UNIVERSITY OF NAIROBI

School of Computing and Informatics

PROJECT REPORT

A CYBERSECURITY MATURITY MODEL AND TOOLKIT FOR SELF-ASSESSMENT

DERICK ONYANGO OUMA

REG. NO.: P53/31555/2019

SUPERVISOR: DR. ANDREW M. KAHONGE

A research project report submitted to the School of Computing and Informatics in partial fulfilment of the requirements for the award of the Degree of Master of Science in Distributed Computing Technology at the University of Nairobi, Nairobi, Kenya.

AUGUST 2021

DECLARATION

I declare that this document and the research it describes are my original work and that they have not been presented in any other university for academic work.

Name: Derick Onyango Ouma

___ _ ____24 August 2021___

Signature Date (DD/MM/YYYY)

This research project has been submitted as partial fulfilment of the requirements for the award of the Degree of Master of Science in Distributed Computing Technology at the University of Nairobi with my approval as the faculty supervisor.

Supervisor: Dr. Andrew Mwaura Kahonge

24-Aug-2021

_____ _____

Signature Date (DD/MM/YYYY)

DEDICATION

This work is dedicated to my family for the love, encouragement, support, prayers and the work they have put in for my academic journey.

ACKNOWLEDGMENTS

I would like to thank the Almighty God for the strength throughout the research. I wish to thank my supervisor Dr. Kahonge for his guidance and support. My gratitude also goes to all the panelists for their assessments and reviews.

ABSTRACT

Cybersecurity landscape is evolving rapidly, and the threats associated with it are not new to most organizations in Kenya, be it small, medium, or large. With the rise of cyber risks such as high-profile cyber-attacks and data breaches, businesses across all industries have stepped up and are making cybersecurity a top priority and a key objective. Conducting a cyber maturity assessment for an organization provides an assurance to the board of directors, senior management, employees, clients, and any other stakeholder on the ability to protect information assets and its preparedness against cyber threats. With this in place, an organization can identify, assess, prioritize, and mitigate its cybersecurity risks in a timely manner.

This study proposes a framework and a toolkit that is meant to help organizations conduct assessments that is crucial in providing informed overview of the organization's cybersecurity posture and data for cybersecurity-related decisions. The toolkit exists in Microsoft Excel that has been designed to have IT security controls that can be implemented to ensure a sound information security management program by organizations. This has been automated into a prototype that will enable a cloud-based assessment to organizations through a software as a service (SaaS) platform.

TABLE OF CONTENTS

DECLARATION i

DEDICATION ii

ACKNOWLEDGMENTS iii

ABSTRACT iv

TABLE OF CONTENTS v

DEFINITION OF TERMS ix

ABBREVIATION/ACRONYMS x

LIST OF FIGURES xi

LIST OF TABLES xii

CHAPTER ONE: INTRODUCTION AND BACKGROUD INFORMATION 1

1.1 Background 1

1.2 Research problem 1

1.3 Objectives of the study 2

1.3.1 Overall objective 2

1.3.2 Specific objectives 2

1.4 Research questions 3

1.5 Justification of the research 3

1.6 Scope of the research 3

1.7 Assumptions 3

CHAPTER TWO: LITERATURE REVIEW 5

2.1 Essential components of a cybersecurity maturity model 5

2.2 Existing work on maturity models, cybersecurity frameworks and regulatory requirements 5

2.2.1 The CREST Maturity Assessment Model 5

2.2.2 Cybersecurity Capability Maturity Model (C2M2) 6
2.2.3 The NICE Capability Maturity Model (NICE-CMM) 6
2.2.4 CERT Resilience Management Model (CERT-RMM) 6
2.2.5 NIST Cybersecurity Framework (CSF) 6
2.2.6 COBIT Capability Maturity Model 7
2.2.7 Central Bank of Kenya Guidance Note on Cybersecurity 8
2.3 Existing work on cybersecurity maturity assessment tools 8
2.4 Summary of review of literature and identified gap 8
2.5 Proposed solution 9
CHAPTER THREE: METHODOLOGY 10
3.1 Research design 10
3.2 Research site 10
3.3 Target population and sampling 10
3.4 Data collection instruments and techniques 11
3.5 Data analysis 12
3.6 System development methodology 12
3.7 Ethical considerations 13
CHAPTER FOUR: SYSTEM ANALYSIS, SYSTEM DESIGN & IMPLEMENTATION 14
4.1 System analysis 14
4.1.1 Feasibility analysis 14
4.1.1.1 Economic feasibility 14
4.1.1.2 Technical feasibility 14
4.1.1.3 Operational feasibility 14
4.1.1.4 Schedule feasibility 15

4.1.2 Requirement elicitation 15
4.1.2.1 Functional requirements 15
4.1.2.2 Non-Functional Requirements 15
4.1.3 System modelling 16
4.1.3.1 Use case diagrams 16
4.1.3.2 Context diagram 18
4.2 System design 18
4.2.1 Conceptual design 18
4.2.2 Database Design 19
4.2.3 User interface design 20
4.3 System implementation 22
4.3.1 Hardware Resources 22
4.3.2 Software Resources 22
4.3.3 Choice of Programming tools, techniques, and technologies 22
4.3.3.1 Java and Spring framework 22
4.3.3.2 MySQL 23
4.3.3.3 Angular JS 23
4.3.3.4 Docker 23
4.4 System testing 23
4.4.1 Walkthroughs with information security experts 23
4.4.2 Module testing 23
4.4.3 Regression testing 23
4.4.4 Integration testing 23
4.4.5 System testing 24

4.4.6 User acceptance testing 24
4.4.7 Test cases 24
4.4.8 Sample screenshots of the toolkit 25
CHAPTER FIVE: RESULTS AND DISCUSSIONS 31
5.1 Prototype evaluation and results 31
5.1.1 Functional evaluation 31
5.1.2 User testing results 31
5.2 Discussion 32
CHAPTER SIX: CONCLUSION AND RECOMMENDATIONS 36
6.1 Summary of findings 36
6.2 Conclusion 36
6.3 Contributions of the study 37
6.4 Future work 37
REFERENCES 38
APPENDIX 40

DEFINITION OF TERMS

- Information Security – This is the practice of protecting the confidentiality, integrity, and availability of information system data from those with malicious intentions.
- Cyber security – Refers to the body of technologies, processes, and practices designed to protect information assets from attack, damage, or unauthorized access.
- Maturity model – This is a measurement of the ability of an organization for continuous improvement in a particular discipline such as cyber security / information security. Basically, it shows how good an organization, system or a process is.
- Cyber security maturity assessment – Refers to rapid assessment of an organization's readiness to prevent, detect, contain, and respond to cyber threats.
- SANs 20 Critical Security Controls – Refers to a list of controls designed to provide maximum benefits toward improving information security posture against real-world threats.
- NIST Cybersecurity Framework – Is a framework based on existing standards, guidelines, and practices on how organizations can manage and reduce cybersecurity risks.

ABBREVIATION/ACRONYMS

- NIST – National Institute of Standards and Technology
- SANs – SysAdmin, Audit, Network, Security
- CSC – Critical Security Controls
- CIS – Center for Internet Security
- COBIT – Control Objectives for Information and Related Technologies
- CIA – Confidentiality, Integrity, and Availability
- GDPR – General Data Protection Regulation
- ISM – Information security model
- CMA – Cyber Maturity Assessment

LIST OF FIGURES

Figure 1 COBIT 5 Assessment indicators 8
Figure 2 Conceptual framework 9
Figure 3 Research process used in this study. 10
Figure 4 High level study of information security management 11
Figure 5: Iterative development (prototyping) process 13
Figure 6: Service provider and customer super admin use case diagram 17
Figure 7: Customer inputter and reviewer use case diagram 17
Figure 8: Context diagram 18
Figure 9: Conceptual design 19
Figure 10: Database design 20
Figure 11: User interface design – Login screen 21
Figure 12: User interface design – Control procedure execution screen 21
Figure 13 Microsoft Excel Cybersecurity Maturity assessment framework showing overall maturity level of an organization. 25
Figure 14 Sample summary scoring for an individual cybersecurity domain 26
Figure 15 Updating customer risk profile based on the organization's annual risk assessment 26
Figure 16 Control requirements in the toolkit. 27
Figure 17 Prototype subscription portal 27
Figure 18 Service provider portal for administration of the toolkit 28
Figure 19 Customer risk profile 28
Figure 20 Execution of a procedure based on the control requirements 29
Figure 21 Control attributes to ascertain level of implementation for the control requirements 29
Figure 22 Overall cyber maturity score for an assessment 30
Figure 23 User experience results 32
Figure 24 Toolkit content 32
Figure 25 A flowchart showing how the toolkit computes a score for a particular control procedure 34

LIST OF TABLES

Table 1 Content analysis for in-depth interviews and focus groups data 12

Table 2 Sample test case 25

Table 3 End user functional evaluation results 31

Table 4 Defined maturity levels 35

CHAPTER ONE: INTRODUCTION AND BACKGROUD INFORMATION

1.1 Background

Cybersecurity landscape is evolving rapidly, and the threats associated with it are not new to most organizations in Kenya, be it small, medium, or large. With the rise of cyber risks such data breaches and network attacks, businesses across all industries have stepped up and are making cybersecurity a top priority and a key objective. The truth is that the importance of cybersecurity has become an undeniable fact. In their research, Serianu (2018) highlighted key challenges in the cybersecurity space such as lack of solid experience and skills, high renumeration rates for the available professionals, increase in organizational spending in cybersecurity and increase in targeted attacks. They also discussed the fact that the country was facing a shortage of skilled people, but also an even more shortage of software developers who can design secure information systems, write safe programs and create solutions needed to contain cyber threats.

Organizations have critical assets that are exposed to cyber threats which exploit vulnerabilities that in turn affect confidentiality, integrity, and availability of information. Information security has become an essential tool for managing security risks. When implemented properly, it creates confidence and trust leading to the success of the business. Already several cybersecurity maturity models have been developed to mitigate security risks to organizations. KPMG (2015), during the ISACA Kenya Annual Conference-Secure Kenya II, defines cyber maturity assessment as an assessment of the readiness level of an organization to protect itself from cyber threats. There is need to adopt a strategy that should outline the expression of the vision, high-level objectives, guiding policy principles and explicit accepted priorities by an organization in a bid to address specific cybersecurity issues (Silensec, 2016). Businesses already have controls at their disposal to help them keep their systems and network safe. This included information security models or frameworks to provide a way for measuring and communicating the cybersecurity readiness to relevant stakeholders thereby ensuring regulatory compliance, corporate responsibility, and improved brand quality (Wilde, 2014).

Conducting a cyber maturity assessment for an organization will therefore provide an assurance on the preparedness against cybersecurity threats. With this in place, an organization can identify, assess, prioritize, and mitigate its cybersecurity risks in a timely manner. This study proposes a maturity model designed from the existing maturity models, frameworks, information security standards and regulations. It also provides an automation of the model through a prototype that aims at enabling organizations carry out self-assessment of their maturity level and security posture without hiring an expert.

1.2 Research problem

An inadequate assessment of an organization’s cyber maturity level could lead to miscalculated priorities and / or sometimes wasted investments. It is therefore important to be aware of the current security posture and the controls in place (Rabii et al., 2020). Organizations must know

what threats they are exposed to and which assets can be targeted. After all, there are limited funds available for investing in cyber security and thus need to mitigate related risks in a resource efficient manner. To mitigate these the risks, an organization needs to assess their preparedness towards information security management through knowing their cybersecurity maturity level which acts as an indicator of the ability to identify and protect information assets against cyber threats. Basically, they need to be aware of the cyber threat landscape they face and should have clear measurement tool and roadmap to improve their cybersecurity risk assessment.

Conducting cybersecurity maturity assessment has been a problem for many since skilled talent remains a challenge even though there are models which can be used. The existing models as discussed in the literature review may not be easily adopted to cover all critical security controls as well as regulations by governments or regulatory bodies, hence the need for customization. In addition, an expert such as cybersecurity consultant or specialist would still be hired to interpret the models and conduct the assessment. This can be expensive since for the assessment to be effective, it should be made a continuous process in the organization's policy and procedures. For instance, in industries such as banking, financial institutions are compelled to outsource the service from consulting firms i.e., the "Big-four" audit firms. These services mostly come at a cost thus growing the organization's budget. This leads towards the following problem statement:

> *"Organizations face an increasing amount of cyber security risks. They need to be fully aware of the threat landscape they face and should carry out continuous assessments on their maturity level in order to determine security posture and use the assessment as a measurement tool to mitigate cyber treats and have a clear roadmap to improve their cyber security risk assessment, without having to spend a lot on hiring an expert all the time whenever an assessment is to be carried out."*

The aim of this study is to design a cyber maturity toolkit for self-assessment that can be used by organizations in different industries without requiring to hire a human expert or consultant.

1.3 Objectives of the study

1.3.1 Overall objective

The aim of this study is to provide a cyber maturity model and toolkit to aid self-assessment for different industries in Kenya especially banking.

1.3.2 Specific objectives

1. To review and evaluate existing cybersecurity models and frameworks that can be used for maturity level assessment across.
2. To design and develop a model for cybersecurity maturity assessment from the already existing models, security frameworks and other applicable regulations.

3. To examine requirements arising from the designed model and determine how they can be transformed into software modules.
4. To develop a prototype that automates the model through a toolkit for self-assessment.

1.4 Research questions

The research questions included:

1. How can industries in Kenya perform cyber maturity assessments?
2. How can a cyber maturity assessment model based on existing models and information security standards be designed?
3. How can the designed model be automated to aid self-assessment?

1.5 Justification of the research

The adoption of information technology by organizations to drive their business and processes, clearly calls for the need for better management of information security. This is due to the rapid growth of the cyberattack surface. According to the global risks report, cyberattack took the second position as the risk of greatest concern for businesses. The expert network also rated cyberattacks on critical infrastructure as the fifth top risk in 2020 (World Economic Forum, 2020).

In this context, an assessment is crucial to provide an informed overview of the current cybersecurity posture and data for decision making. Any organization should understand their cyber preparedness to ensure that top management does not underestimate cyber threats that can cause massive damage. Hence, determining the maturity level helps in identifying gaps and highlighting key areas of focus. Eventually guiding the organization in developing a road map for mitigation of the identified gaps.

1.6 Scope of the research

The scope was the banking sector in Kenya. This sector was considered since the industry is well regulated by the Central Bank of Kenya (CBK) and data could be easily obtained, hence supported the research effectively. Since financial institutions follow guidelines from the same regulator, the findings and results across different banks were not expected to vary with a big margin.

1.7 Assumptions

The assumptions included:

1. Prevailing operational procedures and systems in place are the same in most of the financial institutions.
2. Information from available cybersecurity frameworks and regulatory requirements on cybersecurity was sufficient to aid designing and developing a maturity model especially for local industries.

3. The requirements arising from the designed cybersecurity model could be transformed into software modules and that the modules can be used to validate against what any information security framework implements.

CHAPTER TWO: LITERATURE REVIEW

Many information security models (ISMs) have been developed in the recent past based on a collection of standards, guidelines and best practices in order to assist organizations in addressing security concerns and to preserve confidentiality, integrity and availability of information assets.

This chapter discusses essential components of an ideal maturity model and some of the notable cybersecurity frameworks and maturity models that have been developed in the recent past and any other related work. It also discusses any automation of the models and/or tools that have been developed for conducting cyber maturity assessments.

2.1 Essential components of a cybersecurity maturity model

Maturity models conform to some structural basics (Butkovic & Caralli, 2013). This is important because the structure would provide the link between objectives and best practices and to also facilitate the relationship between current capabilities and improvement roadmaps. And eventually linking them to business goals, standards, and other criteria.

Essential components that form part of this structure include a) Levels – represents the measurement aspect; b) Model domains – defines the categorization like attributes into an area of importance for the subject matter; c) Attributes – are as characteristics and indicators for control implementation; d) Appraisal and scoring methods – are algorithms for a common standard for measurement. For example, important attributes can be valued over less important ones; e) Improvement roadmaps – improvement efforts that can be explored to address the identified gaps during the assessment. (Butkovic et al., 2013).

2.2 Existing work on maturity models, cybersecurity frameworks and regulatory requirements

There are cyber maturity models that have been developed based on the needs of different organizations. The popular ones are currently incorporated into international standards (Aliyu et al., 2020). Some of the notable models include:

2.2.1 The CREST Maturity Assessment Model

CREST (an international accreditation and certification body that represents and supports the technical information security market) developed tools that could be used to perform maturity level assessments. These tools were presented in a spreadsheet-based manner that could be easily used. The tools include: a) Cyber threat intelligence maturity assessment tool that provides a way to conduct a maturity assessment to determine the level attained by organizations in terms of cyber threat intelligence; b) Cyber security incident response maturity assessment tool that assesses status of an organization's cyber incident response capability; c) Penetration testing maturity assessment tool that helps to assess the status of a penetration testing program for an organization.

The CREST assessment tools defined five maturity levels that included Foundation, Emerging, Established, Dynamic and Optimized (CREST, 2014).

2.2.2 Cybersecurity Capability Maturity Model (C2M2)

C2M2 was devised by the US Department of Energy to evaluate and improve information security in the electricity sector. It provided a framework for improving the cybersecurity posture of organizations of all sizes. It focused on assets in use for information technology and operational technology and the environments in which they operate. This model defined ten domains that had a set of cybersecurity practices. Theses domains included risk management; asset, change, and configuration management; identity and access management; threat and vulnerability management; situational awareness; event and incident response; supply chain and external dependencies management; workforce management; cybersecurity architecture; and cybersecurity program management. It also defined four maturity levels i.e., Maturity Indicator Level 0 (MIL0), Maturity Indicator Level 1 (MIL1) through to MIL3.

2.2.3 The NICE Capability Maturity Model (NICE-CMM)

This model was developed by the National Initiative for Cybersecurity Education (NICE) to assist institutions in applying best practices (US Department of Homeland Security, 2014). NICE-CMM defines three main domains that included a) Process and analytics – process represented activities that were associated with the actual steps an organization would take to carry out workforce planning and how they were integrated with other important processes. Analytics represented activities that were associated with supply and demand data and the use of tools, models, and methods to carry out workforce planning analysis. b) Integrated governance – represented activities that were associated with establishing governance structures, guidance provision and development, and driving decision making. c) Skilled practitioners and enabling technology – skilled practitioners represented activities that were associated with establishing workforce planners. Enabling technology represented activities that were associated with the accessibility and use of data systems. NICE-CMM also defined three maturity levels a) limited, b) progressing and c) optimizing.

2.2.4 CERT Resilience Management Model (CERT-RMM)

This model defined practices for operational resilience, security, and business continuity. It also defined twenty-six process areas categorized into four domains that are engineering, operations, enterprise management and process management.

2.2.5 NIST Cybersecurity Framework (CSF)

The National Institute of Standards and Technology (NIST) developed an information security framework which provided a structure for organizations to review their current cyber risk. It conceptualized cybersecurity as five functions of identify, protect, detect, respond, and recover. NIST framework defined five maturity levels that included initial, repeatable, defined, managed

and optimized. It provided a means for evaluating maturity levels, after which an organization would make informed business decisions about where to make further investment and improvement.

2.2.6 COBIT Capability Maturity Model

Control Objectives for Information and Technology (COBIT) provides best practices for Information Technology management. COBIT assessment model was designed to provide organizations with a methodology for reviewing the capability of Information Technology processes (El, Youssfi, & Boutahar, 2016, p. 2). It defined six levels of maturity that include a) Incomplete – a process that has not been implemented or has failed to achieve the intended purpose; b) Performed – a process that has been implemented and achieves the intended purpose; c) Managed – a process that has results specified and therefore managed; d) Established – a process that has been well defined and used throughout the organization; e) Predictable – a process that is consistently executed within defined limits; f) Optimization – a process that is continuously improved to meet relevant business goals.

The measurement framework of COBIT assesses the level of achievement for a given process based on particular attributes. Some of the attributes a process would have include process performance, performance management, work product management, process definition, process deployment, process measurement, process control, process innovation and continuous optimization.

In the measurement framework, COBIT also defined assessment indicators to determine maturity of a process as shown in figure 1 below. These indicators included generic practice referring to activities of generic type; generic resources referring to the resources that aid in achieving the attributes and generic product referring to the sets of characteristics expected to be evident as a result of achieving an attribute. The indicators are further enhanced by carrying out additional performance reviews based on the indicators.

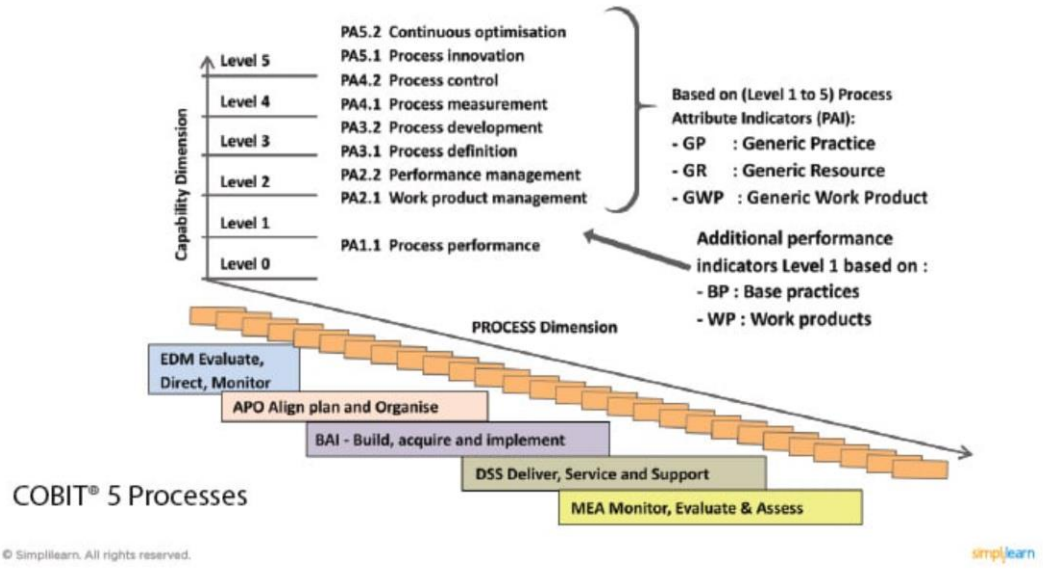


Figure 1 COBIT 5 Assessment indicators

2.2.7 Central Bank of Kenya Guidance Note on Cybersecurity

Central Bank of Kenya under Section 33(4) of the Banking Act, in the Constitution of Kenya issued a guidance note on cybersecurity to be adhered to by financial institutions to maintain stable and efficient banking system. The guidance note set the minimum standards that financial institutions should adopt to develop an effective cybersecurity governance and risk management frameworks.

2.3 Existing work on cybersecurity maturity assessment tools

There are notable automated tools to carry out assessment for maturity levels, be it for cyber security or for IT processes. Some of the tools included a) Self-assessment excel files with separate evaluation sheets that are available for COBIT assessment, NIST framework assessment, CREST assessment and C2M2 assessment; b) COBIT self-assessment tool which is a web-based tool that allows a registered user registered with a paid account to conduct an assessment; and c) iServer for Governance, Risk and Compliance is solution that has to be paid for before an assessment can be performed.

2.4 Summary of review of literature and identified gap

It is evident that there are existing maturity models that have been developed in the recent past. These models can be used or adopted by organizations to carry out maturity assessment. The study also notes that some of these existing models come with toolkits developed in Microsoft Excel to assist in the assessment. However, an expert would still be needed to use the models and the toolkit.

Having the security models in place together with other existing maturity models in other areas such as IT governance, provided sufficient information on designing a cyber maturity assessment model that would ensure a holistic and comprehensive approach to conducting the assessment, ultimately leading to the success of this research.

In addition, the existing frameworks do not outline ways to ensure organizations remain at per with new or recent regulatory requirements that they must comply to. Some of the recent regulations included the General Data Protection Regulation (GDPR) by European Union (BAI, 2018), The Data Protection Act by the Kenyan Government (Kenya Gazette, 2019), and any other regulation that would apply to them.

2.5 Proposed solution

The diagrammatic representation in figure 2 below is a conceptual framework that shows how maturity level (score) for a given organization is computed.

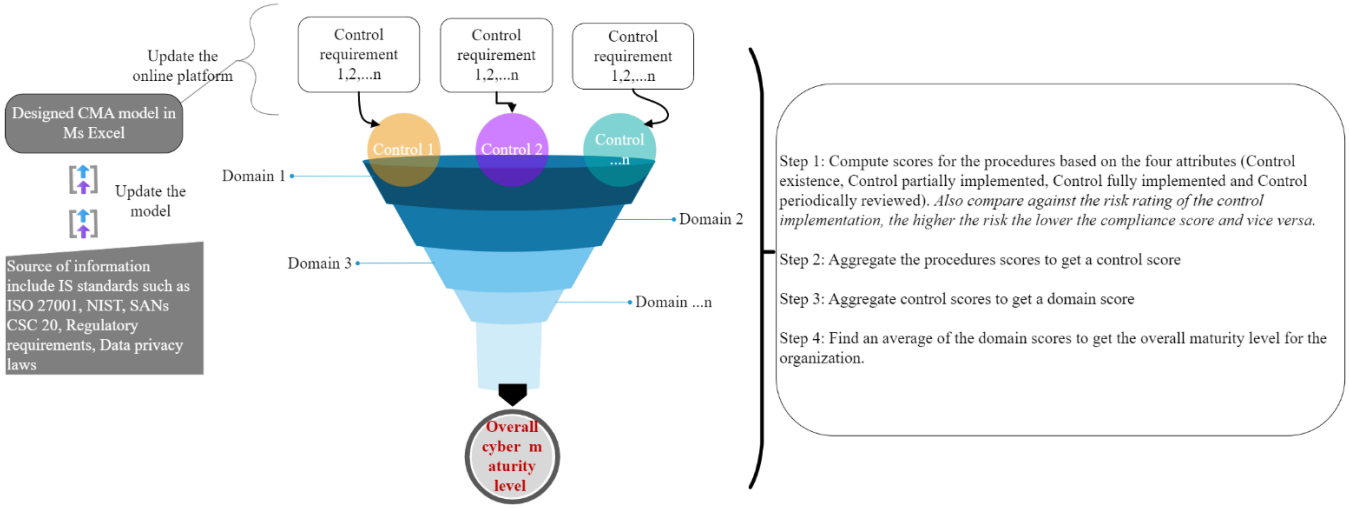


Figure 2 Conceptual framework

The proposed solution consists of the designed framework in Microsoft excel with all applicable IT security control requirements and a prototype to automate it that will be offered as a cloud platform (Software as a service). The service provider will be responsible for frequent update of control requirements in the framework and the system.

CHAPTER THREE: METHODOLOGY

This section describes the research methodology and plans that have been used to achieve the research objectives. Goundar (2019, p. 2) describes a research methodology as a systematic way to solve a problem. Its aim is to give the work plan of a research. This study takes an exploratory research design. According to the Pollfish School, this type of research was used in a problem investigation, in cases where the problem was not clearly defined. It ensures a better understanding of the problem.

3.1 Research design

The open-ended nature of exploratory research enabled alternatives towards gathering information and understanding how organizations especially financial institutions in Kenya manage their cybersecurity programs. This made it possible to further clarify the scope and nature of the problem and in proposing a possible solution. Figure 3 below shows a summary of the approach taken to achieve the objectives for this study.

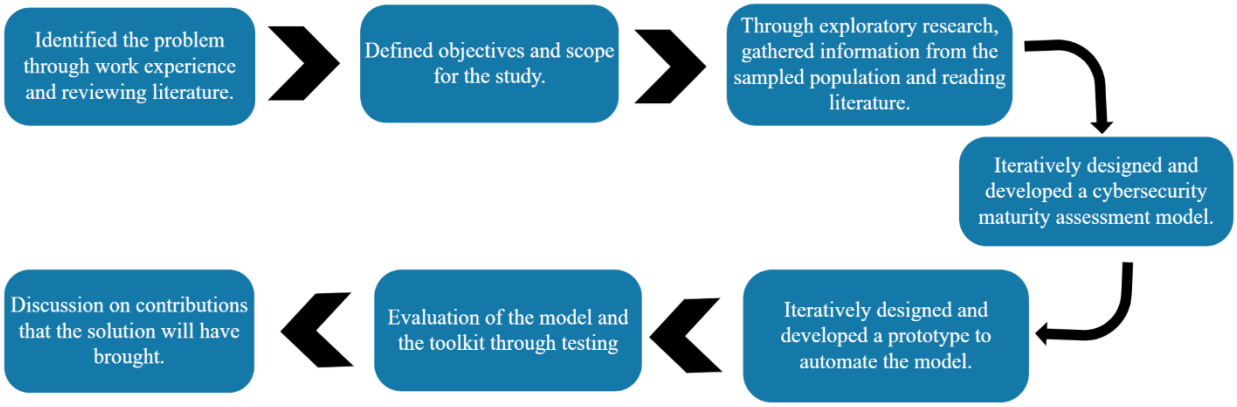


Figure 3 Research process used in this study.

3.2 Research site

This research was a case study of Credit Bank Plc, located in Nairobi County. This facility was chosen, since we had firsthand experience on how the operations were done. The main significance of this site was that the bank operated under the Central Bank of Kenya (CBK) guidelines and management same as the other financial institutions in the country.

3.3 Target population and sampling

The targeted population was all staff members in the banking sector belonging to the functional areas / roles that have a shared responsibility towards management of cybersecurity threats, each playing different roles. According to Central Bank of Kenya guidance note on cybersecurity, payment service providers were required to have a Chief Information Security Officer (CISO), a role that was aimed at creating an organizational culture of shared cybersecurity ownership

(Central Bank of Kenya, 2019, p. 10). The targeted roles included Chief Information Security Officer (CISO), Information Technology (IT) risk, Information Technology (IT) security, Information Communication Technology (ICT), Information Systems Audit – Internal Audit.

Purposeful sampling was used to identify research participants which ensured credibility of the findings (Suri, 2011). It acted as a solution to time, resources, and access to information constraints during the study (Benoot, Hannes, & Bilsen, 2016). Based on the availability of the study sample size, at least one member was selected from each role listed above.

3.4 Data collection instruments and techniques

Data collection is the process of information gathering and measurement based on variables of interest, in a systematic way to answer stated research questions and evaluate the outcome (Kabir, 2016). Kabir also argued that data can be organized into qualitative and quantitative. This study took a qualitative approach to understand information security management and assessments in banks. Figure 4 below is an illustration of how this research was geared towards improving cybersecurity management in organizations by having access to a self-assessment platform where frequent / continuous assessments could be done. This also formed part of the discussions with different respondents.

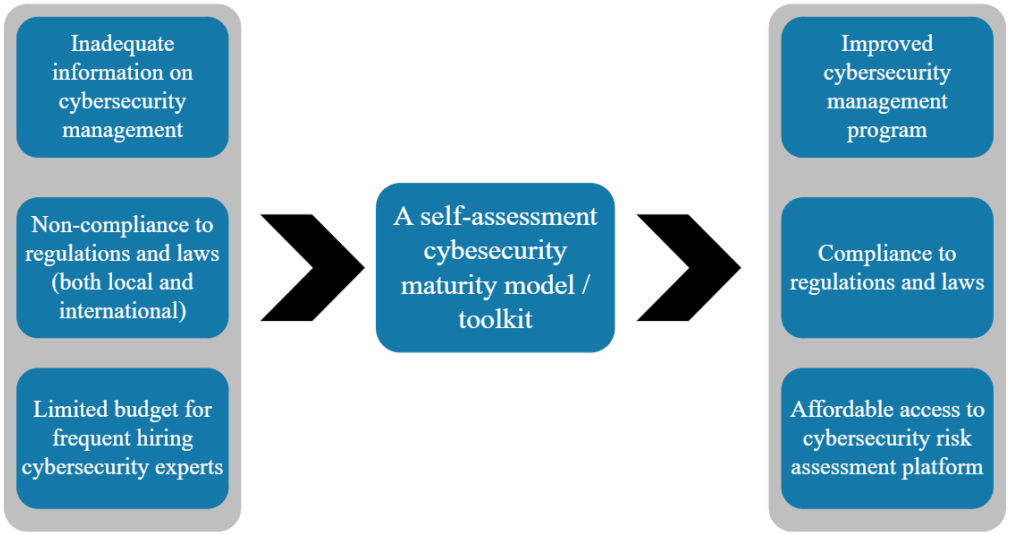


Figure 4 High level study of information security management

Data collection instruments included the use of interviews and focus group discussions. The interview sessions were unstructured and was a direct technique of obtaining insights in which respondents were probed to uncover motivations, beliefs, attitudes, and feelings about information security management. Further to having the interviews, focus group discussions were also held which helped in gathering information on feelings and experiences of the respondents. This aided

analysis, interpretation and arriving at conclusions that informed the development and designing of the cyber maturity assessment model.

3.5 Data analysis

Collected data was qualitative in nature and was analyzed using content analysis to identify common patterns among information security experts. Table 1 below shows a summary of the common patterns that were identified.

Inquiry	**Description**
Knowledge of information security frameworks	Adoption of controls outlined in ISO/IEC 27001
Extent of implementation of the adopted information security framework	None of the respondent could demonstrate 100% implementation of any framework.
Awareness on local and international regulations and laws touching on information security.	Central Bank of Kenya guidance note on cybersecurity, Kenyan data protection law and the European Union data privacy regulations.
Continuous assessment of cybersecurity risks.	Mostly done to comply with the regulator's requirements. However, this was an annual exercise and could not be done more frequently due to budget constraints since cybersecurity experts were limited in the market hence expensive.

Table 1 Content analysis for in-depth interviews and focus groups data

3.6 System development methodology

The prototype to automate the designed model was developed using the iterative development process as shown in figure 5 below. This approach was preferred as it generated the software modules more quickly and more flexible, and that it was easier to test and evaluate the modules.

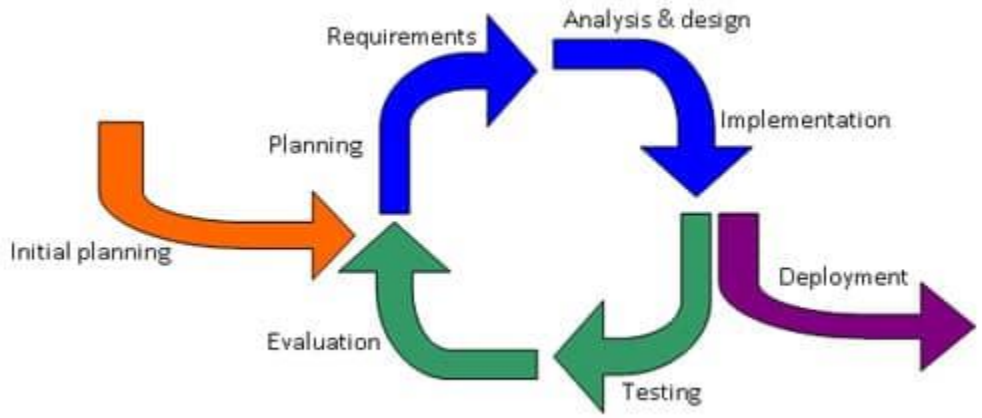


Figure 5: Iterative development (prototyping) process

3.7 Ethical considerations

There were ethical issues which were considered. Participants were informed in advance before taking part in the interview and focus group sessions. Confidentiality of information that was collected was of key priority. Transparency was also important for creating and strengthening trust for adoption of the developed toolkit since decision makers may not evaluate a system that simply provides them with the overall score of their security posture.

CHAPTER FOUR: SYSTEM ANALYSIS, SYSTEM DESIGN & IMPLEMENTATION

This section describes processes that were performed to come up with the software toolkit. These processes included system analysis, system design and high-level architecture of the toolkit.

4.1 System analysis

System analysis involved the investigation of the prototype, identifying problems and using the information noted to introduce further improvements. In addition, it helped to understand how things were done, if the proposed system would be worth undertaking, and the benefits that could accrue from its development The system analysis in the development of the cybersecurity maturity assessment prototype involved feasibility analysis, system requirement gathering and system modelling.

4.1.1 Feasibility analysis

Feasibility analysis is the process by which project feasibility is measured. It was done to find out whether the proposed system was viable in terms of economic, schedule, technical and operation feasibility. This is the test of the proposed solution in terms of its operationalization meeting the objectives with effective use of resources.

4.1.1.1 Economic feasibility

This feasibility was carried out to determine the cost effectiveness of the research project. Given that most of the required resources were readily available, the only monetary resource required was for hosting the toolkit.

4.1.1.2 Technical feasibility

This study involved checking the availability of hardware, software and skilled resource for developing the prototype. The expertise and the tools (development frameworks, development infrastructure) were available for the development of the prototype.

4.1.1.3 Operational feasibility

Operational feasibility determined whether the prototype could adequately solve the problem. Some of the questions that needed to be answered included a) What problem was the system trying to solve, b) To what extend would the system solve the problem, c) Is the solution acceptable, d) Are the system users willing to use the system, e) Was the system going to achieve the research objectives of this study?

It was established that the level to which the system tries to solve the problem was sufficient. It could not be conclusively established if users would be willing to use the toolkit.

4.1.1.4 Schedule feasibility

The project deadline was reasonable and the solution could be designed and implemented within an acceptable period. However, there was an unexpected delay in the execution of one of the objectives of the project.

4.1.2 Requirement elicitation

This section involved using the results of the problem to define the functional and non-functional requirements. The interviews, focus group discussions, review of literature and work experience were all taken into consideration.

4.1.2.1 Functional requirements

The functional requirements for the prototype included:

a. Subscription module
   - A landing web page where a customer (the public) can access services e.g., access to toolkit
   - Ability of the customer to place an order to subscribe to the toolkit
   - Ability to simulate payment by the customer (e.g., through MPESA, Credit cards, etc.)

b. Service provider module
   - The ability to view and act on orders from customers
   - The ability to view and act on simulated payments by customers
   - The ability to monitor and track licenses issued to customers
   - Ability to have configure (e.g., edit, update, delete, enable, disable, add, etc., - domains, controls, control requirements) the toolkit assessment module.

c. Assessment module
   - Provision of a risk profile
   - Provision of cybersecurity domains
   - Provision of cybersecurity controls
   - Provision of control requirements / procedures
   - Provision of risk rating matrix
   - Provision of a scoring matrix
   - Ability to link a control to a domain
   - Ability to link a procedure to a control
   - Ability to link a procedure to the customer risk profile
   - Ability to execute and review the control requirements / procedures.

4.1.2.2 Non-Functional Requirements

These requirements are not the core functionality of the system. However, they play a role in

ensuring a better presentation of functional requirements. These requirements included a) accuracy – this would ensure that the system can schedule and keep correct daily activities; b) speed – the system should have optimal speed; and c) efficiency – the system should be ensuring economical utilization of computer resources by its modules

4.1.3 System modelling

4.1.3.1 Use case diagrams

These are diagrams that are used during the analysis phase to identify and split functionality of the platform. They are made up of actors and use cases. Actors represented the various entities that interact with the platform in enabling and performing cybersecurity maturity assessment.
The use case of this platform consisted of four main actors Service provider, Customer super admin, Customer inputter and Customer reviewer. Figure 6 & 7 shows the design for these actors for the toolkit.

The activities of service provider included:

1. Login
2. Manage the toolkit components such as domains, controls, procedures, risks, etc.
3. Manage customer and / or their licenses
4. Manage customer orders
5. Manage customer payments

The activities of customer super admin included:

1. Login
2. Update company risk profile / register
3. Manage company users

The activities of customer inputter included:

1. Login
2. Conduct an assessment

The activities of customer reviewer included:

1. Login
2. Review an assessment

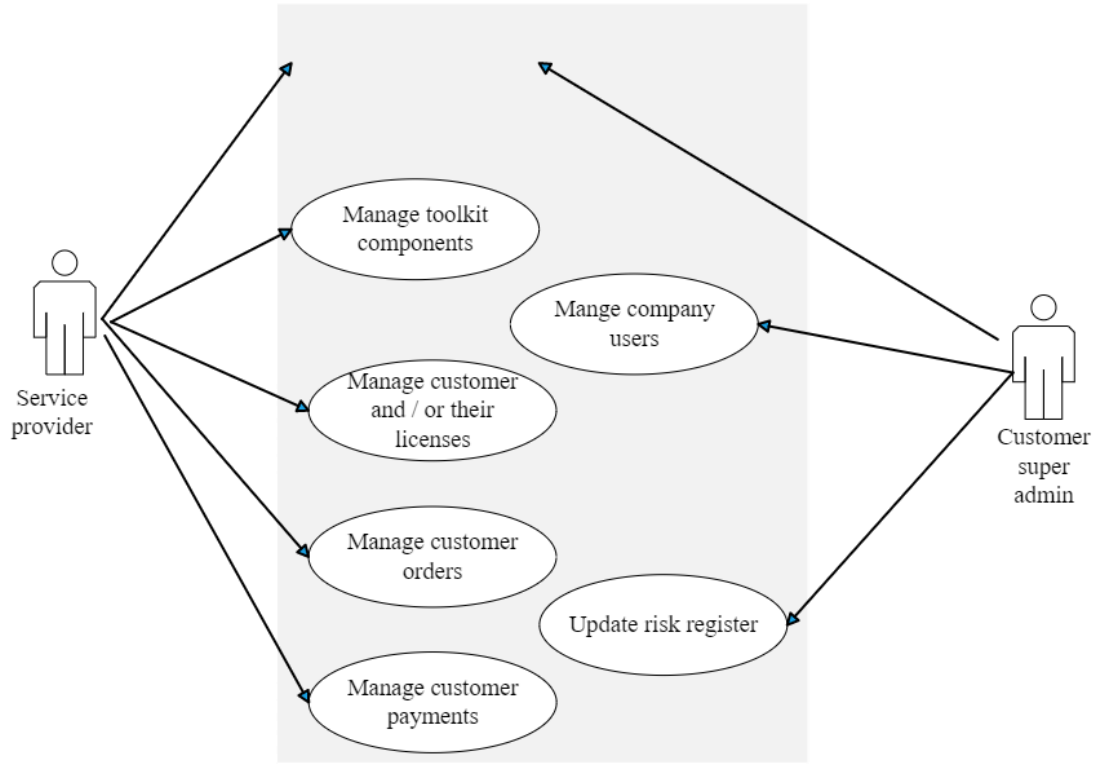


Figure 6: Service provider and customer super admin use case diagram

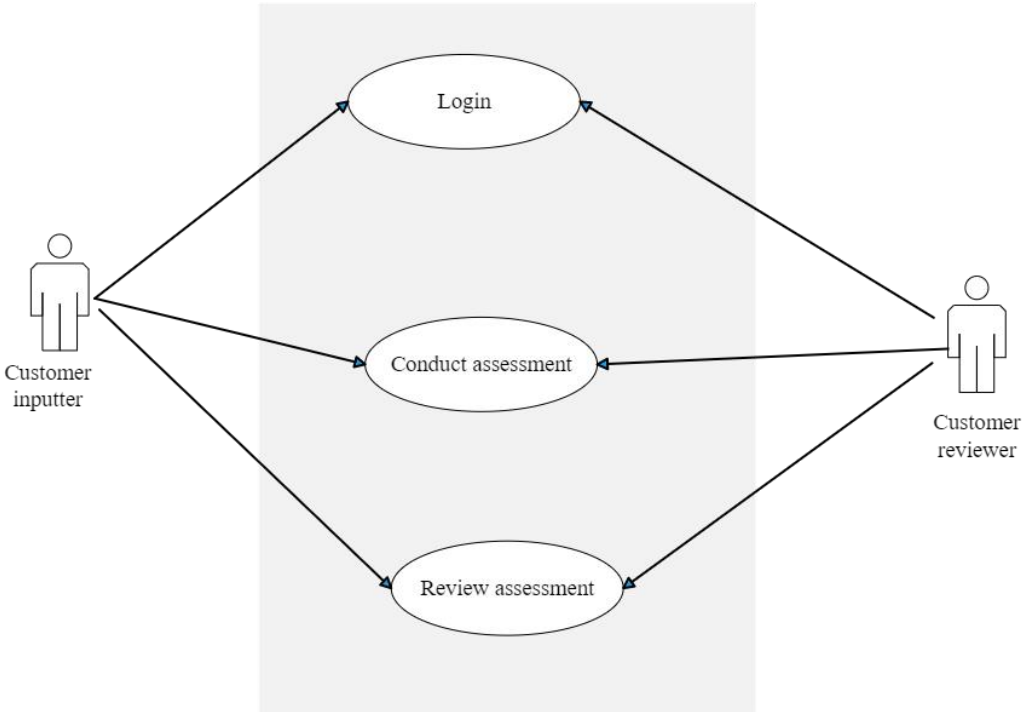


*Figure 7: C*ustomer inputter and reviewer use case diagram

4.1.3.2 Context diagram

The context diagram shown in figure 8 shows the external agents interacting with the system and the data flowing in and out of the system based on these interactions.

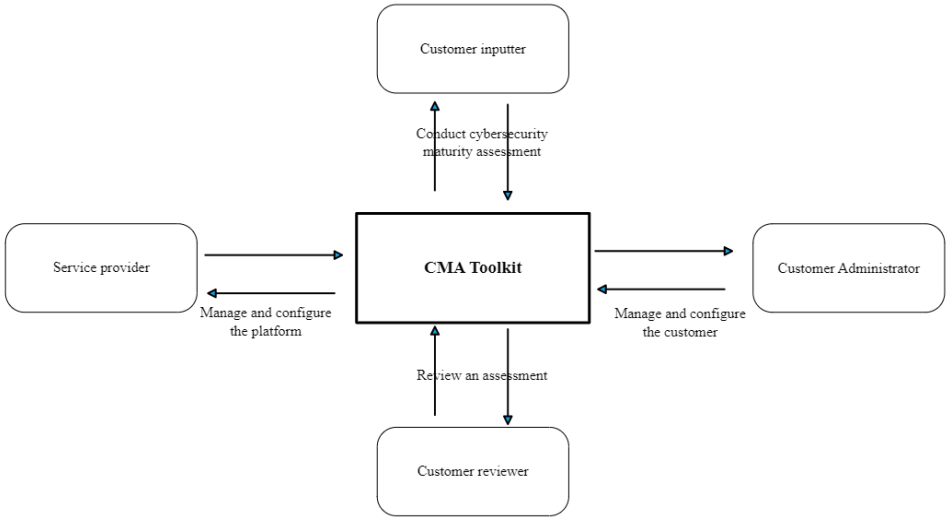


*Figure 8: C*ontext diagram

4.2 System design

System design involved the designing of elements of the prototype such as the user interface screens, architecture, modules and the data that goes through the application. The objective of the design process was to provide sufficient information about the prototype and its elements to enable implementation.

4.2.1 Conceptual design

This is the conceptual model that defines the structure, behavior of a system. Figure 9 below shows the conceptual design of the toolkit that was developed.

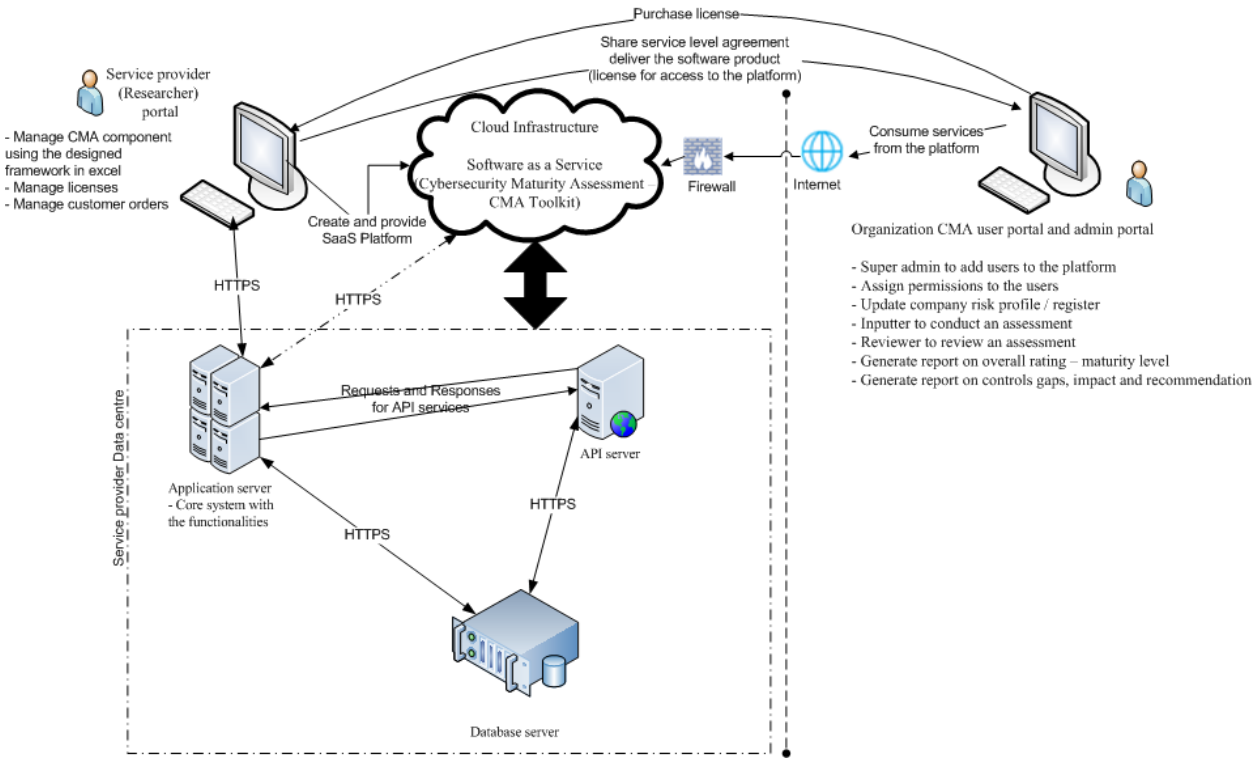


*Figure 9: C*onceptual design

4.2.2 Database Design

Database design involved the determination of data to be stored and how the data elements interrelated. Database management system manages the data accordingly. The database engine used for this toolkit was MySQL relational database and figure 10 below shows the entity relationship of different tables in the database.

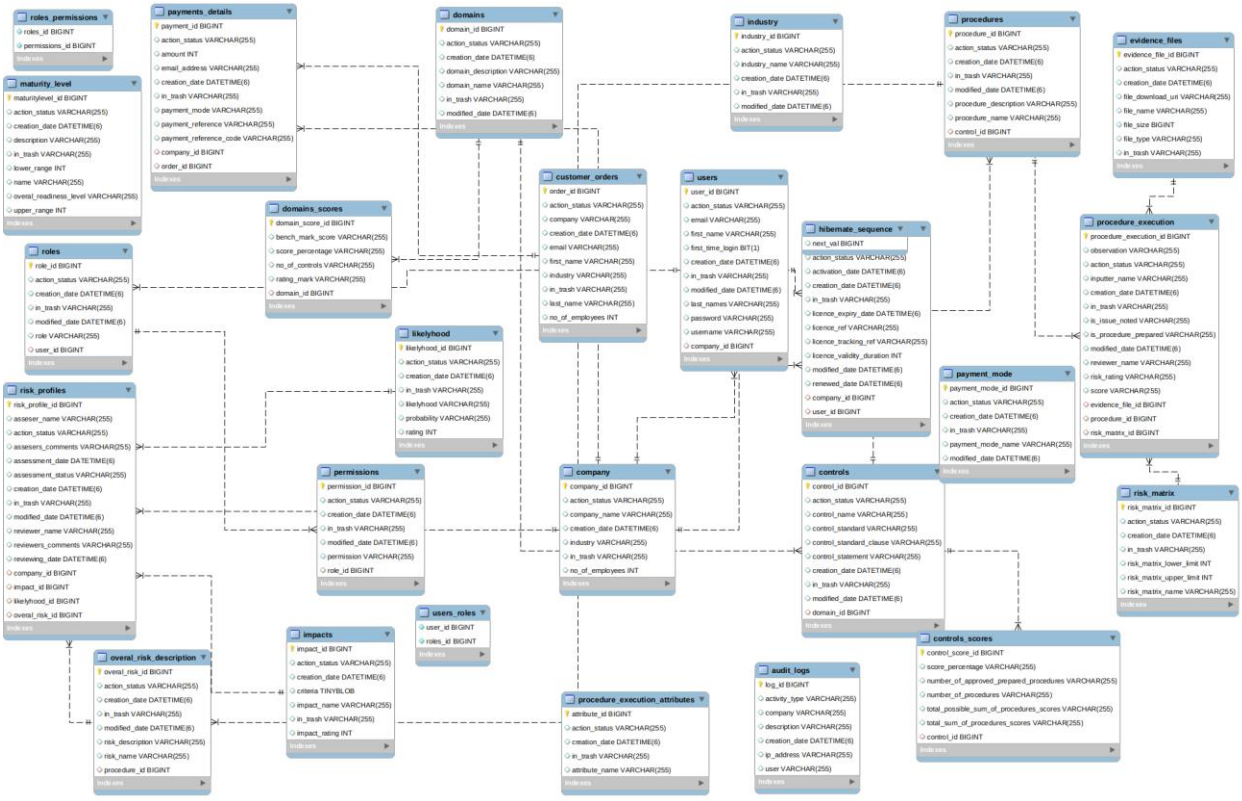


Figure 10: Database design

4.2.3 User interface design

For this prototype, the choice for user interface was based on a thorough investigation on usability and aspects that user like in a page. It was optimized so that user could operate quickly and easily. It is believed that user interface design and experience should be simple and intuitive. Figure 11 and 12 show some of the screen designs that were developed for the toolkit.

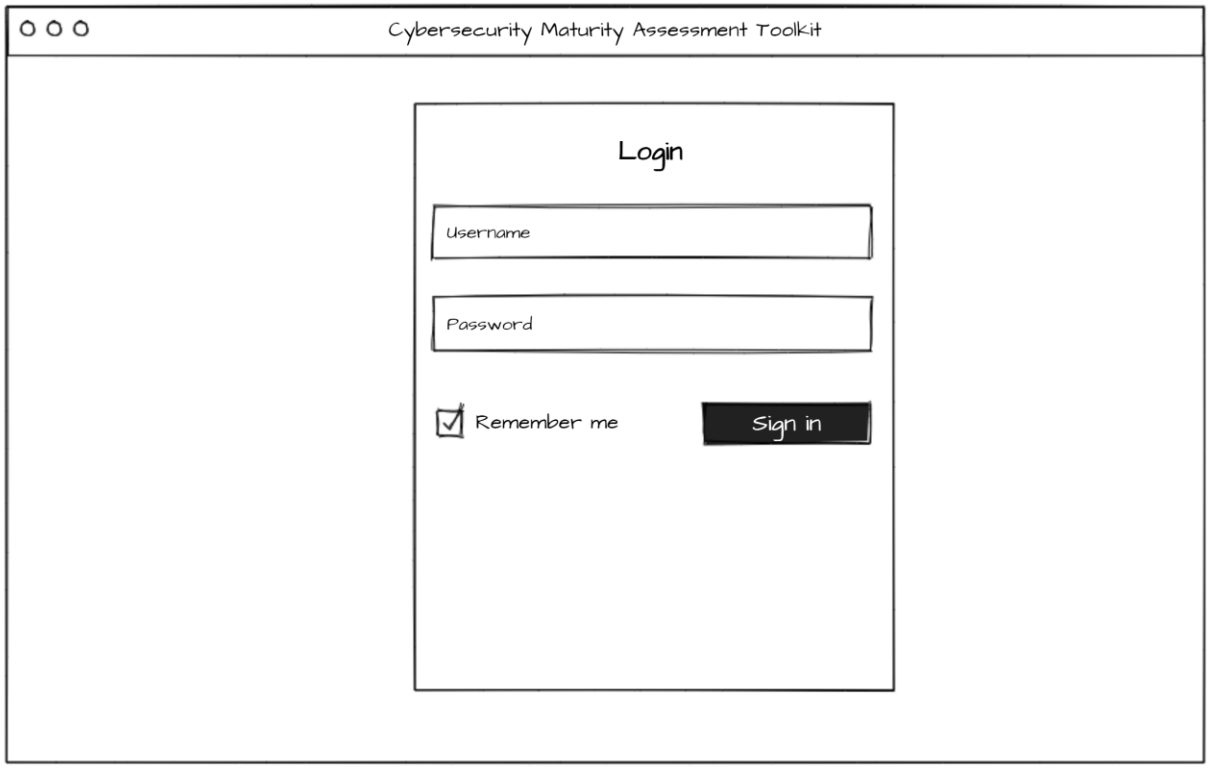


Figure 11: User interface design – Login screen

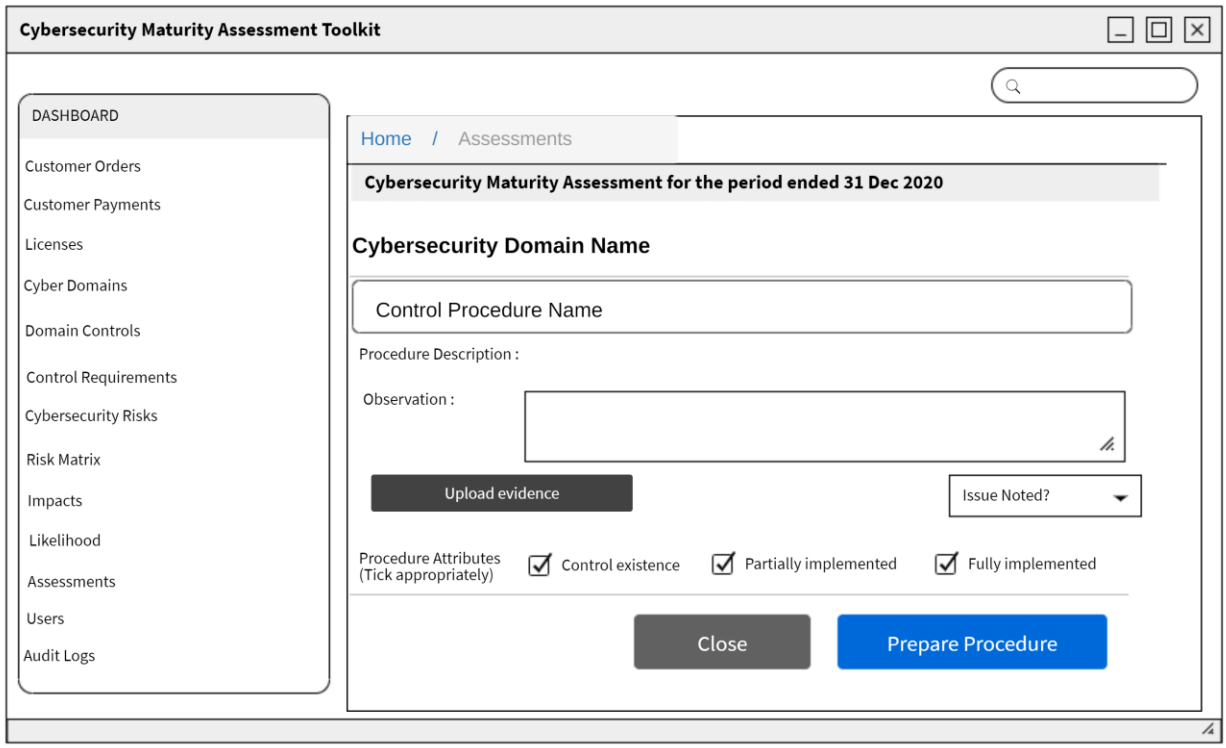


Figure 12: User interface design – Control procedure execution screen

4.3 System implementation

This section describes details on how the prototype was implemented and tested with selected users. It shows the resources that were used, software tools, choice of programming technology and testing of the toolkit.

4.3.1 Hardware Resources

- HP Spectre –Laptop
- Processor – 8 CPUs; 2.3GHz.
- RAM – 16GB
- Hard disk-500 GB (SSD)

4.3.2 Software Resources

Below are software resources that were leveraged during the development of the toolkit.

- IntelliJ JetBrains programming IDE
- MySQL database.
- Visio professional 2019
- Microsoft word 2019
- Microsoft Excel
- Visual paradigm
- Microsoft PowerPoint 2016
- Operating system: Windows OS and Linux (Ubuntu)
- Docker
- Tomcat server
- Git for version control
- Spring Boot framework for backend APIs
- Angular JS

4.3.3 Choice of Programming tools, techniques, and technologies

Web development technologies, tools and languages were used to implement the toolkit. The following gives a description and basis for selecting the web tools used in this project.

4.3.3.1 Java and Spring framework

Java technology was chosen since it's a simple and elegant language with a well-designed, intuitive set of APIs, thus it was easy to write better code with fewer bugs and again reducing the development time. In addition, Java programs are compiled to an intermediate form rather than to native machine-language instructions meaning this architecture would be faster. The backend APIs were developed using spring boot framework, a java framework using Swagger.

4.3.3.2 MySQL

MySQL being an open-source relational database, it was selected for the development of this prototype.

4.3.3.3 Angular JS

This is a JavaScript library for building user interfaces. It made it easy to make interactive user interface. Angular was chosen to come up with the frontend side of the prototype.

4.3.3.4 Docker

Docker made it easier, simpler, and safer to deploy, and test the application. It is a platform that uses OS-level virtualization to deliver software in packages called containers.

4.4 System testing

This is the process of ensuring that the resulting output is a correct function of the input. It involves validating the output against the input to check for consistencies and also checking that the toolkit both the framework and the prototype executes without logical and/or syntax errors. The following techniques were used to evaluate the toolkit:

4.4.1 Walkthroughs with information security experts

This form of testing or technical review was continuous throughout the development cycle. It involved presentation of the prototype to professionals in the information security field. We would then walk through the system functionality and usability and got feedback whether the system could meet the intended purpose.

4.4.2 Module testing

This involved testing the individual components of the system. It was conducted continuously each time a new module was completed. Each module was being tested to ensure correctness in its functionality. Validation tests were carried out on all forms and verification tests carried out against the functional and non-functional requirements.

4.4.3 Regression testing

This was done to uncover new bugs that would be introduced in existing functional areas of a system after changes were made.

4.4.4 Integration testing

This was done to ensure that all the system modules interfaced properly and collaborated well while meeting the overall system specifications.

4.4.5 System testing

This was done to test the entire application to ensure that it functioned as a single unit and met the requirements. All the errors discovered were corrected as desired ensuring that all the modules were operating correctly.

4.4.6 User acceptance testing

Lastly, the prototype was put to test to determine if it can serve the intended purpose. This was to confirm that the system was ready for operational use. During acceptance test, end-users i.e., information security experts tested the toolkit by conducting a sample cyber security maturity assessment and then compared that with the existing assessments that had been carried out.

4.4.7 Test cases

The main intent of this activity was to determine whether the prototype developed had met the expectations in terms of its functionality and other aspects. Table 2 below shows sample test cases that were used.

#	Module	Test	Expected Result	Actual Output
1	Subscription module	Verify that a customer can access the site through the internet.	Ability for a customer to access the site over the internet	The module was accessible.
2	Subscription module	Verify that a customer can place an order.	Ability for a customer to place an order.	Submitting orders to the service provider was successful.
3	Subscription module	Verify that a customer can make payments.	Ability for a customer to make payments.	Making payment was successful.
4	Service provider portal	Verify that license generation for customers work.	Ability to generate licenses.	License generation was successful.
5	Service provider portal	Verify that the service provider can create and update the pre-requisite information needed for an assessment.	Ability to configure domains, controls, procedures, control attributes, cyber security risks, risks likelihood, impacts, risk matrix and maturity levels.	Configuration by the service provider was successful.
6	Customer / assessment portal	Verify that the customer (an organization) can update their risk profile and execute a cyber maturity assessment.	Ability to update risk profile and conduct an assessment.	Updating risk profile and conducting an assessment was successful.

Table 2 Sample test case

4.4.8 Sample screenshots of the toolkit

Figure 13 – 22 show some of the screens that were taken for the toolkit, both the framework in Microsoft Excel and the prototype.

Figure 13 below shows the overall maturity level of an organization. This is obtained when the assessment is done using the developed model in Microsoft excel. It provides the overall score after the aggregation of the respective domain scores done in separate Excel workbooks.

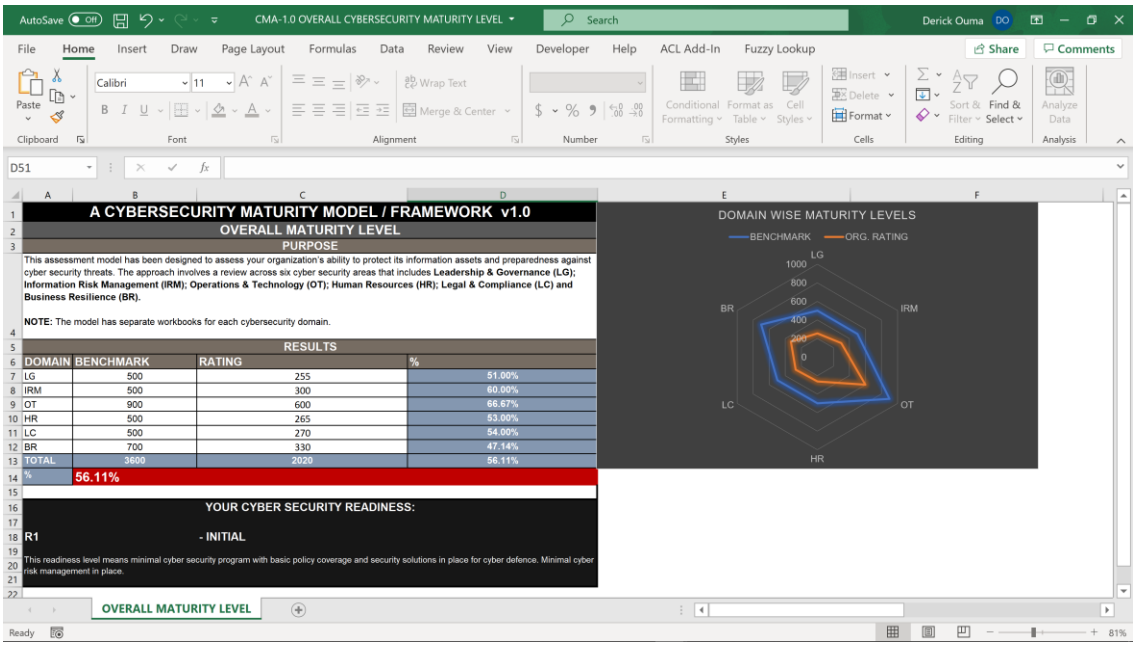


Figure 13 Microsoft Excel Cybersecurity Maturity assessment framework showing overall maturity level of an organization.

Figure 14 below shows a summary of scores for control requirements / procedures under a domain. Every domain has been represented in separate Excel workbooks with control requirements to be assessed to determine the level of implementation hence scores assigned based on what has been achieved by the organization.

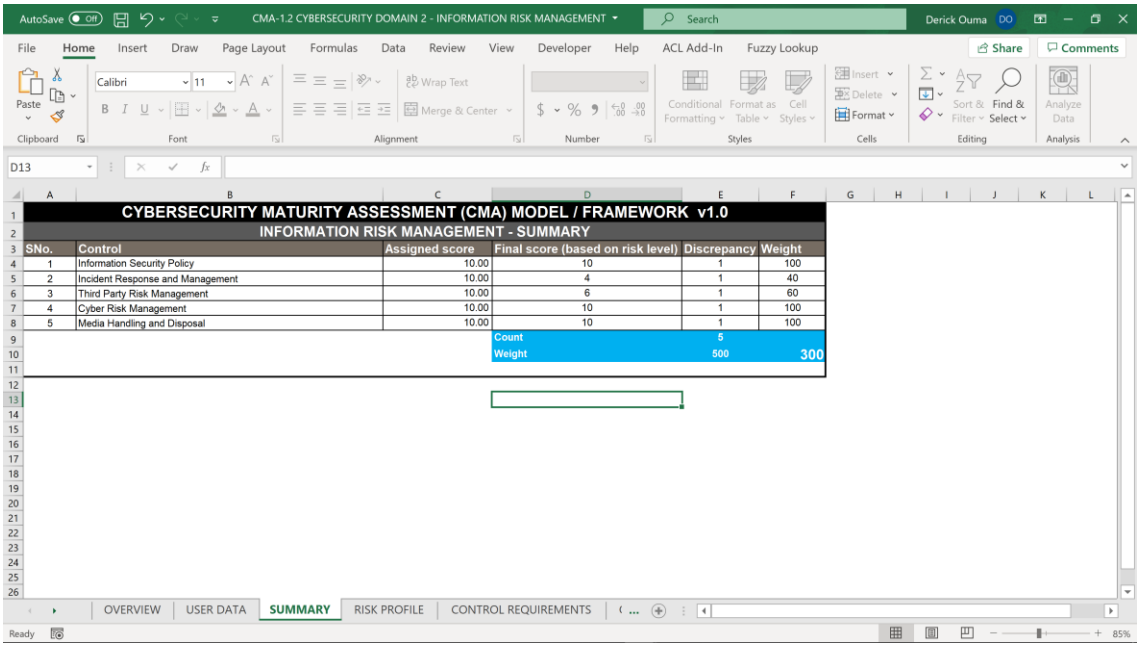


Figure 14 Sample summary scoring for an individual cybersecurity domain

Figure 15 below shows the excel sheet where an organization is required to update their cyber threat / risk profile based on the latest assessment. It was assumed in the study that annual risk assessment is conducted.

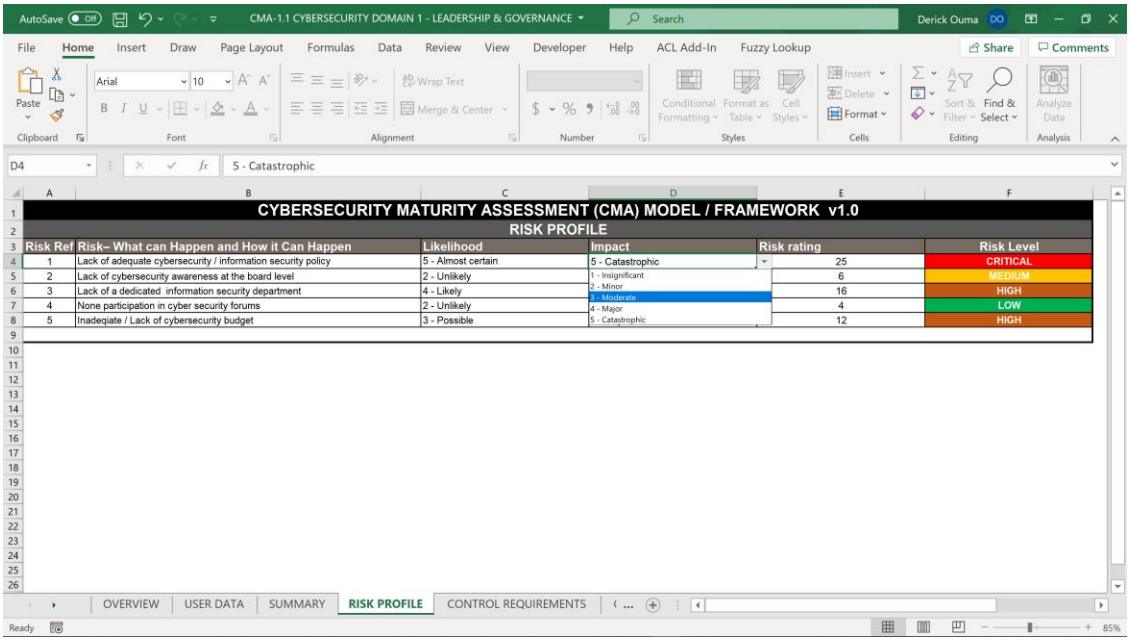


Figure 15 Updating customer risk profile based on the organization's annual risk assessment

Figure 16 below shows control requirements under a specific domain. These control requirements are assessed to determine the level of implementation.

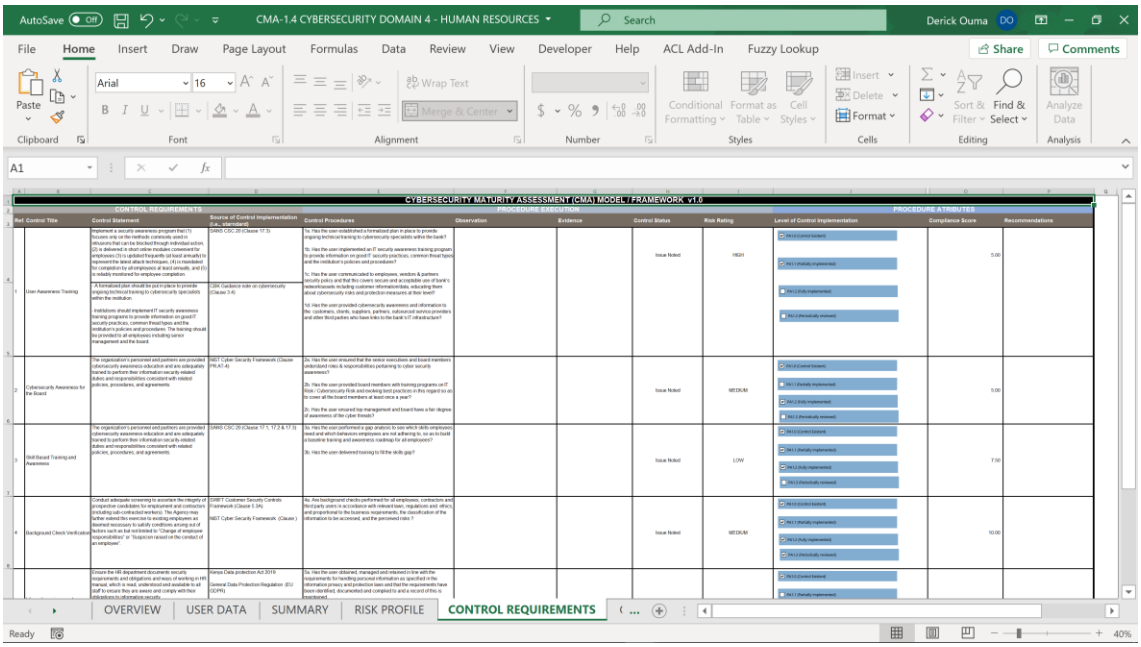


Figure 16 Control requirements in the toolkit.

Figure 17 below shows the prototype site that customers access online to request for subscription to the assessment platform.

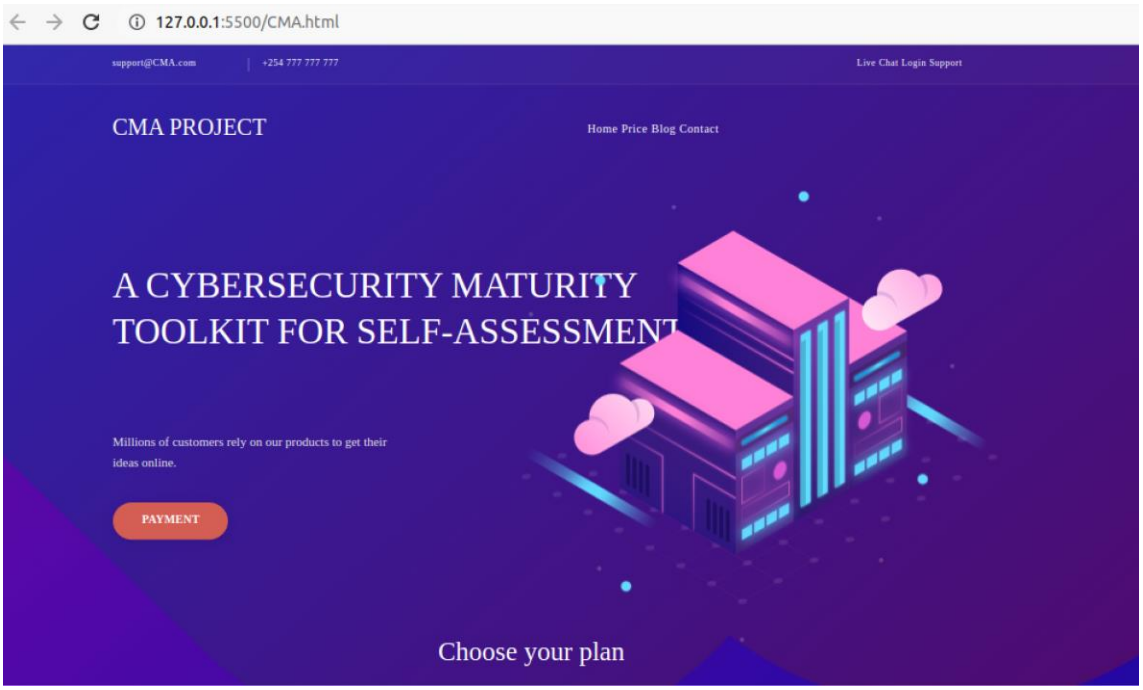


Figure 17 Prototype subscription portal

Figure 18 below shows the prototype portal for the service providers for administration of the assessment platform.

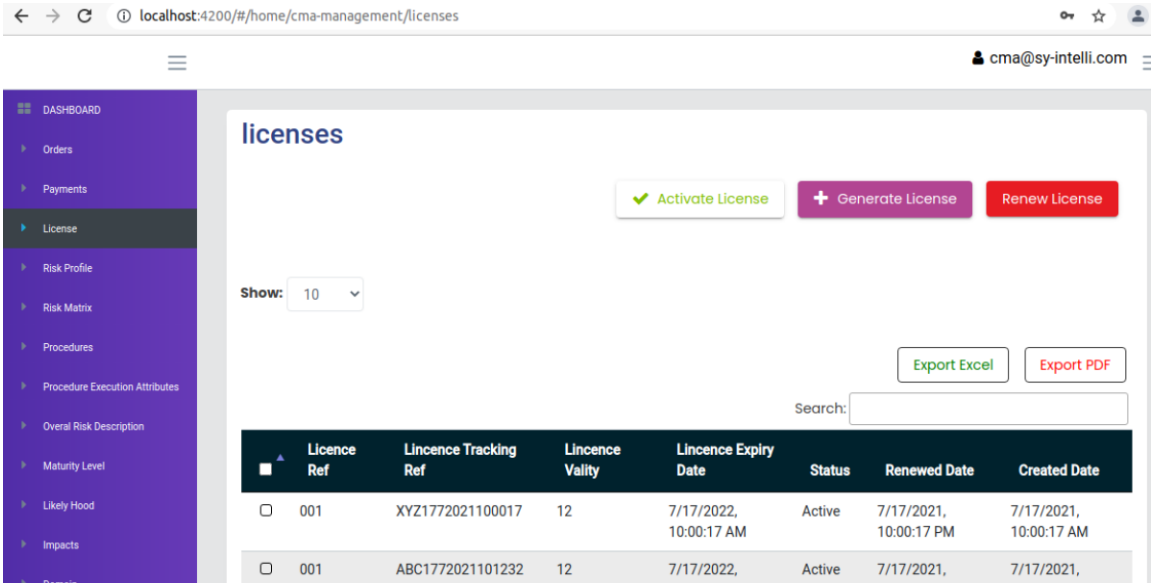


Figure 18 Service provider portal for administration of the toolkit

Figure 19 below shows the prototype customer portal where a user views / updates the organization's risk profile.

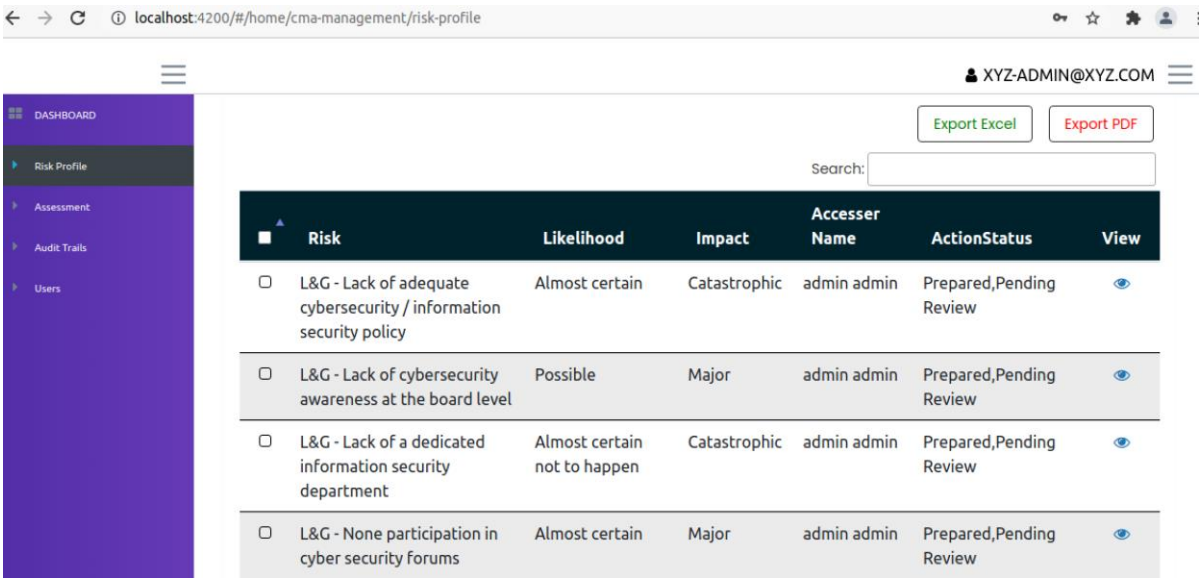


Figure 19 Customer risk profile

Figure 20 below shows the prototype customer portal where a user documents a particular control requirement / procedure.

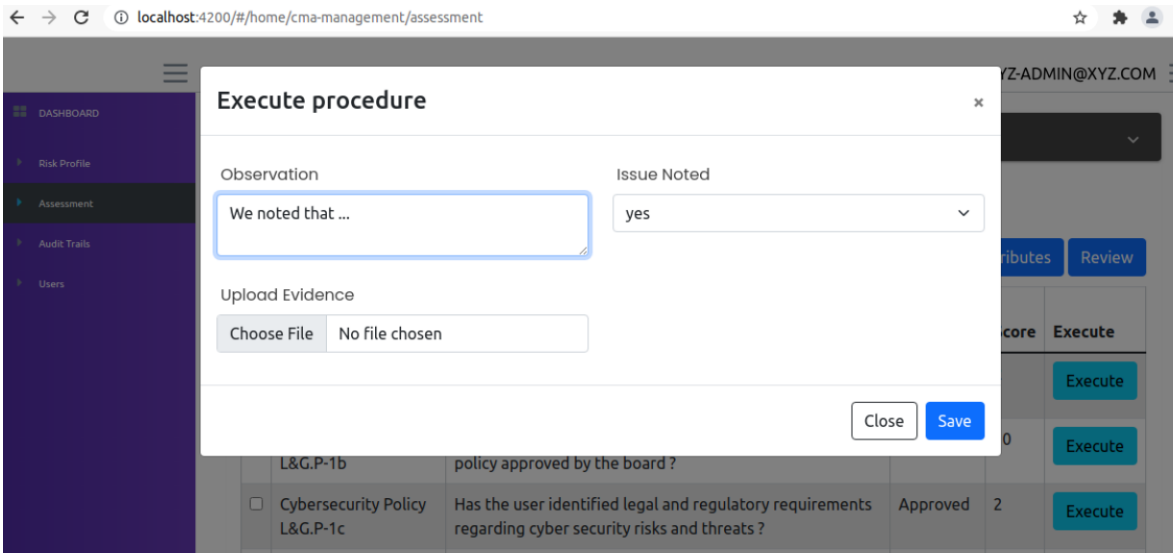


Figure 20 Execution of a procedure based on the control requirements

Figure 21 below shows the prototype customer portal where a user ticks a control attribute based on the documented results. This has to be ticked appropriately before the system can assign a score. The risk level of the control is also checked before assigning the score.

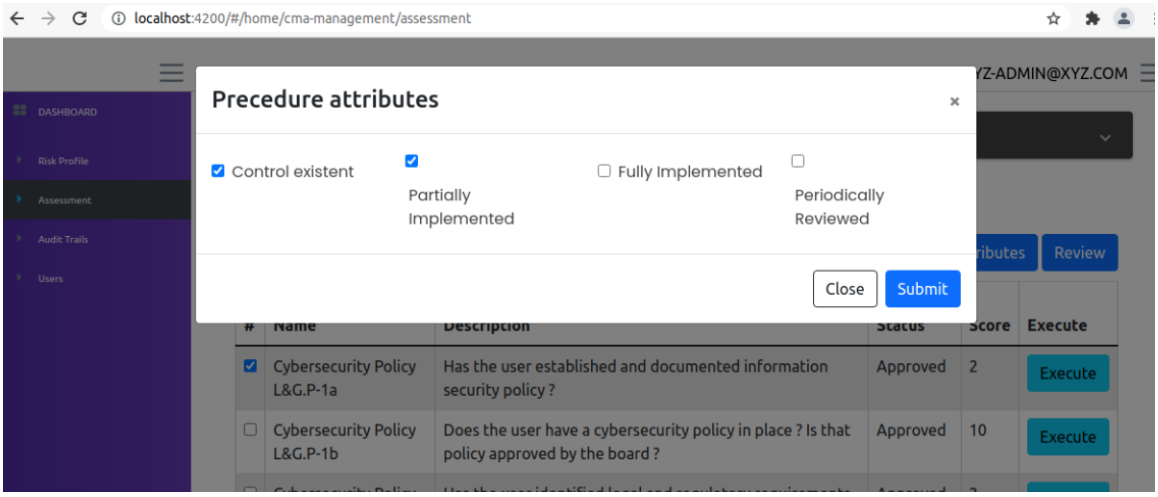


Figure 21 Control attributes to ascertain level of implementation for the control requirements

Figure 22 below shows the overall maturity level of an organization that the user views after successful completion and reviewing all the control requirements using the developed prototype.

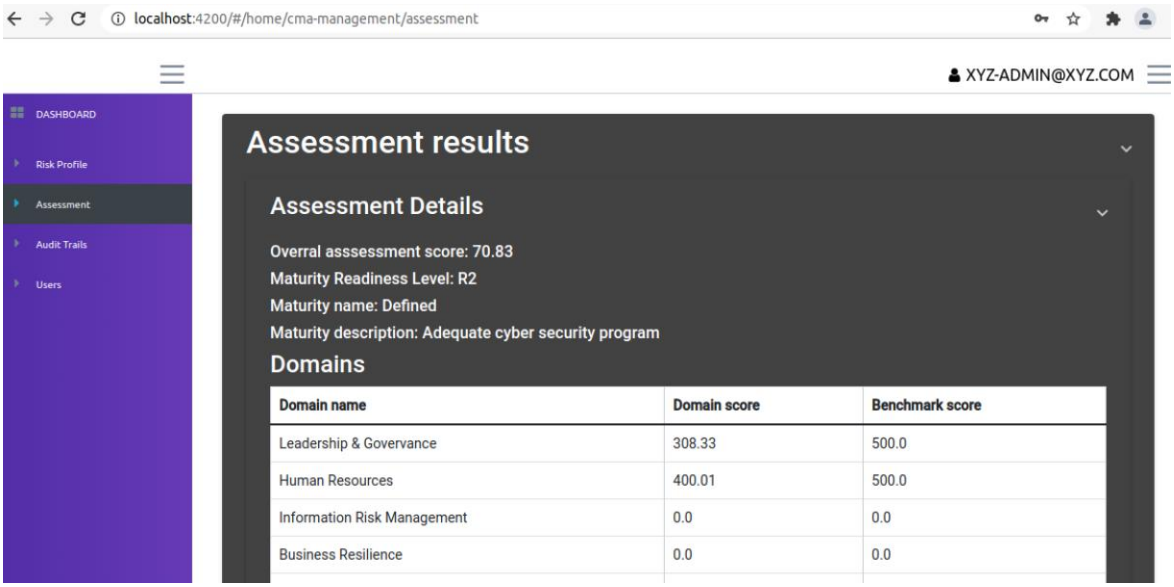


Figure 22 Overall cyber maturity score for an assessment

CHAPTER FIVE: RESULTS AND DISCUSSIONS

This chapter highlights and discusses the evaluation results obtained during testing by information security experts in the banking industry. These experts also compared the outcome from the toolkit and previous assessments that has been done for their respective banks.

5.1 Prototype evaluation and results

5.1.1 Functional evaluation

Table 3 below shows evaluation and results of the modules that are exposed to a customer who would wish to subscribe to the service.

Module	Evaluation	Results
Subscription module	To verify whether one could place an order to subscribe to cybersecurity maturity assessment service.	This was successful.
Subscription module	To verify whether one could simulate payment for the placed order.	This was successful.
Customer portal	To verify whether one could activate their license after successful subscription.	This was successful.
Customer portal	To verify whether the system administrator could create other users in the system i.e., inputter & authorizer.	This was successful.
Customer portal	To verify whether one could update the organization's risk profile based on the annual risk assessment results.	This was successful.
Customer portal	To verify whether one could conduct a cyber maturity assessment and get the maturity level / posture for the organization.	This was successful.

Table 3 End user functional evaluation results

5.1.2 User testing results

A survey was conducted among the experts who tested the system on user experience. Figure 23 below shows a chart with their responses.

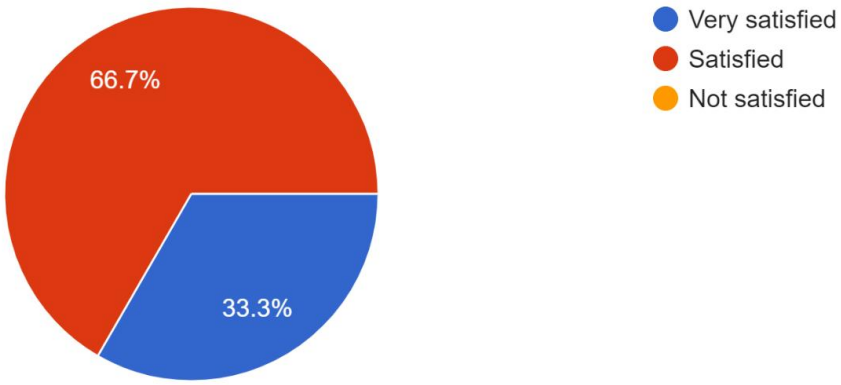


Figure 23 User experience results

The respondents were also asked about whether the content provided in the toolkit was sufficient for conducting the maturity assessment. Figure 24 below shows a chart with the responses.

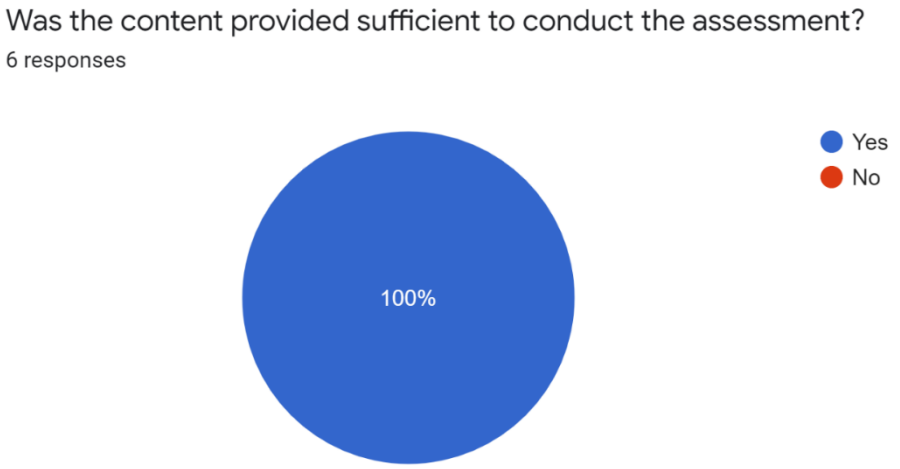


Figure 24 Toolkit content

A question on the correctness of the maturity level compared to assessments that had been done before was also asked and all the experts were of the opinion that it was representation of their cyber security posture in accordance with the Information Technology security controls that had been implemented.

5.2 Discussion

It was evident that the results shown above indicated that targeted users / the experts understood the significance of such a toolkit. A toolkit that could enable their organizations

conduct self-assessments of their security postures and further help in determining information security controls that could require improvements to protect the institution from cyber security threats.

The overall cyber maturity score depicted in the test results above was the measurement of the security posture for that particular organization. This is computed after control procedures are executed, documentation done and evidence uploaded. Upon a review of the executed procedure, the toolkit automatically scores level of achievement. This score is assigned based on the control attributes that included 1. Control existence – consists of a control attribute that exist even without some achievement, 2. Partially implemented – consists of a control attribute with some evidence of an approach to, and some achievement of the defined requirement; 3. Fully implemented – there is evidence of a complete and systematic approach and full achievement of the defined requirement; 4. Periodically reviewed – consists of a fully achieved control that is reviewed to ensure improvements noted are implemented. The flowchart in figure 25 shows how the toolkit assigns the score.

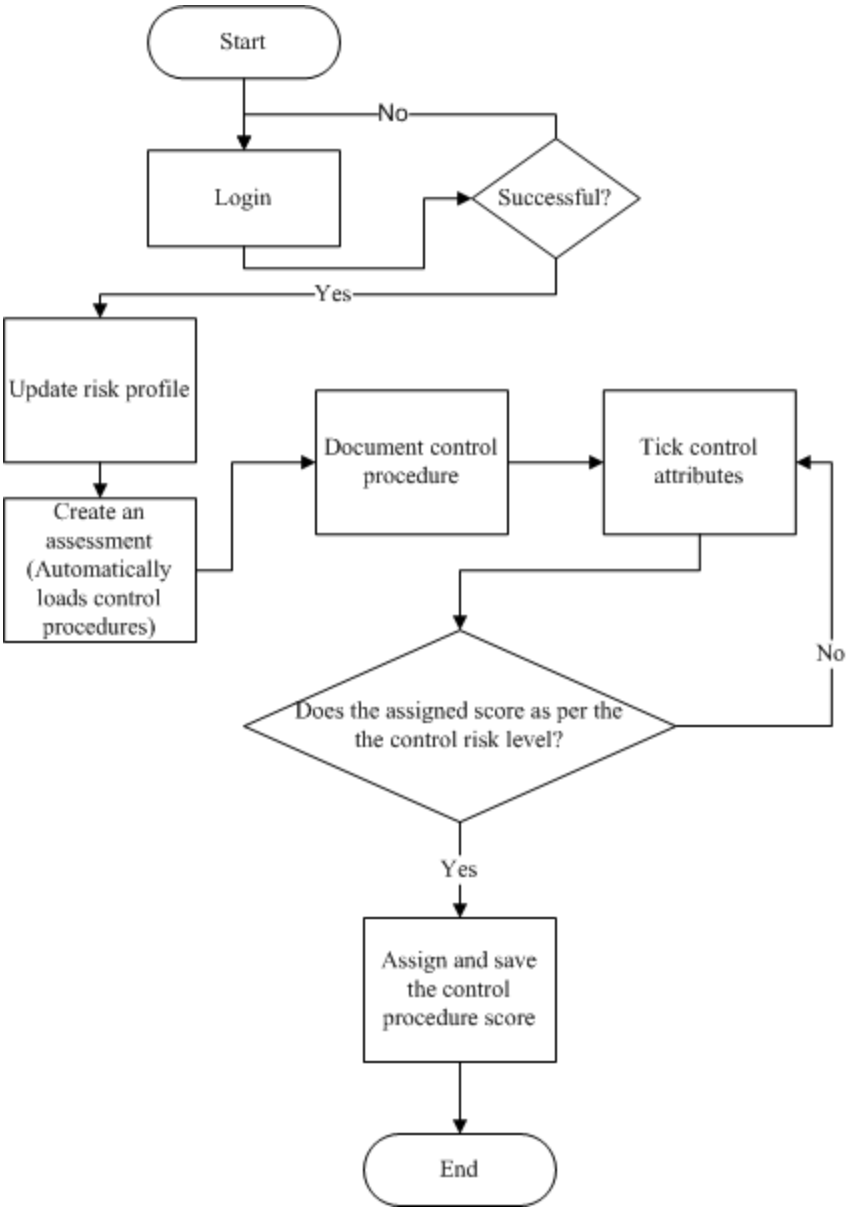


Figure 25 A flowchart showing how the toolkit computes a score for a particular control procedure

The toolkit then aggregates the scores for controls under a particular cyber security domain to calculate the score for that domain. The risk rating assigned to a control also directly affects the score for that control as shown in the above flowchart in figure 26.

Lastly, the toolkit computes the overall score (maturity level) for the assessment using the expression below:

$$\text{Maturity level} = \sum \left(\frac{Domain\ Computed\ Score}{Domain\ Possible\ Score} \right) * 100\%$$

So, maturity level is defined as a measurement of an organization's ability to protect its information assets and level of preparedness against cyber threats.

This study has categorized maturity levels into three levels as shown in table 1 below.

Maturity level	Name	Description	Range
R1	Initial	This level means minimal cyber security program with basic policy coverage and security solutions in place for cyber defense. Minimal cyber risk management in place.	0 – 60%
R2	Defined	This level means adequate cyber security program with policy framework and advanced security solutions in place for cyber defense. Adequate cyber risk management in place.	61 – 84%
R3	Managed	This level means managed, structured and repeatable cyber security program with a defined implemented enterprise policy framework and advanced security solutions aided by technical capabilities in place for cyber defense. Well managed cyber risk management in place.	Above 85%

Table 4 Defined maturity levels

The study adopted a phased approach to design the cybersecurity maturity assessment model. The overall cyber maturity level was arrived through a review of control requirements across six cyber security domains i.e., Leadership and Governance, Information Risk Management, IT Operations, Business Resilience, Human Resources and Legal and Compliance.

CHAPTER SIX: CONCLUSION AND RECOMMENDATIONS

This section provides a summary of the findings. A conclusion has been drawn and recommendation for future research given.

6.1 Summary of findings

The findings noted were based on the research questions:

a) How can industries in Kenya perform cyber maturity assessments?

Through literature review and survey, there were existing cyber maturity models that could be used to conduct the assessments. There also existed information security standards that could equally aid the assessments. However, organizations required the expertise to use or deploy the available standards and models.

b) How can a cyber maturity assessment model based on existing models and information security standards be designed?

The outcome of the study has proven that the available information from existing maturity models, information security standards and governments laws & regulations could be used to design a framework, more customized for organizations across different industries in Kenya. The model was designed and developed using Microsoft Excel that has a consolidation of control requirements. These requirements were presented in way that they were measurable.

c) How can the designed model be automated to aid self-assessment?

A prototype has been developed using existing programming technologies to automate the designed model. It has three modules, namely, subscription module, service provider module and client module. This ensures that the toolkit can be offered as a cloud platform (Software as a service).

6.2 Conclusion

A proof of concept has been presented using the prototype to provide organizations with a toolkit for conducting self-assessment on their cybersecurity posture without hiring an expert every time an assessment is needed. Thus, the overall objective of this study was achieved.

This toolkit consists of the model developed in Microsoft Excel that has control requirements that can be implemented by organizations in different industries in Kenya to ensure that the IT environment is secure and properly setup. The model has also implemented attributes to measure these control requirements to ascertain the extent they have been implemented. It also consists of the developed prototype that was meant to transform the model into software modules. This software is what is offered to customers as a cloud service. The toolkit is to be controlled by the service provider who is responsible for updating control requirements content with notable and improved information security standards / frameworks as well as government

laws and regulations both local and international. On the other hand, customers will be required to subscribe for the service and be issued with an annual license to have access to the platform.

6.3 Contributions of the study

The developed toolkit comes in handy since the only requirement is to have an annual subscription by customers. In addition, the study also ensures organizations will be at per with new regulations by governments to ensure compliance since the toolkit content for the assessments will be updated on a frequently basis by the service provider.

6.4 Future work

Future work should focus on exploring other technologies that can be used to improve the toolkit especially machine learning to make it intelligent. This will ensure processing of evidence uploaded during the assessments to ascertain correctness, completeness, and authenticity.

REFERENCES

Arnesen H., Grete A., Jacobsen B. & Omenaas E. (2017). *The Research Handbook,* 7th ed., Oslo University Hospital.

BAI (2018). GDPR: The General Data Protection Regulation. *SSRN Electronic Journal*. Retrieved from https://ld-connect.bai.org/docs/default-source/ whitepapers -and -articles/gdpr.pdf?sfvrsn=2

Benoot, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology*, 16(1), 1–12. https://doi.org/10.1186/s12874-016-0114-6

Bleerton A. 2017. *An approach to information Security for SMEs based on the Resource-Based View theory*, pp. 1-3

Butkovic M. & Caralli R. (2013) *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale.* Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_69194.pdf

Central Bank of Kenya. (2019). *Guideline on cybersecurity for payment service providers*. Retrieved from https://www.centralbank.go.ke/wp-content/uploads/2019/07/GuidelinesonCybersecurityforPSPs.pdf

Dmitrijs N. (2010). *Application of CobiT Maturity Model in Information Security Management and Arising Problematic Issues: scientific papers, university of Latvia*, vol. 757, pp. 53–63.

El, S., Youssfi, K., & Boutahar, J. (2016). CAT5:A Tool for Measuring the Maturity Level of Information Technology Governance Using COBIT 5 Framework. *International Journal of Advanced Computer Science and Applications,* 7(2), 1–7. Retrieved from : https://doi.org/10.14569/ijacsa.2016.070253

Goundar. (2019). Research Methodology and Research Method. *Research Methodology and Research Method*, 2. Retrieved from https://www.researchgate.net/publication/333015026

KPMG. (2015). *ISACA Kenya Annual Conference - Secure Kenya II: Data Protection, Privacy and Cyber Security.* Retrieved from http://isaca.or.ke/downloads/Data-Protection-Privacy-and-Cybersecurity.pdf

Malan, R. & Bredemeyer, D. (2004). *Conceptual Architecture.* Retrieved from http://www.bredemeyer.com/ArchitectingProcess/ConceptualArchitecture.htm#:%7E:text=The%20conceptual%20architecture%20diagram%20identifies,the%20responsibilities%20of%20each%20component

Oates, B. J. (2006). *Researching Information Systems and Computing* (First ed.). London, United Kingdom: SAGE Publications Ltd.

Rabii, A., Assoul, S,. Touhami, K,. & Ounsa, R. (2020). *Information and cyber security maturity models: a systematic literature review.* Retrieved from https://www.emerald.com/insight/2056-4961.htm

Ranjit K., (2011). *Research Methodology: a step-by-step guide for beginners,* 3rd ed., Los Angeles: SAGE Publications.

Sani, A., Firdaus, A., Ryul Jeong, S., & Ghani, I. (2013). A Review on Software Development Security Engineering using Dynamic System Method (DSDM). *International Journal of Computer Applications*, 69(25), 33–44. https://doi.org/10.5120/12131-8527

Serianu. (2018). *Africa Cyber Security Report – Kenya.* Retrieved from https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf

Suri, H. (2011). Purposeful Sampling in Qualitative Research Synthesis. *Qualitative Research Journal*, 11(2), 63–75. https://doi.org/10.3316/qrj1102063

Taherdoost, H. (2016). Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research. *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.3205040

The Open University. (2005). *Action Research Guide for Associate Lecturers*, 7–8. Retrieved from http://www.open.edu/openlearnworks/course/view.php?id=1592

University of Southern California. (2020). *Research Guides: Organizing Your Social Sciences Research Paper: Independent and Dependent Variables*. Retrieved from https://libguides.usc.edu/writingguide/variables

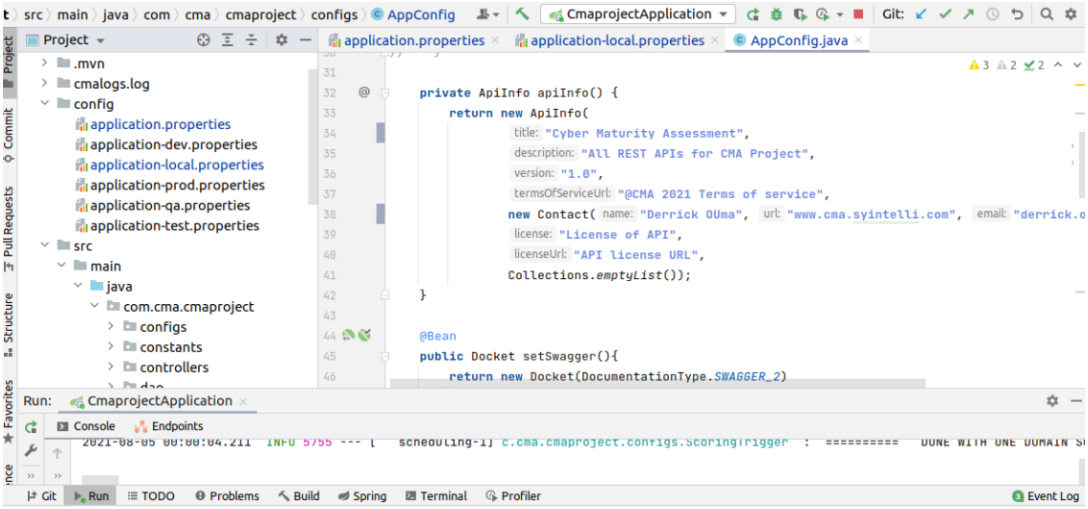
APPENDIX

API Samples

127.0.0.1:9099/procedure-assessment/view/109/219


```
{
  "code": 200,
  "status": "Success",
  "message": "Viewed Successful",
  "date": "2021-08-04T17:03:39.665+00:00",
  "data": {
    "overalAssessmentResult": "70.83",
    "maturityLevel": {
      "id": 124,
      "overalReadinessLevel": "R2",
      "name": "Defined",
      "lowerRange": 61,
      "upperRange": 84,
      "description": "Adequate cyber security program",
      "actionStatus": "Approved",
      "intrash": "NO",
      "creationDate": "2021-06-20T09:37:42.718+00:00"
    },
    "procedures": [ … ], // 27 items
    "assessmentGraphData": {
      "domainsDataForGraph": [
        {
          "domainId": 5,
          "domainName": "Leadership & Governance",
          "domainScore": "308.33",
          "domainBenchMarkScore": "500.0",
          "numberOfControls": "5"
        },
        {
          "domainId": 7,
          "domainName": "Human Resources",
          "domainScore": "400.01",
          "domainBenchMarkScore": "500.0",
          "numberOfControls": "5"
```


Backend source code



Frontend source code