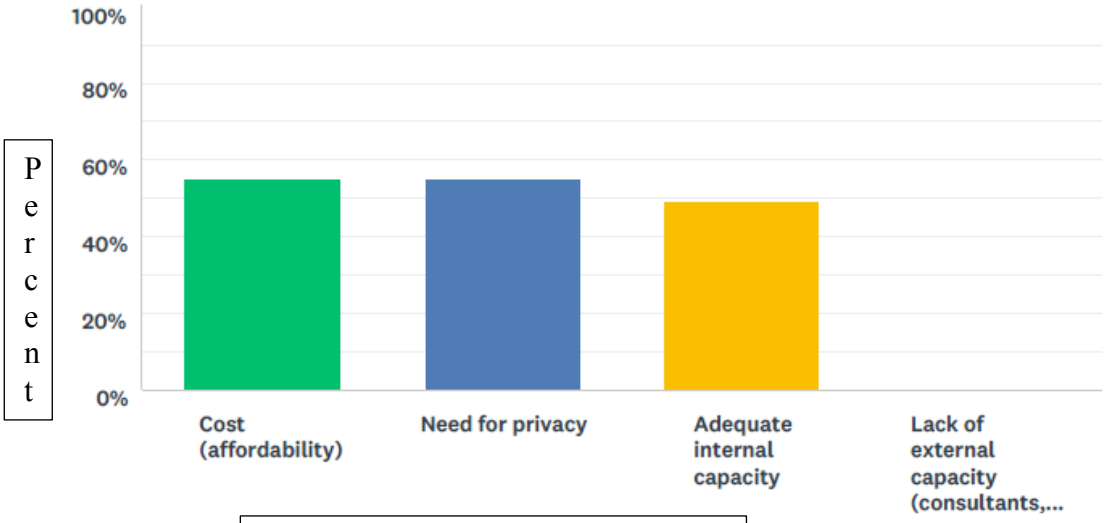
Table 4.3: Resources used in assessing Cybersecurity preparedness

ANSWER CHOICES	RESPONSES	
Internal resources	26.53%	13
External resources (consultancy, outsourcing, etc)	12.24%	6
Both internal and external resources	61.22%	30
TOTAL		49

The findings in table 4.3 show that the organisations mainly used both internal and external resources in assessing Cybersecurity preparedness with a few exclusively using internal and external resources.

4.3.4 Reasons for Use of Internal Resources

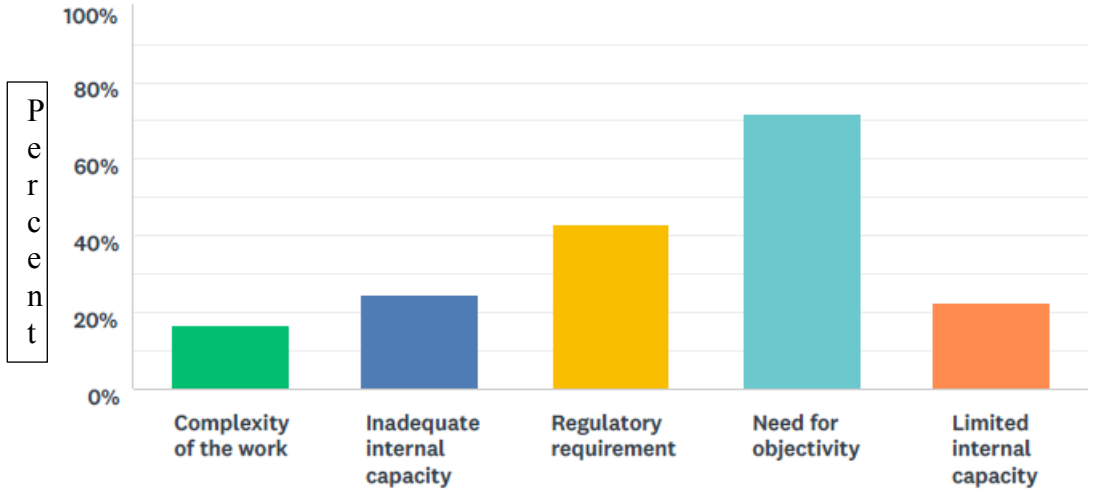
Figure 4.7: Reasons for use of internal resources



The study sought to determine the reasons the organizations used internal resources in assessing Cybersecurity preparedness and found out that the main reasons were cost, need for privacy and adequate internal capacity.

4.3.5 Reasons for Use of External Resources

Figure 4.8: Reasons for use of external resources

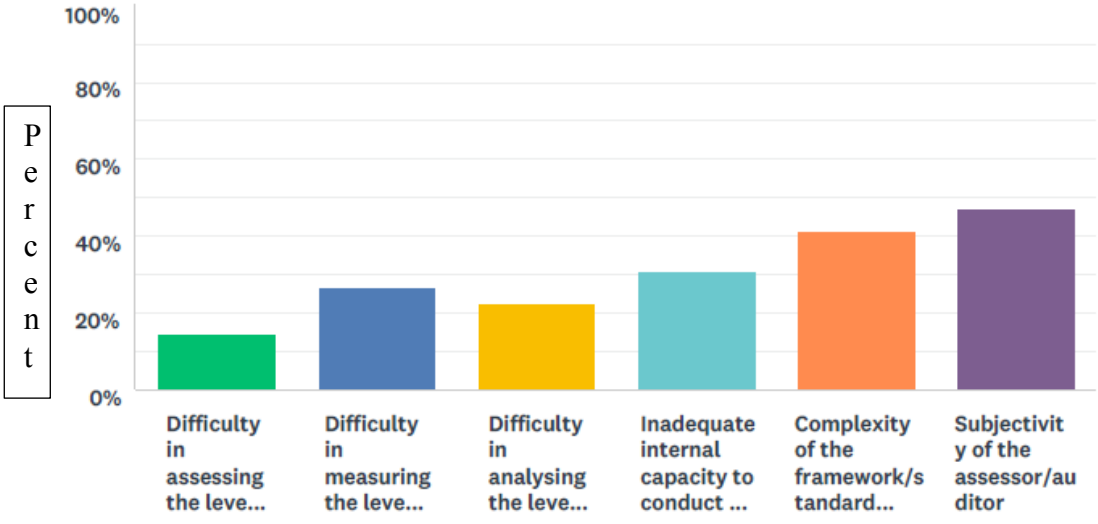


Reasons for use of external resources

The findings in figure 4.8 indicate that the organisations used external resources because of the need for objectivity. The other reasons inlcuded, regulatory requirements, inadequate internal capacity, complexity of the work and limited internal capacity.

4.3.6 The Challenges with the Current System of Cybersecurity Readiness Assessment

Figure 4.9: The Challenges With The Current System Of Cybersecurity Readiness Assessment



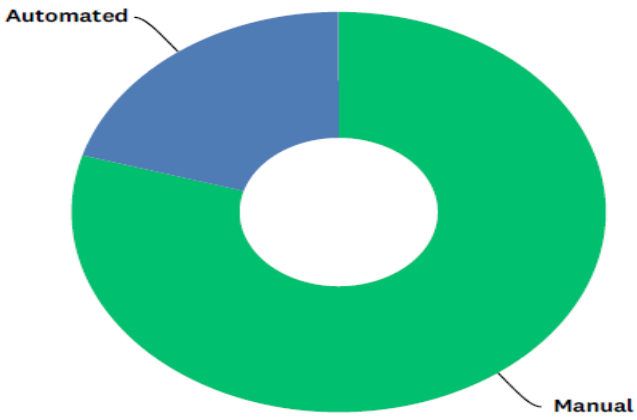
The challenges with the current system of cybersecurity

The study sought to determine the challenges with the current system of cybersecurity readiness assesment. The findings in Figure 4.9 indicate that the organisations faced some challenged with their current system of cybersecurity readiness assessment. The main ones were the subjectivity of the asseossor/auditor and the complexity of the frameworks/standards. The minor challenges were difficulty in assesing the level of preparedness due to ambiguity of the tool, difficulty in measuring the level of preparedness due to ambiguity of the tool, difficulty in analysing the level of preparedness due to ambiguity of the tool and inadequate internal capacity to conduct the assessment.

4.4 Level of Automation of the Assessment of Cybersecurity Preparedness

4.4.1 Manual versus automated ways of measuring Cybersecurity readiness assessment

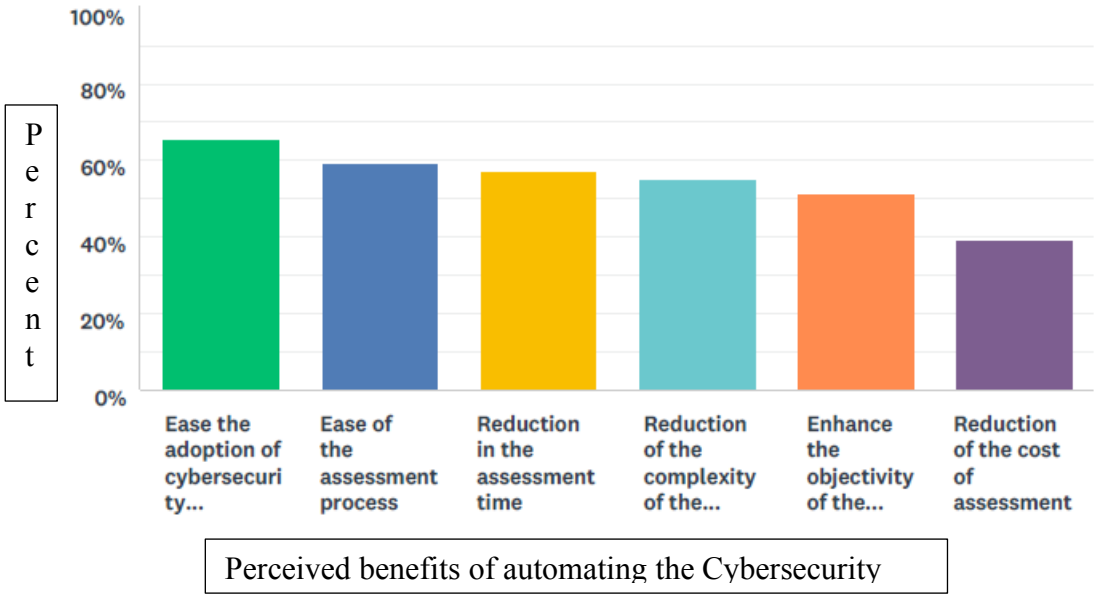
Figure 4.10: Manual versus automated ways of measuring Cybersecurity readiness assessment



The study sought to find out if the organisations did manual or automated ways of measuring Cybersecurity readiness assessment. The findings in Figure 4.10 indicate that most of the organizations have a manual or automated mechanism for measuring its level of cybersecurity preparedness.

4.4.2 Perceived Benefits of Automating The Cybersecurity Readiness Assessment

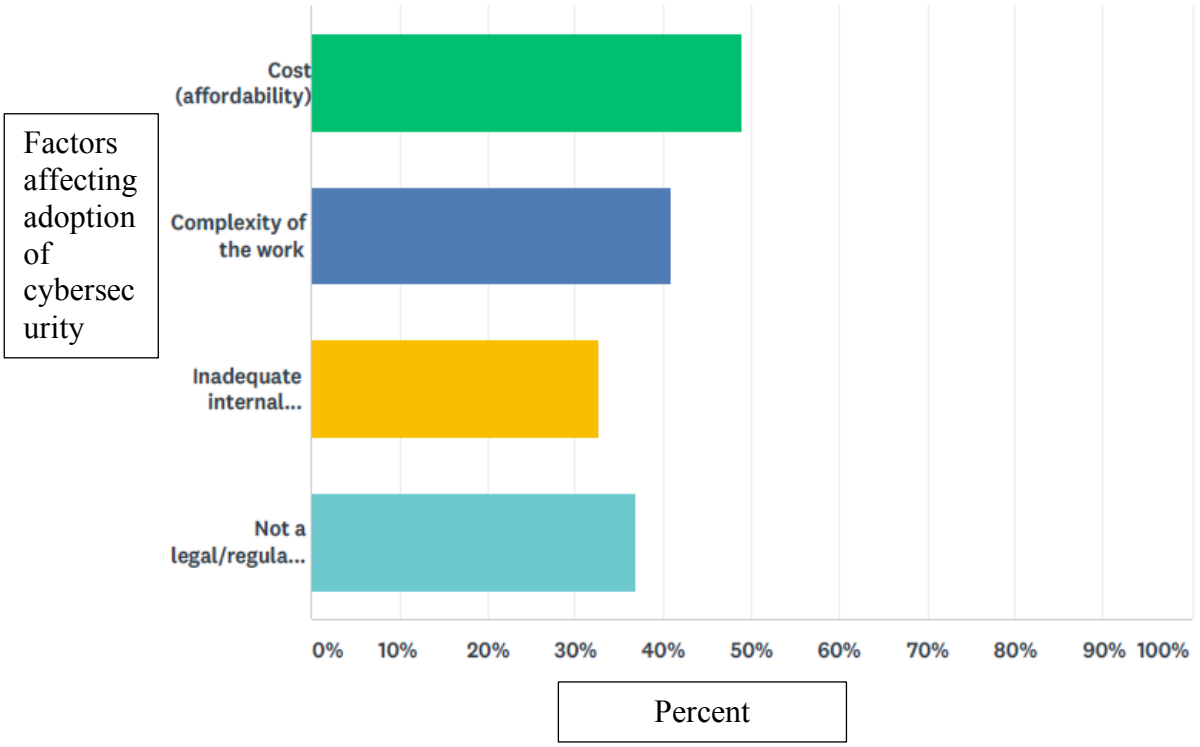
Figure 4.11: Perceived benefits of automating the Cybersecurity readiness assessment



The study sought to find out the perceived benefits of automating the Cybersecurity readiness assessment in the organisations. The findings in Figure 4.11 indicate that the main benefits of an automated mechanism for assessing an organization's cybersecurity preparedness in the organisations were easing the adoption of cybersecurity frameworks or standards, easing of the assessment process, reduction in the assessment time, reduction of the complexity of the process and enhancing the objectivity of the assessment process. The other benefit was the reduction of the cost of assessment.

4.5 Factors affecting adoption of cybersecurity framework or standard

Figure 4.12: Factors affecting adoption of cybersecurity framework or standard



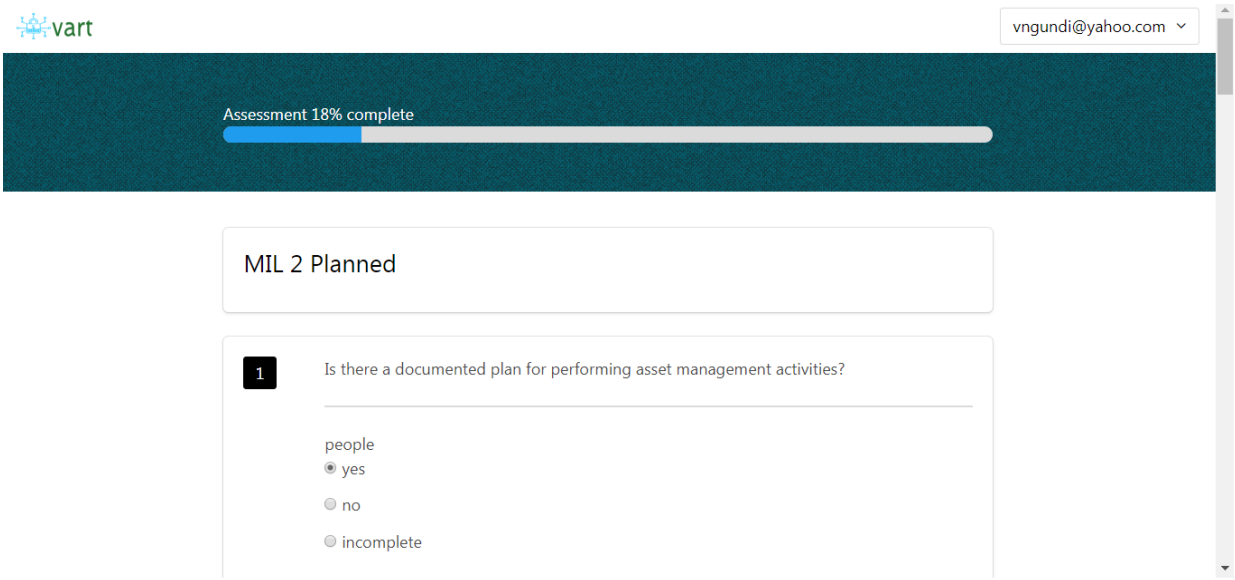
The study sought to determine the factors affecting adoption of cybersecurity framework or standard in the organisations. The findings in Figure 4.12 indicate that the main factor affecting the adoption of a cybersecurity framework or standard in the organisations was the cost (affordadbility) with the other factors being complexity of the work, inadequate internal capacity, the fact that it was not a legal/regulatory requirement

4.6 The VART Prototype

The VART was developed to squarely deal with objectives (iv) of this study, that is, to design and implement a simple toolkit for cyber security assessment.

4.6.1 The User Interface (UI)

Figure 4.13: The User Interface (UI)



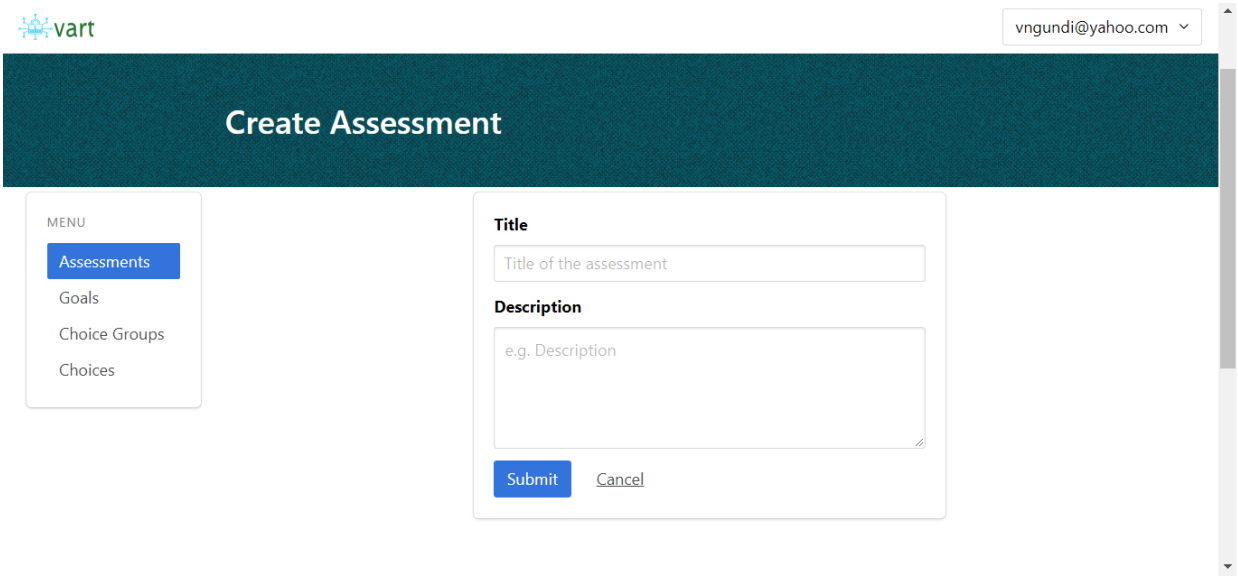
The User Interface (UI) for the prototype allowed the user to perform the following key functionalities activities among other things;

- Entry of Cybersecurity domains, goals and practices
- Easy management of the various cybersecurity assessment elements.
- Self-assessment of the current cyber security situation

4.6.2 Database/Storage

The VART toolkit is purely databases driven. The aspect of cybersecurity domains, goals and practices were all captured in the database by a user with administrative privileges.

Figure 4.14: A Form for Capturing Domains into the Local Database



4.6.3 Logical Operations

The logical operations included in the coding were used in scoring according to a pre-configured scoring rubric as indicated below. The scoring rubric is a three stage process involving:

Step 1: Score the Practice Performances per Domain

Each practice in a domain is scored as follows:

- *Performed* when the question is answered with a "Yes" (green)
- *Not performed* when a question is answered with an "Incomplete" (yellow) or "No" (red) or "Not Answered" (grey)
- If "Not Answered" (grey) is shown, the question was left blank and is scored the same as a "No"

Step 2: Score the Goal Achievement per Domain

Each goal within the domain is then scored as the following:

- Achieved when all practices are performed (green)
- Partially achieved when some practices are performed (yellow)
- Not achieved when no practices are performed (red)

Step 3: Score the Maturity Indicator Level per Domain

Each domain is assigned a MIL based on the following:

- MIL0 if only some of the goals are achieved
- MIL1 if all of the goals are achieved
- MIL2 if MIL1 is achieved and all of the MIL2 questions are answered Yes
- MIL3 if MIL2 is achieved and all of the MIL3 questions are answered Yes
- MIL4 if MIL3 is achieved and all of the MIL4 questions are answered Yes
- MIL5 if MIL4 is achieved and all of the MIL5 questions are answered Yes

4.6.4 Reporting and Reports Capabilities

Figure 4.15: Results Landing Page

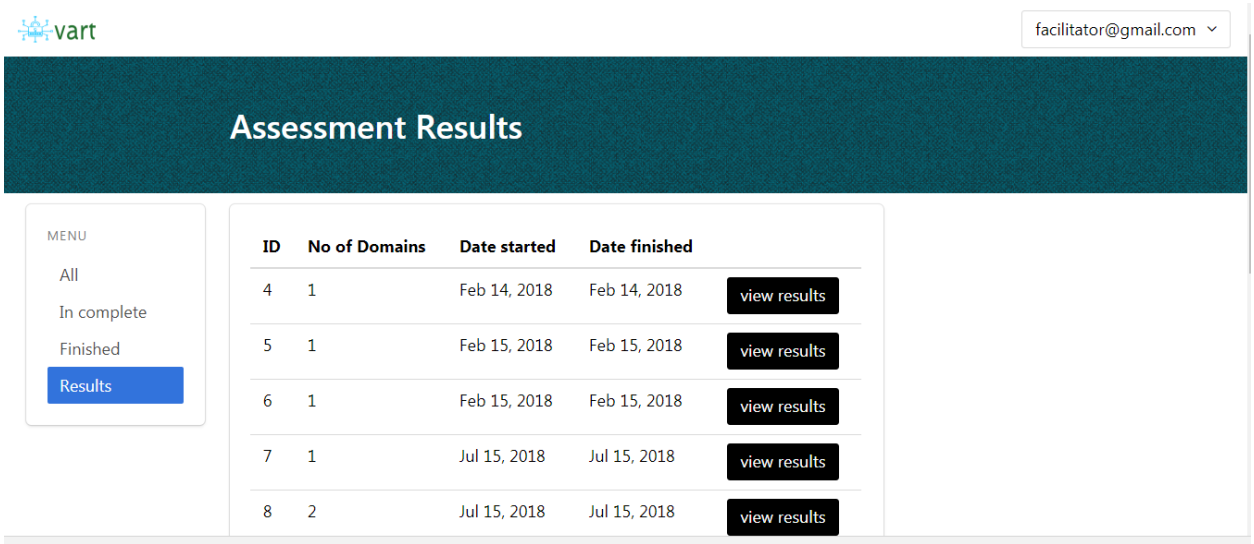
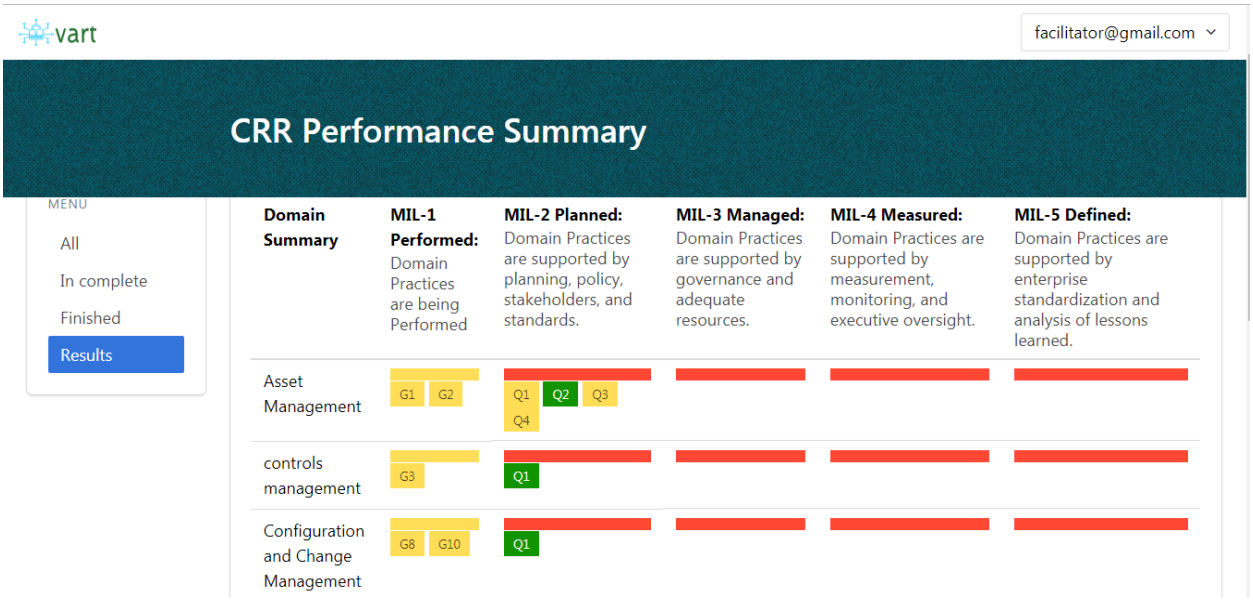


Figure 4.16: The VART Reports Interface



The VART prototype provided a reporting provision which could allow a user to get various reports on a given search criteria. The application also keeps history of the assessments so that it can be easier for a manager to track the performance over a period of time.

4.7 The Proposed System Vs Other Systems

The key difference between our VART and other systems is that this is a low-cost system and does not require any specialized training. Therefore, the VART can be used for self-assessment by any person in management without necessarily having an ICT background.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

From the analysis and data collected, the following discussions, conclusion and recommendations were made. The conclusions and recommendations were made with respect to the objectives set in the study.

5.2 Conclusions

The study confirmed the need for an automated proactive cybersecurity capability self-assessment toolkit. With respect to the objective on investigating how organizations determine or assess their level of preparedness against cyber security threats, it was established that while most organizations do have a mechanism, a large majority of them were done manually. It was further established that most organizations avoid using external consultants to conduct cybersecurity capability assessments mainly due to the related costs and the need for privacy.

On the objective of determining the frameworks available for Cyber security readiness assessment, the study established that the most common framework in use by Kenyan organisations are ISO 27001, NIST, ITIL, COBIT and PCI DSS. On the objective of determining which of these frameworks are utilized and reasons for their utilization or lack of it among key business organizations in Kenya, the study established that some of the challenges in adoption included difficulty in assessing, measuring and analyzing the level of capability or preparedness. A large majority of the organizations also indicated that they use a manual system of assessment and that an automated system would be important in assessing their organization's cybersecurity preparedness especially because it would ease the adoption of cybersecurity capability assessment frameworks; ease the

complexity of assessment and the time it takes to conduct such; enhance the objectivity of the assessment process and reduce related costs.

One outcome of the study is the need for an automated cyber security preparedness assessment toolkit. This is in relation to the objectives of designing and implementing a simple toolkit for cyber security assessment, and demonstrating the effectiveness of proactive self-assessment using the developed toolkit. The automated cyber security preparedness assessment toolkit will significantly reduce the costs of assessment as it is a tool mainly meant for proactive self-assessment using facilitators that are internal to the organization. This is particularly useful for Small and Medium Enterprises (SME's) which form a majority of Kenyan enterprises.

Having an internal self-assessment tool will also address the need for privacy. The automated toolkit will also ease the difficulty in assessing, measuring and analyzing the level of capability or preparedness, while enhancing the objectivity of the assessment process and reduce related costs. The cyber security preparedness assessment toolkit may also go a long way in enhancing organizational planning by facilitating the creation of an action plan for addressing weaknesses and leveraging strengths identified in the assessment. The toolkit may also be used to enhance resource optimization through the performance summary which may give some initial insights into where to invest in cybersecurity improvements. Indeed, the toolkit may contribute to overall organizational process improvement given the toolkit provides an organization with information on its current level of cybersecurity capabilities as a baseline for initiating a data-driven process improvement.

5.3 Recommendations

Based on the findings and the results of the study, the following were the recommendations of the study:

(i) Further development of the cyber security preparedness assessment toolkit to enhance its reporting mechanism, in particular to automate the identification of gaps between Goals and between Maturity Indicator Levels (MILs).

(ii) The cyber security preparedness assessment toolkit is modelled around the CERT Resilience Management Model and NIST Cybersecurity Framework. Further developed should incorporate other frameworks, especially those used by Kenyan enterprises, including ISO 27001, ITIL, COBIT and PCI DSS.

(iii) The cyber security preparedness assessment toolkit should be further enhanced to include the capability of comparing the maturity of an organization across cybersecurity capability assessment frameworks.

REFERENCES

Aho, J. & Nevala, J. (2016). *Keskisuomalaisten yritysten kyberturvallisuus. Jyväskylä.*. Principal Regional Council of Central Finland and Jyväskylänkoulutuskuntayhtymä. Retrieved from http://edu360.fi/wpcontent/uploads/2016/08/Yrityspuolen_kybertutkimus-FINAL-20160829

Amanatullah, Y., Ipung H.P., Juliandri A, & Lim C. (2013). Toward cloud computing reference architecture: Cloud service management perspective. *Jakarta*, 1-4, 13-14.

Apache Software Foundation. (2016). *MapReduce Tutorial*. Retrieved from: https://hadoop.apache.org/docs/stable/hadoop-mapreduceclient/hadoop-mapreduce-clientcore/MapReduceTutorial.

Arief M. D. & Gultom, A. (2005). *Cyber Law*: Information and Technology Law Aspects, Bandung, Refika Aditama.

Barwise, M. (2010). *What is an internet worm*?. BBC.

Bethencourt, J., Sahai, A. & Waters, B. (2007). *Ciphertext-policy attribute based encryption*, in S&P.

Boateng, R., & Olumide, L. (2011). Sakawa- Cybercrime and Criminality in Ghana. *Journal of Information Technology Impact,* 11(2), 85-100.

Booz A. H. (2011). *Cyber Operations Maturity Framework*: A Model for Collaborative, Dynamic Cybersecurity. Booz Allen Hamilton Inc

Boyd, K & Crawford, B (2012). Critical Questions for Big Data in Information, *Communication & Society*, 15: 662-675.

Callegati, F., Cerroni, W. & Ramilli, M. (2009). I*EEE Xplore - Man-in-the-Middle Attack to the HTTPS Protocol.* ieeexplore.ieee.org: 78–81.

Christensson, P. (2006). *Malware Definition*. Retrieved from https://techterms.com

Christensson, P. (2016). *Social Engineering Definition*. Retrieved from https://techterms.com.

Christensson, P. (2017). *Ransomware Definition*. Retrieved from https://techterms.com.

Cloud Security Alliance (2013). *Expanded Top Ten Big Data Security and Privacy challenges.* A Cloud Security Alliance Collaborative research.

COBIT (2011). *Information System Audit and Control Association* (ISACA), Retrieved from: http://www.isaca.org.

Coulouris, P., Dollimore, N. & Kindberg, L. (2011). System Models. In: M. Horton, M. Hirsh & M. Goldenstein, eds. *Distributed Systems, Concepts and Design.* Boston: Addison Wesley, 48-56.

Department of Economic and Social Affairs, (2011). *Cybersecurity*: A global issue demanding a global approach, http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html, posted

Elliott, A, & Knight, S. (2010) *Role explosion: acknowledging the problem*. In: International conference on software engineering research and practice. Retrieved from http://knight.segfaults.net/papers/20100502%20-%20Aaron%20Elliott%20-%20WOLRDCOMP%202010%20Paper

Executive Order 13636, (2013). *Improving Critical Infrastructure Cybersecurity*, US Federal Register. Retrieved form https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.

Fisher, R. L. (2009). Who is a teacher educator? In C.L. Klecka, S.J. Odell, W.R. Houston, & R.H. McBee (Eds.), *Visions for teacher educators: Perspectives on the association of teacher educators' standards* (29-44). Maryland: Rowman & Littlefield Education.

GCSCC (2014). *Cybersecurity Capability Maturity Model*. The Global Cyber Security Capacity Centre (GCSCC). Retrieved from https://www.sbs.ox.ac.uk/cybersecuritycapacity/system/files/CMM%20Version%.

Geers, K. (2011). *Strategic Cyber Security*. Kenneth Geers.

Goyal, A, Jain, O. Pandey, & Sahai, A (2008). *Bounded ciphertext policy attribute based encryption*, in ICALP.

Goyal, V, . O. Pandey, A. Sahai, & Waters,B (2006). *Attribute-based encryption for fine-grained access control of encrypted data*, in CCS.

Greitzer, F. L., & Frincke D. A., (2010). *Combining Traditional Cyber Security audit Data with Psychosocial Data:* Towards Predicyive Modeling for Insider Threat Mitigation. in Probst Christian W., et.al. Insider Threats in Cyber Security, New York, Springer, 85-86.

Hesterman (2014) *CRCnetBASE.* [Online] Available at: http://www.crcnetbase.com/isbn/978-1-4822-4421-

Hirsjärvi S., Remes P. & Sajavaara P. (2010). *Tutki ja kirjoita*. Helsinki: Tammi.

HLEG. (2008). *Report of the Chairman of High-Level Experts Group*. High-Level Experts Group. Retrieved from http://www.itu.int/en/action/cybersecurity/Documents/gcachairman-report.

IBM X-Force Research. (2015). *Cyber Security Intelligence Index*. IBM Corporation. Retrieved From http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03073usen/SEW03073USEN.

ITU. (2014a). *Global Cybersecurity Index* 2014. International Telecommunication Union. Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.

Jamwal, D. (2010). Analysis of Software Development Models. *International Journal of Computer Science and Technology[IJCST],* I(2), 61-64.

Joint Task Force Transformation Initiative (2013). *Guide for Applying the Risk Management Framework to Federal Information Systems*: A Security Life Cycle Approach, NIST (updated 6/5/140 – https://csrc.nist.gov/publications/detail/sp/800-37/rev-1.

Katal, A.,Wazid M, & Goudar R.H. (2013). Big data: Issues, challenges, tools and Good practices. *Noida*: 2013, pp. 404–409.

Kauppinen, T., & Kivikoski, J. (2016). *Tutkimus suomalasten PK-yritysten digitaalisuudesta ja tietoturvasta*. Helsinki. Sep 2016. Principal Elisa Oyj and Yrittäjäsanomat. Retrieved from http://hub.elisa.fi/download/9327

Klumpp, T., (2013). *File Sharing, Network Architecture, and Copyright Enforcement-An Overview*, Edmonton: University of Alberta ,

Kothari, B. (2004). *Research Methodology:Methods and Techniques.* 2nd ed. New Delhi: New Age International (P) Ltd.

Kumar, N., Zadgaonkar, A. S. & Shukla, A., (2013). Evolving a New Software Development Life Cycle Model SDLC-2013 with Client Satisfaction. *International Journal of Soft Computing and Engineering [IJSCE],* III(1), 216-221.

Li FH, Wang W, Ma JF, & Liang XY. (2008) Action-based access control model and administration of actions. Acta Electronica Sinica, 36(10), 1881–1890.

Linning, S., (2014). *MailOnline.* [Online] Retrieved from: http://www.dailymail.co.uk/news/article

Lior A. O. (2011). *Security Issues in NoSQL Databases*. International Joint Conference of IEEE TrustCom-11/IEEE ICESS 11/FCST-11, 2011

Madhusudhan R. N., & Nagaraju, C., A. A., (2017). Protecting Privacy of Big Data in presence of untrusted Mapper and Reducer, *Indian Journal of Computer science & Engineering*, 8(3), 201- 209.

McDaniel, P. (2011) Data Provenance and Security. *IEEE Security & Privacy*. 9(2).

McKinsey Company. (2014). *Risk and responsibility in a hyper connected world*. World Economic Forum and McKinsey & Company. Retrieved from http://www.mckinsey.com.

Ministry of Information and Communications Technology, (2013). *The Kenya National ICT Master Plan 2014-2017-Towards a Smarter Kenya,* Nairobi: Ministry of Information and Communications Technology.

Nguyen, H. & Vai, M., (2010). RAPID Prototyping Technology. *Lincoln Laboratory Journal,* XVIII(2), 17-27.

NIST SP 800-30 (2018). *Risk management guide for information technology systems*, Review. 1, Retrieved from: http://www.nist.gov

Nykodym, N., Taylor, R. & Vilela, J. (2005). Criminal profiling and insider cyber-crime. *Computer Law & Security Report*, 408-414.

Padhy, R. P. Patra M. R. & Satapathy, S. C. (2011). RDBMS to NoSQL: Reviewing Some Next Generation Non-Relational Database's, *International Journal of Advanced Engineering Sciences and Technologies*, 11(1015), 15 – 30.

Ponemon Institute (2013). *Live Threat Intelligence. Impact Report conducted*. Ponemon Institute LLC.

Priya P. S. & Chandrakant P. N. (2014). Securing Big Data Hadoop: A Review of Security Issues, Threats and Solution. *International Journal of Computer Science and Information Technology*, 5 (2), 1-6.

PwC & Iron Mountain. (2012). *Beyond Cyber Threats: Europe's First Information Risk Maturity Index.* PricewaterhouseCoopers LLP. Retrieved from http://www.continuitycentral.com.

Ramzan, Z. (2010). *Phishing attacks and countermeasures*. In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security. Springer.

Stouffer, P. (2017). NISTIR 8183: Cybersecurity Framework Manufacturing Profile," National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/

Such, J.M. Vidler, J., Seabrook, T. & Rashid, A. (2015). *Cyber Security Controls Effectiveness*: A Qualitative Assessment of Cyber Essentials. Technical Report SCC-2015-02, Security Lancaster, Lancaster University, 2015.

Suihkonen, R. (2016). *Tuhoa rakkauskirjeet, äläkä usko joka soittajaa. Keskisuomalainen Oyj.* Retrieved from http://www.ksml.fi/arkisto

Sunderland, D. & Trompeter, G.M. (2017) Multinational Group Audits: Problems Faced in Practice and Opportunities for Research. AUDITING: *A Journal of Practice & Theory:* 36(3), 159-183

Tomlin M., (2015). *Advancing Small Business Cyber Maturity: An application of the NIST Cybersecurity Framework.* Master's thesis, Royal Holloway, University of London.

Toor, S. Z., (2010). Managing Applications and Data in Distributed Computing Infrastructures. *Department of Information Technology, Uppsala University, Sweden,* 1404-5117, 1-41.

Tutorialspoint(2017).*Tutorialspoint.com.*[Online]Availableat:https://www.tutorialspoint.com/software_architecture_design/distributed_architecture.htm.

TutorialsPoint(I)Pvt.Ltd,(2016).*www.tutorialspoint.com*[Online]Availableat:https://www.google.com/search?sitesearch=www.tutorialspoint.com

Vincentas, J (2013). *Trojan Horse in SpyWareLoop.com.* Spyware Loop.

Walia, E. S. & Gill, E. S. K., (2014). A Framework for Web Based Student Record Management System using PHP. *International Journal of Computer Science and Mobile Computing,* III(8), 24-33.

APPENDICES

Appendix A: Questionnaire Form

Survey on Organizational Cybersecurity Readiness Assessment

Dear Respondent:

This questionnaire aims at assessing how organizations determine or assess their level of preparedness against cyber security threats and to further determine the frameworks available for cyber security readiness assessment, which of these frameworks are utilized, and reasons for their utilization or lack of it among key business organizations in Kenya. This survey is strictly for academic purposes and will not be shared with any third party. Responding to the questionnaire is voluntary and the responses will be kept strictly confidential. To further protect your opinions and enhance anonymity, you will not be required to fill your name on the questionnaire.

Background of the Topic

There has been an exponential growth in adoption of computer technology to reap benefits presented by ICTs. However, cyber security threats are on the rise and threaten to erode these gains. There is therefore need for organizations to defend themselves against these threats and thus the need for a mechanism for organization to assess their level of cybersecurity preparedness.

The survey consists of four sections as follows:

Part-A: Employee Profile

This section aims at understanding the employee's role at the organization, general demographics and departmental composition.

Part-B: Assessment of Organizational Cybersecurity Preparedness

The aim of this section is to understand how an organization conducts assessment of its cybersecurity preparedness, identifying any challenges.

Part-C: Level of Automation of the Assessment of Cybersecurity Preparedness

The section aims at determining whether an organization employs a manual or automated system of assessing its cybersecurity preparedness.

Part-D: Adoption of Cybersecurity Frameworks/Standards

This section aims at establishing whether an organization has adopted any cybersecurity framework or standard.

Instructions: Please indicate your response to the following questions by marking the appropriate option(s).

Part-A: Employee Profile

1. Gender
    - ○ Male
    - ○ Female
2. Age
    - ○ 20-30
    - ○ 31-40
    - ○ 41-50
    - ○ Above 50
3. Your role:
    - ○ CISO
    - ○ CIO
    - ○ Director
    - ○ Information Security Manager
    - ○ IT Manager
    - ○ Information Security Officer
    - ○ IT Officer
    - ○ Audit Manager
    - ○ Risk Manager
    - ○ CEO

4. Approximate number of employees in the organization:
    - ○ 0-10
    - ○ 11-20
    - ○ 21-30
    - ○ 31-40
    - ○ Above 40
5. Average age group of the employees:
    - ○ 20-30
    - ○ 31-40
    - ○ 41-50
    - ○ Above 50
6. To which managerial level do you belong?
    - ○ Entry level
    - ○ Junior level
    - ○ Middle level
    - ○ Senior Management level

Part-B: Assessment of Organizational Cybersecurity Preparedness

7. Has your organization adopted any mechanism for measuring its cybersecurity preparedness (framework or standard or other methodology)?
    - ○ Yes
    - ○ No
8. If Yes, which framework or standard? (you can select multiple responses)
    - ☐ NIST

- ☐ ISO 27000
- ☐ PCI DSS
- ☐ COBIT
- ☐ ITIL
- ☐ No particular standard (in-house/internally developed cybersecurity assessment methodology)

9. Does your organization routinely assess its level of cybersecurity preparedness?
   - ○ Yes
   - ○ No
10. If yes, what is the frequency of your organization's cybersecurity assessments?
   - ○ Daily
   - ○ Weekly
   - ○ Monthly
   - ○ Quarterly
   - ○ Yearly
   - ○ Adhoc
11. Does your organization use internal and/or external resources to assess its level of cybersecurity preparedness?
   - ○ Internal resources
   - ○ External resources (consultancy, outsourcing, etc)
   - ○ Both internal and external resources
12. What would best describe the reasons for your organization's use of internal resources in assessing its cybersecurity preparedness? *(you can select multiple responses)*

- ☐ Cost (affordability)
- ☐ Need for privacy
- ☐ Adequate internal capacity
- ☐ Lack of external capacity (consultants, etc)

13. What would best describe the reasons for your organization's use of external resources in assessing its cybersecurity preparedness? *(you can select multiple responses)*
    - ☐ Complexity of the work
    - ☐ Inadequate internal capacity
    - ☐ Regulatory requirement
    - ☐ Need for objectivity
    - ☐ Limited internal capacity
14. What best describes the challenges with the current system of cybersecurity assessment in your organization? *(you can select multiple responses)*
    - ☐ Difficulty in assessing the level of preparedness due to ambiguity of the tool
    - ☐ Difficulty in measuring the level of preparedness due to ambiguity of the tool
    - ☐ Difficulty in analysing the level of preparedness due to ambiguity of the tool
    - ☐ Inadequate internal capacity to conduct the assessment
    - ☐ Complexity of the framework/standard your organization has adopted (NIST, ISO 27001, PCI DSS, COBIT, ITIL, etc)
    - ☐ Subjectivity of the assessor/auditor

Part C: Level of Automation of the Assessment of Cybersecurity Preparedness

15. Does your organization have a manual or automated mechanism for measuring its level of cybersecurity preparedness?
    - ○ Manual

- ○ Automated

16. If automated, please describe your system for accessing cybersecurity assessment?

……

……

……

17. Do you think having an automated system would be useful/important in the assessment of an organization's level of cybersecurity preparedness?

- ○ Yes
- ○ No

18. What would you best consider the benefits of an automated mechanism for assessing an organization's cybersecurity preparedness? *(you can select multiple responses)*

- ☐ Ease the adoption of cybersecurity frameworks or standards
- ☐ Ease of the assessment process
- ☐ Reduction in the assessment time
- ☐ Reduction of the complexity of the process
- ☐ Enhance the objectivity of the assessment process
- ☐ Reduction of the cost of assessment

Part-D: Adoption of Cybersecurity Frameworks/Standards

19. What best describes why your organization hasn't/wouldn't adopt a cybersecurity framework or standard? *(you can select multiple responses)*

- ☐ Cost (affordability)
- ☐ Complexity of the work
- ☐ Inadequate internal capacity
- ☐ Not a legal/regulatory requirement

20. Do you think the adoption of a cybersecurity framework or standard would contribute to improving the level of your organization's cybersecurity preparedness?

    - ○ Yes
    - ○ No

Thank you for completing the survey!