CYBERSECURITY CAPABILITY MATURITY MODEL FOR CRITICAL INFORMATION TECHNOLOGY INFRASTRUCTURE AMONG NIGERIA FINANCIAL ORGANIZATIONS IDI MOHAMMED UNIVERSITI TEKNOLOGI MALAYSIA

Thesis · August 2019

CITATIONS
0

READS
195

1 author:

Idi Mohammed
Yobe State University
5 PUBLICATIONS **0** CITATIONS

SEE PROFILE

CYBERSECURITY CAPABILITY MATURITY MODEL FOR CRITICAL INFORMATION TECHNOLOGY INFRASTRUCTURE AMONG NIGERIA FINANCIAL ORGANIZATIONS

IDI MOHAMMED

UNIVERSITI TEKNOLOGI MALAYSIA

PSZ 19:16 (Pind. 1/13)

UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / POSTGRADUATE PROJECT REPORT AND COPYRIGHT

Author's full name : Idi Mohammed

Date of Birth : 2nd January 1987

Title : Cybersecurity Capability Maturity Model for Critical Information Technology Infrastructure among Nigeria Financial organizations

Academic Session : 2018/2019

I declare that this thesis is classified as:

☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)*

☑ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

1. I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:
2. The thesis is the property of Universiti Teknologi Malaysia
3. The Library of Universiti Teknologi Malaysia has the right to make copies for the purpose of research only.
4. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

SIGNATURE OF STUDENT	**SIGNATURE OF SUPERVISOR**
MCS172045	DR. SITI HAJAR OTHMAN
MATRIC NUMBER	**NAME OF SUPERVISOR**
Date: 15 APRIL 2019	Date: 15 APRIL 2019

NOTES : If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction

"I hereby declare that I have read this dissertation and in my opinion this dissertation is sufficient in term of scope and quality for the award of the degree of Master of Computer Science"

Signature	:	_____
Name of Supervisor	:	DR. SITI HAJAR OTHMAN
Date	:	15 APRIL 2019

BAHAGIAN A - Pengesahan Kerjasama*

Adalah disahkan bahawa projek penyelidikan tesis ini telah dilaksanakan melalui kerjasama antara _____dengan _____

Disahkan oleh:

Tandatangan : Tarikh :

Nama :

Jawatan :

(Cop rasmi)

** Jika penyediaan tesis atau projek melibatkan kerjasama.*

BAHAGIAN B - Untuk Kegunaan Pejabat Sekolah Pengajian Siswazah

Tesis ini telah diperiksa dan diakui oleh:

Nama dan Alamat Pcmeriksa Luar **:**

Nama dan Alamat Pcmeriksa Dalam **:**

Nama Penyelia Lain (jika ada) **:**

Disahkan oleh Timbalan Pendaftar di SPS:

Tandatangan : Tarikh : 15JULAI 2018

Nama :

CYBERSECURITY CAPABILITY MATURITY MODEL FOR CRITICAL INFORMATION TECHNOLOGY INFRASTRUCTURE AMONG NIGERIA FINANCIAL ORGANIZATIONS

IDI MOHAMMED

A dissertation submitted in fulfilment of the
requirements for the award of the degree of
Master of Computer Science

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

APRIL 2019

DECLARATION

I declare that this dissertation entitled *"Cybersecurity Capability Maturity Model for Critical Information Technology Infrastructure among Nigeria Financial Organizations"* is the result of my own research except as cited in the references. The dissertation has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature	:	.....
Name	:	IDI MOHAMMED
Date	:	15 APRIL 2019

DEDICATION

This dissertation is dedicated to my country, whom despite financial difficulties approved my sponsorship to attend this course at this research University.

ACKNOWLEDGEMENT

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my supervisor, Dr. Siti Hajar Othman, for encouragement, guidance, critics and friendship. I am also very thankful to Dr. Anazida Binti Zainal for her guidance, advices and motivation. Without their continued support and interest, this dissertation would not have been the same as presented here.

I am also indebted to Tertiary Education Trust Fund (TetFund) of Nigeria for funding my studies. The committee of Provosts, Deans and Directors of Yobe State University, Damaturu also deserve special thanks for their nomination.

My fellow postgraduate student should also be recognised for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family member.

ABSTRACT

The effectiveness of Nigeria Cybersecurity strategy can have serious effect on the Cybersecurity stance of the country and significantly impact how well the country financial critical IT infrastructures are protected. In order to measure the strength and weaknesses of Cybersecurity, organizations can implement the develop Cybersecurity Capability Maturity Model. Cybersecurity Capability Maturity Model (C2M2) for Nigeria financial organizations as a security oriented model to determine the level of Cybersecurity strength in Nigeria financial organizations. The develop model provided five maturity levels; Nothing Exists, Basic, Progressed, Advanced, and Innovative. The goal of this research is to build up a model that will validate the level of Cybersecurity strength in Nigeria financial organizations. Seven organizations which includes Guarantee Trust Bank , United Bank for Africa, Union Bank of Nigeria, First Bank of Nigeria, Stanbic-IBTC Bank, Federal Mortgage Bank, and Polaris Bank all located in Damaturu are chosen to measure their Cybersecurity preparedness using the develop model. Fully in-structured interview are performed with IT officers in case study. Results analysis show that all organizations in case study are at Advanced level.

ABSTRAK

Keberkesanan strategi Cybersecurity Nigeria boleh memberi kesan yang serius terhadap pendirian Cybersecurity negara dan memberi kesan yang signifikan terhadap infrastruktur TI kritikal kewangan negara yang dilindungi. Untuk mengukur kekuatan dan kelemahan Keselamatan Siber, organisasi dapat melaksanakan pembangunan Model Kematangan Kemampuan Cybersecurity. Model Kematangan Keupayaan Cybersecurity bagi organisasi kewangan Nigeria sebagai model berorientasi keselamatan untuk menentukan tahap kekuatan Cybersecurity di organisasi kewangan Nigeria. Model pembangunan menyediakan lima tahap kematangan; Tiada apa-apa wujud, Asas, Kemajuan, Lanjutan, dan Inovatif. Matlamat penyelidikan ini adalah untuk membina satu model yang akan mengesahkan tahap kekuatan Cybersecurity di organisasi kewangan Nigeria. Tujuh organisasi yang merangkumi Guarantee Trust Bank , United Bank for Africa, Union Bank of Nigeria, First Bank of Nigeria, Stanbic-IBTC Bank, Federal Mortgage Bank, dan Polaris Bank semua yang terletak di Damaturu dipilih untuk mengukur kesediaan Cybersecurity mereka menggunakan model pembangunan. Temubual yang berstruktur sepenuhnya dilakukan dengan pegawai IT dalam kajian kes. Analisis keputusan menunjukkan bahawa semua organisasi dalam kajian kes berada di tahap Lanjutan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Cisco Inc define Cybersecurity as the practice of protecting network systems from digital attacks (Cisco, 2018). These attacks are usually planned at accessing, changing, or damaging sensitive data or interrupting common business processes(Cisco, 2018). Implementing efficient Cybersecurity procedures is mostly difficult today because the number of devices are more than the number of people (Cisco, 2018). Possible Cybersecurity threat nowadays as identify by Cisco Inc includes; Ransom ware, Malware, Social engineering and Phishing.

Cyberspace offer avenue for communications, Cybercriminals are lawbreakers that violet the use of Cyberspace whereas Cybersecurity is mean to protect Cyberspace. Also Cybersecurity is all about protecting data that is initiated in electronic form.

Cybercrime has become a new trend that is progressively rising as the IT continues to penetrate every aspect of our daily life and no one can guess its future (Omodunbi, Odiase, Olaniyan, & Esan, 2016). Casey consider Cybercrimes to be any illegal activities that involves computers and internet, including crimes that do not rely heavily on computers (Casey, 2005). According to (Adesina, 2017) Cybercrimes refers to any criminal activities which take place through the internet. Thus in general, Cybercrime refers to any crimes committed with the use of internet as a tools to target any victim. It consist of crimes that have been made by computers, such as dissemination of computer viruses, network intrusions, identity theft and stalking.

For any organization to achieve the security of its cyberspace against cyber crime, the organization need to evaluate the level of their Cybersecurity capability and search for their problem and solve them. Cybersecurity Capability Maturity Model (C2M2) is develop as a tool to analyze the capability maturity level of organization to protect it critical infrastructure in cyberspace.

1.2 Problem Background

The development of the information technology (IT) and the increase access to web resources has give rise to new opportunities for financial transactions, as well as those who engage in illegal activities. Financial systems, all over the globe, play fundamental roles in the development and growth of the economy (Dai, Huu, & Zoltán, 2017). The rise of, and rapid progress in, IT based systems, are primary to essential changes in how financial organizations interact with their clients. Internet banking has turn into the self-service deliverance canal that allows banks and various other business to provide information and offer services to their clients more handiness via the internet (OECD, 2008). However, the presence of bank in the cyberspace has also give chance to cyber criminals to infiltrate into customers sensitive information such as credit card information. Over twenty years, dishonest cyber space groups have continued to use the internet to commit offenses; this has suggested mixed reaction of panic in the society along with a rising unease concerning the state of cyberspace security (Barclay, 2014).

Earlier to the year 2001, the trend of cyber crime was not internationally related with Nigeria (Adesina, 2017). From then, the country has acquired an international dishonor in cyber criminality, particularly identity theft, aided through the use of the internet. Since the issue of cyber security is raising attention in the mind of Nigerians, This dissertation give an overview of Cybercrime issues in Nigeria financial organizations, identify the categories of attack against the financial institutions in Nigeria, identify who are those actors and finally explain the challenges of mitigating such criminalities and to examine current Cybersecurity

maturity models and propose a model that will be use by Nigerian financial organizations to evaluate their critical IT infrastructures applicability.

1.3 Problem Statement

Nigeria has a status for having a class of Cyber Threat actors popularly called 419 scams. These 419 scammers trick people into revealing their financial identities in other to use it and making money transfer. While these abuses have resulted in real financial damages, these Cyber Threat actors are seen as funny in the society. However, this is far from actuality and our image of Nigerian Cyber Threat actors must to be reorganize. Research carryout by professionals (Ibikunle & Eweniyi, 2013) shows that Nigeria has only 1,500 certified Cybersecurity Professionals and that the Nigeria is the most targeted nation of such attacks in Africa (Odumesi, 2014).

Strengthen the negative aspects of the problem is inadequate standards against which the Nigerian financial organizations can measure their current security status. To properly secure IT critical infrastructure and accurately report on its readiness to survive Cyberthreat, the Nigerian financial organizations need a common measurement tools in addition to NCSS standard controls and AUMMCS-1, to provide a framework for assessing and reporting Cybersecurity readiness. The Inadequate standard tools, Inadequate IT security professionals, immature cyber laws are the weakness to secure critical IT infrastructure among Nigeria financial organizations (Hassan, 2012).

To truly be effective, a Cybersecurity program must continually evolve and improve. This research focuses on addressing Inadequate standard tools by developing a Cybersecurity capability maturity model for Nigeria financial organizations.

1.4 Research Aims

The main aim of this research is to develop a Cybersecurity Capability Maturity Model (C2M2) for Nigeria financial organizations.

1.5 Research Objectives

The objectives of the research are :

(a) To identify and investigate Cybersecurity capability security domain components based on the existing Cybersecurity capability models which are relevant to the financial organizations

(b) To develop Cybersecurity capability maturity model specific for critical IT Infrastructure security in financial organizations

(c) To evaluate the maturity level of the Cybersecurity capabilities for critical IT infrastructure among Nigeria financial organizations.

1.6 Research Questions

This research is carried out based on the following questions

(a) What are the Cybersecurity capability security domain components based on the existing Cybersecurity capability models relevant to the financial organizations.

(b) How to develop the Cybersecurity capability maturity model specific for critical IT infrastructure security in financial organizations.

(c) How to evaluate the maturity level of the Cybersecurity critical IT infrastructure among Nigeria financial organizations.

1.7 Research Scope

In order to reach the objectives stated above, the scope of this study is limited to the following:

(a) The study is focusing on Cybersecurity Capability Maturity Models and specially to Nigeria finacial organizations.

(b) Research assessment is accomplished by performing a fully in-structured interview with IT Officers in order to assess the maturity level of the selected case study as mention above.

1.8 Research Significance

The main significance of this research is to contribute to the development of the Cybersecurity area that will be easy for the Nigeria Financial organizations to apply to their organization in other to evaluate their strength in protecting their critical IT Infrastructure against any Cyberthreat.

1.9 Research Structure

This dissertation is structured into six chapters. To accelerate understandings to the dissertation, a brief overview of the contents of each chapter are as follows:

Chapter 1 Introduction of the research and serves as a road map to reader through brief description on the contributions of this dissertation.

Chapter 2 Literature Review for the dissertation through previous related published papers. This includes the reviews of research related to the method and process of C2M2 development.

Chapter 3 Research Design provides the methodology used on this dissertation. The research design comprises of three phases namely; 1) Investigating the existing C2M2 2) Model Development and 3) Data Collection and Analysis.

Chapter 4 Performs three steps of development process, Model validation using Comparison with other validated models and Frequency-based selection techniques.

Chapter 5 Data analysis provide details on how respondent organizations practices are measure to find out their C2M2-level. Seven organizations responded name Union Bank, Guarantee Trust Bank, First Bank, Polaris Bank, Stanbic-IBTC Bank, United Bank for Africa and Federal Mortgage Bank of Nigeria. at the end of the analysis, recommendations to achieve the Innovative Level for responded organizations are listed.

Chapter 6 Summary of achievement, research limitations, recommendation for future work and Conclusion.

1.10 Chapter Summary

In conclusion, this chapter mainly discussed about the preliminary information about the research. Problem background and research aim is pointed out for reader to have a better understanding on the reason this research are needed. Besides that, the objectives, research scope, and research contribution are also provided to clear information on areas that been focused on this dissertation. In the next chapter (Chapter two), literature review of the thesis will be elaborate, discuss, and discussion of relevant C2M2..

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter emphasis on the discussion of related research previously performed in C2M2. However, the component of this chapter covered the following aspect: Cybersecurity issues in Nigeria, Capability Maturity Models, and From this chapter the project was built up and lastly summary of the chapter.

2.2 Cybercrime in Nigeria

In Nigeria, Cybercrime has been identified in 1996 shortly after the arrival of internet in the country (Ibikunle & Eweniyi, 2013). The Nigerian Communications Commission (NCC) says "*Nigeria now ranks third worldwide in Cybercrimes behind the UK and the U.S* ". Nigeria's Banks have become victim of e-fraud mostly due to wrong and careless organization of customers' records (Grau & Kennedy, 2014). The Cybercriminals in Nigeria are generally well-known as Yahoo-Boys.

In Nigeria, Group of all ages are engage in Cybercrimes, but particularly the young (Lazarus & Holloway, 2017). Several youth involves in Cybercrime with the aim of a money gain venture since the tools for hacking has become inexpensive to get and use them without much knowledge of cyber systems (Lazarus & Holloway, 2017).

2.2.1 Types of Cybercrime in Nigeria

Hacking, Software Piracy, Pornography and Credit Card or ATM Fraud as the most prevalent Cybercrime in Nigeria as identified by (Hassan, 2012).

(a) **Hacking:** Some Nigerian are engaged in cracking of a security codes for e-commerce database systems in order to destroy or steal data.

(b) **Software Piracy:** This refers to stealing of legally protected software. This includes illegal copying or sharing of software sources or packages examples like games. In Nigeria an Operating System Software like Windows 10, can be purchase below $5 with embedded crack software called windows loader.

(c) **Pornography:** Commonly consist of videotapes and films with high degree of sexual contents. Pornography is consider act of disruptive behavior in Nigeria.

(d) **ATM/Credit Card Fraud:** This refers to stolen Card numbers by hackers when user types the credit card number for withdrawing money using ATM card or when online transaction. Hackers have develop a key-logger software that can read key-press by user during transaction and send to then.

Furthermore, DDoS Attack, DoS Attack, Phishing, Virus Dissemination , Cyber Plagiarism, Cyber Terrorism , Cyber Stalking, Cyber Defamation are also identified as categories of Cybercrime (Hassan, 2012).

2.2.2 Courses of Cybercrime in Nigeria

Unemployment, Quest for Wealth, and Lack of strong Cybercrimes law are the major courses of cyber crimes in Nigeria as identified by (Hassan, 2012).

(a) Unemployment is the most major causes of Cybercrime in Nigeria. Nigerian Institutions graduates half-Million youth yearly and about half of this graduates cannot find jobs. This has automatically amplified the rate at which some Nigerian youths take part in hacking for their means of livelihood.

(b) Quest for Wealth is also identified as one of the causes of Cybercrime in Nigeria. You will find that a huge gap exists between the rich and the rest of the population in Nigeria. this make youth of these days are very ravenous, they are not prepared to start a small scale business thence they attempt to level up in Cybercrime for survival (Hassan, 2012).

(c) lack of strong Cyber laws: In Nigeria, there must be implementation of strict laws concerning cyber criminals. furthermore, when criminal offences occur, there is need to penalize perpetrators for the crime they've committed for the reason that cyber crimes reduces the nation's viable edge (Lazarus & Holloway, 2017).

2.2.3 Impact of Cybercrime in Nigeria

The rise of cybercrime has negative impact on Nigeria (Adesina, 2017). The Central Bank of Nigeria (CBN) reported that e-banking fraud suitcases between 2014 to 2017 is $15.475 million. According to CBN, whereas the value of fraud committed across internet has been on the decline as at 2017, the attack on mobile devises and ATM has been on the raised. From $2.03 million in 2015, the value of fraud committed across the counter falling to $1.42 million and $0.72 million in 2016 and 2017 (Idowu, 2018).

On the other hand, fraud via ATM channels has been on the increase from $1.00 million in 2015, it rise to $1.29 million in 2016 and increase further to $1.38 million in 2017. Similarly mobile payment fraud rise to $0.96 million in 2017 having dropped slightly from $0.69 million in 2015 to $0.65 million in 2016 (Hassan, 2012).

In addition to financial loss, cybercrime has brought disrepute to Nigeria from all over the world. For example, in India, it was claimed that about 90% of foreigners arrested for cybercrimes in Hyderabad city since 2013 were Nigerians (Hassan, 2012). According to Nigerian Communications Commission (NCC), says Nigeria in 2017 ranks third worldwide in cybercrimes following the United Kingdom and the United States. There are three basic types of online frauds through which Nigerians commit the cybercrime - lottery, jobs, and matrimonial scams (Olayemi, 2014).

2.2.4 Problems of combating Cybercrime in Nigeria

The troubles obstructing the success of law enforcement agencies in fighting cybercrime in Nigeria as identified by (Olayemi, 2014) are:

(a) There is no existing law to sufficiently deal with challenges of technology with regard to security violates and Cybercrime. Therefore, absence of legislation to tackle Cybercrime makes it unfeasible to prosecute criminals.

(b) The lack of a national network gateway for Nigeria had made it hard to segregate and resolve the real hacking.

(c) Lack of standard national Cybersecurity framework for the control of country presence in space to manage Cybersecurity-related risk.

(d) Insufficient statistics on the level and degree of cybercrime events in the country.

(e) The Nigerian Police is the top-level law enforcement agency in the country, their investigation unit personnel are not Cybersecurity experts and Insufficient cyber forensic laboratory within any Division of the Nigerian Police to investigate and analyze cybercrime related issues.

2.3 Nigeria Cybersecurity Framework

In an effort to combat cybercrime in Nigeria, the Nigeria Federal Ministry of Information and Communication in December, 2014 officially release National Cybersecurity Strategy (NCSS), which consist of short, medium and long term mitigation strategies covering all national priorities, addressing the nation's cyber risk coverage (MICT, 2014).

The Central Bank of Nigeria which is the government regulatory body for all financial organizations in the country on June 25th, 2018 have published risk-based Cybersecurity framework and guidelines for Commercial banks and e-payment service in Nigeria (CBN, 2018). According to CBN, due to the recent increase in the number and sophistication of cyber-security threats against Nigeria financial organizations, it has become mandatory for these organizations to strengthen their cyber defenses if they are to remain safe and sound.

Risk-based Cybersecurity framework is the official Cybersecurity assessment tools use by Nigeria organizations to measure their strength against Cyberattacks.

2.4 Critical Infrastructure

The term critical infrastructure describes assets that are vital for the operational of the general public and economy. It includes telecommunication, Banking/Finance electricity generation; transmission and distribution, water distribution and transport system (Schukat, 2014). Telecommunication play a vital role to financial organizations. Telecommunications over the years in Nigeria is one of the economic back bone of the country's income generation.

Study confirmed that competitions in the telecommunication has progress performance over control provision around the world, resulting in faster increase of capacity , low pricing, quality of service and wider access (Eshun, 2009).

Economic growth policies in the developed countries progressively more include telecommunications as a critical component of the economic (Eshun, 2009).

2.4.1 Critical Infrastructure Sector Identification

An organized and rigorous method must be applied to list any subject as of critical infrastructure sectors as depicted in Figure 2.1 (Singh, Gupta, & Ojha, 2014). The process involved three different stages: discovering important literature on the subject, suggesting sessions with experts, and face-to-face interrogation with experts.

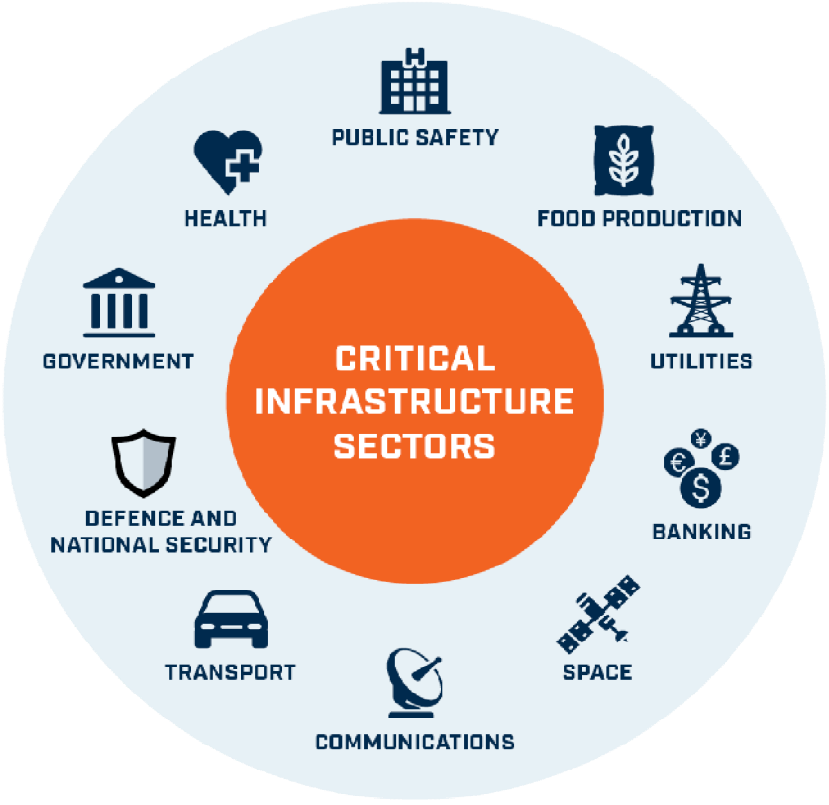


Figure 2.1 Critical Infrastructure Sectors (Singh et al., 2014)

2.4.2 Critical Infrastructure Protection

Protecting cyber-enabled critical infrastructure against malicious attacks is a main challenge for the operators of those facilities (Depoy et al., 2005). László (2009) identify National Infrastructure Protection Plan and systematic approach for critical infrastructure protection. International policies and practices sketch out the phases of how critical infrastructure should be protected.

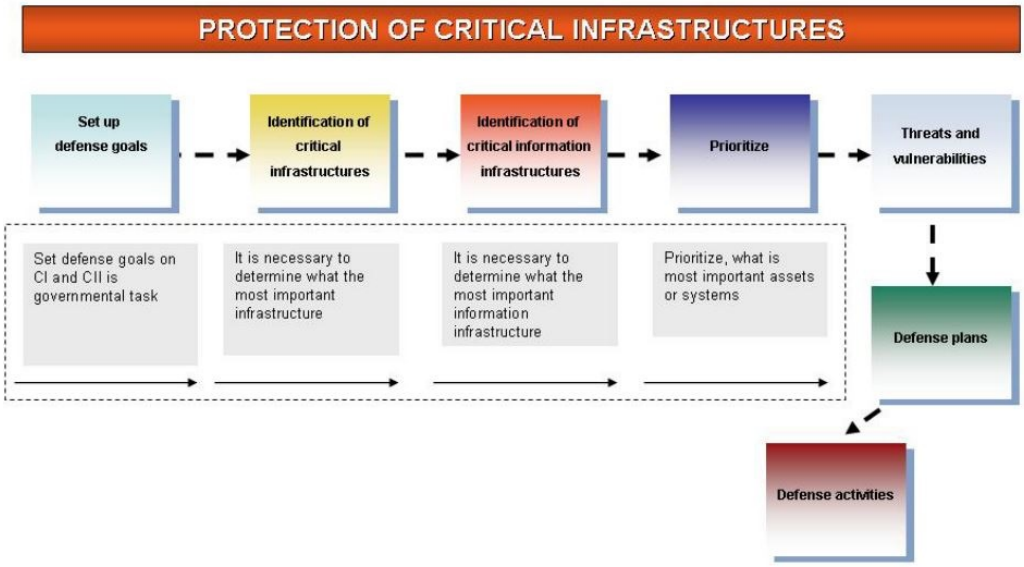


Figure 2.2 Phases of Critical Infrastructure Protection (László, 2009)

Figure 2.1 show that protection of critical information infrastructures build up different phases. Every phases include a methodology, nevertheless the systematic approach is not misplaced. Further visible approach is in the United States National Infrastructure Protection Plan (NIPP). As show in Figure 2.3.

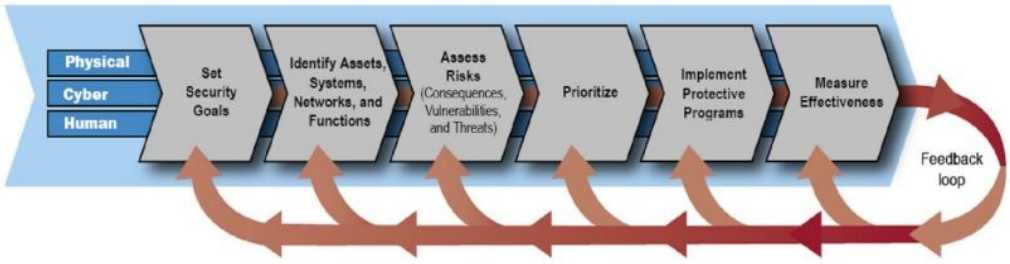


Figure 2.3 National Infrastructure Protection Plan framework (László, 2009)

2.5 Overview of Maturity Model

A maturity model is a set of characteristics, attributes, indicators or patterns that signify the capability and the sequence in a particular discipline (Rea-Guaman, Sanchez-Garcia, Feliu, & Calvo-Manzano, 2017). A maturity model, therefore, provides a point of reference which an organization can assess their level current practices, processes and methods, and establish objectives and priorities for improvement.

The software development industry has been widely adopting the usage of maturity models since 1993 when the Capability Maturity Model (CMM) for software was first introduced twenty years ago (De Bruin, Freeze, Kaulkarni, & Rosemann, 2005). CMM was the beginning of the many research for maturity models and since then there are many attempts to apply the framework in other application domain(De Bruin et al., 2005).

The assessment of an organization's capabilities in an application domain or specific process can be analyzed using maturity model (Röglinger, Pöppelbuß, & Becker, 2012). There are several levels in a maturity model and process of maturity ins form through these levels of logical path in the maturity model. The organization's capabilities in specific application domain as well as process are indicated through the maturity levels in the maturity model (Röglinger et al., 2012).

Organization can use the maturity model to analyze the level of the their maturity and use the result as a guide and aim to achieve a higher maturity level for the organization, or to use it to control the organization's progress as well as assuring their Cybersecurity capabilities(White, 2011).

As stated earlier, there is sequence of level in maturity models. The sequence of levels in maturity models start from an initial state and the level ends in a mature state(U.S. Department of Energy, 2014a). The level of maturity of an organization can be determined using maturity model by evaluating elements that has been selected and rating the capabilities of the elements. Actions needed to be done to

increase the level of maturity for the elements (Hansen, 2016). The total number of levels in a maturity models might differ from each model and the more level a maturity level have, the more difficult it will be to provide a description for each level (U.S. Department of Energy, 2014a). The complexity of the maturity model will also increase as the number of levels increases. (Angel, Feliu, Calvo-Manzano, & Sanchez-Garcia, 2017).

The theories on the evolvement of the capabilities of an organization that is done in a step-by-step approach together with desired, predictable or logical maturation path can be represented using maturity models(De Bruin et al., 2005). The current level of maturity of an organization represents the organization's capabilities in terms of specific processes or application domains which includes Cybersecurity or IT management (Wendler, 2012).

According to Wendler (2012), the progress of the levels in maturity is sequential by nature and needs to occur hierarchically. With the end goal to achieve the highest level of maturity, an organization needs to meet the preconditions for each the previous maturity levels in the maturity model, this is why maturity models are also known as stage models, stage-of-growth models or stage theories model (De Bruin et al., 2005). The maturity model is used as a scale to measure the criteria and characteristics needed to achieve each maturity level on its path to achieve the highest maturity level (Becker, Knackstedt, & Pöppelbuß, 2009). The criteria needed in order to evaluate the capabilities can be processes, application targets or conditions and they need to be measurable (Wendler, 2012). CMM usually have five logical stages in which an organization manages its processes. The Stage representation of CMM is as presented in Figure 2.4.

2.5.1 Importance of using Maturity Models

It is important to use maturity models in order to evaluate the capabilities of certain elements in organization. The maturity models can be used as a benchmark for their

security. By using maturity models, organizations can identify the gaps in a certain elements and come out with plans in order to improve the gaps.

It is also important to use maturity models in order to define the organization's current state or their future state and the attributes the organization must achieve in order to attain the future state (Butkovic & Caralli, 2013).

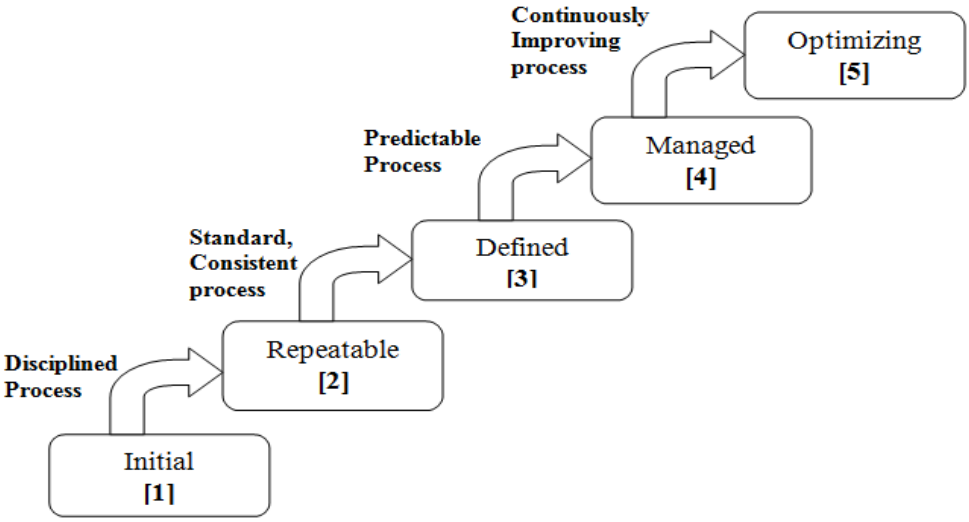


Figure 2.4 Capability Maturity Model Version 1.1 (Paulk, Curtis, Chirssis, & V., 1993)

2.5.2 Limitations of Maturity Models

The maturity models have some limitations which are the maturity models might not be able to measure accurately which may give the user a data that is inaccurate. As previously clarified, the maturity models might give an inaccurate data. Therefore, not only does it increase the cost of the implementation but the benefit is actually reduce, for example the process that has been improved based on a wrong maturity models results might not be compliance to the overall process.

An organization who achieved a higher level of maturity for the elements they are evaluating might feel more confidence with their current plan but in actuality the confidence is put at the wrong place if the result is wrong (Mehravari, 2001).

According to Röglinger, Pöppelbuß, & Becker (2012) maturity models has lack of empirical foundation and will oversimply reality. They said that some maturity models might disregard the number of other possibility result maturation paths. They also belived that istead of focusing on the elements which can actualy assist in the evolution and changes, they chose to focus on the series levels' predefined 'end state' (Röglinger et al., 2012).

Also due to the nature of being step-by-step and over-simplified, maturity models fails to understand the complexities of the domain which the maturity is use on (De Bruin et al., 2005). Therfore, maturity models will not provide meaniful information for its users(De Bruin et al., 2005).

2.6 Types of Maturity Models

According to Mehravari (2014) identify three types of maturity models, namely; Progression Maturity Models, Capability Maturity Models (CMM), and Hybrid Maturity Models.

2.6.1 Progression Maturity Models (PMM)

This refers to Simple succession or scaling of an attribute, prototype, follow or characteristic (Mehravari, 2001). In PMM (as shown in Figure 2.5), Levels explain upper states of accomplishment, progression, completeness, or advancement. Higher levels may be illustrated as "tool-enabled" while lesser level may be describe as "primitive" . An example Maturity Progression Model for Counting is shown in Figure 2.5.

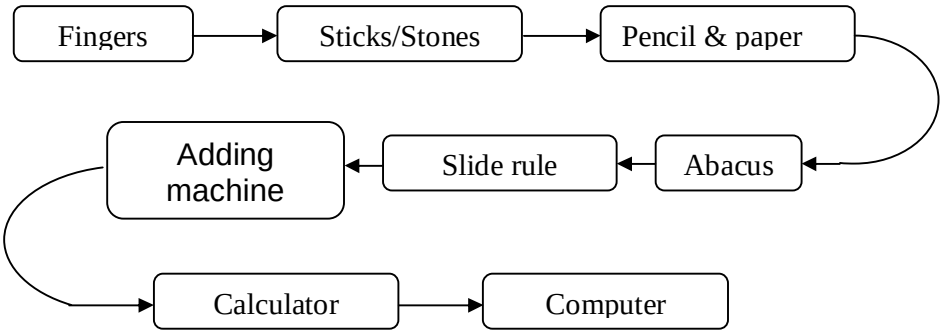


Figure 2.5 Maturity Progression for Counting (Mehravari, 2001)

2.6.2 Capability Maturity Models (CMM)

Capability Maturity Model (CMM) was developed in 1989 as an approach for improving the software process by Software Engineering Institute (SEI) of Carnegie-Mellon University (Kaur, 2014). The fundamental motivation behind utilizing CMM is to assess the maturity of software development processes and to recognize the main practices that are vital to enhance these processes. In addition, the levels in a CMM show state of organizational maturity essential to process maturity such as

$$unplanned \rightarrow managed \rightarrow defined \rightarrow quantitatively\ managed \rightarrow optimized$$

The basic maturity approach of the CMM framework can be relevant to other domains like Cybersecurity capability maturity model (Butkovic & Caralli, 2013). The benefit of Capability Maturity Model as identify by Mehravari (2001) includes; affords for estimate of core competencies, Provides for thorough measurement of capability and provide a pathway to quantitative estimate. While the drawback includes; at times it is complicated to comprehend and use (i.e. high implementation cost), it may not transform into genuine results and finally, likely false sense of achievement (Mehravari, 2001).

2.6.3 Hybrid Maturity Models (HMM)

This model can be formed by overlaying features of the progressive model with capability characteristics from capability maturity models (Saco, 2008). Example of hybrid maturity models are Smart Grid Interoperability *Maturity Model* (SG-IMM) and Electricity Subsector Cybersecurity *Capability Maturity Model* (ESC2M2)(Saco, 2008).

This type of model reproduces conversions between levels that are alike to a capability model but architecturally use the patterns, characteristics, attributes, or indicators of a progression model (Caralli, Knight, & Montgomery, 2012).

The benefit of hybrid maturity model is that, it provide the thoroughness of a capability maturity model while taking up the ease of use and clarity of progression models (Caralli et al., 2012). While the drawback of this model as indentify by Mehravari (2001) includes “Maturity” theory is approximated (i.e., not as accurate as CMM) and combination of qualities with institutionalizing uniqueness at each level can be unreasonable.

2.7 Components of Maturity Models

Regardless of the difference among maturity models, the majority of them have some similarities in terms basic structure. This structure is essential as it provides a connection between objectives, assessments, and best practices, and it aid associations between present capabilities and progress roadmaps by connecting them to business goals, standards, and other criteria.

2.7.1 Levels

levels signify the intermediary states in a maturity model (Butkovic & Caralli, 2013). Depending on the structural design, a model's level may express a progressive step, or they may characterize an expression of capability or other attribute that can be precise by the model (Butkovic & Caralli, 2013). Levels are significant as they stand for the measurement part of a maturity model, and if the scaling is wrong or partial, the model itself may not be able to validated or generate poor or conflicting results (Butkovic & Caralli, 2013).

2.7.2 Domains

Model domains basically describe the capacity of a maturity model (Butkovic & Caralli, 2013). In CMMs, the domains are regularly (but optional) referred to as process areas as they are a set of processes that make up a larger process (Butkovic & Caralli, 2013). Model such as the CMMI, might have a representation that requires a prescribed progression through the domains to achieve the intended result (U.S. Department of Energy, 2014a).

2.7.3 Attributes

Attributes stand for the core content of the model and are grouped by level and domain (Butkovic & Caralli, 2013). They are normally based on experimental practice, principles, or other expert knowledge and can be expressed as characteristics, indicators, practices, or processes. In CMMs, attributes are essential for supporting process enhancement regardless of the process being modelled (Butkovic & Caralli, 2013).

Cybersecurity Capability Maturity Models (C2M2) was drive from CMM, Some selected C2M2 relevant to area of study will be discuss in the next section.

2.8 Cybersecurity Capability Maturity Model (C2M2)

In 1987, Humphrey develop a capability maturity model (CMM) for software quality evaluation (Humphrey, 1988). This model is improve by U.S department of energy for the assessment of Cybersecurity capabilities for power-grid comprised of a maturity model and evaluation (U.S. Department of Energy, 2014a).

According to (Le & Hoang, 2016) this model has been modified for cyber security for three reasons. Firstly, security models based on CMM have been applied with sensible successes for many fields (Le & Hoang, 2016). Secondly, CMM provide a full managing process for cyber security (Le & Hoang, 2016). Finally, it can also be expanded to cover numerous security aspects or domains (Le & Hoang, 2016).

Recently, CMM has been adopted for securing many important services such as health, education, e-government and e-commerce. In critical public infrastructure such as transportation, water supply and electricity (P. D. Curtis & Mehravari, 2015).

City Group in 2000 develop improved version of CMM title *"Information Security Evaluation Maturity Model"* (ISEM) (Le & Hoang, 2016). Until now, a dozen of CMMs has been developed and applied to diverse area and organizations of various size.

2.8.1 Information Security Management Maturity Model(ISM3)

ISM3 was developed by ISM3 group in 2007 with focus on measuring, specifying, implementing and enhancing process oriented information security management systems (Karokola, Kowalski, & Yngström, 2011). ISM3 has five levels namely; Undefined, Defined, Managed, Controlled and Optimized.

The advantage of ISM3 is that it recognized organizational practices as a security issue. Furthermore, it is based on earlier cyber security standards and practices like ISO 9000, and ISO 17799/27001 (Karokola et al., 2011). In this model, Cybersecurity measurement is based on evaluating activities, effectiveness and quality.

2.8.2 Cybersecurity Capability Maturity Model (C2M2)

This Model was developed by Carnegie Mellon University and U.S. Department of energy. The first version was published in 2014 (Angel et al., 2017).

The model have four maturity levels (i.e no practices, initial practices, stable practices and practices stabilized) which are applied in parallel to each model domain. According to (Angel et al., 2017) the model regarded as descriptive rather than prescriptive.

2.8.3 Systems Security Engineering Capability Maturity Model (SSE-CMM)

This Model was developed by US National Security Agency (NSA). It has three versions, the first version was released in 1996 and the last version(3.0) was published in 2003 (Angel et al., 2017).

The SSE-CMM was design with five maturity levels, namely ; Performed Informally, Planned and Tracked, Well Defined, Quantitatively Controlled, and Continuously Improving (Angel et al., 2017). The model is considered a general model not focus more on Cybersecurity, but it is a model that has been adapted for that reason due to the lack of models particular to Cybersecurity (Angel et al., 2017).

2.8.4 Community Cyber Security Capability Maturity Model (CCSMM)

Developed in 2006 by the University of San Antonio, Texas (White, 2011). the CCSMM is design to address the requirements of U.S communities to develop a practicable and sustainable plan for Cybersecurity. The model defines five maturity levels; Initial, Established, Self-assessed, Integrated, and Vanguard (White, 2011).

The model identifies the characteristics of communities and states as their Cybersecurity programs mature (Angel et al., 2017). It uses the community knowledge of Cybersecurity, Cybersecurity training and education, security policies and procedures and sharing of information within and outside organizations in order to evaluate their strength against Cyberattack.

2.8.5 African Union Maturity Model for Cybersecurity (AUMMCS)

Developed in 2015 by Centre for Cyber Security University of Johannesburg, South Africa to concentrate on 2014 African Union Convention on Cyber Security and Personal Data Protection (Von Solms, 2015). The Model is developed to signify to Member States how well compares to the requirements of the Convention.

This model have four Maturity Levels (MLs); Nothing exists at all, Very Basic position, Progressed position, and Stable position (Von Solms, 2015). The model does not cover the full Convention, it can be seen as a very simplified result and the model can be viewed as partial.

2.8.6 Federal Financial Institutions Examination Council Capability Maturity Model (FFIEC-CMM)

Federal Financial Institutions Examination Council1 (FFIEC) in 2015 developed the Cybersecurity Assessment Tool (Assessment), on behalf of its

members, to aid organizations identify their risks and determine their Cybersecurity maturity (FFIEC, 2015a). The Assessment provides businesses with a repeatable and considerable practice to advance Cybersecurity preparedness over time.

The Model have five maturity levels; Baseline, Evolving, Intermediate, Advanced, and Innovative(FFIEC, 2015a). The model match organization's maturity level to the organization's inherent risk.

2.9 Comparison of Cybersecurity Capability Maturity Models

According to the review by (Angel et al., 2017), the C2M2 that are mainly revealed in scientific research papers are Cybersecurity Capability Maturity Model(C2M2), Systems Security Engineering Capability Maturity Model (SSE-CMM), Community Cyber Security Maturity Model (CCSMM) and National Initiative for Cybersecurity Education – Capability Maturity Model (NICE).

This research explore more C2M2 that relevant to Cybersecurity and area of study in addition to C2M2, SSE-CMM, CCSMM and NICE. These include ISM3, African Union Maturity Model for Cyber Security (AUMMCS), and Federal Financial Organizations Examination Council Capability Maturity Model (FFIEC-CMM). The identify models will be compare based on developers, year of last revision, Cybersecurity orientation, maturity level, Application area and documentation for implementation. Table 2.1 shows the value of the features for each of the models.

The comparative study shows that the C2M2s have a major similarity. The main variation is identified in the application sector which they are designed for.

Figure 2.6 Comparison of Cybersecurity Capability Maturity Models

Model/Features	C2M2	SSE-CMM	CCSMM	NICE	ISM3	AUMMCS	FFIEC-CMM
Developers	US Department of Energy	US National Security Agency	University of San Antonio US	US National Security Agency	ISM3 Group	Center for Cyber Security University of Johannesburg	US Federal Financial Institutions Examination Council
Year of last revision	2014	2003	2006	2014	2007	2015	2015
Cybersecurity oriented	Yes	No	Yes	Yes	Yes	Yes	Yes
Maturity level	4	5	5	3	5	4	5
Application sector	Energy & Fuels	Security Engineering	Communities	Workforce	Organization	African Union Members' State	Financial Industries
Documentation	Medium	High	Low	Medium	Medium	Low	High

The most important results identify in the evaluation are the following:

(a) SSE-CMM and C2M2 are considered more universal

(b) SSE-CMM and FFIEC-CMM models offer more information for the accurate categorization and valuation of their practices, and offer more comprehensive guiding principle to advance the maturity indicators levels.

(c) AUMMCS cover the area of study both provide low categorization and guidelines to achieve the maturity indicators level.

(d) Only FFIEC-CMM focused directly to financial organizations, and it provide details documentation and guidelines. Therefore, FFIEC-CMM will be the best to adopted by the Nigeria financial organizations.

2.10 Identification of Research Gap

From the literature review above there is no model that is specific to Nigeria financial sector, despite they are victims of the cyber-war. The Risk-based Cybersecurity framework and guidelines for commercial banks and e-payment service uses currently is a risk-based framework not a capability model. The research expected contribution after thorough analysis of the existing C2M2 is to propose a C2M2 for Nigeria financial organizations. However, all the existing models cannot be adopted as they are limited to their own scope which might not suite Nigeria financial organizations operations.

The gap found in the previous models are mostly lack of consistency of components and even if the components are the same the operations or testimonials within the components varies with one another to suite their need, therefore adoption completely is very difficult without modification. Also in the existing Models, testimonials are tested with conclusions.

From these limitations the researcher was motivated to conduct this research so that suitable model will be proposed to the Nigeria financial organizations that suite their operational needs.

2.11 Chapter Summary

This Chapter in brief reviews based on previous research regarding the specifically C2M2. Numerous sub topics have been mentioned in this chapter to cover all of the needs and requirement of the dissertation. Cybersecurity issues in Nigeria, critical infrastructure, financial organizations as critical infrastructure, Capability Maturity Modes, Cybersecurity Capability Maturity Models, and comparison of the existing C2M2s review are presented. Research Design that provides the methodology used on this dissertation will be presented in the next chapter(Chapter three).

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

In chapter 2, problems as well as required backgrounds and related literature to this dissertation has been discussed in details. In this chapter, the justification of the research methodology based on a systematic research framework will be discuss. There will be stages in the research framework and each stage will be assessed and used as a roadmap to obtain the objectives of this dissertation. Therefore, choosing the right methodology is important to ensure that this dissertation is done in a proper manner.

3.2 Research Methodology

Research methodology explains how a research will be accomplished. This means that what data should be compressed and how the data will be balanced, established and analyze. It can also be referred to as the progression and measures that will be tailing in order to collect the required data which will properly serve the research objectives. The primary objective of the research is to develop Cybersecurity Capability Maturity Model (C2M2) for Critical Infrastructure among Nigeria financial organizations. To meet this objective the researcher study various C2M2. There are two types of research method available, qualitative and quantitative. For the research subject, both methods for the research organization will be employed. Also, web sources were utilized to discover the data that was not straightforwardly accessible from distributed papers.

3.3 Research Framework

Research framework is used to diagrammatically explain the specific steps used during this research. Basically, it is used as a guideline by investigators to zoom-in on the scope of research.

Figure 3.1 reveals the research framework used in this research. It reveal the methodology steps implemented in this research. The study is spitted into three phases. Phase 1 is based on study and investigates the Cybersecurity issues in Nigeria as well as existing Cybersecurity Capability Maturity Models (C2M2) and recognizing different levels of this model. Phase II is to develop C2M2 for the case study. Finally, Phase III contains data collection, analysis and organizing findings and discussion of results.

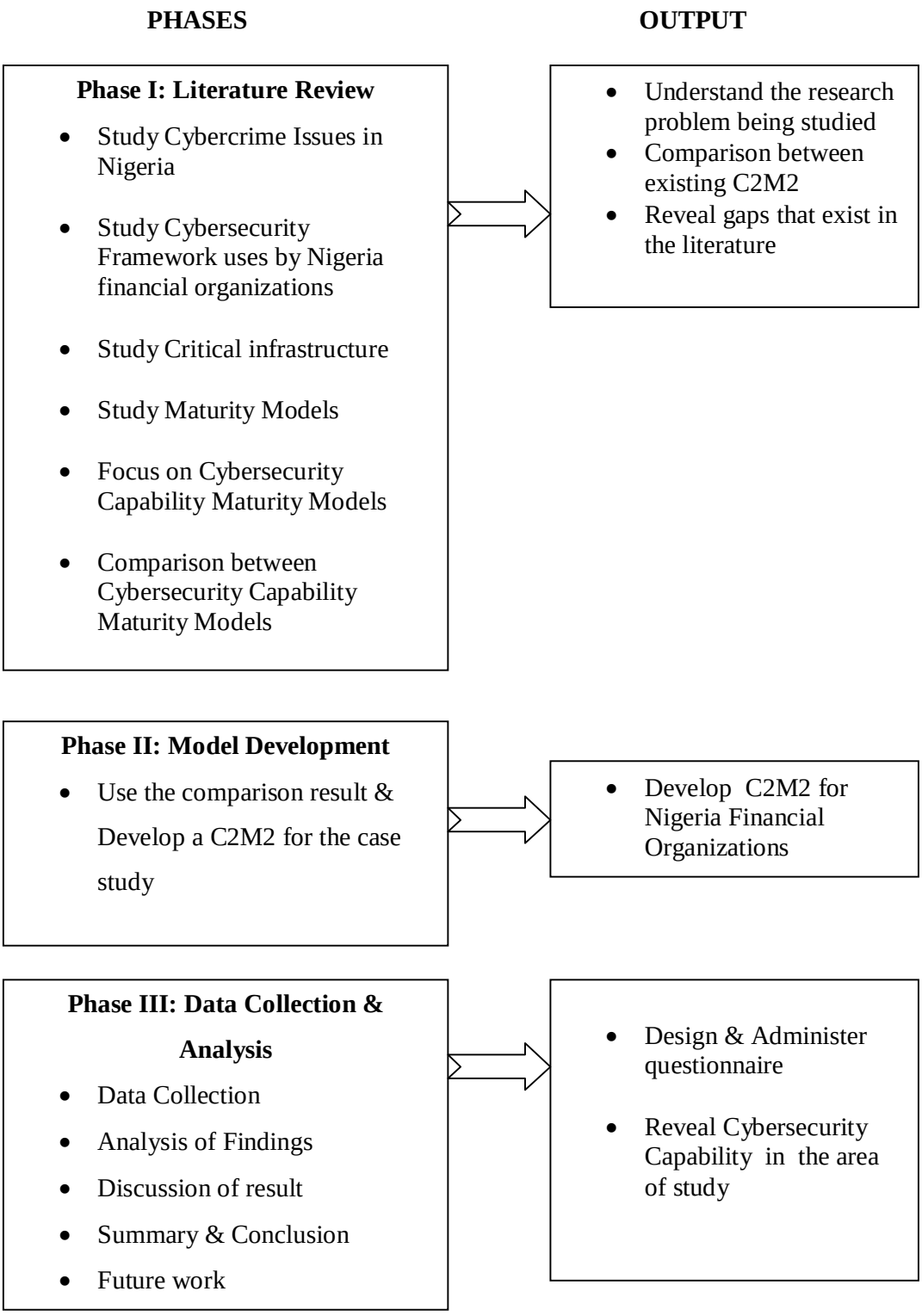


Figure 3.1 Research Framework

3.4 Research Design

The research will be accomplished by three major phases. The following subsections will express each phase briefly.

3.4.1 Phase I: Investigating the existing C2M2

During this phase considering that is the primary phase, studying literature review and relevant research started. It has taken into consideration the most useful topics to identify and determine the data of Chapter two and the type of information that requires assisting in appreciate this research. The literature review which utilized in this research is concentrated on the relevant issues with: Cybercrime issues in Nigeria, Cybersecurity Framework uses by Nigeria financial organizations, Critical infrastructure, Maturity Models, Cybersecurity Capability Maturity Models, and Comparison between Cybersecurity Capability Maturity Models.

In order to find related literature, several resources are utilized such as; Google scholar, Science Direct, Springer Link, Emerald, IEEE explore and so on. related website, special forums, articles are used as well.

3.4.2 Phase I: Model Development

To be able to develop C2M2 for case study, fourteen relevant C2M2s will be utilize systematically during the development process. The development process will consist of design and validation. Seven out of fourteen C2M2s will be use for development while the other seven will be use for validation. To validate the propose model, Comparison with other models and frequency-based selection techniques will be utilize.

3.4.3 Phase III: Data Collection and Analysis

Uses of questionnaire and locking through existing Cybersecurity capability maturity model documentations will be utilize as techniques of data collection for this dissertation.

3.4.3.1 Questionnaire

The research will utilize questionnaires to gather primary data from organizations due the sensitivity of this research. Few organization were willing to concede a meeting . The first set questionnaires was distributed on 19th November, 2018. These went to one government bank (Central Bank of Nigeria) and four commercial Banks (Guarantee Trust Bank, Polaris Bank, First Bank of Nigeria, First City Monument Bank, and Diamond Bank) all banks located in Damaturu, Nigeria and the distribution was done manually and using email. At the time of this report Seven banks responded namely; Union Bank, First Bank, Federal Mortgage Bank of Nigeria, Guarantee Trust Bank, Stanbic IBTC Bank, United Bank for Africa and Polaris Bank (See Appendix A for respondent details).

3.4.3.2 Cybersecurity Capability Maturity Model Documentations

Several authors documentations on C2M2 served as key sources of my secondary research data. These includes Department of Homeland Security Cybersecurity Capability Maturity Model White Paper (US Department of Homeland Security, 2014), Comparative Study of Cybersecurity Capability Maturity Models (Angel et al., 2017), Maturity Models in Cybersecurity: a systematic review (Rea-Guaman et al., 2017), Capability maturity model, version 1.1 (Paulk et al., 1993), A Maturity Model for part of the African Union Convention on Cyber Security (Von Solms, 2015), and FFIEC Cybersecurity Assessment Tool (FFIEC, 2015a).

3.4.3.3 Data Analysis

Data analysis is the process of inspecting, cleaning, transforming, and modeling data with the objective of discovering useful information, arriving at conclusions, and supporting the decision making process (Merriam, 2009). The Microsoft Excel application was very useful during this sorting and presentation of data for analysis. The closed ended answer from the respondent were converted to digit ranging from 1 to 5, average score was measure for each domain and capability maturity level is obtained.

3.5 Chapter Summary

This chapter provides a guide for the researcher to follow in carrying out the study. This chapter discussed the research methodology designed for this particular dissertation which comprised of three phases. First phase study and review investigation with the previous literature. Second phase emphasize on development of C2M2 and finally, the third phase reveal how data will be collected and analyze.

CHAPTER 4

DESIGN AND IMPLEMENTATION

4.1 Introduction

This chapter comprises of four main sections. The first second and third section consist of three logical phases of activities namely 1) Phase-1 Panning, 2) Phase-2 Design, 3) Phase-3 Validation, and 4) Evaluation.

In the Phase I, literature review of the existing C2M2 were conducted. In chapter two, seven C2M2 which include C2M2 (Christopher et al., 2014), SSE-CMM (Ferraiolo, 2000), CCSMM (White, 2011), NICE (US Department of Homeland Security, 2014), ISM3 (Vicente, 2007), AUMMCS (Von Solms, 2015) and FFIEC-CMM (FFIEC, 2015b) have been systematically studied. Comparison of the existing Cybersecurity Capability Maturity Models was presented in chapter two table 2.1. AUMMCS which is covering the area of study was found not have adequate components to be able to address the current Cybersecurity challenges.

In the Phase II, drafted C2M2 for case study was verified, issues were cited and corrected before proceeding to next Phase. The last Phase validate the Propose Model against other valid C2M2s using comparison with other models and frequency based selection techniques. Propose model concept that do not pass degree of confidence after validation were drop, while concepts with acceptable degree of confidence were re-organize and final C2M2 drafted. The development process are graphically present in Figure 4.1.

Evaluation section discus Procedure and documentation on how to use the final model are outline. Graphical evaluation flow chart are provide for each domain.

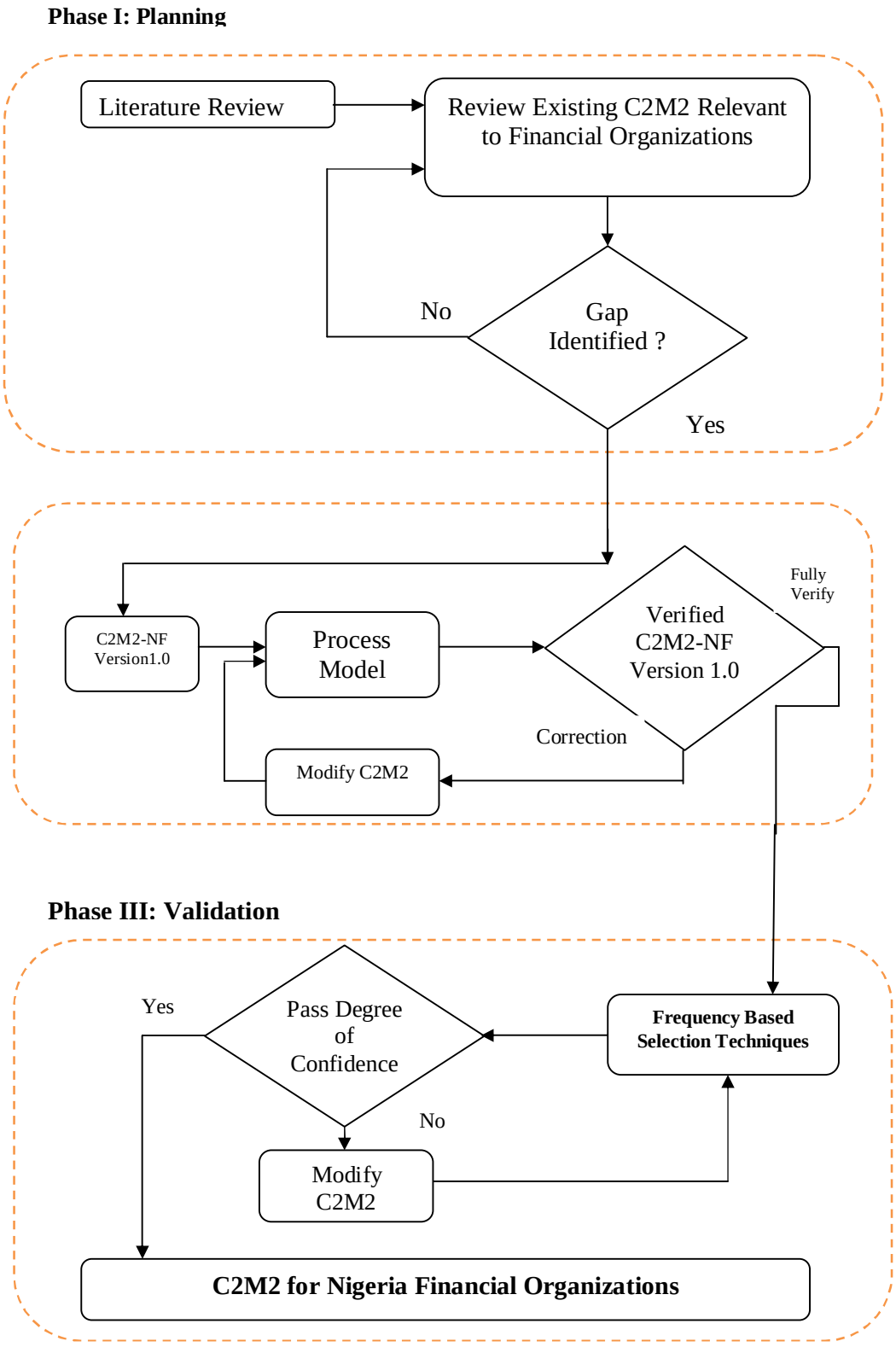


Figure 4.1 C2M2-NF Development Process

4.2 Phase I: Planning

This phase is considered as the first step to this development process. The activities involve in this phase include: planning of the model, indentifying domains and maturity level indicators (MiLs). Table 4.1 present the propose model concepts with regard to their original sources. To be able to draft the first version of model, five maturity models (Table 4.1) were compared carefully with the aim of identifying strengths in them that could be adopted. Also seven Maturity model were use to validate the drafted model.

Table 4.1 Sources of Model Components

Component	**Source**
Nothing exists	African Union C2M2 (Von Solms, 2015)
Basic	African Union C2M2 (Von Solms, 2015)
Progressed	African Union C2M2 (Von Solms, 2015)
Advanced	Federal Financial Examination Council (FFIEC, 2015b)
Innovative	Federal Financial Examination Council (FFIEC, 2015b)
Legal Regulations	Developing a Cyber Counterintelligence Maturity Model for Developing Countries(Jaquire & Von Solms, 2017)
Governance	Developing a Cyber Counterintelligence Maturity Model for Developing Countries(Jaquire & Von Solms, 2017)
Security Culture	Cyber Security Management Model for Critical Infrastructure (Limba, Plėta, Agafonov, & Damkus, 2017)
Incidence Management	Cyber Security Management Model for Critical Infrastructure (Limba et al., 2017)
Technology Management	Cyber Security Management Model for Critical Infrastructure (Limba et al., 2017)
Access Control	Cyber Security Management Model for Critical Infrastructure (Limba et al., 2017)
Risk Management	Federal Financial Examination Council (FFIEC, 2015b)

4.3 Phase II: Design

In this section the selected components presented in Table 4.1 are use to develop the propose model. A graphical representation of the proposed model will is presented in Figure 4.2 and Figure 4.3. The propose model will be referred to as C2M2-NF Version 1. This is to enable validation of the C2M2-NF V1. using the Comparison with other models and the Frequency-based selection techniques. After the validation, final version of C2M2-NF will be presented.

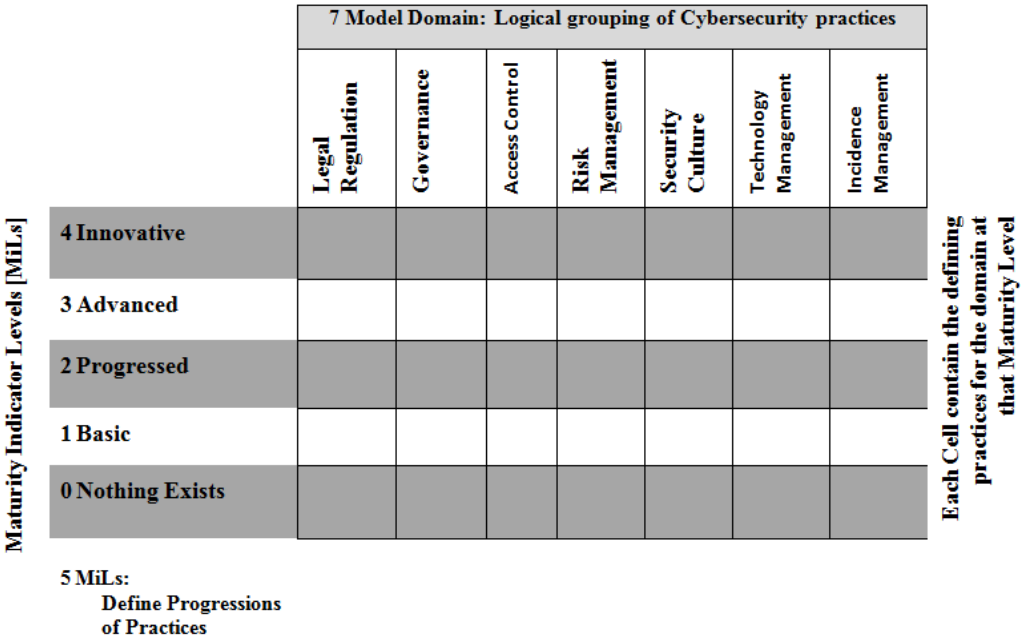


Figure 4.2 C2M2-NF Version 1.0 (Block View)

Figure 4.2 presented the block view of the propose model, its show all the adapted component presented in Table 4.1. Figure 4.4 will present the C2M2-NF V1.0 in tree view, this is to allow all activities associated with the seven (7) domains presented in Figure 4.2 to be include in the model structure.

The Maturity Indicator Levels(MiLs) are significant as they stand for the measurement part of a maturity model, and if the scaling is wrong or partial, the model itself may not be able to validated or generate poor or conflicting results (Butkovic & Caralli, 2013). The propose model adapted five (5) MiLs as presented in Table 4.1. The oval-view of adapted MiLs are presented in Figure 4.3.

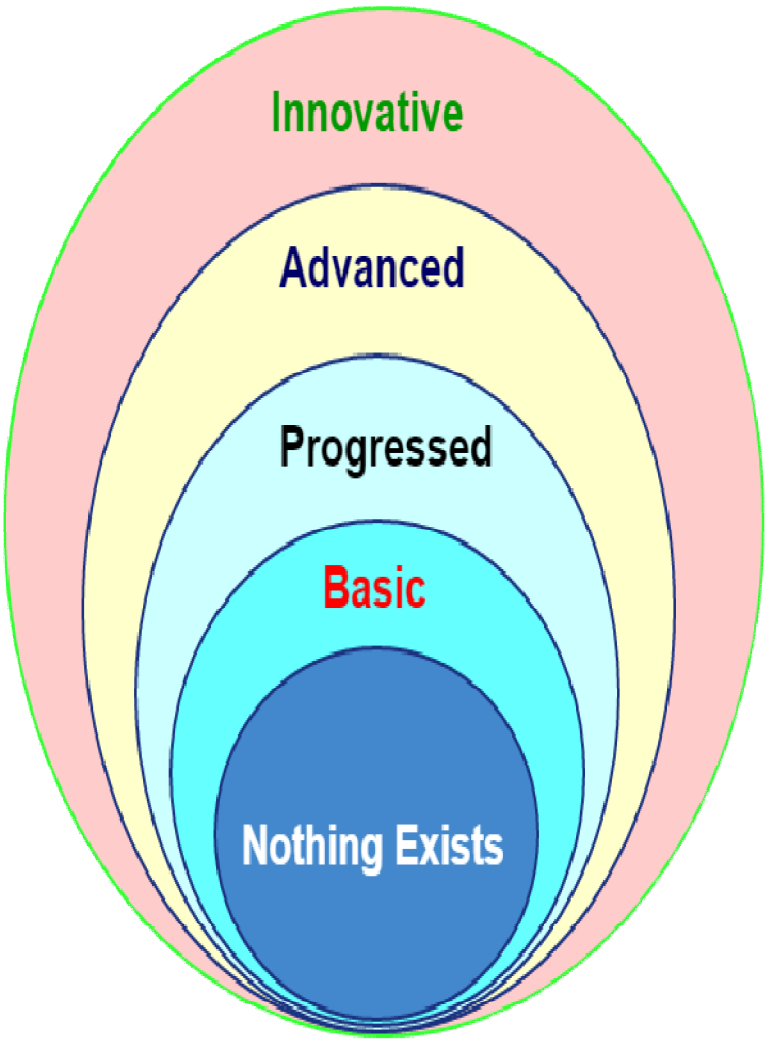


Figure 4.3 Maturity Indicator Levels (MiLs) of C2M2-NF V1.0

Model domains basically describe the capacity of a maturity model. Each domains comprise of appraisal factors and contributing segments. Within each component, declarative statements that express activities behind the assessment factor at each maturity level.

Domains are refers to as objectives according to (Von Solms, 2015). The C2M2-NF V1.0 is develop with seven (7) domains as presented in Figure 4.2. Figure 4.4 also present the testimonials associated with each domain C2M2-NF V1.0.

Table 4.2 Description of C2M2-NF V1 Maturity Indicator Levels (MiLs)

Level	Caption	Description
MiLs-0	Nothing Exists	Indicates that a specific practice in C2M2 process is not being performed. If MiLs-0 is assigned, no further assessment of maturity indicator is performed because incomplete processes are not institutionalized. (Von Solms, 2015)
MiLs-1	Basic	MiLs-1 Performed indicates that a specific practice in C2M2 process is being performed. Once MiLs-1 is attained, testimonial related to higher MiLs can be asked to determine if the practice is institutionalized to higher degrees of maturity. (Von Solms, 2015)
MiLs-2	Progressed	MiLs-2 means that there is sufficient and substantial support for the existence of the practice. (Von Solms, 2015)
MiLs-3	Advanced	MiLs-3 means that there is significant increases for the existence of the practice. (FFIEC, 2015b).
MiLs-4	Innovative	MiLs-4 indicates that there is an update review of practice on timely basis. (FFIEC, 2015b)

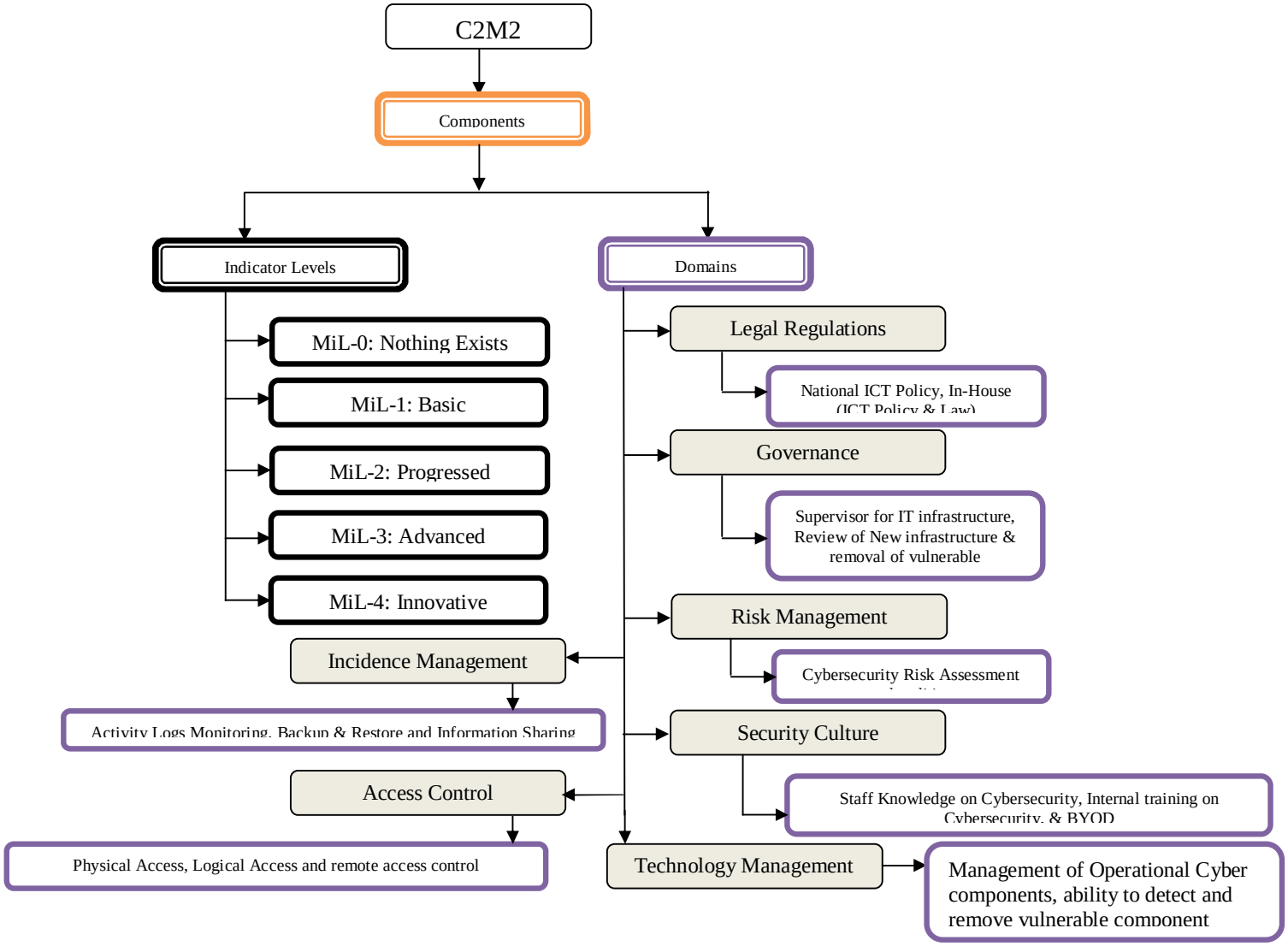


Figure 4.4 C2M2-NF Version 1.0 (Tree View)

4.4 Phase III: Validation of C2M2-NF V1.0

Validation is used to ensure that the Model concepts are appropriate to be used in an organization or not appropriate to be applied. Validation is the task of demonstrating that the C2M2-NF V1.0 model is a realistic representation of the actual system. Model validation can ensure that its composition, judgment and causal relationships and the representation of the domain are satisfactory for the intended purpose (Othman, 2012). As stated in the first chapter, the concepts will be validated using *Comparison against other models* and *Frequency-Based Selection* Technique.

The concepts in this model include both domains and maturity level indicators. In the validation process, C2M2-NF V1.0 was validated against seven (7) valid models using the above mentioned techniques. The next section explain in details how C2M2-NF V1.0 concepts to be validated. Using *Comparison to Other Models* technique, concept of the C2M2-NF V1.0 model being validated are compared to concept of other (valid) models. *Frequency based selection* is a an attribute choice technique that evaluates the significance of entity concepts in the model developed (Othman, 2012). Their usage will enable a frequency count of the individual C2M2-NF V1.0 concepts.

4.4.1 C2M2-NF V1.0 against C2M2 for IT Services (P. Curtis, Mehravari, & Stevens, 2015).

C2M2 for IT Services focuses on the evaluation of Cybersecurity practices related with typical enterprise IT services, along with allied enabling IT assets and the platform in which they operate. It is based on a combination of existing Cybersecurity Capability Maturity Models.

As presented in Figure 4.5, the model is organized with ten (10) domains and four (4) maturity indicator levels. Table 4.3 present Support of the concepts in C2M2-NF V1.0 by C2M2 for IT Services. The supported concepts include Maturity Indicator Levels (Nothing Exists, Basic, Progressed and Advanced) and the domain

concepts (Risk Management, Governance, Security Culture, Access control and Incidence Management).

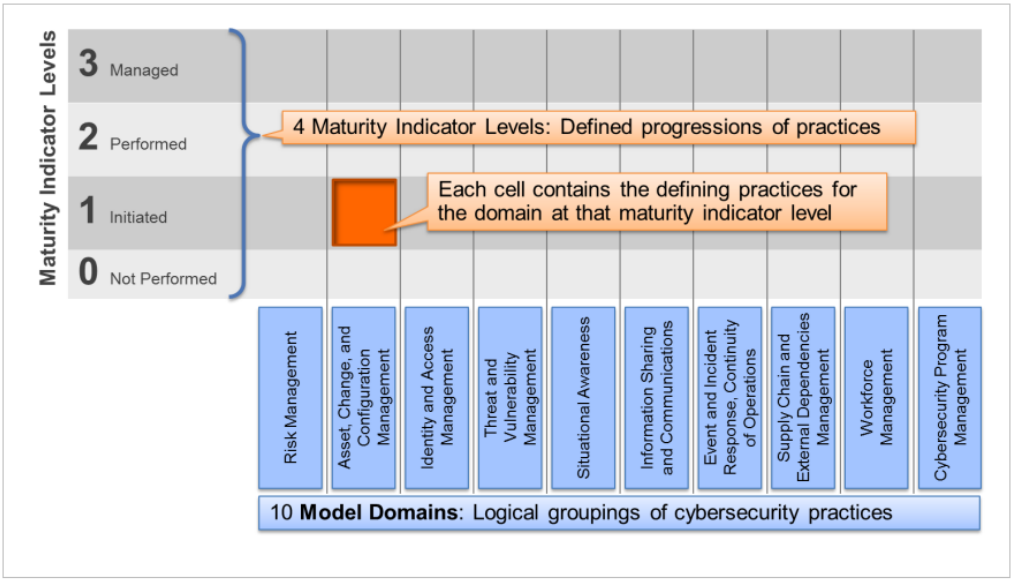


Figure 4.5 C2M2 for IT Services (P. Curtis et al., 2015)

Table 4.3 Support of the concepts in C2M2-NF V1.0 by C2M2 for IT Services

C2M2 for IT Services	C2M2 for IT Services Description	C2M2-NF V1.0	C2M2-NF Description
Not Performed	Practices are not performed	Nothing Exists	Indicates that a specific practice in C2M2 process is not being performed
Initial	Initial practices are performed but may be ad hoc	Basic	Performed indicates that a specific practice in C2M2 process is being performed
Performed	Practices are more complete or advanced than at Initial	Progressed	There is sufficient and substantial support for the existence of the practice
Manage	Practices are more complete or advanced than at Performed	Advanced	There is significant increases for the existence of the practice
Risk Management	Establish, operate, and maintain an enterprise Cybersecurity risk management program.	Risk Management	This is the organizations capability to accurately identify risks that are rising around the organization and ensuring they have the professional practices to control the impact of these risks.
Threat and Vulnerability Management	Establish and maintain plans, procedures, and respond to Cybersecurity threats and vulnerabilities	Governance	Supervisor for IT infrastructure, Review of New infrastructure & removal of vulnerable infrastructure
Supply Chain & External Dependency	Establish and maintain controls to manage the Cybersecurity risks associated with services and assets that are dependent on external entities		

Situational Awareness	Establish and maintain activities and technologies to collect, analyze, alarm and alert, present, and use operational and Cybersecurity information	Security Culture	Staff Knowledge on Cybersecurity, Internal training on Cybersecurity, & BYOD
Identity and Access Management Purpose	Create and manage identities for entities that may be granted logical or physical access to the organization's assets.	Access Control	Physical Access, Logical Access and remote access management control
Information Sharing and Communications	Establish and maintain relationships with internal and external entities to collect and provide Cybersecurity information, including information about threats and vulnerabilities	Incidence Management	Activity Logs Monitoring, Backup & Restore and information sharing among operational staff

4.4.2 C2M2-NF V1.0 against C2M2-NF Version 1.0 against Electrical Subsector Cyber Security Capability Maturity Model (ES-C2M2) (Adler, 2013).

ES-C2M2 is an extended CERT CMM called the Electrical Subsector Cyber Security Capability Maturity Model, or ES- C2M2 (Adler, 2013). ES-C2M2 defines ten domains of Cyber Security performance: Risk, Asset, Access, Threat, Situation, Sharing, Response, Dependencies, Workforce, and Cyber.

Each domain in ES-C2M2 encompasses several objectives. Each objective, in turn, consists of a set of Cyber Security practices. ES-C2M2 is reasonably uncomplicated, an organization can classify the practices vital for each objective in the related ES-C2M2 domains to progress towards the needed maturity levels. ES-C2M2 confirm Nothing Exists, Basic, Progressed, Advanced, Risk Management, Governance, Access control and Incidence Management.

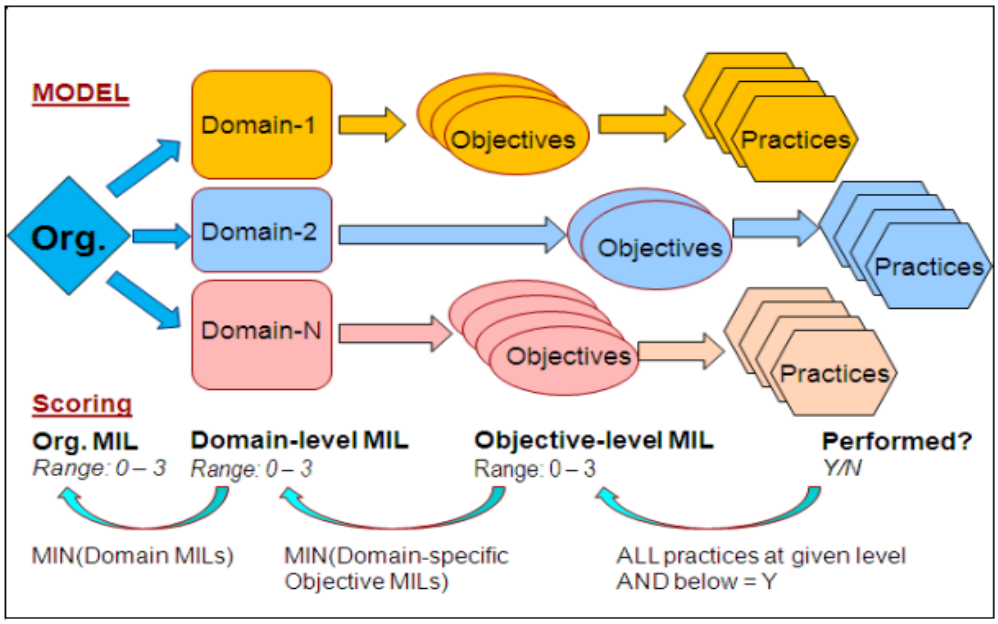


Figure 4.6 Electrical Subsector Cyber Security Capability Maturity (Adler, 2013)

Table 4.4 Support of the concepts in C2M2-NF Version 1.0 by ES-C2M2

ES-C2M2	ES-C2M2 Description	C2M2-NF V1.0	C2M2-NF Description
MiL0	No Practices are being performed	Nothing Exists	Indicates that a specific practice in C2M2 process is not being performed
MiL1	Initial practices are performed but may be ad hoc	Basic	Performed indicates that a specific practice in C2M2 process is being performed
MiL2	Practices are performed against a documented plan	Progressed	There is sufficient and substantial support for the existence of the practice
MiL3	Domain activities are further institutionalized and managed	Advanced	There is significant increases for the existence of the practice
Risk	Establish Cybersecurity Risk Management Strategy	Risk Management	This is the organizations capability to accurately identify risks that are rising around the organization and ensuring they have the professional practices to control the impact of these risks.
Asset	Manage Asset Inventory, Configuration, changes and activities	Governance	Supervisor for IT infrastructure, Review of New infrastructure & removal of vulnerable infrastructure
Threat	Identify and Respond to Threats	Incidence Management	Activity Logs Monitoring, Backup & Restore and information sharing among operational staff
Sharing	Share Cybersecurity information		
Access	Establish and maintain identities and Control access	Access Control	Physical Access, Logical Access and remote access management control

4.4.3 C2M2-NF V1.0 against Systems Security Engineering Capability Maturity Model (SSE-CMM) (Roger, Dorathy, James, Gloria, & Kerinia, 1995)

The SSE-CMM was design with six maturity levels, namely ; not Perform, Performed Informally, Planned and Tracked, Well Defined, Quantitatively Controlled, and Continuously Improving (Angel et al., 2017). The model is considered a general model not focus more on Cybersecurity, but it is a model that has been adapted for that reason due to the lack of models particular to Cybersecurity (Angel et al., 2017). Except legal regulation, all other concept of C2M2-NF Version 1.0 confirm by SSE-CMM.

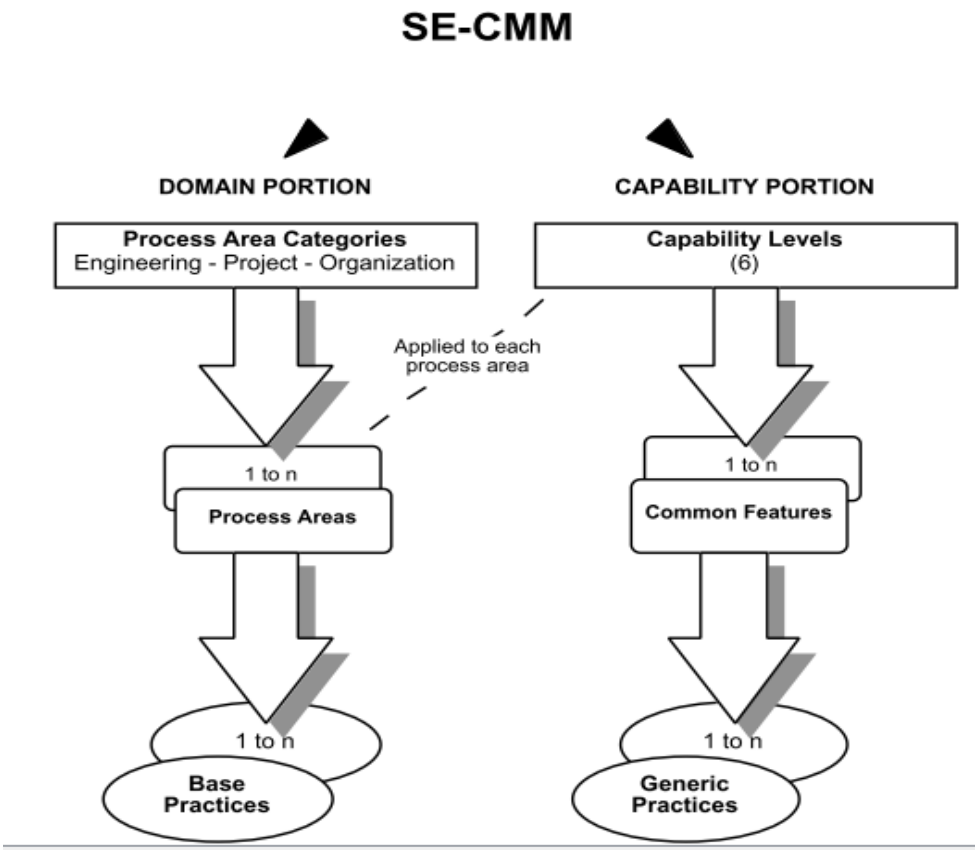


Figure 4.7 Systems Security Engineering Capability Maturity Model (Roger et al., 1995)

Table 4.5 Support of the concepts in C2M2-NF Version 1.0 by SSE-CMM

SSE-CMM	ES-C2M2 Description	C2M2-NF V1.0	C2M2-NF Description
Not Performed Description	There is general failure to perform the base practices in the process area.	Nothing Exists	Indicates that a specific practice in C2M2 process is not being performed
Performed Informally	Base practices of the process area are generally performed.	Basic	Performed indicates that a specific practice in C2M2 process is being performed
Planned and Tracked Description	Base practices of the process area are planned and tracked	Progressed	There is sufficient and substantial support for the existence of the practice
Quantitatively Controlled	Performance is objectively managed, and the quality of work products is quantitatively known.	Advanced	There is significant increases for the existence of the practice
Continuously Improving Description	The organization is able to continuously improve its process by gathering quantitative data from performing the defined processes and from piloting innovative ideas and technologies.	Innovative	Indicates that there is an update review of practice on timely basis.
Manage Risk	An organized, analytic process to identify what can go wrong, to quantify and assess associated risks, and to implement/control the appropriate approach for preventing or handling each risk identified	Risk Management	This is the organizations capability to accurately identify risks that are rising around the organization and ensuring they have the professional practices to control the impact of these risks.
Monitoring	Monitor, Control Technical Effort and Coordinate with Suppliers	Governance	Supervisor for IT infrastructure, Review of New infrastructure & removal of vulnerable infrastructure
		Incidence Management	Activity Logs Monitoring, Backup & Restore and information sharing among operational staff
Knowledge	Provide Ongoing Skills and Knowledge	Security Culture	Staff Knowledge on Cybersecurity, Internal training on Cybersecurity, & BYOD

4.4.4 C2M2-NF V1.0 against Global Cyber Security Capacity Centre (GCSCC) Cybersecurity Capability Maturity Model (C2M2)

The Global Cyber Security Capacity Centre-C2M2 was develop by Oxford University Global Cyber Security Capacity Centre in 2014. With the mission to increase the scale and effectiveness of cyber security capacity building, both within the UK and internationally(GCSCC, 2014) . This Model considered cyber security capacity in dimensions; devising cyber policy and strategy, encouraging responsible cyber culture within society, building cyber skills into the workforce and leadership , creating effective legal and regulatory frameworks and controlling risks through organization, standards and technology (GCSCC, 2014).

The Model comprises of five levels of maturity in the Capability Maturity Model; Start-up, Formative, Established, Strategic and Dynamic. Graphical representation was not provided in the model documentation. Global Cyber Security Capacity Centre (GCSCC) Cybersecurity Capability Maturity Model (C2M2) support all concepts in C2M2-NF Version 1.0 except Advanced maturity indicator level.

Table 4.6 Support of the concepts in C2M2-NF Version 1.0 by Global Cyber Security Capacity Centre-C2M2

GCSCC-C2M2	GCSCC-C2M2 Description	C2M2-NF V1.0	C2M2-NF Description
Start-up	At this level either nothing exists, or it is very embryonic in nature.	Nothing Exists	Indicates that a specific practice in C2M2 process is not being performed
Formative	Some features of the indicators have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined - or simply "new"	Basic	Performed indicates that a specific practice in C2M2 process is being performed
Established	The elements of the sub-factor are in place, and working	Progressed	There is sufficient and substantial support for the existence of the practice
Dynamic	At the Dynamic level, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances.	Innovative	Indicates that there is an update review of practice on timely basis.
Risk Management	Risk management procedures are used to create a response plan able to produce a repeatable course of action in the event of an incident.	Risk Management	This is the organizations capability to accurately identify risks that are rising around the organization and ensuring they have the professional practices to control the impact of these risks.

Corporate Governance, Knowledge and Standards	Management know what their strategic assets are, have put specific measures in place to protect them, and know the mechanism by which they are protected.	Governance	Supervisor for IT infrastructure, Review of New infrastructure & removal of vulnerable infrastructure
Incidence Response	Emergency response capacity is clearly identified and distributed, with framework funding	Incidence Management	Activity Logs Monitoring, Backup & Restore and information sharing among operational staff
Cyber culture and society	Cybersecurity best practices are widely known across organization at all level	Security Culture	Staff Knowledge on Cybersecurity, Internal training on Cybersecurity, & BYOD
Legal and regulatory frameworks	Legislation protecting the right of individuals and organizations in the digital environment has been adopted.	Legal Regulations	This comprises orders with the purpose of forcing organizations to protect their critical IT Infrastructure against cyberattacks.

4.4.5 C2M2-NF V1.0 against Community Cyber Security Maturity Model(CCSMM)

The CCSMM is design to address the requirements of U.S communities to develop a practicable and sustainable plan for Cybersecurity. The model defines five maturity levels; Initial, Established, Self-assessed, Integrated, and Vanguard (White, 2011).

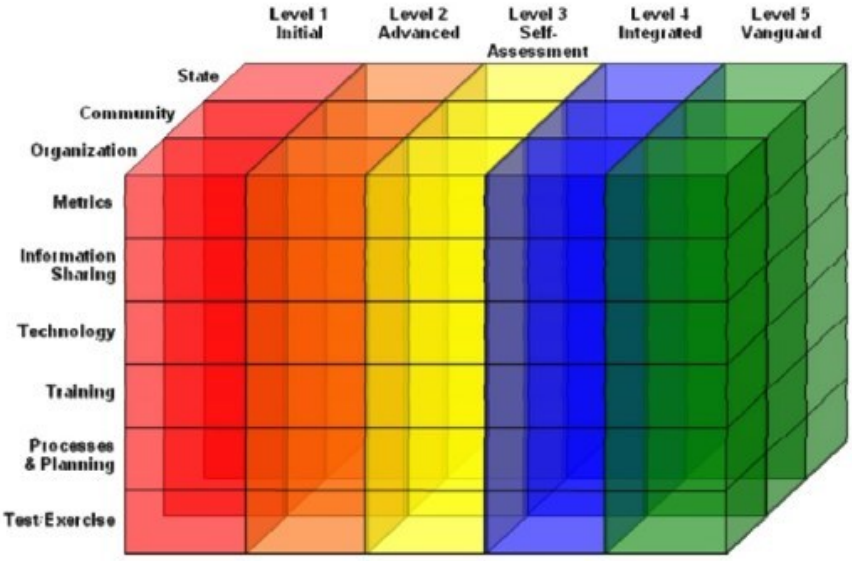


Figure 4.8 Community Cyber Security Maturity Model (White, 2011)

The Community Cyber Security Maturity Model uses the community knowledge of Cybersecurity, Cybersecurity training and education, security policies and procedures and sharing of information within and outside organizations in order to evaluate their strength against Cyberattacks. CCSMM support only two domain concept and drop level-0 MiLs.

Table 4.7 Support of the concepts in C2M2-NF Version 1.0 by Community Cyber Security Maturity Model(CCSMM)

CCSMM	CCSMM Description	C2M2-NF V1.0	C2M2-NF Description
Initial	Minimal Cybersecurity awareness, information sharing and little inclusion of Cybersecurity into continuity of operations plan.	Basic	Performed indicates that a specific practice in C2M2 process is being performed
Advanced	Initial evaluation of Cybersecurity policies and procedures	Advanced	There is significant increases for the existence of the practice
Self-Assessed	Autonomous tabletop Cybersecurity exercises with assessments of information sharing, policies and procedures.	Progressed	There is sufficient and substantial support for the existence of the practice
Vanguard	Fully integrated fusion/analysis centre, combining all source physical and cyber information. create and disseminate near real world picture	Innovative	Indicates that there is an update review of practice on timely basis.
Training	Individual knowledge within the community need to know how to secure their own systems, otherwise they may be taken over and used in a distributed denial of service attack on the community itself	Security Culture	Staff Knowledge on Cybersecurity, Internal training on Cybersecurity, & BYOD
Policy	policies, processes, and procedures that will be part of cyber security program.	Legal Regulation	This comprises orders with the purpose of forcing organizations to protect their critical IT Infrastructure against cyberattacks.

4.4.6 C2M2-NF V1.0 against Capability Maturity Model and metrics framework for Cyber Cloud Security (CMMCCS) (Le & Hoang, 2017)

The CMMCCS address cloud computing Cybersecurity issues (Le & Hoang, 2017). It provides the guidance to support the organizations implement and enhance their cyber security capabilities on cloud system (Le & Hoang, 2017). CSCMM outline twelve (12) domains; Governance, Risk, and Compliance management ,

Audit and Accountability , Identities and Access Management, Data and Information protection, Incident response, Infrastructure and facilities security, Human resource management, Security awareness and training, Cloud application security, Virtualization and isolation, Interoperability and portability, and finally Cloud connections and communication security.

CMMCCS comprises four (4) maturity levels range from level 0, level 1, level 2 and level 3. No further description to were given to these maturity levels. CMMCCS confirm all domain concepts except legal regulation.

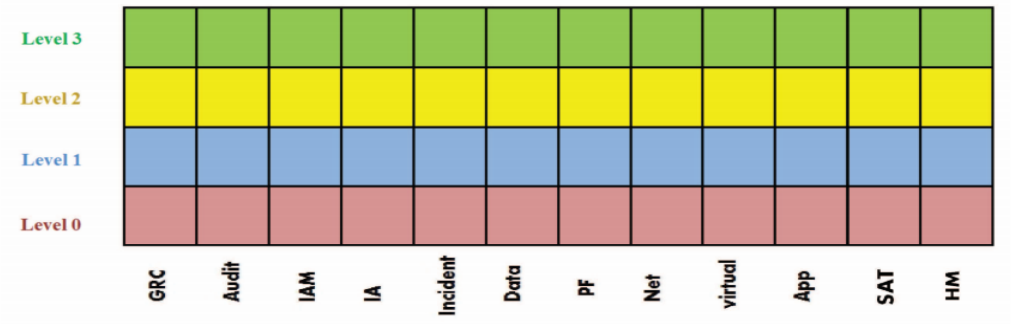


Figure 4.9 Capability Maturity Model and metrics framework for Cyber Cloud Security (CMMCCS) (Le and Hoang, 2017).

Table 4.8 Support of the concepts in C2M2-NF Version 1.0 by Capability Maturity Model and metrics framework for Cyber Cloud Security (CMMCCS)

CMMCCS	**CMMCCS** Description	C2M2-NF V1.0	C2M2-NF Description
Governance, Risk, and Compliance management	This concept focuses on establishing, operating, and maintaining cyber security risk management programs that identify, analyse, and mitigate cyber security risk to the organization	Risk Management	This is the organizations capability to accurately identify risks that are rising around the organization and ensuring they have the professional practices to control the impact of these risks.
		Governance	Supervisor for IT infrastructure, Review of New infrastructure & removal of vulnerable infrastructure
Incident response	The major concerns in Incident response are related to establishing and maintaining plans, procedures, and technologies to detect, analyse, and respond to cyber security incidents and events	Incidence Management	Activity Logs Monitoring, Backup & Restore and information sharing among operational staff

Security awareness and training	This domain aims to create a culture of security and ensure the ongoing suitability and competence of all personnel	Security Culture	Staff Knowledge on Cybersecurity, Internal training on Cybersecurity, & BYOD
Identities and Access Management	This domain ensures authentication, authorization, and administration of identities.	Access Control	Physical Access, Logical Access and remote access management control
Infrastructure and facilities security	The security of an IT system also depends on the security of its physical infrastructure and facilities		

4.4.7 C2M2-NF V1.0 against Cybersecurity Capability Maturity Model (C2M2) (Christopher et al., 2014)

The C2M2 focuses on the implementation of Cybersecurity practices associated with the information technology (IT) and operations technology (OT) assets and the environments in which they operate (Christopher et al., 2014).

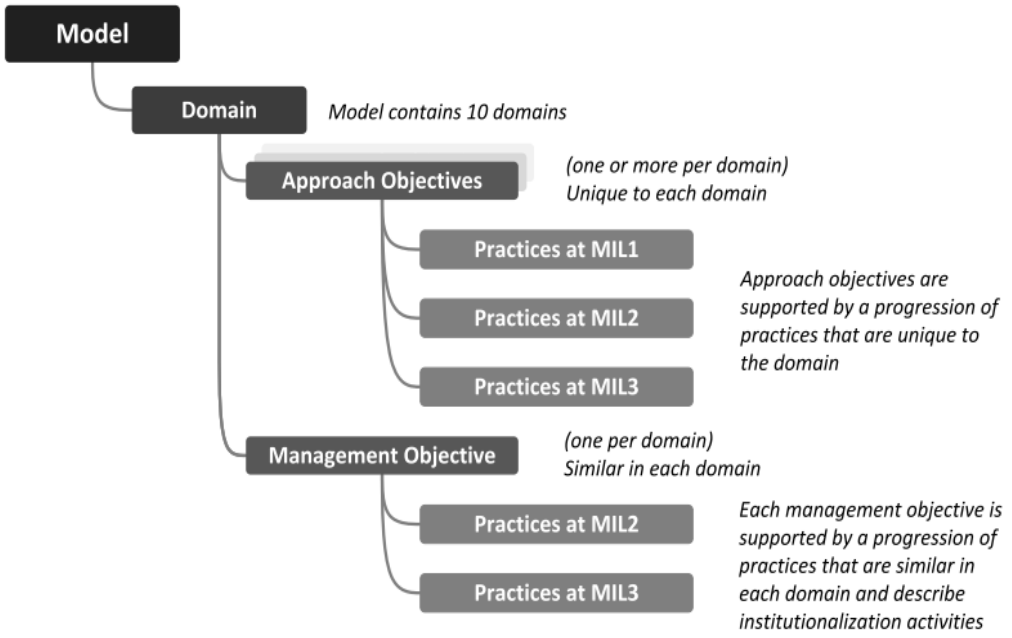


Figure 4.10 Cybersecurity Capability Maturity Model (C2M2) (Christopher et al., 2014)

The C2M2 also comprises of four maturity levels (i.e. no practices, initial practices, stable practices and practices stabilized) which are applied in parallel to each model domain. According to (Angel et al., 2017) the model regarded as descriptive rather than prescriptive. The Model focus on ten (10) sets of Cybersecurity practises.

Table 4.9 Support of the concepts in C2M2-NF Version 1.0 by Cybersecurity Capability Maturity Model (C2M2)

C2M2	**C2M2 Description**	**C2M2-NF V1.0**	**C2M2-NF Description**
MIL0	The model contains no practices for MIL0	Nothing Exists	Indicates that a specific practice in C2M2 process is not being performed
MIL1	MIL1 contains a set of initial practices	Basic	Performed indicates that a specific practice in C2M2 process is being performed
MIL2	The practices in the domain are being performed according to a documented plan	Progressed	There is sufficient and substantial support for the existence of the practice
MIL3	At MIL3, the activities in a domain have been further institutionalized and are now being managed	Advanced	There is significant increases for the existence of the practice
Risk Management	Cybersecurity risk is defined as risk to organizational operations (including mission, functions, image, and reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information, IT, and/or OT.	Risk Management	This is the organizations capability to accurately identify risks that are rising around the organization and ensuring they have the professional practices to control the impact of these risks.
Workforce Management	developing plans for key Cybersecurity workforce roles (e.g., system administrators) to provide appropriate training, testing, redundancy, and evaluations of performance.	Governance	Supervisor for IT infrastructure, Review of New infrastructure & removal of vulnerable infrastructure
Event and Incident Response, Continuity of Operations	A Cybersecurity incident is an event or series of events that significantly affects or could significantly affect critical infrastructure.	Incidence Management	Activity Logs Monitoring, Backup & Restore and information sharing among operational staff
Situational Awareness	Situational awareness involves developing near-real-time knowledge of a dynamic operating environment.	Security Culture	Staff Knowledge on Cybersecurity, Internal training on Cybersecurity, & BYOD

4.5 Estimating Degree of Confidence of C2M2-NF Version 1.0

Degree of Confidence (DoC) is a real number in the range [0,1] that expresses the reliability of the estimate (Wood, 2018). DoC is calculate using the formula [1]. The obtain results will be refers to as score in the process.

$$\text{Degree of Confidence (DoC)} = \frac{Frequency\ of\ ceoncept}{Total\ Valid\ Models} \text{ x } 100 \quad - \quad - \quad - \quad - \quad [1]$$

Table 4.11 present the summary of comparison of C2M2-NF V1.0 against other valid models discuss in the Comparison against other models. The higher their score, the more significant the concepts are considered to the C2M2-NF V1.0 domain. Concepts that have a low down score are likely for deletion. Table 4.10 define five (5) categories of concepts based on their DoC values.

Table 4.10 Degree of Confidence Result interpretation

Doc Score (Range in %)	**DoC Result**
70-100	Very Strong
50-69	Strong
30-49	Moderate
11-29	Mild
0-10	Very Mild

(Othman, 2012)

As demonstrated in Table 4.3, very strong DoC is assigned to concepts that appear frequently in the valid models, whereas Very Mild DoC is other end of the scale. Table 4.11 shows DoC values all C2M2-NF concepts.

Table 4.11 Comparison of C2M2-NF V1.0 against other valid models with frequency and DoC values

C2M2-NF V1.0 Components	Valid Models							Frequency	DoC
	C2M2 for IT Service(P. Curtis et al., 2015)	ES-C2M2 (Adler, 2013)	SSE-CMM (Roger et al., 1995)	GCSCC-C2M2 (GCSCC, 2014)	CCSMM (White, 2011)	CMMCCS (Le & Hoang, 2017)	C2M2 (Christopher et al., 2014)		
Noting exists	√	√	√	√			√	5	71
Basic	√	√	√	√	√		√	6	85
Progressed	√	√	√	√	√		√	6	85
Advanced	√	√	√		√		√	5	71
Innovative			√	√	√			3	43
Legal Regulation				√	√		√	3	43
Governance	√	√	√	√		√	√	6	85
Technology Management				√				1	14
Incidence Management	√	√	√	√		√	√	6	85
Access Control	√	√						2	28
Risk Management	√	√	√	√		√	√	6	85
Security Culture	√		√	√	√	√	√	6	85

From Table 4.11, result of DoC show that two component of C2M2-NF V1.0 are liable to be drop. The components are Technology Management and Access Control. Figure 4.11 present graphical frequency of C2M2-NF V1.0 components and their strength.

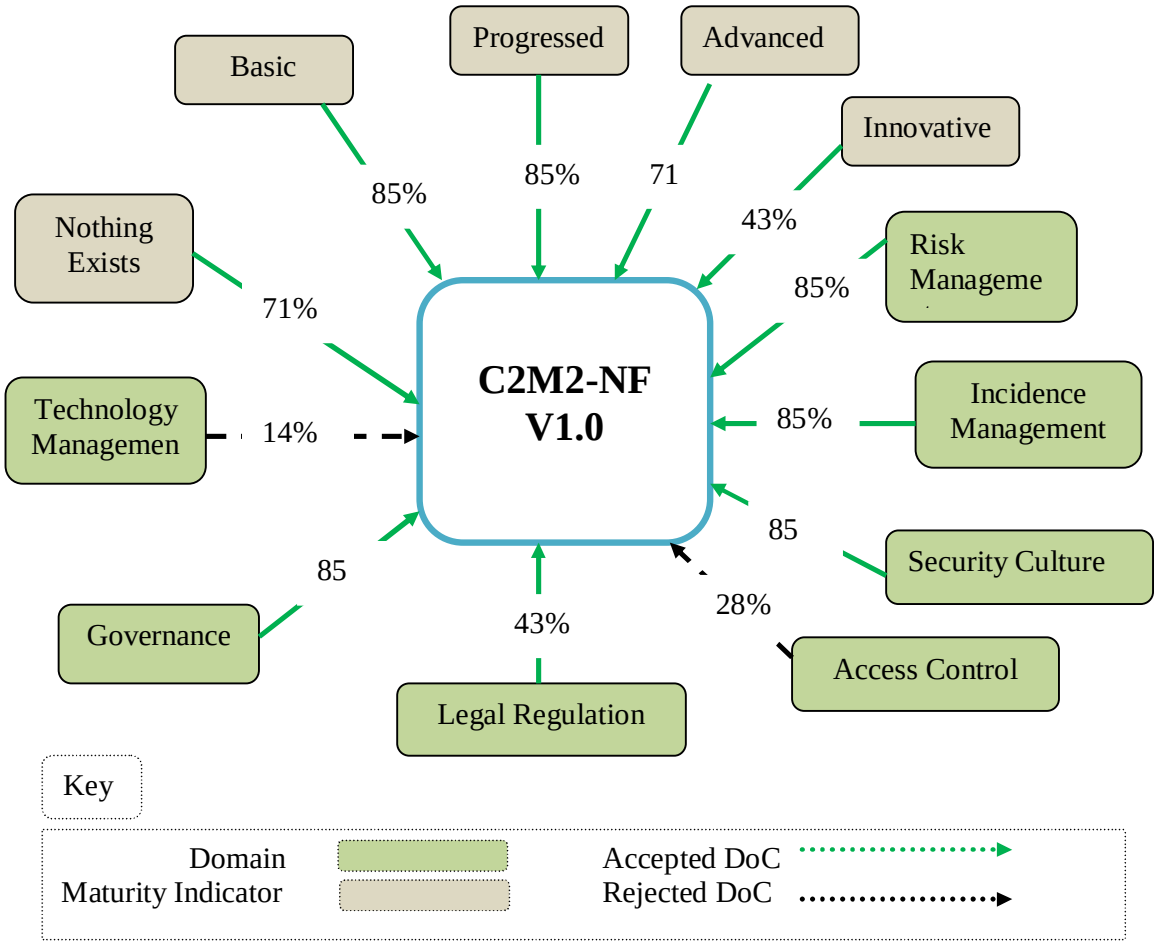


Figure 4.11 Degree of Confidence values of C2M2-NF Version 1.0

Figure 4.11 show that all five Maturity Level Indicators(MiLs) passed the Frequency-Based selection technique test, while five out of seven selected domains passed. Two domains were drop as their DoC percentage fall below moderate class.

The next step is to drop unacceptable component and regroup the acceptable components to construct the final C2M2-NF refers to as C2M2-NF Version 2.0. Degree of Confidence values of C2M2-NF Version 2.0 is show in figure 4.12. Figure 4.13 and Figure 4.14 show the final version of C2M2-NF. In the C2M2-NF V2.0, two domains were drop due to lower score in DoC.

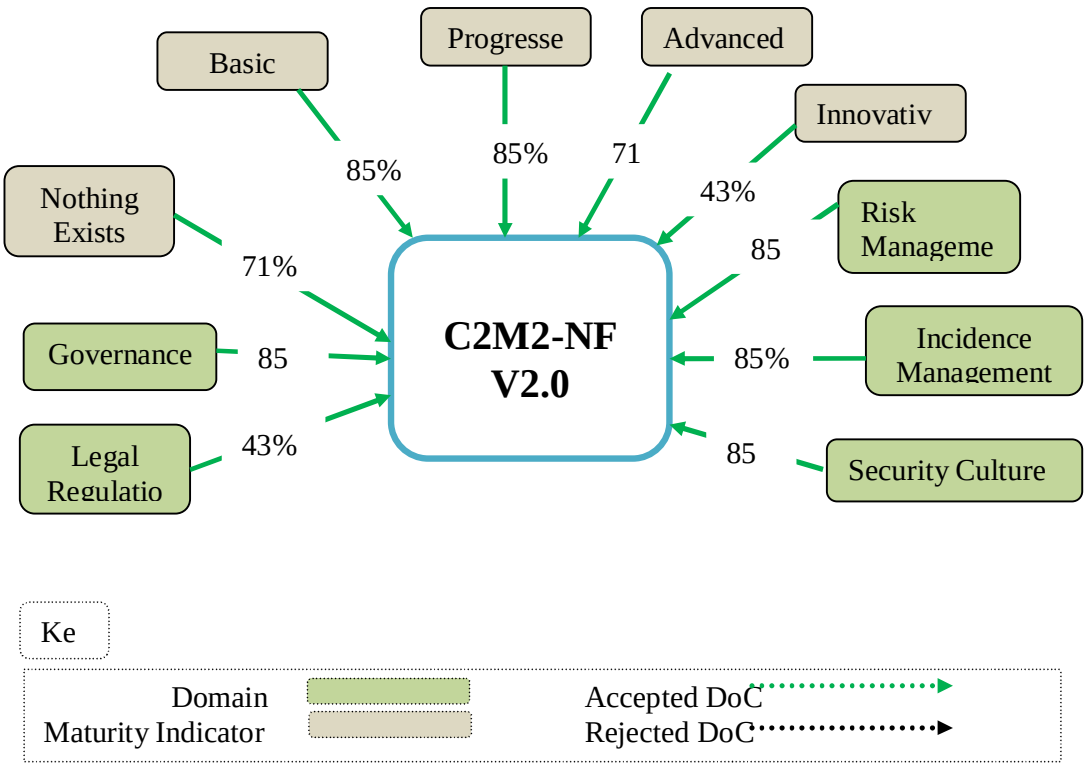


Figure 4.12 Degree of Confidence values of C2M2-NF Version 2.0

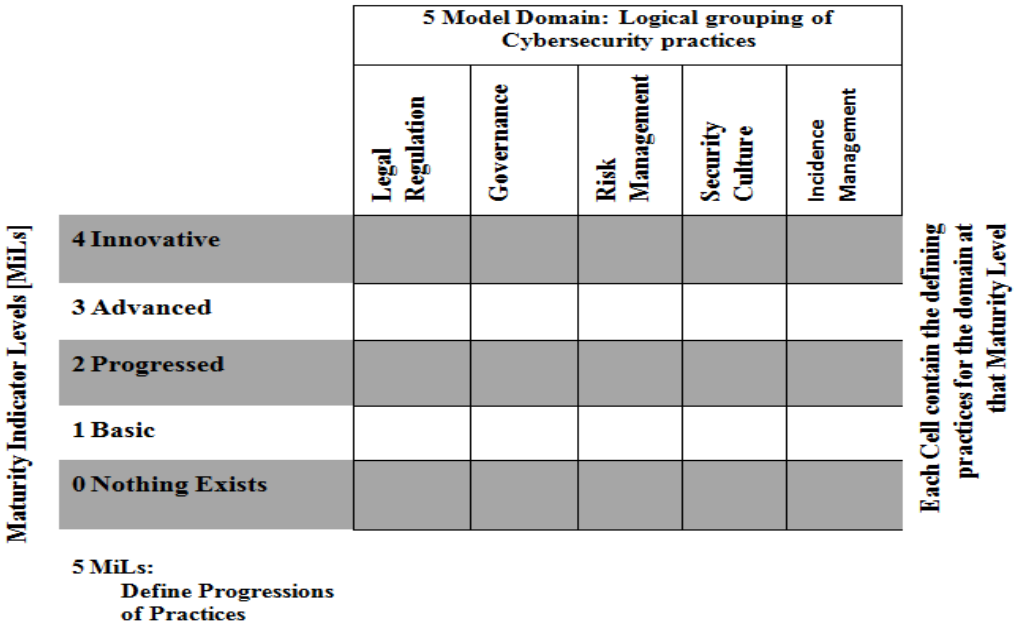


Figure 4.13 C2M2-NF Version 2.0 (Block View)

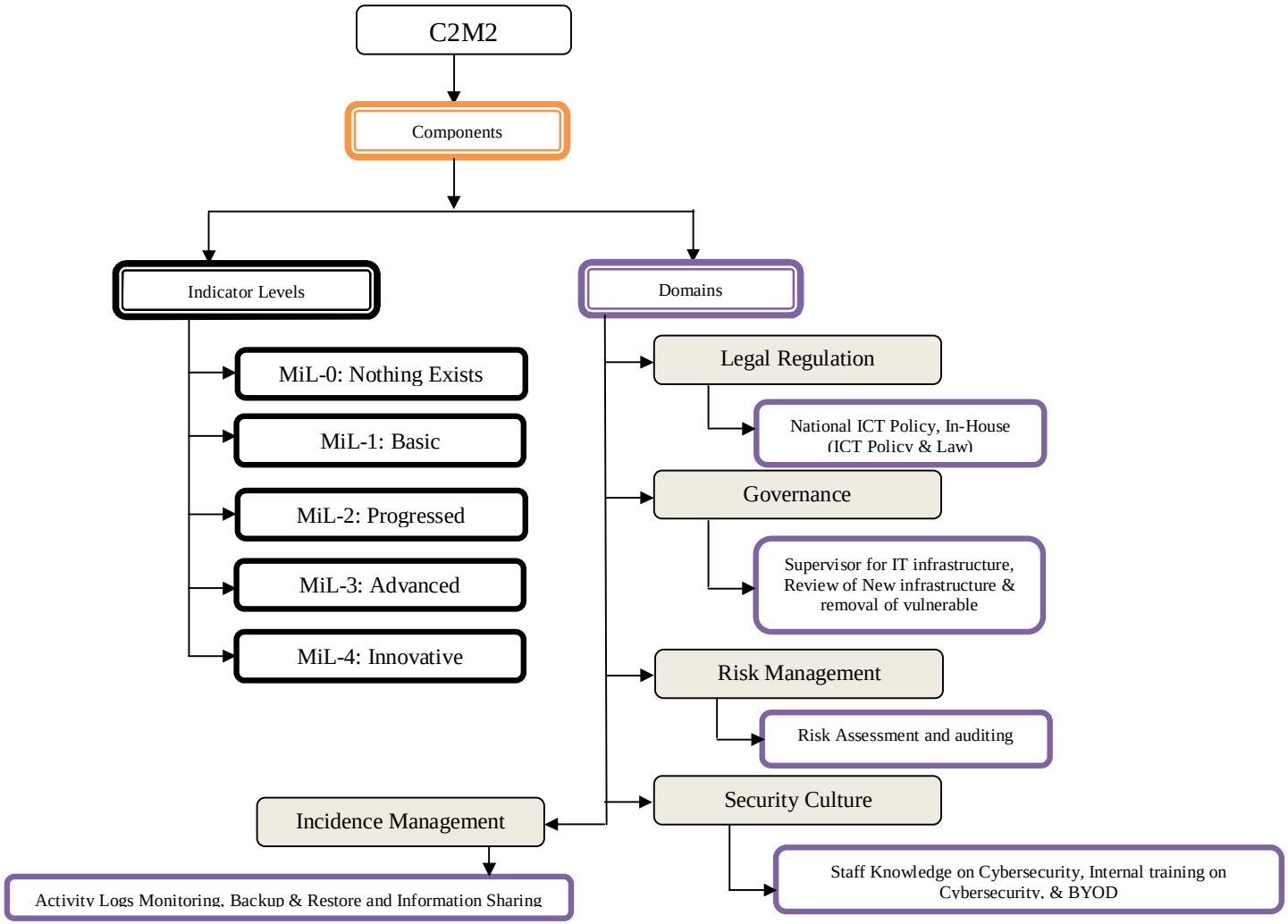


Figure 4.14 C2M2-NF Version 2.0 (Tree View)

4.6 Using the Validated C2M2-NF Version 2.0

The C2M2-NF Version 2.0 is meant to be used by any Nigeria financial organization to evaluate its Cybersecurity capabilities always and to communicate its capability levels in consequential conditions. Figure 4.15 present the suggested approach for using Cybersecurity Capability Maturity Model by US Department of Energy.

According to US Department of Energy (2014) an organization performs an evaluation against C2M2, uses that evaluation to discover gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements plans to address the gaps. In this chapter how organization can evaluate its maturity levels are presented, Chapter five provide details of how data will be analyze while the prioritize and implementation of plan is left for organizations who wish to use the model.

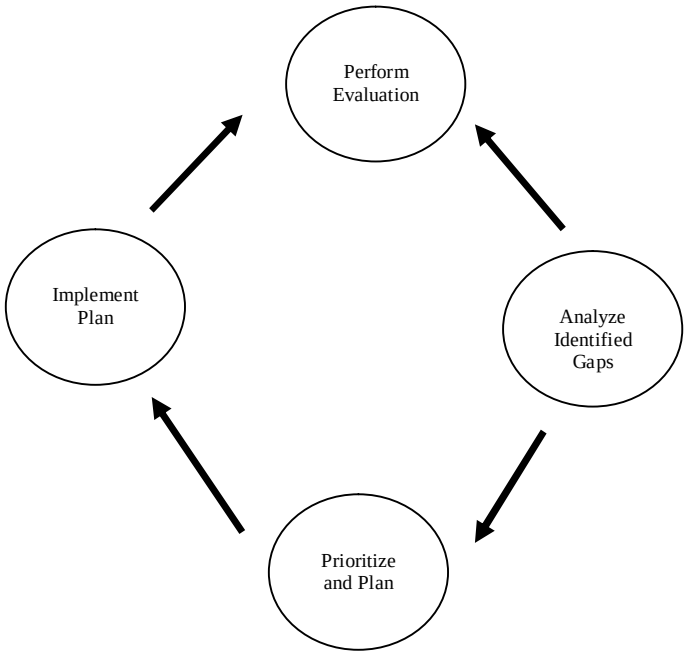


Figure 4.15 Recommended Approach for Using C2M2
(U.S. Department of Energy, 2014b)

U.S. Department of Energy (2014) recommend that an organization must select an appropriate personnel to perform evaluation. This is because Cybersecurity terms familiarity by the evaluation personnel is mandatory. C2M2-NF Version 2.0 is develop with five domains, each domain is first evaluated independently so that missing Cybersecurity practices are easily indentify. The role of Maturity Indicator Levels (MiLs) in evaluation is limited to scaling. As presented in Figure 4.14: C2M2-NF Version 2.0 (Tree View), the leave nodes attached to domain component show the necessary practice recommended by the researcher. In this develop model, practices are refer to as testimonials. The testimonials in each domains are Legal Regulation (National ICT Policy and In-House ICT Policy & Law), Governance (Supervisor for IT infrastructure, Review of New infrastructure & removal of vulnerable), Risk Management (Risk Assessment and Auditing), Security Culture (Staff Knowledge on Cybersecurity, Internal training on Cybersecurity, & BYOD) and finally Incidence Management (Activity Logs Monitoring, Backup & Restore and Information Sharing).

To perform evaluation using C2M2-NF V2.0, graphical evaluation flow chart are provide below for each domain. This will allow easy evaluation of Cybersecurity practices.

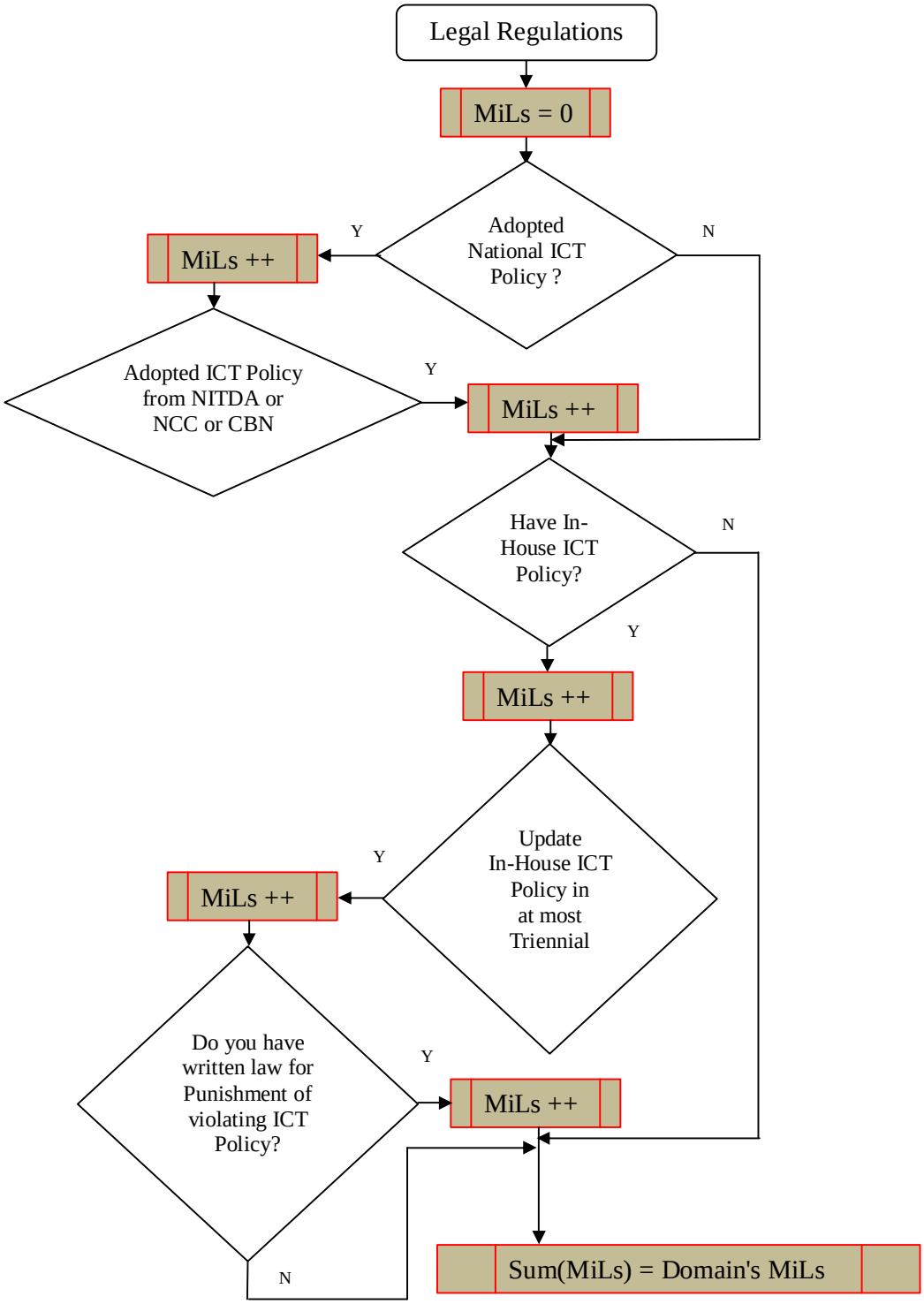


Figure 4.16 Legal Regulation flow diagram

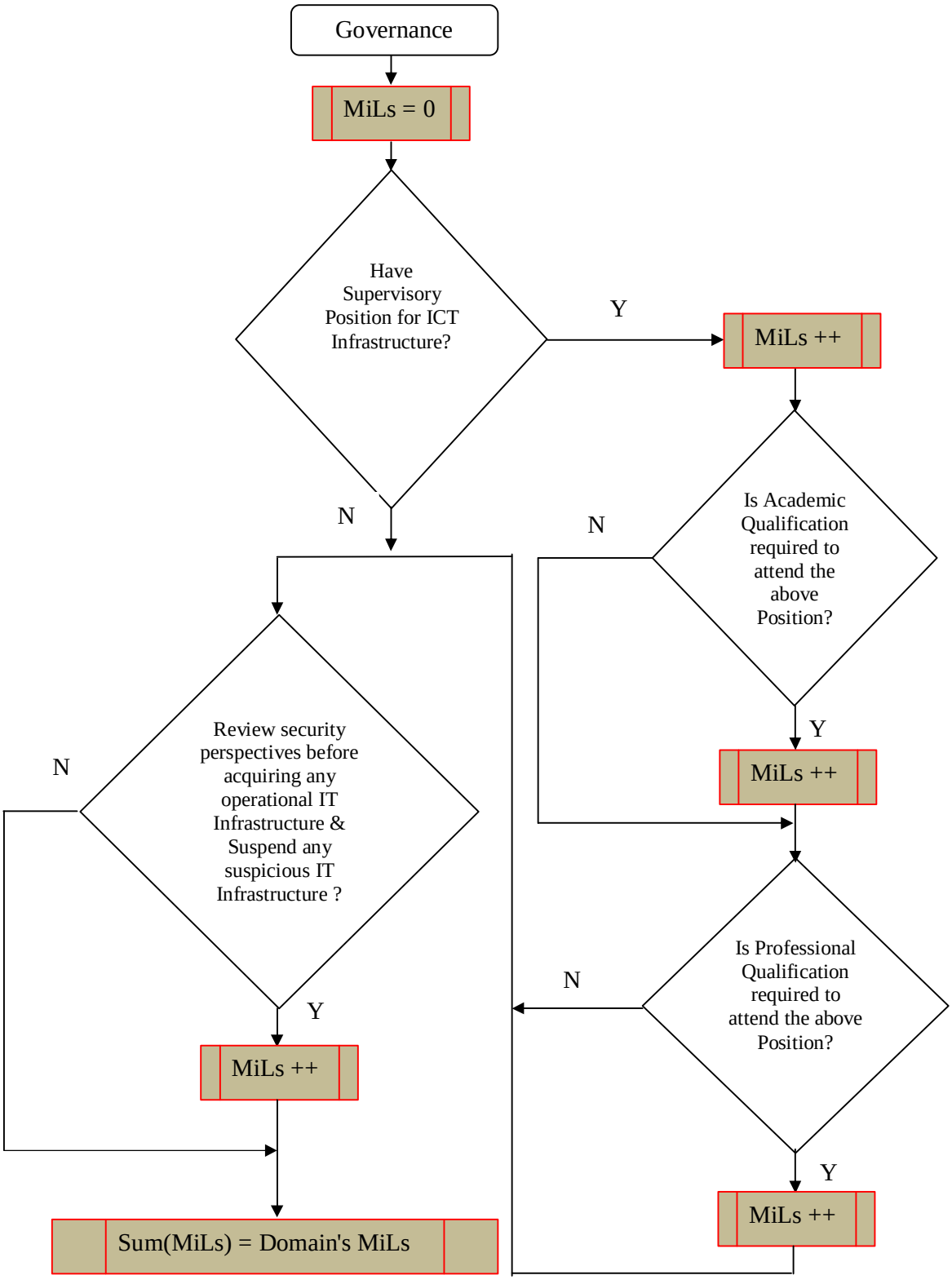


Figure 4.17 **Governance flow diagram**

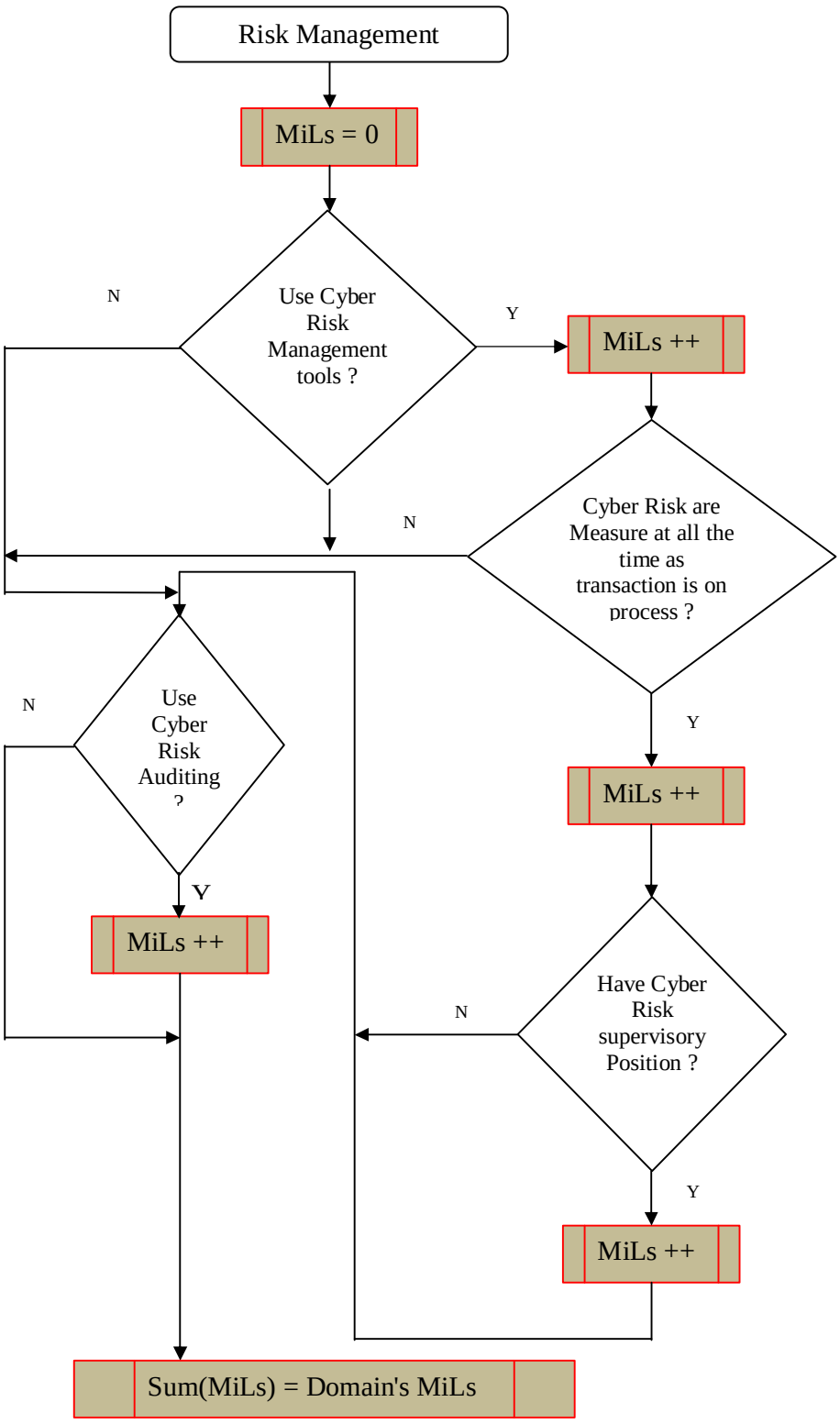


Figure 4.18 Risk Management flow diagram

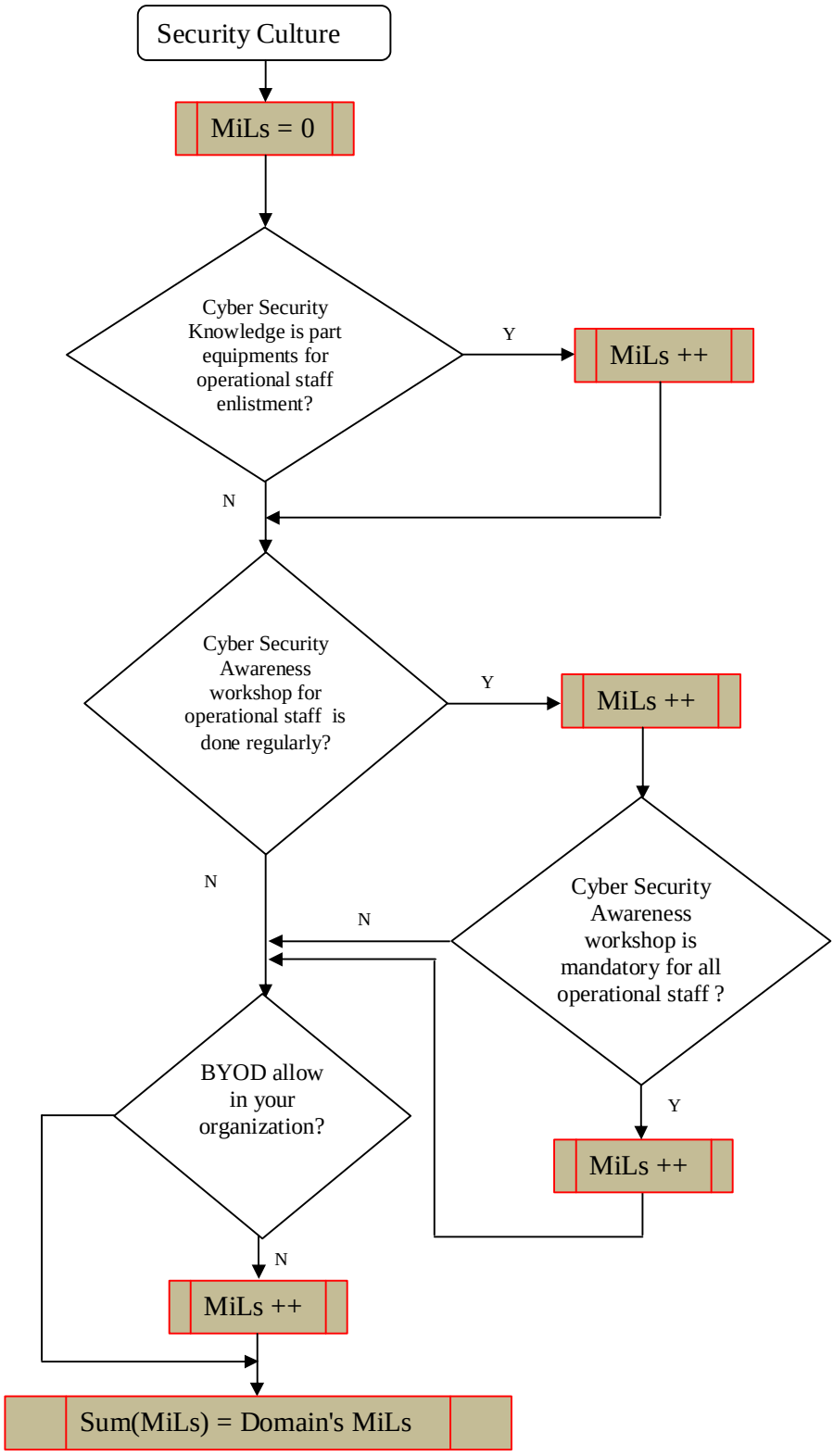


Figure 4.19 Security Culture flow diagram

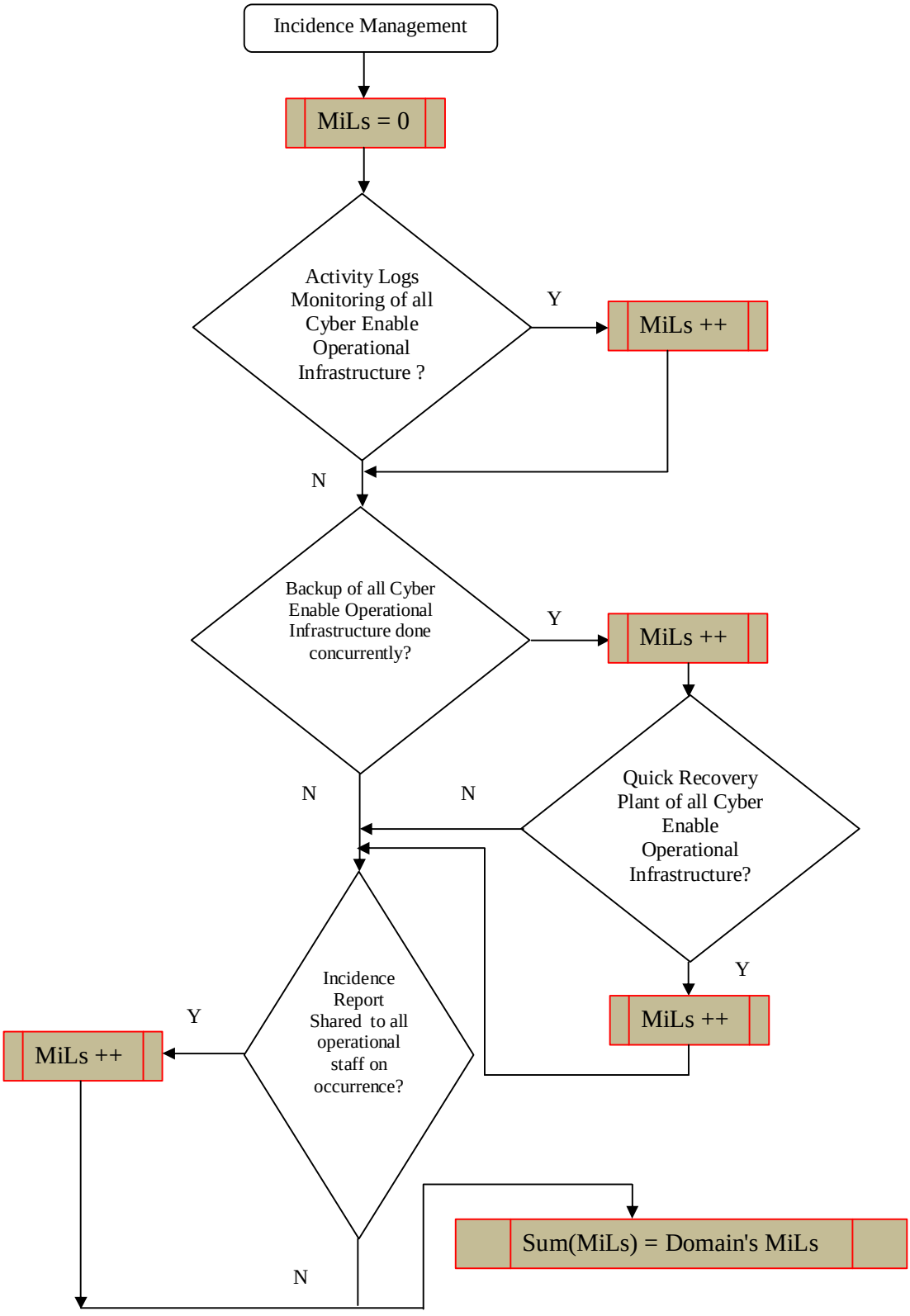


Figure 4.20 Incident Management flow diagram

4.7 Chapter Summary

In this chapter, the researcher resented the development steps of Cybersecurity Capability Maturity Model (C2M2). Based on the author researches, there is no other previous work that relates to developing a C2M2 by categorizing the development process in three phases as mentioned in this chapter. The C2M2-NF Version 2.0 is intended to become an effective model for measuring Cybersecurity capabilities among Nigeria financial organizations.

In the synthesis of C2M2-NF, fourteen (14) related C2M2 were collected. From these fourteen models, seven selected for the development of the C2M2-NF Version 1.0 while the remaining seven models were used for comparison in other to validate the drafted model, these validation resulted in final model called C2M2-NF Version 2.0.

CHAPTER 5

DATA ANALYSIS

5.1 Introduction

This chapter focuses on analysis of the collected data, also discuss the results derived from the questionnaire that was distributed among Nigeria financial organizations. Researcher utilize meta-chart.com to presents results in Bar Chart. The data analyze in this chapter is based on the testimonials mentioned in the chapter 4 using Google-form (See Appendix A). Results section provide detail analysis of the collected data.

5.2 Results

This section presents the results of the survey of this dissertation. The results are presented in categories according to domains of the proposed model. One hundred and sixty-nine (169) questionnaires were distributed in total by email. Ten (10) questionnaires were distributed manually. Also ten (10) Google-drive form's link was send to the selected case studies. At the time of this report none of one hundred and sixty-nine (Email) and ten (manual) organizations responded, only seven respondent through Google-drive form. This is due to the nature of such organizations that one IT officer will be working for three states, and those who are present in their station has title knowledge to respond to this questionnaire.

All seven (7) of the respondent organizations are located in Nigeria. Although, the IT officers or the Bank officials who responded are working within the North-Eastern Nigeria Region. In this section, seven(7) respondent feedback on their activities based on presented testimonials per domains of the C2M2-NF V2.0 are presented. Each respondent is code with two or three letters extracted from respondent's organization. Table 5.1 present respondent with their code.

Table 5.1 Respondent Organization and their Code

S/No	Respondent' Organization	Code
1	Union Bank	UB
2	First Bank	FB
3	Federal Mortgage Bank of Nigeria	FMB
4	Guaranty Trust Bank	GTB
5	Stanbic IBTC Bank	SIB
6	United Bank for Africa	UBA
7	Polaris Bank	PB

The aim of creating this code is ensure simplicity when referring a respondent. The next section presents respondent feedback based on propose model domains, each domain is capture and analyze.

5.2.1 Legal Regulations

This comprises orders with the purpose of forcing organizations to protect their critical IT Infrastructure against cyber-attacks. It contain the whole vision of all legislation acts which will be used in daily activities of an organizations. Table 5.2 present respondent activities on this domain.

Table 5.2 Respondent practice on Legal Regulation domain

No	Testimonials	Respondent						
		UB	FB	FMB	GTB	SIB	UBA	PB
1	Do your organization adopt National ICT Policy ?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	1
2	If above is Yes, Which National ICT Policy do your organization adopted?	CBN ICT Policy	CBN ICT Policy	CBN ICT Policy	CBN ICT Policy	CBN ICT Policy	CBN ICT Policy	CBN ICT Policy
	Maturity Level Points Earn	1	1	1	1	1	1	1

3	Do your organization have in-house ICT Policy?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	1
4	Do your organization have penalty for breach of ICT Policy	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	1
Total Maturity Level Points Earn		4	4	4	4	4	4	4

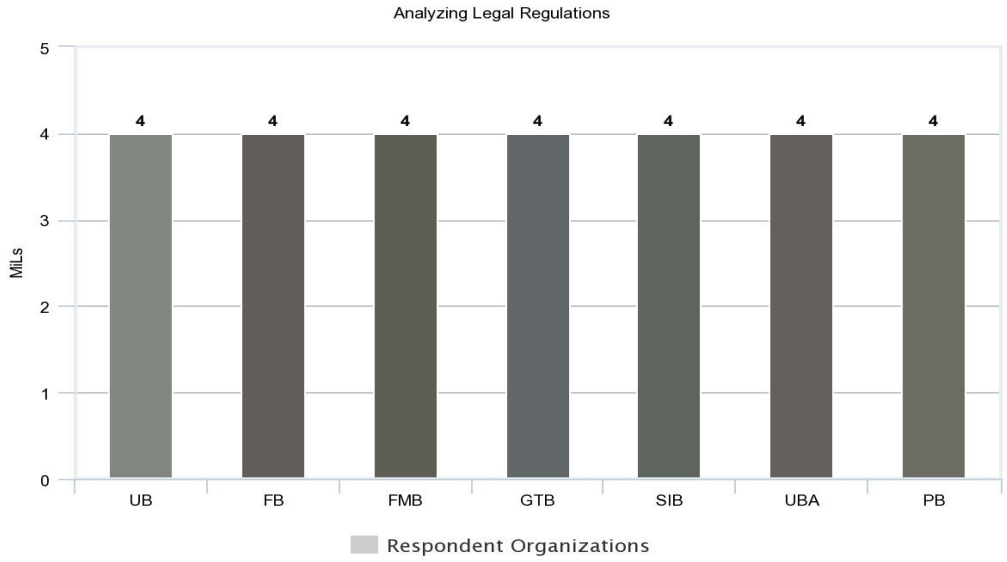


Figure 5.1 Analysis of Legal Regulations Domain

From Table 5.2 and Figure 5.1, all the respondent organizations are at the innovative level. This indicate that all practice are performed and fully fulfill.

5.2.2 Governance

This refers to how the organization govern it operational staffs in terms or supervision and orders of operational IT Infrastructure. Table 5.5 present respondent activities on this domain.

Table 5.3 Respondent practice on Governance domain

No	Testimonials	Respondent						
		UB	FB	FMB	GTB	SIB	UBA	PB
1	Do you have Supervisory Position for IT Infrastructure in your Organization?	Yes	Yes	Yes	No	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	0	1	1	1
2	If Yes, what qualification is required for IT Supervisory Position?	Acad. & Prof.	Acad. & Prof.	Acad. & Prof.		Acad. & Prof.	Acad. & Prof.	Acad. & Prof.
	Maturity Level Points Earn	1	1	1	0	1	1	1
3	If Yes, what is the minimum working experience to attend IT Supervisory Position in your organization	10	10	5		5	10	10
4	Does your organization review Cybersecurity perspective before acquiring/adopting and new operational IT infrastructure?	Yes	Yes	Yes	Yes	Yes	Don't Know	Yes
	Maturity Level Points Earn	1	1	1	1	1	0	1
5	*If Yes, from where your organization acquired operational IT infrastructure*	Trusted Vendors	Trusted Vendors	Trusted Vendors	Trusted Vendors & In-House Develop	Vendors & In-House Develop		Trusted Vendors
	Maturity Level Points Earn	1	1	1	1	1	0	1
Total Maturity Level Points Earn		4	4	4	2	4	2	4

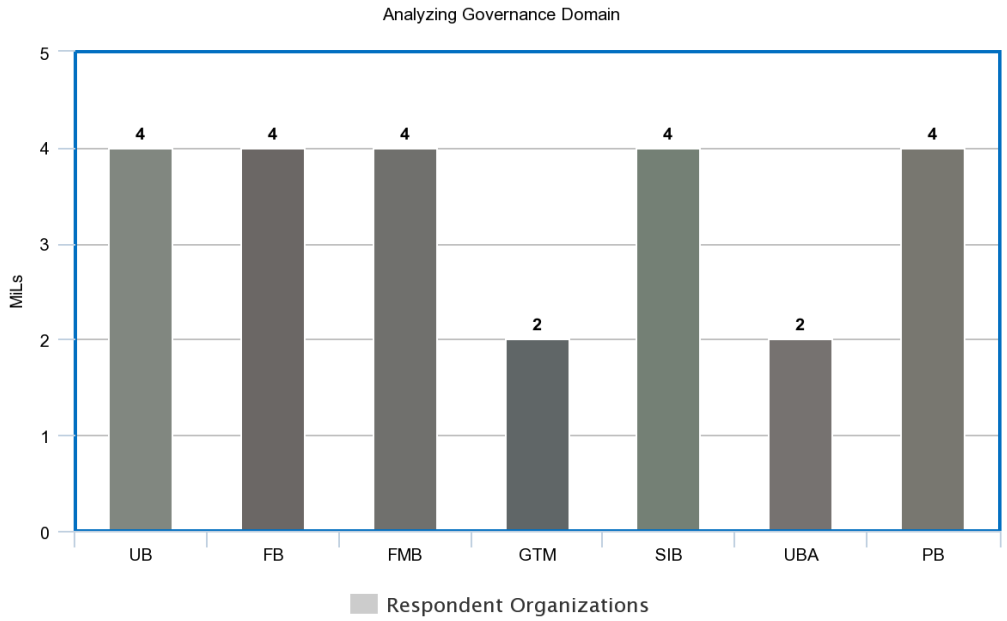


Figure 5.2 Analysis of Governance Domain

From Table 5.3 and Figure 5.2, five (5) organizations are at the innovative level while two (2) organizations are at progressed level. This indicate that the organizations require more effort to advance.

5.2.3 Risk Management

This is the organizations capability to accurately identify risks that are rising around the organization and ensuring they have the professional practices to control the impact of these risks. Table 5.4 present respondent activities on this domain.

Table 5.4 Respondent practice on Risk Management domain

No	Testimonials	Respondent						
		UB	**FB**	**FMB**	**GTB**	**SIB**	**UBA**	**PB**
1	Do your organization uses cyber-risk assessment tools?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	1
2	If Yes, which tool is your organization using?	**CBN Cyber-Risk Assessment tool**	**CBN Cyber-Risk Assessment tool**	**CBN Cyber-Risk Assessment tool**	**CBN Cyber-Risk Assessment tool**	**CBN Cyber-Risk Assessment tool.**	**CBN Cyber-Risk Assessment tool.**	**CBN Cyber-Risk Assessment tool.**
	Maturity Level Points Earn	1	1	1	1	1	1	1
3	If Yes, how frequent do your organization measure Cyber-Risk?	Don't know	Don't know	Don't know	Don't know	Don't know	Don't know	Don't know
4	Do your organization have Cyber Risk Supervisory Position?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	1
5	*Do your organization uses Cyber-Risk auditing ?*	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	1
Total Maturity Level Points Earn		4	4	4	4	4	4	4

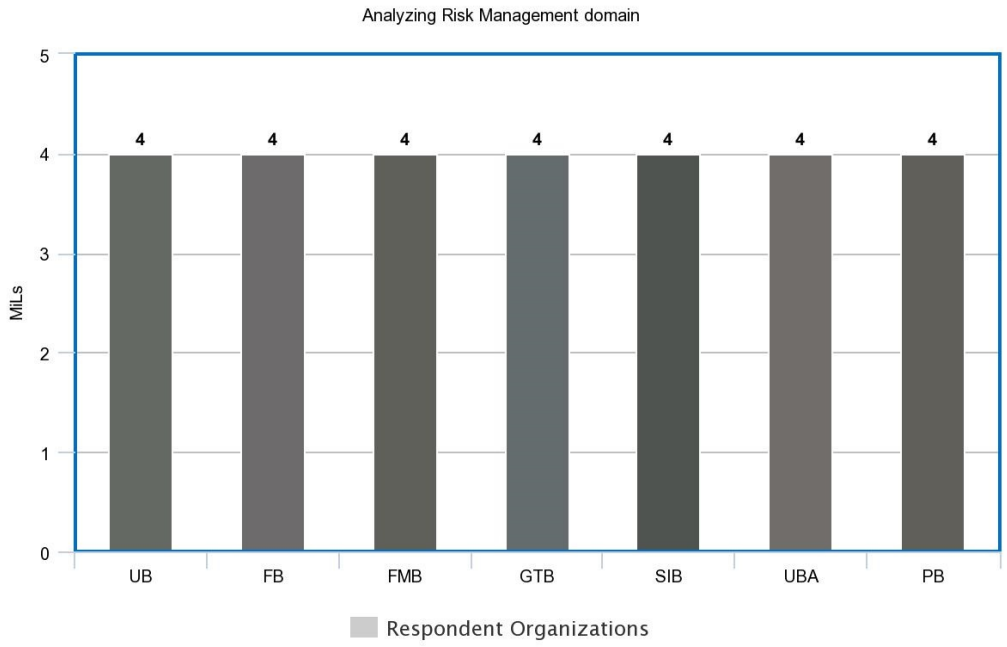


Figure 5.3 Analysis of Risk Management domain

From Table 5.4 and Figure 5.3, all the respondent organizations are at the innovative level. This indicate that all practice are performed and fully comply.

5.2.4 Security Culture

This is to evaluate the organization operational staff knowledge on Cybersecurity. Security must be understandable for every organization member and each member must have an ability to learn how to defend the organization and themselves from cyber security incidents as mistakes can be critical to the security of the organization. Table 5.7 present respondent activities on this domain.

Table 5.5 Respondent practice on Security Culture domain

No	Testimonials	Respondent						
		UB	**FB**	**FMB**	**GTB**	**SIB**	**UBA**	**PB**
1	Do your operational staffs have knowledge on Cybersecurity?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	1
2	If Yes, Rate their Cybersecurity Knowledge	**Basic**	**Basic**	**Basic**	**Advanced**	**Intermediate**	**Basic**	**Intermediate**
3	Do your organization organized internal workshop for operational staff on Cybersecurity ?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	1
4	Is Cybersecurity knowledge part of skills required for employment of operational staff in your organization?	No	No	No	No	No	No	No
	Maturity Level Points Earn	0	0	0	0	0	0	0
5	Do you allow Bring Your Own Device (BYOD) ?	No	No	No	No	No	No	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	0
Total Maturity Level Points Earn		3	3	3	3	3	3	2

From Table 5.5 and Figure 5.4, all the respondent organizations are at the Advanced level except PB at the progressed level. This indicate all the organizations ignore Cybersecurity knowledge as part of their requirement for employment of operational staff while PB allows Bring Your Own Devices(BOYD) to be practice.

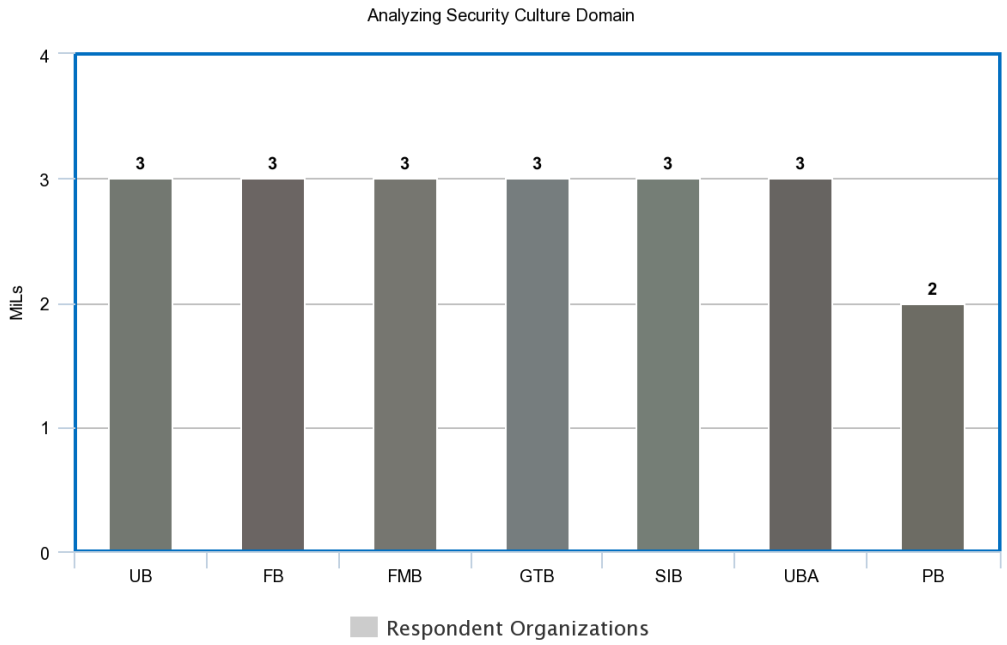


Figure 5.4 Analysis of Security Culture

5.2.5 Incidence Management

This comprises of special strategy regarding the cyber incident consequence management. This contain a detail planned and directions about the organization recovery strategy if any cyber security incidents occur and the usual work of the organization is interrupted. Table 5.8 present respondent activities on this domain.

Table 5.6 Respondent practices on incidence management domain

No	Testimonials	Respondent						
		UB	**FB**	**FMB**	**GTB**	**SIB**	**UBA**	**PB**
1	Do your organization monitor the activity logs of IT control enabled operational component?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	1
2	If Yes, how do you monitor the activity logs?	**Manual + Automatic**	**Automatic**	**Automatic**	**Manual + Automatic**	**Automatic**	**Automatic**	**Manual + Automatic**
3	Do Your organization backup transactions logs of IT control enabled operational components ?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	1
4	*If Yes, how frequent do you backup?*	After every transaction logs	After every transaction logs	After every transaction logs	Don't know	After daily transaction logs	After daily transaction logs	After daily transaction logs
5	Do your organization have disaster recovery plan for IT control enabled component?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maturity Level Points Earn	1	1	1	1	1	1	1
6	Do you share incidence report to all Operational Staff ?	No	Yes	Yes	No	No	No	No
	Maturity Level Points Earn	0	1	1	0	0	0	0
Total Maturity Level Points Earn		3	4	4	3	3	3	3

From Table 5.6 and Figure 5.5, two (2) organization attend Innovative level while the remaining five (5) respondent organizations are at the Advanced level. The results show that five organizations lack cyber incident's information sharing.

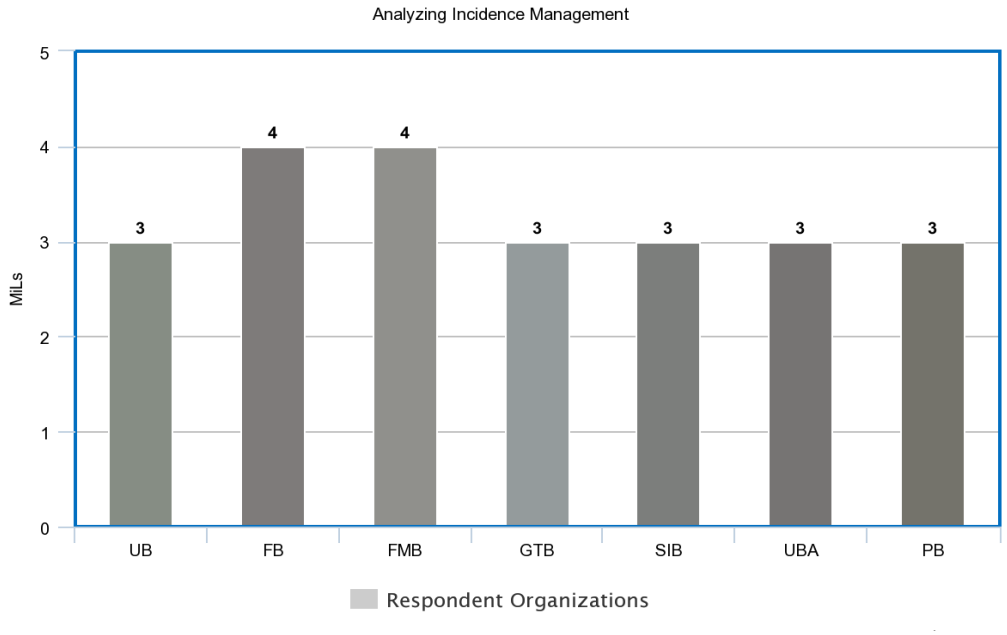


Figure 5.5 Analysis of Incidence Management

5.3 Overall Results

This section summarizes the overall result of the responded organizations to find the entire maturity level of each organization in study. Table 5.7 present the results summary.

Table 5.7 Summary of overall Maturity Indicator Levels

No	Domains	Respondent Maturity Indicator Levels (MiLs)						
		UB	FB	FMB	GTB	SIB	UBA	PB
1	Legal Regulation	4	4	4	4	4	4	4
2	Governance	4	4	4	2	4	2	4
3	Risk Management	4	4	4	4	4	4	4
4	Security Culture	3	3	3	3	3	3	2
5	Incidence Management	3	4	4	3	3	3	3
Average MiLs		**3.6**	**3.8**	**3.8**	**3.2**	**3.6**	**3.2**	**3.4**

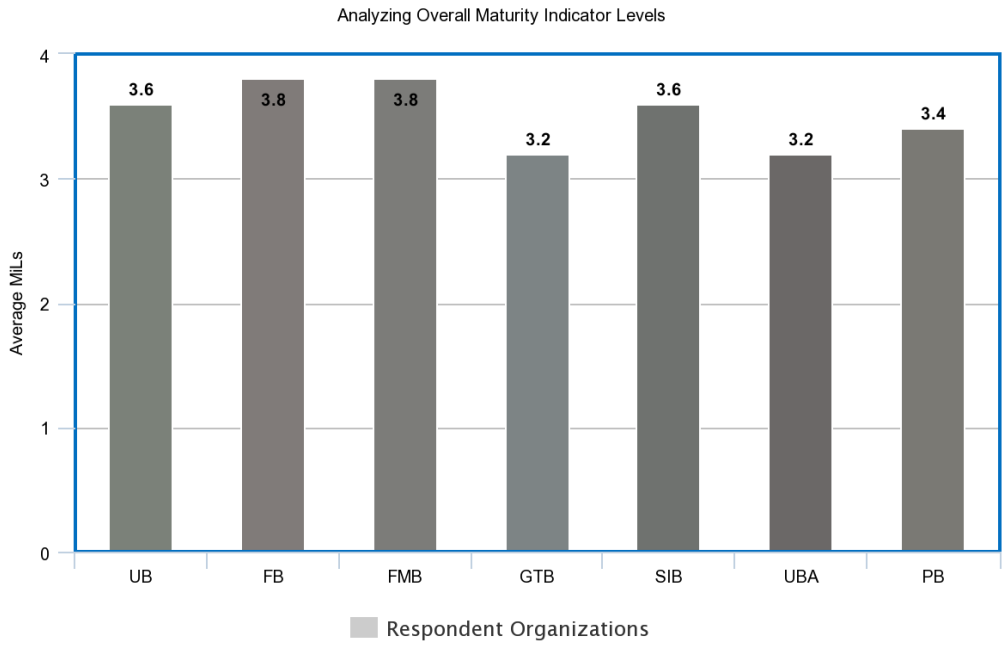


Figure 5.6 Analysis of Overall Maturity Indicator Levels

From Table 5.7 and Figure 5.6 none of the responded organizations attend Innovative level. Equally, all organizations attend Advanced level. Table 5.10 below summarizes what each organization required to attend Innovative level.

Table 5.8 Recommendations to achieve the Innovative Level

S/No	Respondent' Organization Code	Practices Necessary to attend Innovative Level
1	UB	1. Cybersecurity knowledge should be part of skills required for employment of operational staff. 2. Incidence report should be shared to all Operational Staff
2	FB	1. Cybersecurity knowledge should be part of skills required for employment of operational staff.
3	FMB	1. Cybersecurity knowledge should be part of skills required for employment of operational staff.
4	GTB	1. Supervisory Position for IT Infrastructure required in the Organization. 2. Cybersecurity knowledge should be part of skills required for employment of operational staff. 3. Incidence report should be shared to all Operational

		Staff.
5	SIB	1. Cybersecurity knowledge should be part of skills required for employment of operational staff. 2. Incidence report should be shared to all Operational Staff
6	UBA	1. Organization required to review Cybersecurity perspective before acquiring/adopting and new operational IT infrastructure. 2. Cybersecurity knowledge should be part of skills required for employment of operational staff. 3. Incidence report should be shared to all Operational Staff
7	PB	1. Cybersecurity knowledge should be part of skills required for employment of operational staff. 2. Incidence report should be shared to all Operational Staff 3. The practice of Bring Your Own Device need to be address

5.4 Chapter Summary

This chapter discussed about data analysis. The first section provide information about the responded organizations, codes were given to organizations for easy reference. Then data analysis approach in this study was discussed. Analyzing five domains with their testimonials according the responded organizations' practices were examined. The results of capability maturity level for each organization was determined. Finally, what each organization is missing in its practices to attend the highest level were presented.

CHAPTER 6

DISCUSSION AND CONCLUSION

6.1 Introduction

This chapter will discuss and conclude this dissertation. This chapter includes summary of achievements, study limitations, recommendations for future research and finally conclusion of the study.

6.2 Summary of Research Achievements

This dissertation, having been conducted successfully, has come up with the subsequent achievements.

(a) A detailed literature research on Cybersecurity issues in Nigeria and Cybersecurity Capability Maturity Models(C2M2) relevant to financial organizations. This can give great comprehension of this area of study to future researchers who may wish to further research on C2M2 relevant to financial organizations.

(b) C2M2 which can be use to evaluate financial organization preparedness on Cybersecurity has been develop.

(c) Methodology provides iterative process on how to develop C2M2, this can useful for future researchers on this area.

(d) Cybersecurity strength on case study identified.

6.3 Dissertation Limitations

Regardless of the huge achievement in this dissertation, some limitations of this dissertation includes:

(a) The study able to analyze data only from banks in Nigeria particularly in North-Eastern region. While the research was initially design to cover all financial organizations in Nigeria.

(b) Questionnaires distributed across One hundred and sixty-nine (169) financial organizations in Nigeria via email did not receive attention in many organizations despite the simplicity of questionnaire structure. This, however, means that the dissertation outcome might not be generated, as sample were only from seven (7) financial organizations.

6.4 Future Work Recommendations

In order to improve the results of the study in the future, improvements could be made to the study. The model can possibly be enhanced by considering the following recommendations.

(a) Testimonials in Domains

To enhance the domain, more testimonial needs to be added in order to balance each domain.

(b) Automate C2M2 Transformation

Automate the transformation of the C2M2 from the conceptual to the implementation phase.

(c) C2M2 sharing platform

A one stop centre platform can be set up for sharing the information among the developers of C2M2, system developers and also the domain experts.

6.5 Conclusion

This dissertation produced a five-level maturity model for evaluating Cybersecurity preparedness among Nigeria financial organizations. An increase dependency on IT infrastructure by financial organizations is courses an increases in Cyberattacks to their operational infrastructure and some key elements are presented in chapter one.

In **chapter two**, literature review further explain the concept of Cybersecurity and maturity modeling, and proceeded to discuss trends in Cybersecurity Capability Maturity Model(C2M2). Previous attempts and efforts to produce C2M2 were also highlighted in the chapter. All these set the atmosphere for understanding and furthering the course of developing C2M2 which had not been attempted.

Chapter three explain about the method that has been used to carry out this research. Also discussion about the phases inside the operational framework is done and the description for each research step was briefly explained.

Chapter four of this dissertation went in detail in explaining the Model development process. Individual activities which characterized the various development stages are also discussed. The different components, maturity levels, and domain of the proposed model are also explained. Model validation using comparison against other valid models and frequency-based selection techniques.

Overall results are presented in chapter five, presentation of results are done with the aid of tables and charts. The concluding chapter summarizes the dissertation by starting with achievements, limitations, recommendations for future works and conclusions draw from the dissertation.

REFERENCES

Adesina, O. S. (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science*, *13*(4), 19–29. https://doi.org/10.3968/9394

Adler, R. M. (2013). A dynamic capability maturity model for improving cyber security. *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, 230–235. https://doi.org/10.1109/THS.2013.6699005

Angel, M. R.-G., Feliu, T. S., Calvo-Manzano, J. A., & Sanchez-Garcia, I. D. (2017). Comparative Study of Cybersecurity Capability Maturity Models, *770*, 114–127. https://doi.org/10.1007/978-3-319-67383-7

Barclay, C. (2014). Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (CM2). *Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World - Impossible Without Standards?, K 2014*, 275–282. https://doi.org/10.1109/Kaleidoscope.2014.6858466

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Butkovic, M. J., & Caralli, R. a. (2013). Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale, (November), 1–37. Retrieved from http://www.sei.cmu.edu

Caralli, R., Knight, M., & Montgomery, A. (2012). Maturity models 101: a primer for applying maturity models to smart grid security, resilience, and interoperability, (November), 1–10. Retrieved from http://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_58920.pdf

Casey, E. (2005). {C}omputer {C}rime and {D}igital {E}vidence, 429–435.

CBN. (2018). Risk-based Cybersecurity framework and guidelines for deposit money banks and payment service providers. *Animal Genetics*, *39*(5), 561–563. Retrieved from https://www.cbn.gov.ng/Out/2018/BSD/RISK BASED CYBERSECURITY FRAMEWORK Exposure Draft June.pdf

Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., … Dolan, T. (2014). Cybersecurity Capability Maturity Model

(C2M2). *Department of Homeland Security*, (February), 1–76. Retrieved from https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program

Cisco. (2018). Cisco 2018 Annual Cybersecurity Report. *Science and Engineering Indicators 2018*, 1–8. https://doi.org/10.1002/ejoc.201200111

Curtis, P. D., & Mehravari, N. (2015). Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. In *2015 IEEE International Symposium on Technologies for Homeland Security, HST 2015*. https://doi.org/10.1109/THS.2015.7225323

Curtis, P., Mehravari, N., & Stevens, J. (2015). Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0. *Defense Technical Information Center*, (April).

Dai, N., Huu, P., & Zoltán, R. (2017). The current state of information communication technology in critical infrastructure: the case of Vietnam. *Hadmérnök*, (Xii), 173–179. Retrieved from http://hadmernok.hu/174_17_rajnai.pdf

De Bruin, T., Freeze, R., Kaulkarni, U., & Rosemann, M. (2005). Understanding the Main Phases of Developing a Maturity Assessment Model. *Australasian Conference on Information Systems (ACIS)*, (December), 8–19. https://doi.org/10.1108/14637151211225225

Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G. B., & Wyss, G. (2005). Risk Assessment for Physical and Cyber Attacks on Critical Infrastructures. *MILCOM 2005 - 2005 IEEE Military Communications Conference*, 1–9. https://doi.org/10.1109/MILCOM.2005.1605959

Eshun, F. A. (2009). THE ROLE TELECOMMUNICATION ON BANKING SERVICES IN GHANA, 1–71.

Ferraiolo, K. (2000). The Systems Security Engineering Capability Maturity Model. *International Systems Security Engineering Association*, 64. Retrieved from https://csrc.nist.gov/csrc/media/publications/conference-paper/2000/10/19/proceedings-of-the-23rd-nissc-2000/documents/papers/916slide.pdf

FFIEC. (2015a). FFIEC Cybersecurity Assessment Tool, *3506*(1557).

FFIEC. (2015b). FFIEC Cybersecurity Assessment Tool Overview for Chief Executive Officers and Boards of Directors, *1*(June), 1–5.

GCSCC. (2014). Cyber Security Capability Maturity Model (CMM). *Global Cyber Security Capacity Centre University of Oxford*, (Cmm), 1–45. Retrieved from http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM Pilot version A.15.12.2014.pdf

Grau, D., & Kennedy, C. (2014). TIM Lecture Series – The Business of Cybersecurity. *Technology Innovation Management Review*, *4*(4), 53–57.

Hansen, R. (2016). Cyber security capability assessment.

Hassan, A. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science …*, *2*(7), 626–631. Retrieved from http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf

Humphrey, W. S. (1988). Characterizing the Software Process: A Maturity Framework. *IEEE Software*, *5*(2), 73–79. https://doi.org/10.1109/52.2014

Ibikunle, F., & Eweniyi, O. (2013). Approach To Cyber Security Issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE)*, *1*(1), 100–110. Retrieved from http://ijcrsee.com/index.php/ijcrsee/article/view/11/114

Jaquire, V., & Von Solms, S. (2017). Developing a cyber counterintelligence maturity model for developing countries. *2017 IST-Africa Week Conference, IST-Africa 2017*, (Cci), 1–8. https://doi.org/10.23919/ISTAFRICA.2017.8102288

Karokola, G., Kowalski, S., & Yngström, L. (2011). Secure e-government services: Towards a framework for integrating it security services into e-government maturity models. *2011 Information Security for South Africa*, (C), 1–9. https://doi.org/10.1109/ISSA.2011.6027525

Kaur, J. (2014). Comparative Study of Capability Maturity Model. *International Journal of Advanced Research in Computer Science & Technology*, *2*(1), 47–49.

László, K. (2009). Possible Methodology for Protection of Critical Information Infrastructures.

Lazarus, S. I., & Holloway, R. (2017). Causes of Socioeconomic Cybercrime in Nigeria, (October). https://doi.org/10.1109/ICCCF.2016.7740439

Le, N. T., & Hoang, D. B. (2016). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, 1–7. https://doi.org/10.1109/PCCC.2016.7820663

Le, N. T., & Hoang, D. B. (2017). Capability maturity model and metrics framework

for cyber cloud security. *Scalable Computing*, *18*(4), 277–290. https://doi.org/10.12694/scpe.v18i4.1329

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues*, *4*(4), 559–573. https://doi.org/10.9770/jesi.2017.4.4(12)

Mehravari, N. (2001). Everything you always wanted to know about PPRA. *Positive Living (Los Angeles, Calif.)*, *10*(2), 35–37.

Merriam, S. (2009). Qualitative Research A Guide to Design and Implementation Revised, 9.

MICT. (2014). National Cybersecurity Strategy, *Feel safe*. Retrieved from https://www.cert.gov.ng/file/docs/NATIONAL_CYBESECURITY_STRATEGY.pdf

Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116–125. https://doi.org/10.5897/IJSA2013.0510

OECD. (2008). PROTECTION OF ' CRITICAL INFRASTRUCTURE ' AND THE ROLE OF INVESTMENT POLICIES RELATING TO NATIONAL SECURITY May 2008 This report is published under the OECD Secretariat ' s responsibility and was prepared by Kathryn Gordon (Senior Economist , OECD) and, (May). Retrieved from http://www.oecd.org/daf/inv/investment-policy/40700392.pdf.

Olayemi, O. J. (2014). Full Length Research Paper A socio-technological analysis of cybercrime and cyber security in Nigeria, *6*(3), 116–125. https://doi.org/10.5897/IJSA2013.0510

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention *, *1*(1).

Othman, S. H. (2012). *Metamodelling Approach for Managing Disaster Management Knowledge*.

Paulk, M. C., Curtis, B., Chirssis, M. B., & V., W. and C. (1993). Capability maturity model, version 1.1. *IEEE Software*, *10*(4), 18–27. https://doi.org/10.1109/52.219617

Rea-Guaman, A. M., Sanchez-Garcia, I. D., Feliu, T. S., & Calvo-Manzano, J. A. (2017). Maturity Models in Cybersecurity: a systematic review. *Iberian Conference on Information Systems and Technologies, CISTI*.

https://doi.org/10.23919/CISTI.2017.7975865

Roger, B., Dorathy, K., James, A., Gloria, C., & Kerinia, C. (1995). Maturity Model Systems Engineering Capability Maturity Model Project, (November). Retrieved from http://resources.sei.cmu.edu/asset_files/MaturityModule/1995_008_001_16355.pdf

Röglinger, M., Pöppelbuß, J., & Becker, J. (2012). Maturity models in business process management. *Maturity Models in Business Process Management*, *18*(2), 328–346.

Saco, R. M. (2008). Maturity Models. *Industrial Management*, *50*(4), 11–15. https://doi.org/10.1081/E-ESCM-120047797

Schukat, M. (2014). Securing critical infrastructure. *DT 2014 - 10th International Conference on Digital Technologies 2014*, 298–304. https://doi.org/10.1109/DT.2014.6868731

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying critical infrastructure sectors and their dependencies: An Indian scenario. *International Journal of Critical Infrastructure Protection*, *7*(2), 71–85. https://doi.org/10.1016/j.ijcip.2014.04.003

U.S. Department of Energy. (2014a). Electricity subsector cybersecurity capability maturity model, (February), 89. Retrieved from http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

U.S. Department of Energy. (2014b). Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2), (February). Retrieved from http://energy.gov/sites/prod/files/2014/03/f13/ONG-C2M2-v1-1_cor.pdf

US Department of Homeland Security. (2014). Department of Homeland Security Cybersecurity Capability Maturity Model White Paper.

Vicente, A. (2007). Information Security Management Maturity Model.

Von Solms, S. H. B. (2015). A maturity model for part of the African Union Convention on Cyber Security. *Proceedings of the 2015 Science and Information Conference, SAI 2015*, 1316–1320. https://doi.org/10.1109/SAI.2015.7237313

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology*, *54*(12), 1317–1339. https://doi.org/10.1016/j.infsof.2012.07.007

White, G. B. (2011). The community cyber security maturity model. *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, 173–178. https://doi.org/10.1109/THS.2011.6107866

Wood, M. (2018). Simple Methods for Estimating Confidence Levels, or Tentative Probabilities, for Hypotheses Instead of P Values, (March). Retrieved from http://woodm.myweb.port.ac.uk/

Appendix A QUESTIONNAIRE

(Responses through Google Web-form)

Who has responded?

Email
hadizaiu99@gmail.com
musamusa950@gmail.com
umarahassan@gmail.com
lawanwali1@gmail.com
rabiu.abdulsalam11@gmail.com
habujeta@gmail.com
gasmatic2014@gmail.com

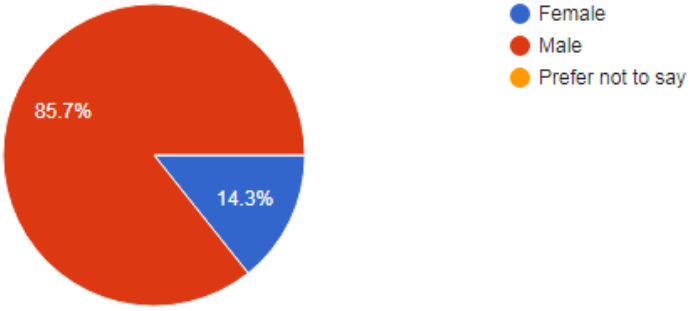
Name

7 responses

Hadiza Iliyasu Usman
Musa Musa
UMARA HASSAN
Lawan Isah Wali
Rabiu Abdulsalam
Habubakar Mohammed
MOHAMMED GASMA

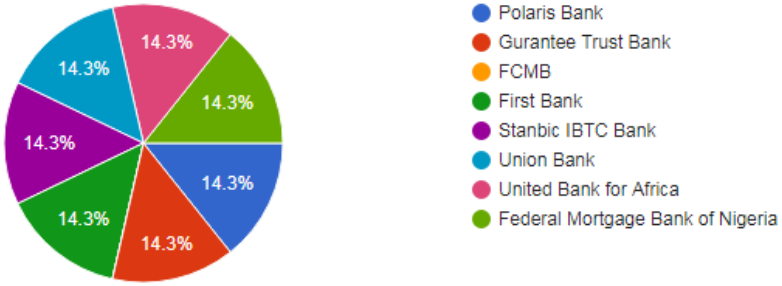
Gender

7 responses



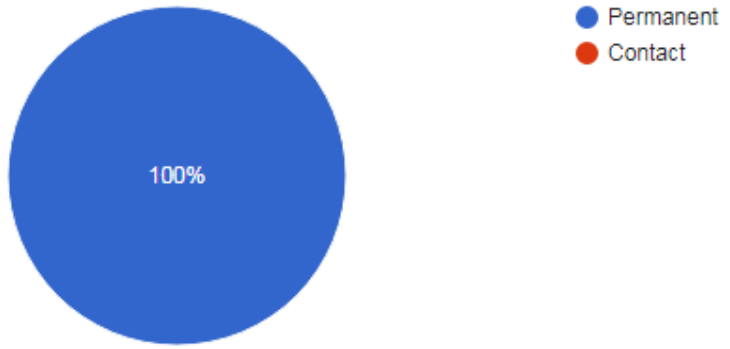
Organization

7 responses



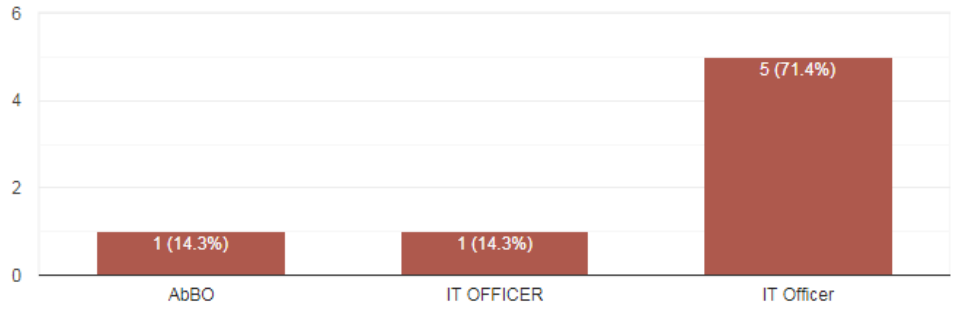
Employment Type

7 responses



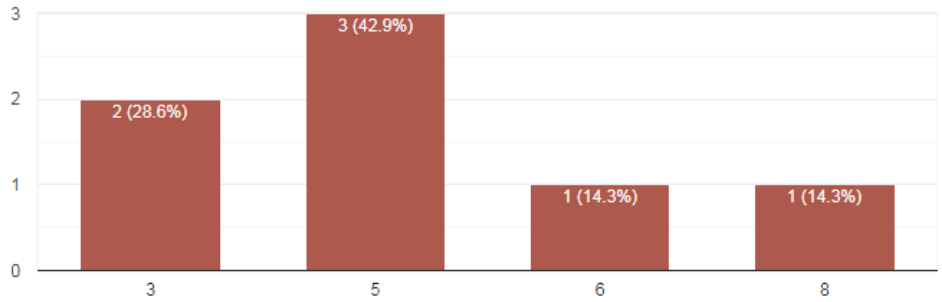
Rank/Position

7 responses



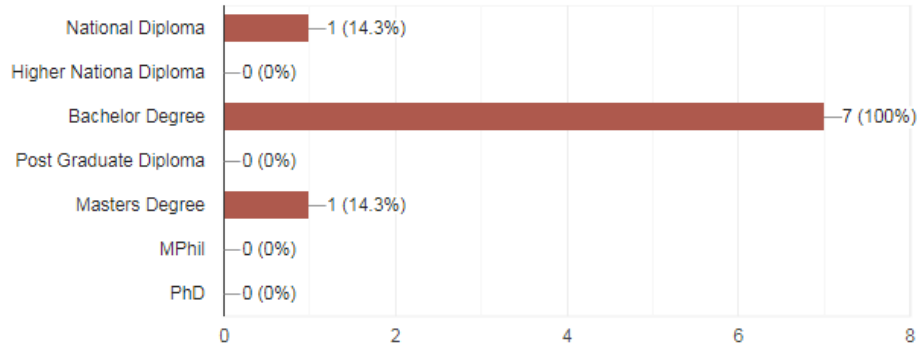
Working Experience (in Years)

7 responses



Educational Qualifications (IT/Computing)

7 responses



Professional IT Qualification

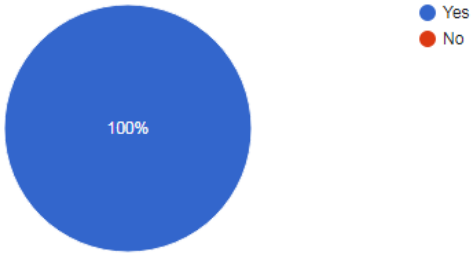
7 responses

Certified Information Systems Security Professional
CCNA
Certified Information Systems Security Professional
Bsc Computer Science
CCNA Security

Legal Regulations

Do your organization adopt National ICT Policy ?

7 responses

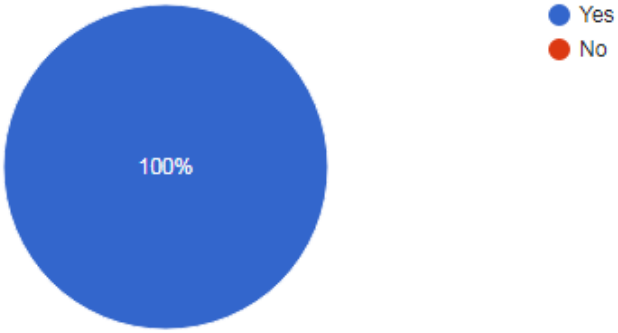


If above is Yes, Which National ICT Policy do your organization adopted?

7 responses

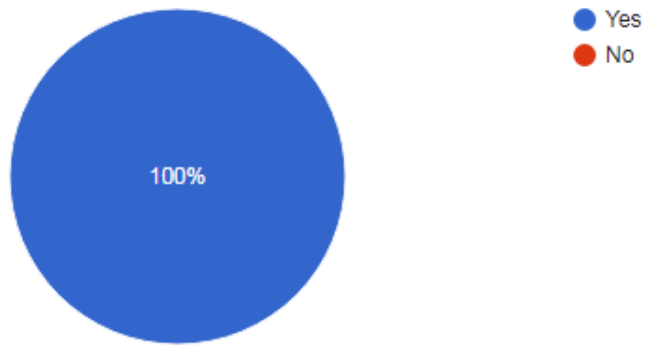
Do your organization have in-house ICT Policy?

7 responses



Do your organization have penalty for breach of ICT Policy

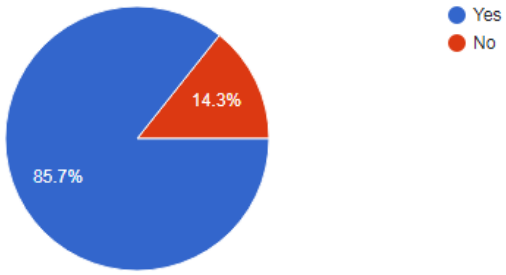
7 responses



Governance

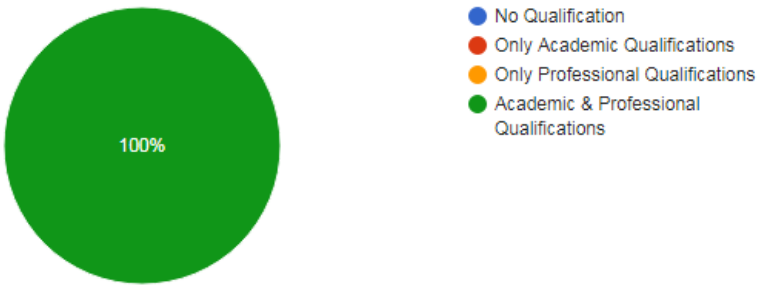
Do you have Supervisory Position for IT Infrastructure in your Organization?

7 responses



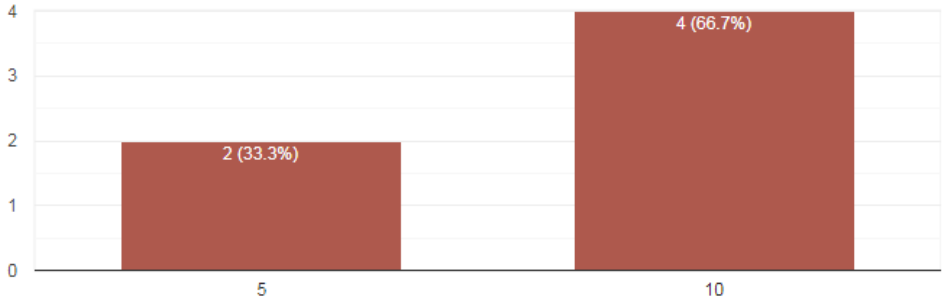
If Yes, what qualification is required for IT Supervisory Position?

6 responses



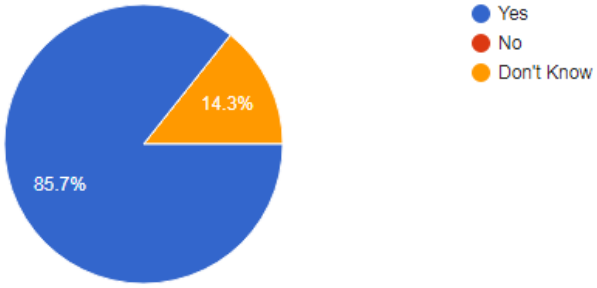
If Yes, what is the minimum working experience to attend IT Supervisory Position in your organization

6 responses



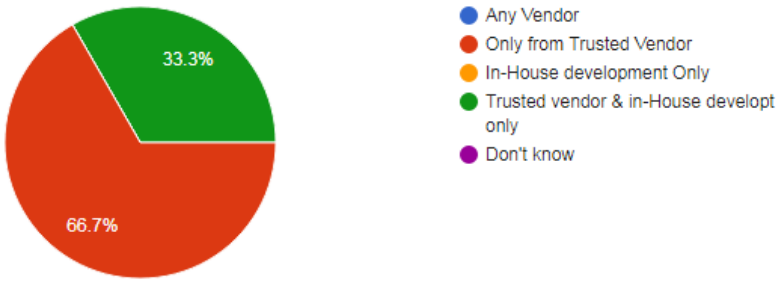
Does your organization review Cybersecurity perspective before acquiring/adopting and new operational IT infrastructure?

7 responses



If Yes, from where your organization acquired operational IT infrastructure

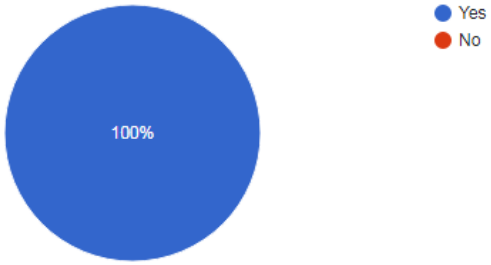
6 responses



Risk Management

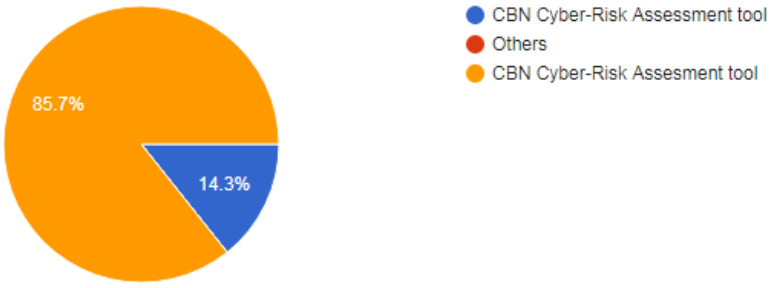
Do your organization uses cyber-risk assessment tools?

7 responses



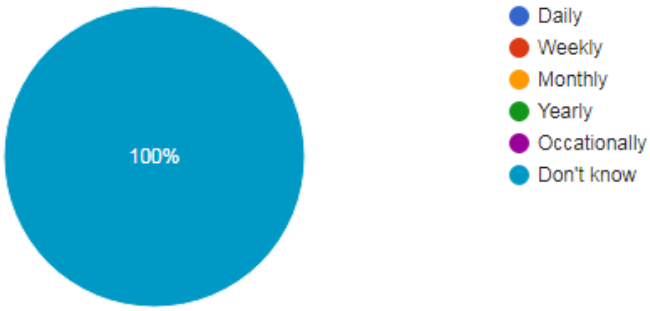
If Yes, which tool is your organization using?

7 responses



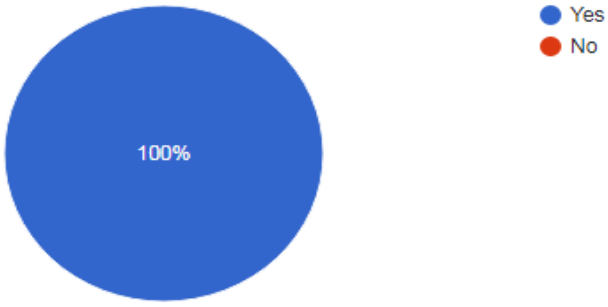
If Yes, how frequent do your organization measure Cyber-Risk?

7 responses



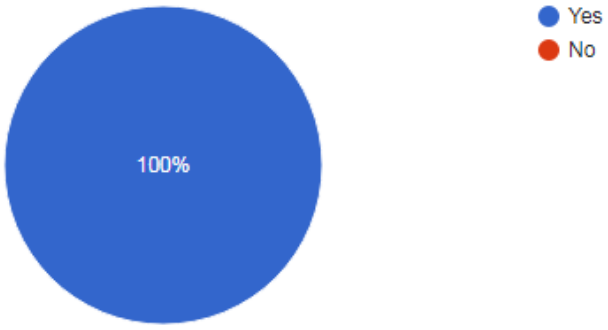
Do your organization have Cyber Risk Supervisory Position?

7 responses



Do your organization uses Cyber-Risk auditing ?

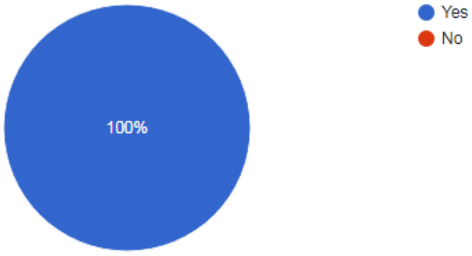
7 responses



Security Culture

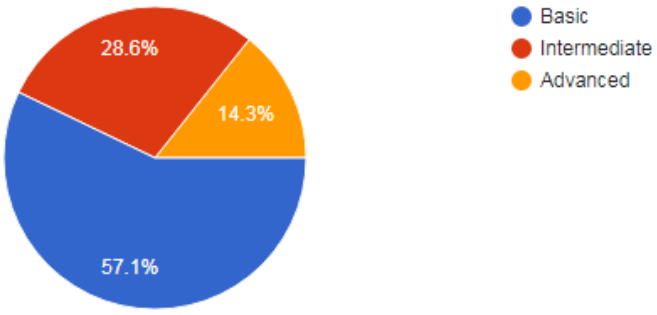
Do your operational staffs have knowledge on Cybersecurity?

7 responses



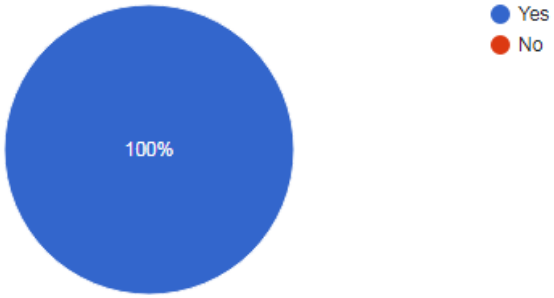
If Yes, Rate their Cybersecurity Knowledge

7 responses



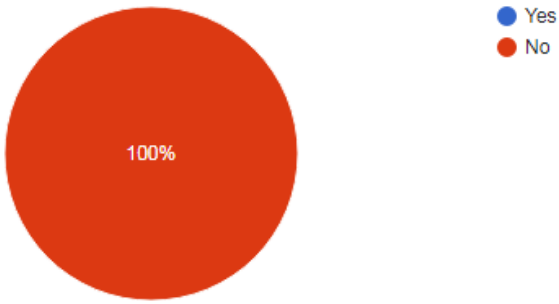
Do your organization organized internal workshop for operational staff on Cybersecurity ?

7 responses



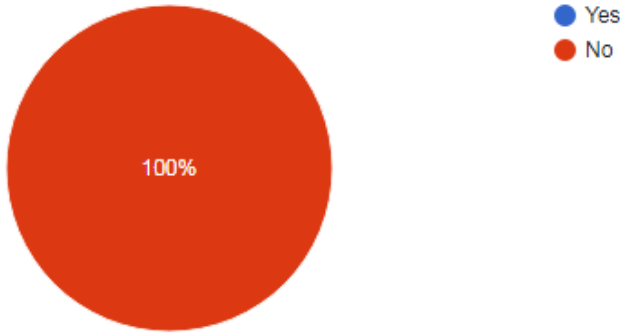
Is Cybersecurity knowledge part of skills required for employment of operational staff in your organization?

7 responses



Do you allow Bring Your Own Device (BYOD) ?

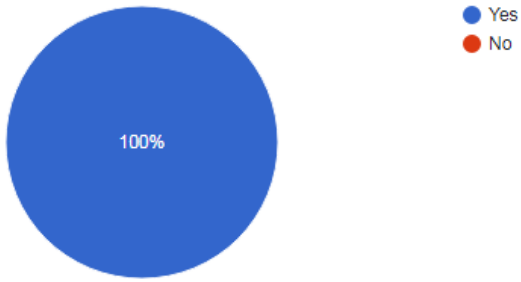
7 responses



Incidence Management

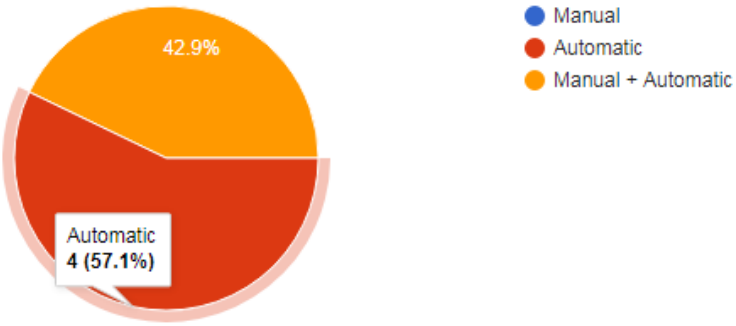
Do your organization monitor the activity logs of IT control enabled operational component?

7 responses



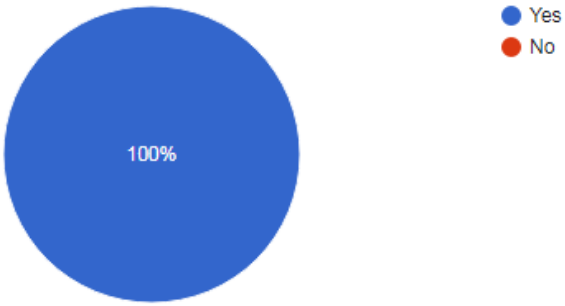
If Yes, how do you monitor the activity logs?

7 responses



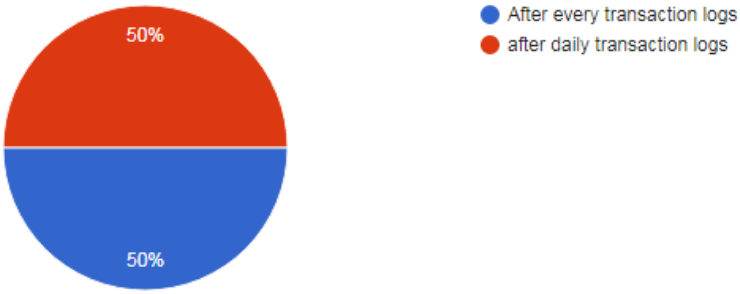
Do Your organization backup transactions logs of IT control enabled operational components ?

7 responses



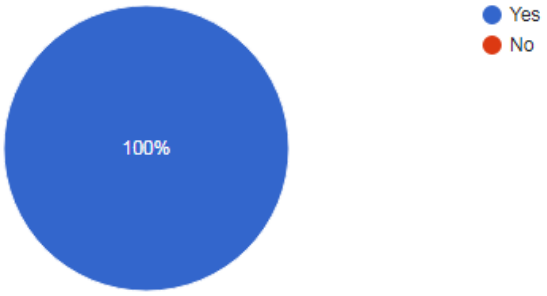
If Yes, how frequent do you backup?

6 responses



Do your organization have disaster recovery plan for IT control enabled component?

7 responses



Do you share incidence report to all Operational Staff ?

7 responses