UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

MANAGING CYBERSECURITY AS A BUSINESS RISK IN INFORMATION TECHNOLOGY-BASED SMES

ABDULRAHIM NABIHAH RISHAD

REG NO: P54/6187/2017

SUPERVISOR: CHRISTOPHER A. MOTURI

A research project report submitted to the School of Computing and Informatics in partial fulfillment of the requirements for award of Master of Science in Information Technology Management of the University of Nairobi

May, 2019

DECLARATION

This project is my original work and to the best of my knowledge this research work has not been submitted for any other award in any University.

Signature: ___________________________________ Date: __________________________

Student Name: Abdulrahim Nabihah Rishad

Registration Number: P54/6187/2017

This research has been submitted for examination with my approval as University Supervisor.

Signature: ___________________________________ Date: __________________________

Christopher A. Moturi

School of Computing and Informatics

University of Nairobi

ACKNOWLEDGEMENT

I would like to thank the Almighty God for His wisdom and strength throughout this journey. My sincere gratitude also goes to the School of Computing and Informatics, University of Nairobi for availing to me an opportunity to pursue a Master of Science in Information Technology Management. I am also thankful to all the lecturers and in particular my supervisor, Mr. Christopher A. Moturi for his support, time and invaluable contribution. I appreciate the review done by Dr. Daniel Orwa. I would also like to thank my colleagues at my work place for their endless encouragement and support.

Thank you and God bless.

DEDICATION

I dedicate this study to my parents for their love and continuous support throughout this study.

ABSTRACT

Background

Digitization has led to an increase in exposure to risks of cybercrime especially if minimal or no controls are put in place. SMEs are core to the growth of the African economy however their continued dependency on technology is driving them deeper into risk as they lack adequate cybersecurity controls.

Problem

SMEs that are developing technology-based solutions need an effective way to manage cyber-risks as part of their business risks. There is therefore need to determine key factors that influence the management of cyber-risks in Kenyan SMEs that are developing technology-based solutions and develop a strategy which will provide a roadmap for managing cyber-risk as a business risk.

Purpose

The aim of this study was to determine the key cybersecurity risks being faced by Kenyan SMEs and to develop an implementation strategy which will provide a roadmap for managing cyber-risk as a business risk.

Methodology

The research was a case study. It focused on in depth understanding of the cybersecurity risk management practices within the selected SME. Both quantitative and qualitative research was done. The quantitative data obtained was classified numerically for it to be analyzed. The qualitative data collected from primary sources was systematically organized to facilitate analysis.

Findings

The research findings reveal that cybersecurity investment, cybersecurity management, training and awareness, cybersecurity policy programs, cybersecurity vulnerability management programs, real time network monitoring and incident management play a big role in the management of cyber-risk within SMEs. The implementation strategy developed provides a roadmap with proposed timelines to assist in the management of cyber-risk.

Conclusion

The study proved that the NIST cybersecurity framework is suitable for the SME environment. This cybersecurity strategic plan was developed outlining an implementation roadmap to improve the cybersecurity posture of the organization based on the gaps identified within the environment supplemented by literature review.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CBK – Central Bank of Kenya

CERT - Computer Emergency Response Team

COSO - Committee of Sponsoring Organizations of the Treadway Commission

CTO – Chief Technology Officer

DLP – Data Loss Prevention

HRM – Human Resource Manager

ICT – Information and Communications Technology

IRA – Insurance Regulatory Authority

ISMS – Information Security Management System

ITSM – Information Technology Service Management

KNBS – Kenya National Bureau of Statistics

KPI – Key Performance Indicators

LDAP – Lightweight Directory Access Protocol

MSEA – Micro and Small Enterprise Authority

NIST – National Institute of Standards and Technology

PSP – Payment Service Provider

RM – Risk Management

SASRA - Sacco Societies Regulatory Authority

SLA – Service Level Agreement

SME –Small and Medium-sized Enterprises

USD – United States Dollar

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

DEFINITION OF TERMS

Business Risk – Business risk is the possibility a company will have lower than anticipated profits or experience a loss rather than taking a profit.

Cybercrime – Cybercrime is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Cyber-Risk – The exposure to harm or loss resulting from breaches of or attacks on information systems.

Cybersecurity – Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access.

Perpetrator – Person (s) who carries out a harmful, illegal, or immoral act.

Risk Management - ICT risk management is the application of risk management methods to information technology in order to manage ICT risk.

Security Awareness Training - A formal process for educating employees about computer security.

Service Level Agreements –SLA is a commitment between a service provider and a client. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user.

Small and Medium Sized Enterprises – Businesses whose personnel fall below two hundred and fifty (250).

Vendor – A vendor, or a supplier, is a supply chain management term that means anyone who provides goods or services to a company or individual(s).

CHAPTER ONE

INTRODUCTION

1.1 Background to the Problem

Globally, organizations are getting more digitized as they adopt more technology-based solutions. This has led to an increase in exposure to risks of cybercrime especially if minimal or no controls are put in place. Cyber-risk matters affect organizational risks, guidelines and technology. The state of cybercrime report 2017 (CSO, 2017) states that the prediction of the cost of cybercrime will increase to approximately $6 trillion in the year 2021. As a result of the rising tide of cybercrime, information security spending has been pushed to more than $86.4 billion in the year 2017 (Gartner, 2017).

The Africa cybersecurity report 2017 (Serianu, 2017) states that the approximate cybercrime costs in the year 2017 was $3.5 Billion. The country with the highest cost of cybercrime was Nigeria with an estimated cost of $649 Million. Kenya was second within the continent with an approximated cost of $210 Million. This was a significant rise as compared to the year 2016 where the estimated cost of cybercrime was $2 Billion in the African continent. In 2016, Kenya had an estimated cybercrime cost of $175 Million as stated in the Africa cybersecurity report 2016 (Serianu, 2016). The cost of cybercrime has significantly increased in Kenya by $35 Million. The report further states that over ninety (90) per cent of African organizations are operating below the security poverty line significantly exposing themselves to cybersecurity risks.

One of the ways of defining cyber-risk is risk related to online activity, electronic commerce, information systems, networks and data storage (PricewaterhouseCoopers, 2013). Cyber-risk refers to the potential loss or harm resulting from compromising the technical infrastructure within an organization (RSA, 2016).

SMEs create around 80% of Africa’s employment opportunities are provided by SMEs (World Economic Forum, 2010). The large percentage clearly indicates that they are core to the growth of the African economy. They provide numerous employment opportunities and contribute a large percentage of the national income of African countries. In Kenya SMEs account for approximately 81.1% of the employment opportunities within the country (KNBS, 2016). However, SMEs currently lack mature cybersecurity controls. SMEs are frequently automating their processes and this has increased their cybersecurity risk exposure (Serianu, 2017).

Cybersecurity related threats and incidents are considered to have a more adverse effect in larger organizations and adequate investment is put into the cyberthreat mitigation strategies. SMEs however lack affordable options and hence lack capacity to handle incidents which puts these businesses at higher risk. SMEs in Africa, particularly in Kenya, are facing a number of challenges including the highly priced cybersecurity services, restricted budgets and the lack of adequately skilled personnel. The increase in cyber-risks has led to the increased attention in managing cyber-risks as part of business risks. The most widely consumed cybersecurity solutions within the SME sector is antivirus products. SMEs were found to be implementing cybersecurity solutions and services at a slower rate than larger companies (Verbano & Venturini, 2013).

SMEs require the adoption of a cyber-risk management plan of action with clearly described guidelines which will enable them achieve cyber-resilience in the long run.

1.2 Problem Statement

The lack of adequate cybersecurity controls must be addressed by the entire SME sector. Digitization has led to an increase in exposure to risks of cybercrime especially if minimal or no controls are put in place. SMEs that are developing technology-based solutions need an effective way to manage cyber-risks as part of their business risks so as to improve their organization's cybersecurity readiness. There is therefore need to determine key factors that impact cyber-risk management in Kenyan SMEs that are developing technology-based solutions and develop a strategy which will provide a roadmap for managing cyber-risk as a business risk.

1.3 Research Objectives

i. To determine the key cybersecurity risks being faced by SMEs that are developing technology-based solutions.

ii. To review cybersecurity standards and recommend that which will be most applicable to SMEs that are developing technology-based solutions.

iii. To undertake a cybersecurity risk assessment in a selected SME.

iv. To develop an implementation strategy which will provide a roadmap for managing cyber-risk as a business risk.

1.4 Research Questions

The research sought to answer the following questions:

1. Which key cybersecurity risk areas are being faced by Kenyan SMEs that are developing technology-based solutions?
2. What type of measures have been put in place to prevent occurrence of cybersecurity breaches?
3. Which are the various standards and frameworks developed and adopted in management of cyber-risk?
4. What is the road map to address the challenges with the current cybersecurity practices?
5. How can a cybersecurity strategy address management of cybersecurity risks?

1.5 Significance of the Study

Majority of SMEs currently rely on ICT as an essential tool for meeting their business objectives. The findings in this research study provides a guidance on SMEs in Kenya on the management of cyber-risks as part of their business risks. This will enable SMEs to establish a common cyber-risk management strategy to combat cybercrime which will in turn enable them to gain higher visibility levels on risk exposure areas within the organization. A well-defined cybersecurity risk management plan helps them to adequately respond to incidents, resolve in a timely manner and put in adequate incident recovery processes. This study also helps the Government assess whether the current legislations are adequate for addressing cybersecurity risks. Regulatory bodies are provided with further insight on which key cybersecurity risk areas they need to focus on as they are developing and updating their guidelines. For the stakeholders including technology service providers, it assists in fostering a cybersecurity culture promoting the appropriate and safe cyberspace use.

CHAPTER TWO

LITERATURE REVIEW

2.1 An Overview of Cybercrime

Cyberspace has become an essential component of modern society (Radunović & Rüfenacht, 2016). Cybercrime refers to unlawful acts wherein the computer is either a target or a tool or both (Karali, Panda & Panda, 2015). The increased use of ICT is boosting the hazard of cyberattacks across the globe (Karim, 2016). During the 1980s, the banking industry had become prime cybercrime targets by insiders and self-replicating malware made its first appearance. Cybercrime accelerated as a result of the emergence of the internet towards the end of the 1990s. In the first half of the 2000s, the first denial of service attacks against large websites were executed and later on more diverse attacks were performed such as identity theft. Script injection and cross-site scripting were performed in the second half of the 2000s. The unfolding of the Tor software and the "Silk Road" platform was noted in the 2010s (Klaper & Hovy, 2014).

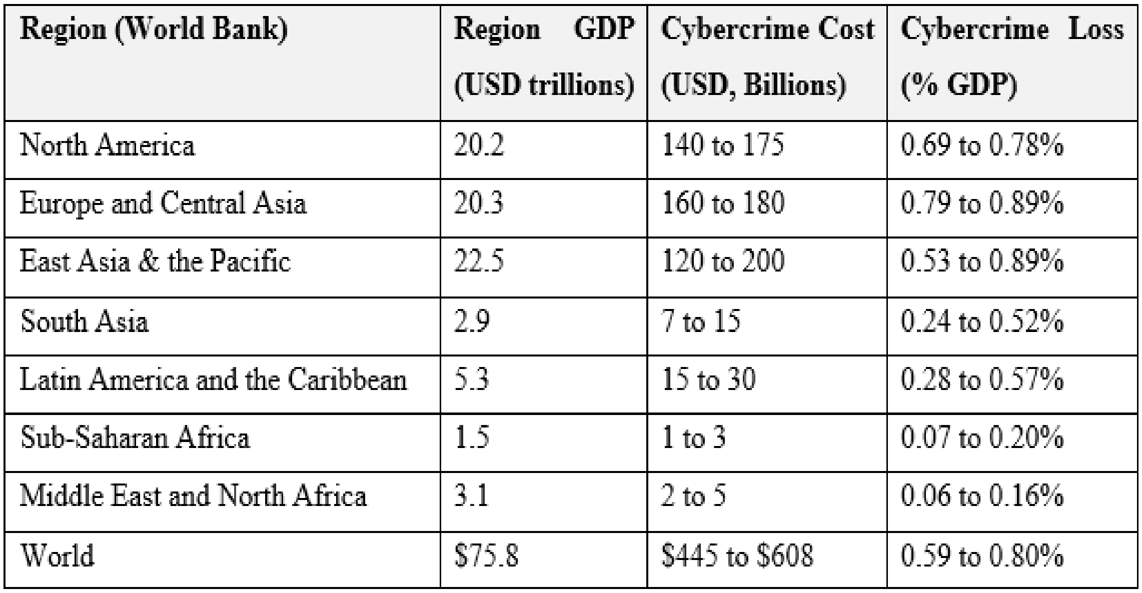
It is found that in the current decade, there is a remarkable increase of crime rate on internet. Pathak & Nanded (2016) found that the most recent trend in cybercrime is ransomware.

The consequences of cybercrime include higher exposure to cybercrimes due to inherent vulnerabilities. Antonescu & Birău (2015) found that resource allocation and technology must be achieved at high levels for both the security and protection strategies implemented within an organization.

2.2 The Cost of Cybercrime

In the year 2016, the cost of cybercrime was predicted to increase globally to $6 trillion annually by 2021. The costs associated with cybercrime are inclusive of data loss and destruction, money loss, decrease in the levels of productivity, unauthorized disclosure of personal data as well as financial data as well as reputational damage within an organization (Cybersecurity Ventures, 2017). Predictions have been made that the number of users on the internet will increase to 6 billion by the year 2022 and internet users will have increased to 7.5 billion by the year 2030 (Cybersecurity Ventures, 2017).

Table 1 Regional Distribution of Cybercrime

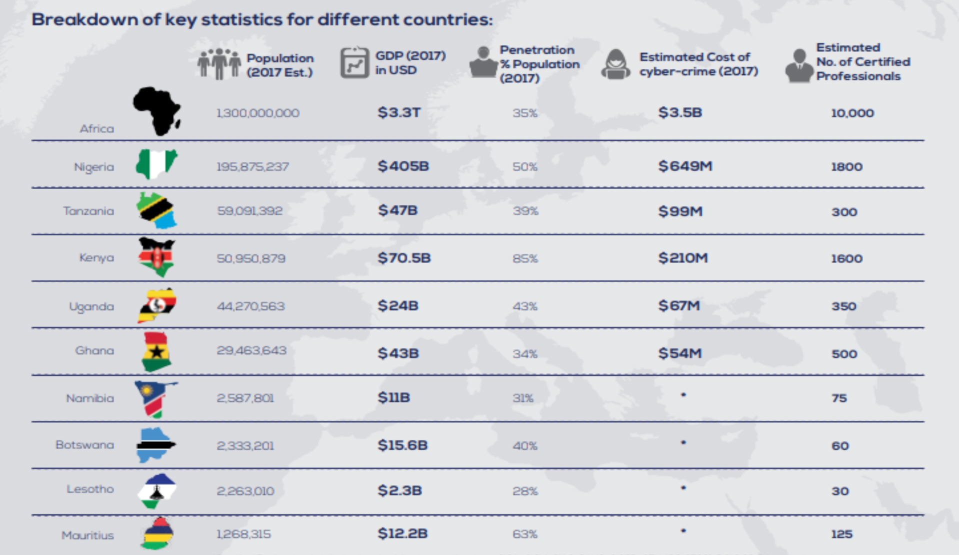


Region (World Bank)	Region GDP (USD trillions)	Cybercrime Cost (USD, Billions)	Cybercrime Loss (% GDP)
North America	20.2	140 to 175	0.69 to 0.78%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
Middle East and North Africa	3.1	2 to 5	0.06 to 0.16%
World	$75.8	$445 to $608	0.59 to 0.80%

Source: McAfee, 2017

The Africa cybersecurity report 2017 (Serianu, 2017), indicates that the year 2017 was for the most part a tough year for local organizations with respect to cybersecurity. Cybersecurity threats and data breaches greatly increased indicating that cybercriminals have now become more skilled.

Table 2 Breakdown of Cybercrime statistics for African Countries



Breakdown of key statistics for different countries:

	Population (2017 Est.)	GDP (2017) in USD	Penetration % Population (2017)	Estimated Cost of cyber-crime (2017)	Estimated No. of Certified Professionals
Africa	1,300,000,000	$3.3T	35%	$3.5B	10,000
Nigeria	195,875,237	$405B	50%	$649M	1800
Tanzania	59,091,392	$47B	39%	$99M	300
Kenya	50,950,879	$70.5B	85%	$210M	1600
Uganda	44,270,563	$24B	43%	$67M	350
Ghana	29,463,643	$43B	34%	$54M	500
Namibia	2,587,801	$11B	31%	•	75
Botswana	2,333,201	$15.6B	40%	•	60
Lesotho	2,263,010	$2.3B	28%	•	30
Mauritius	1,268,315	$12.2B	63%	•	125

Source: Africa Cybersecurity Report (Serianu, 2017)

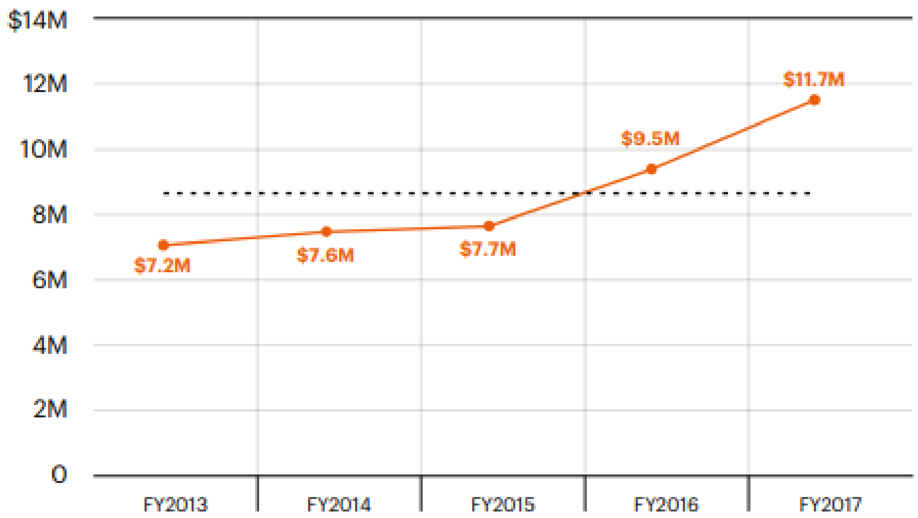


Figure 1 The average cybercrime cost globally

Source: 2017 Cost of cybercrime study (Accenture, 2017)

Accenture (2017) compiled the trends in cybercrime costs globally over a period of five years. It was noted that the cost increased steadily for a period of three years after which significant increases have been noted from the year 2016.

2.3 Consequences of Cybersecurity

The heightened role of information technology and the rise of the e-commerce sector has turned cybersecurity into a very crucial policy issue all over the world (Kaur, Sharma & Singh, 2015). Ponsard, Grandclaudon & Dallons (2018) found that as a result of the technological evolution, cyber security tends to be overlooked yet new cybersecurity threats are continuously emerging increasing exposure to cyberattacks. The increase in the frequency and complexity of cybersecurity attacks within the industry has increased the cost of preventing and recovering from cyberattacks (Watkins, 2014). Klaper & Hovy (2014) found that cybersecurity impacts are particularly critical for governments however some of the common cyberattack methods can be mitigated by educated citizens. Yeboah-Boateng (2013) found that being connected leads to an exposure to exploitable vulnerabilities which can violate the confidentiality of sensitive information. Cybercrime disrupts business transactions leading customers to worry causing reputational damage (Smith, Smith & Smith, 2010).

SMEs are especially vulnerable to these cyberthreats as they lack the resources to arm themselves in defense of cybercriminals (van Ommen, 2014). Osborn (2015) found that the lack of more affordable options for SMEs could result in them and the wider supply chain being at risk. Antonescu & Birău (2015) found that resource allocation and technology must be achieved at high levels for both the security and protection strategies implemented within an organization.

2.4 Cybercrime in SMEs

Cybersecurity risk management is still a serious issue for the SME sector as they are exposed to similar threats as more mature companies but with limited resources (Sadok & Bednar, 2016). The main reason that makes SME easier targets is that they undervalue their data (Hayes & Bodhani, 2013).

The PwC-UK (2015) survey states that security breaches were recorded by 74% of small businesses. The worst breach was noted to cost on average £75,200 indicating an increase of £10,200 from the previous year at the lower end and on the higher end it had increased to £310,800 (Sadok & Bednar, 2016). ICT security management in SMEs is an offshoot of applied business informatics that considers ICT security issues raised by computer technology (Polkowski & Dysarz, 2017).

Cybersecurity continues to be a challenge for SMEs and their business partners. The challenge being faced is that larger organizations are now mitigating security problems making SMEs a prime target for cybercrime activity (Twisdale, 2018). Despite the limited resources as compared to larger organizations, SMEs are still in a position to achieve cyber-risk resiliency (Dahlberg & Guay, 2015). Larger organizations have made great progress in their practices and internal processes however due to the limited resources in smaller organizations there is still work to be done in this area (Henson & Garfield, 2016). Chak (2015) found that SMEs lack the funding, knowledge and human capital to sufficiently defend themselves against the various cybercriminals.

2.5 Cybercrime Risk Management

Cyber-risk management addresses the processes in place to control cyber-threat related risks. The risks resulting from cyber-threats are referred to as cyber-risks (Refsdal, Solhaug, & Stølen, 2015). Key cyber-risk management factors in SMEs include:

2.5.1 Information Technology Capability and Investment

Firms often fail to understand why cybersecurity is essential. Some of the reasons mentioned included cost, time and complexity was cost, although time and complexity (Henson & Garfield, 2016). Research shows that majority of organizations carry out penetration testing, vulnerability assessments and audits which indicates that they rely on more than one technique for assurance. Majority are not aware about how much is being invested which shows that it there is still need for improvement in allocation of resources for cybersecurity initiatives (Research data, 2019). Hills & Atkinson (2016) found that a large number of SMEs have limited resources and are limited in cybersecurity investments. As a result of the increase in dependence on information systems, availability of the systems is critical for SMEs development (Santos-Olmo, Sánchez, Caballero, Camacho & Fernandez-Medina, 2016). Investing in security does not provide easily measurable benefits besides the perception of security (Kluitenberg, 2014). Fielder et al. (2018) found that as a result of the changing cyber threat landscape, investing still remains a challenging matter even if adequate resources are readily available.

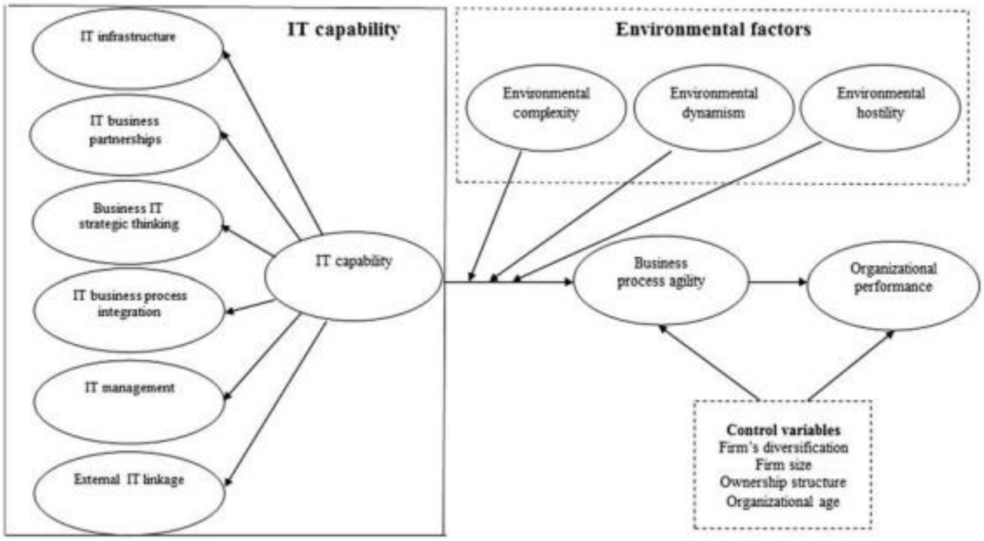


Figure 2 Factors affecting IT capability

Source: (Bhatt & Grover, 2005).

2.5.2 Management Attitude towards Security

Research shows that majority of the organizations still haven’t yet matured their cybersecurity functions. For most organizations, cybersecurity is managed in-house by someone who is tasked as a secondary role (Research data, 2019). A dedicated role is critical in the development and implementation of a cybersecurity program within an organization. Security function integration into business processes should be carried out by SMEs by engaging the internal stakeholders in the risk analysis and policy development processes (Sadok & Bednar, 2016). The whole organization should be committed with management support (Ponsard, Grandclaudon & Dallons, 2018).

2.5.3 Vendor Management

The 2017 Africa cybersecurity report (Serianu, 2017) reported that several attacks launched had vendor involvement in common. Negligent employees and third parties such as outside vendors are the primary cause of most breaches (Banham, 2017). Clear identification of external interfaces should be done and related to the identified assets to assist in determining the levels of protection needed (Ponsard, Grandclaudon & Dallons, 2018).

2.5.4 Training and Awareness

One of the key components of information security programs is awareness however SMEs still do not see themselves as targets and believe that mitigation initiatives are overly technical in nature and cost intensive (Topping, 2017). (Moturi & Mwasambo, 2016) found that most eCommerce organizations in Kenya have been affected by social engineering and phishing as the leading social engineering threat with 100% of cases tapped. Research shows that cybersecurity is now becoming a matter of growing concern as a result of the rise in social engineering attacks as majority of the respondents are to a very great degree concerned. It was however noted that not all organizations have invested in cybersecurity trainings (Research data, 2019).

There is an increase in the need to sensitize employees on cybersecurity matters as they are now the weakest link in comparison to technical vulnerabilities within their organizations (Aldawood & Skinner, 2018). The core information system users within organizations are now more exposed to cyber threats which results to both financial and information loss at individual, business and government level (Nilsen, Levy, Terrell & Beyer 2017). There is a definite identified need for cybersecurity education within SMEs (Valli, Martinus & Johnstone, 2014).

2.5.5 Information Security Policies

In the same way financial resources are protected, information assets must also be protected by the defined security policies and procedures. The information security policies must be applied across all areas of the institution. Likewise, SMEs also need to implement these security policies, which may otherwise jeopardize their entire business and, consequently, their operational and financial viability (Almeida, Carvalho & Cruz, 2018).

2.5.6 Business Continuity Management

Research has found that SMEs are not adequately prepared for crisis and as a result the consequences are more severe. The planning for and response to events is currently not given enough consideration within SMEs (Sullivan & Branicki, 2011). In addition to implementing BCM solutions to achieve higher resilience in SMEs, other controls should be implemented due to the weaknesses of the BCM concept (Dahlberg & Guay, 2015).

2.5.7 Bring Your Own Devices Management

Research shows that majority of Kenyan organizations allow their employees to use their personal devices (Research data, 2019). BYOD has been adopted by SMEs in Tanzania as a means of bypassing the investment required in organisational ICT resources (Kabanda & Brown, 2014). SMEs are required to formulate policies on the use of BYOD to avoid employees thinking that their personal devices were being used without due consideration to personal costs.

2.6 Cybersecurity Guidelines in Kenya

2.6.1 CBK Guidelines on Cybersecurity for Payment Service Providers

This guideline outlines minimum standards that should be adopted by PSPs for the development of effective cybersecurity risk management and cybersecurity governance frameworks (CBK, 2018). It is applicable to institutions licensed under the banking act. The guidelines identify three core areas:

2.6.1.1 Goverance

Bank’s leadership are required to implement strategic controls to facilitate a proactive approach to cybersecurity. It defines the roles for Board of Directors, Senior Management and Chief Information Security Officer.

2.6.1.2 Regular Independent Assessments and Tests

When analyzing the cybersecurity threat landscape within an organization, it requires collaborative efforts between the following three functions: Risk Management and both Internal and External (CBK, 2018). Internal and external auditors are mandated to develop a comprehensive approach in analyzing the bank's cyberthreat environment.

2.6.1.3 Awareness

All institutions are mandated by CBK to review their cybersecurity strategy, policy, and framework regularly based on each institution's threat and vulnerability assessment. Maintenance of awareness programs for the stakeholders is also a requirement for the banks.

2.6.2 SASRA Guideline on Risk Management Practices for Deposit-Taking Sacco Societies

SASRA released a set of guidelines on cybersecurity risk management for deposit-taking Saccos. The guidelines outline minimum standards which Saccos should adopt for development of effective cybersecurity governance and risk management frameworks.

The guidelines identify the following core areas:

2.6.2.1 Governance and Strategy

This section defines the roles of the board, senior management and head of ICT in relation to ICT strategy and risk management. Saccos are required to develop an ICT strategy in alignment with the overall business plan of the Sacco, ICT risk assessment plan and an ICT operational plan (SASRA, 2015).

2.6.2.2 Risk Management

The guideline requires the institutions to develop a risk management program which includes; risk identification, risk assessment, measuring and reporting, risk mitigation.

2.6.2.3 Internal Control and Audit

The internal audit department's function is defined within the guidelines. It also outlines the minimum aspects that should be scoped within the internal audit plan.

2.6.3 IRA Guidelines to the Insurance Industry on the Business Continuity Management

These guidelines require insurers to implement a holistic business approach when developing their business continuity management plans based on the insurers nature of business and scale of operations.

The guideline outlines the following key requirements:

i. Identification, assessment and management of possible risks associated with business continuity to ensure compliance to both financial and service obligations;

ii. A business continuity management policy must be approved by the board which incorporates business continuity risks and controls;

iii. A business continuity plan must be developed and maintained which outlines detailed procedures that can be executed to manage disruptions in business;

iv. Annual and periodic reviews of the business continuity plan must be done by both internal audit and external auditors;

v. In the event of any disruptions, the authority must be notified.

2.7 Cyber-Risk Management Frameworks

2.7.1 NIST Cybersecurity Framework

NIST have developed a framework for improving critical infrastructure cybersecurity (NIST, 2018). The framework is made up of the core, implementation tiers and framework profile. The framework has been designed to be used and adopted by various organization regardless of size including SMEs. It is flexible which allows it to be used by organizations that are starting to establish their cybersecurity programs. The framework can also be used by organizations with bigger budgets and more mature cybersecurity programs (NIST, 2018).

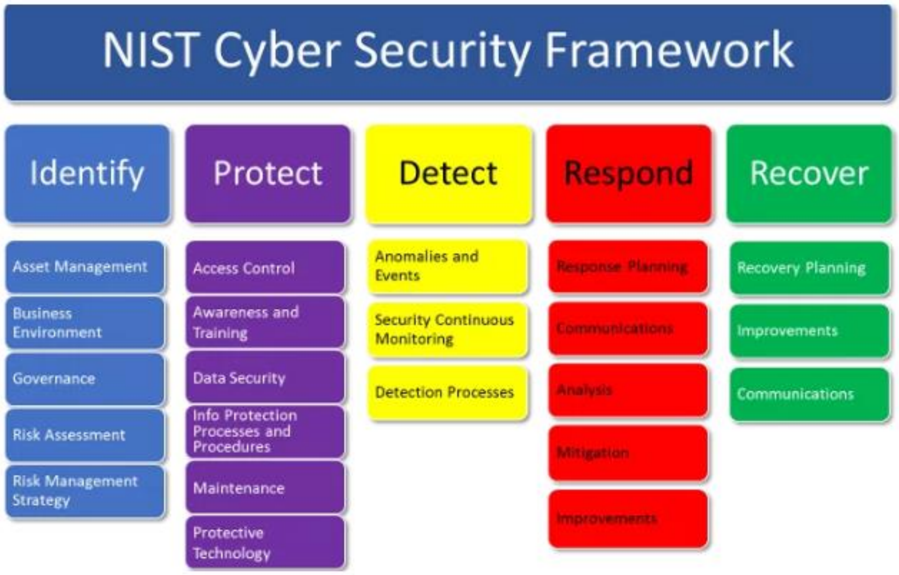


Figure 3 NIST Cybersecurity Framework

Source: Introduction to the NIST Cybersecurity Framework for a landscape of menaces (Paganinin, P.,2017)

The **Identify** module of the framework involves developing an organizational understanding within the organization to manage cybersecurity risks.

The **Protect** module of the framework deals with the development and implementation of proper security controls vital for the delivery of core services related to infrastructure.

The **Detect** module deals with the development and implementation of steps taken to establish the source of occurrence of a cybersecurity event in a timely manner.

The **Respond** module deals with developing and implementing appropriate actionable activities regarding a cybersecurity event that has been detected.

The **Recovery** module deals with the development and implementation of resilience plan activities.

2.7.2 CIS Critical Security Controls

These controls recommend a set of key action points that should be taken as cyberdefense measures in order to stop cyberattacks. The controls are both specific and actionable. The controls were created by national security teams, organizations within law enforcement and forensics and incident response organizations.

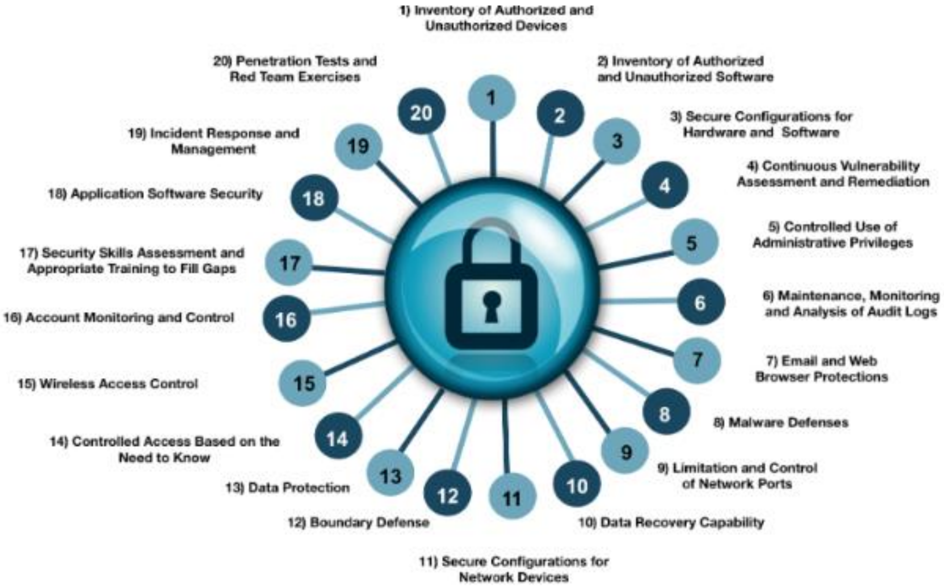

1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software
4) Continuous Vulnerability Assessment and Remediation
5) Controlled Use of Administrative Privileges
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports
10) Data Recovery Capability
11) Secure Configurations for Network Devices
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Security Skills Assessment and Appropriate Training to Fill Gaps
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Figure 4 CIS Controls

Source: SANS: CIS Critical Security Controls

These set of controls were aimed at providing organizations with a less detailed but prioritized number of controls that are required to be first implemented before yielding results and is therefore not as comprehensive as other frameworks (Gerberding, 2017).

2.7.3 COSO Enterprise Risk Management Framework

The COSO framework takes into account the demands resulting from the constantly changing business environment and addresses the need for organizations to take into consideration the constantly evolving business environment in their risk management practices (COSO, 2018). The three main concepts addressed are; objectives, components and organizational structure.

The internal control components may be used by organizations to determine their cyberprofile in order for them to securely and vigilantly secure their cybersecurity risks (Deloitte, 2015).

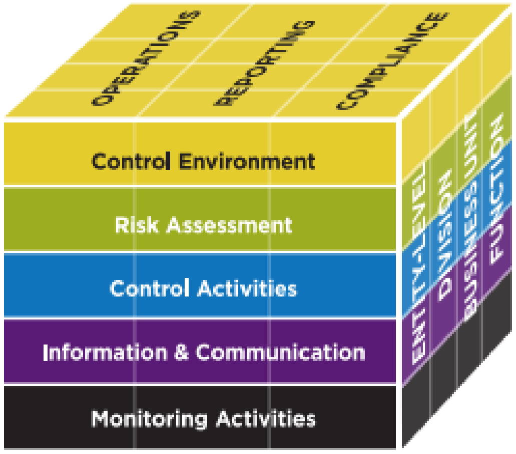


Figure 5 The COSO Cube

Source: COSO in the Cyber Age (Deloitte, 2015)

Control Environment – The control environment addresses the board's understanding of the cyber-risk profile of the organization and how well informed they are on the measures being taken by the organization to manage the evolving cybersecurity risks.

Risk Assessment – Risk assessment addresses whether the organization and its stakeholders has understood how cybersecurity risks can impact their operating, reporting and compliance objectives.

Control Activities – Control activities addresses whether the internal control activities have been developed within the organization which enables them to manage cyber-risk within the tolerance levels defined by the organization. It also addresses whether these activities have been formally documented.

Information and Communication – This addresses whether the organization has identified requirements for the management of cyber-risk internal control. This includes the definition of both internal and external communication protocols which are used in supporting the internal control function.

Monitoring Activities – This addresses activities developed by the organization for monitoring their cyber-risk profile. The organization is required to develop and perform assessments on the effectiveness of the internal cyber-risk controls developed. It also addresses how deficiencies are communicated and prioritized for remedial action.

2.7.4 ISO/IEC 27001:2013

ISO/IEC 27001 standard provides organizations with a model for the establishment, implementation, operation, monitoring, maintaining and improvement of the ISMS program. Nowadays, there is growing interest for SME to get ISO27001 certified in order to improve their ICT Security. Most organizations adopt ISO17001 to achieve compliance with various regulations and corporate government rules around information key security (Candiwan, 2014).

The process involves six steps which requires the various departments within an organization to collaborate:

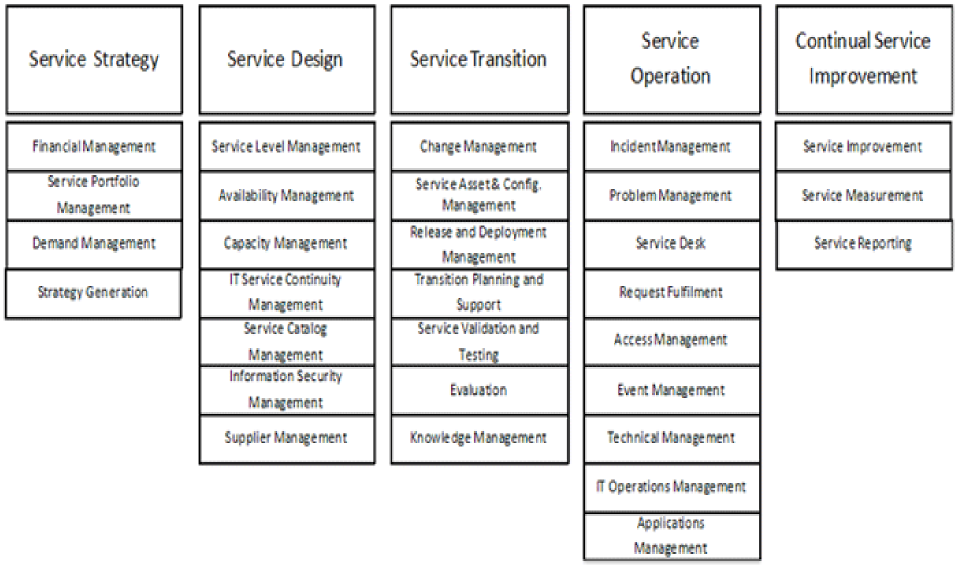
1. Security policy definition.
2. Definition and scoping of the ISMS.
3. Carrying out of a risk assessment.
4. Management of the risks that have been identified.
5. Determining the control objectives and controls that need to be implemented.
6. Applicability statement preparation.

2.7.5 Italian Cybersecurity Framework

The Italian cybersecurity framework is aimed at developing a baseline for comparison of internal business practices in order to prevent and remediate cyber-risks. The framework can be used by an organization to develop a cybersecurity strategy based on the nature of business, its size and other unique characteristics of the organization (Roberto & Luca, 2015). It has been realized in alignment with the NIST and has been adopted by the Italian government (Roberto & Luca, 2016). The framework has a specific focus on SMEs and has been tailor-made for the Italian market. It derives from the NIST Framework the basics of framework core, profile and implementation tier.

2.7.6 Information Technology Infrastructure Library (ITIL) Framework

The ITIL framework defines ICT service management practices which focus on the alignment of ICT services with the unique business needs. The framework defines processes and key action points that can be implemented by an organization for the establishment of an integrated strategy for value delivery at minimum competency levels. These controls are neither organization nor technology specific. It lets organizations establish baselines from which planning, implementation and measurement can be done.



Service Strategy	Service Design	Service Transition	Service Operation	Continual Service Improvement
Financial Management	Service Level Management	Change Management	Incident Management	Service Improvement
Service Portfolio Management	Availability Management	Service Asset & Config. Management	Problem Management	Service Measurement
Demand Management	Capacity Management	Release and Deployment Management	Service Desk	Service Reporting
Strategy Generation	IT Service Continuity Management	Transition Planning and Support	Request Fulfilment	
	Service Catalog Management	Service Validation and Testing	Access Management	
	Information Security Management	Evaluation	Event Management	
	Supplier Management	Knowledge Management	Technical Management	
			IT Operations Management	
			Applications Management	

Figure 6 ITIL Framework

Source: ITIL Lite: Vital ITIL by Malcolm Fry

Service Strategy – This details guidelines on the design, development and implementation of service management from an organizational capability view.

Service Design – This entails guidelines on the design and the development of both services and the process for service management.

Service Transition – This details guidelines for capability improvement of new and changed services transitioning into operations.

Service Operation – This provides guidance on effectiveness achievement when delivering and supporting services so as to ensure both service provider and customer value.

Continual Service Improvement – It includes the guidelines for the creation and maintaining of customer value.

2.7.7 Control Objectives for Information and Related Technologies (COBIT)

COBIT provides a set of ICT controls which when organized form a logical framework of ICT-related processes and enablers (Haes & Grembergen, 2015). The framework enables well-defined processes for policy development as well as best practices for ICT management within organizations. COBIT enables clear policy development and good practice for ICT control throughout organizations. The framework also emphasizes on the need for compliance to regulatory requirements and enables alignment and implementation of the ICT governance and control framework (ISACA, 2018).

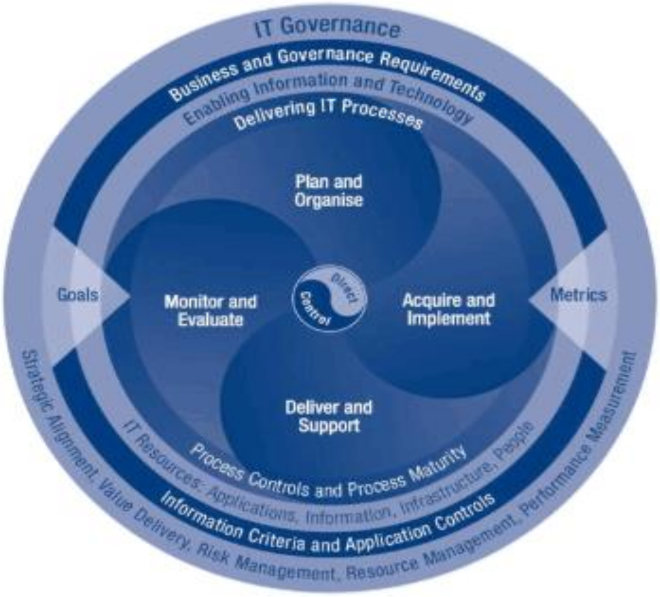

IT Governance
Business and Governance Requirements
Enabling Information and Technology
Delivering IT Processes
Plan and Organise
Goals
Monitor and Evaluate
Direct
Control
Acquire and Implement
Metrics
Deliver and Support
Process Controls and Process Maturity
IT Resources: Applications, Information, Infrastructure, People
Information Criteria and Application Controls
Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement

Figure 7: COBIT Framework

Source: COBIT 4.1 Framework for IT Governance and Control (ISACA)

The four domains covered by COBIT are as described below:

Plan and Organize - This covers the use of technology within an organization and how best it can be done to achieve the company's goals and objectives.

Acquire and Implement - The aim is to identify its ICT requirements acquiring the technology and to implement it within the company's current business processes. This also handles the development of a maintenance plan for ICT systems and components.

Delivery and Support - This handles the management of delivery services.

Monitor and Evaluate – This covers the needs assessment strategy defined by the company and whether the current ICT system is still meeting its design objectives and the necessary controls for compliance to regulatory requirements.

2.7.8 ISSA 5173 (UK)

The ISSA (UK) standard outlines recommendations for SMEs on information security controls. The standard is aimed at encouraging SMEs to safeguard both customers and employees' data and raise their data security awareness levels. The prioritization scheme defined by the standard is interesting however it currently has not been actively developed (Ponsard, Grandclaudon & Dallons, 2018).

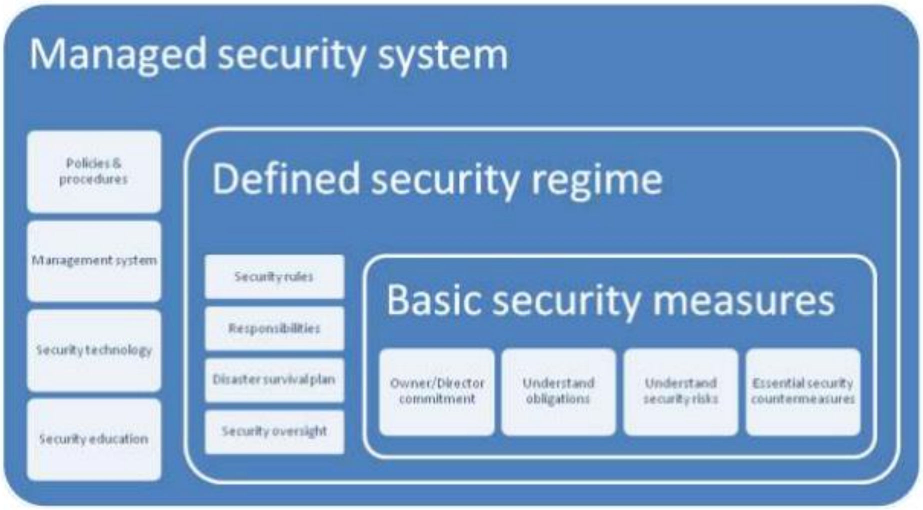


Figure 8 An example of how security controls can be prioritized

Source: Information Security for Small and Medium Sized Enterprises (ISSA-UK 5173)

2.7.9 Summary of frameworks

Table 3 Comparison table for Frameworks

FRAMEWORK NAME	ORGANIZATION	DESCRIPTION	SOURCE
COSO	COSO	• Designing and evaluation of internal control effectiveness is done in a more formal structure using the COSO framework. • COSO accentuates the use of management's decision making ability on policies and procedures for decision making.	(Deloitte, 2017) (Leal,2016)
CIS Security Controls	SANS	• The CIS controls provide more distinct and practicable methods to detect and prevent cybersecurity attacks. • The development of the controls was aimed at providing organizations with a set of smaller and more prioritized actionable controls that are first required to be implemented in order to produce results immediately and is therefore not as comprehensive as other frameworks.	(Gerberding, 2017)
ISO 27001:2013	ISO	• Provides a standard for the management of Information Security. • One of the constraints of the ISO standard is that it only provides details on what needs to be achieved and lacks the details on what needs to be done in order to attain the requirements.	(Leal, 2016)
NIST	NIST	• It is a detailed risk management framework. • The controls are flexible and can be easily customized and implemented as part of an organization's overall risk management strategy.	(Gerberding, 2017)
COBIT	ISACA	• Inputs, outputs, key activities, objectives, and performance measures are defined for each process in COBIT.	(Leal, 2016)

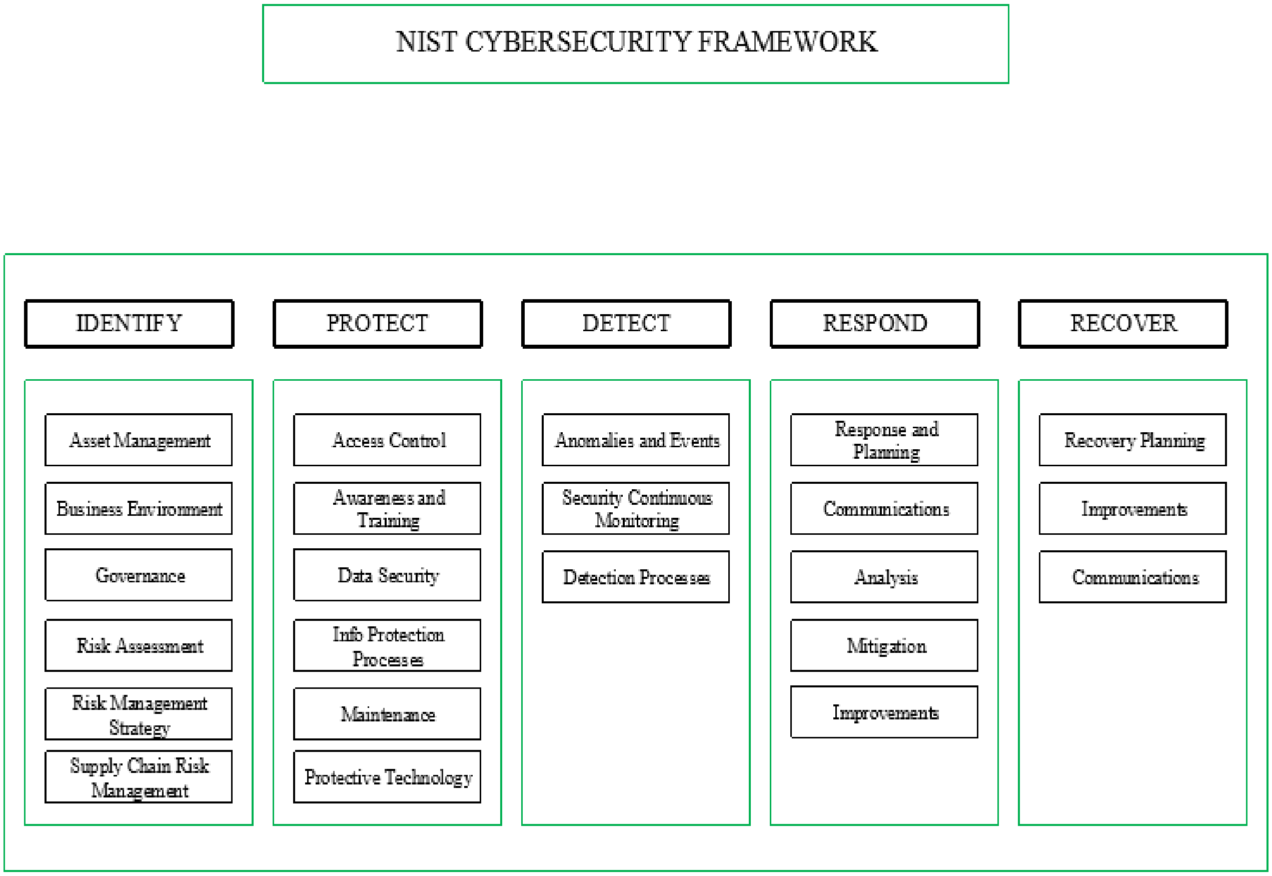
FRAMEWORK NAME	ORGANIZATION	DESCRIPTION	SOURCE
		- Implementation still remains a challenge as the framework lacks technical details to support it.	
ITIL	ITIL	- It is used to align ICT resources to business goals. It is useful for increasing visibility into internal processes. - Implementation is a demanding activity in need of substantial dedicated resources - The ITIL philosophy often requires organizations to change their culture in order to embrace the new processes	(Iden & Eikebrokk, 2014).
ISSA 5173 (UK)	ISSA	- The standard has currently not been actively developed but it presents an prioritization scheme that is interesting.	(Ponsard, Grandclaudon & Dallons, 2018)

2.8 Cybersecurity Strategy

An organization can become a victim to cybersecurity vulnerabilities without a well-defined and implemented cybersecurity strategy. A cybersecurity strategy may not necessarily eliminate security threats however it provides a better chance for planning, reviewing and evaluating an organization's exposure to security incidents (Mierzwa & Scott, 2017). The goal of a cybersecurity strategy is the alignment of organizational wide efforts to achieve or make improvements on their cyber security posture. The overall objective of the cybersecurity strategy is to find a balance between acceptable norms defined by a country and internet presented opportunities (Azmi, Tibben & Win, 2016). Bell (2017) found that SMEs provide a good foundation for cybersecurity strategy implementation as they lack silos. However, it is also important to note that SMEs are challenged due to resources and may not be able to allocate someone to implement the strategy within the organization.

2.9 Conceptual Framework

A conceptual framework is a model of presentation, whereby graphical or diagrammatic relationships between the variables in the study are represented. The conceptual framework was adapted as is from the NIST cybersecurity framework from the literature review results.



The **identify** module of the framework involves developing an organizational understanding within the SME of cybersecurity risk management. The categories of the identify function are:

1. Asset Management – Facilities that enable the SME to achieve its business objectives relative to the SMEs risk strategy.
2. Business Environment – Understanding and prioritization of the SMEs mission and objectives which is used to inform cybersecurity roles and responsibilities as well as decisions around risk management.
3. Governance - Policies and procedures that inform management practices of cybersecurity related risks.
4. Risk Assessment – Organizational cybersecurity risks are understood according to operations assets as well as individuals.
5. Risk Management Strategy – Establishment of priorities and risk tolerances that support decisions around risks.
6. Supply Chain Risk Management – Establishment and implementation of processes for supply chain risk management.

The **protect** module of the framework deals with the development and implementation of proper security controls vital for the delivery of core services related to infrastructure. The categories of this function are:

1. Access Control – Limited authorized access has been provided to the SMEs critical physical and logical assets.
2. Awareness and Training – Cybersecurity training and awareness programs have been established within the SMEs.
3. Data Security – Confidential data is protected and managed within the SME according to the defined risk strategy.
4. Information Protection Processes and Procedures – Information security policies and procedures are developed and maintained within the SME.
5. Maintenance – Information system components are maintained according to the SMEs policies and procedures.
6. Protective Technology – Management of the technical security solutions is managed consistently with the SMEs policies and procedures.

The **detect** module deals with development and implementation of steps taken to establish the source of occurrence of a cybersecurity event in a timely manner. The categories in this function are:

1. Anomalies and Events - Anomalous activity is detected and the potential impact of events is understood within the SME.
2. Security Continuous Monitoring – Cybersecurity monitoring of information systems and assets is done within the SME.
3. Detection Processes – Maintenance and testing of detection processes is carried out within the SME.

The **respond** module deals with developing and implementing appropriate actionable activities regarding a cybersecurity event that has been detected. The categories in this function are:

1. Response Planning – Maintenance and execution of response processes is carried out to affirm response to incidents detected within the SME.
2. Communications – The response activities within the SME are coordinated with the stakeholders.
3. Analysis – Response and recovery activities within the SME are analyzed to ensure effectiveness.
4. Mitigation – Event impact minimization and incident resolution activities are carried out within the SME.
5. Improvements – Lessons learnt from previous detection and response activities are used to improve the SME response activities.

The **recovery** module deals with the development and implementation of resilience and restoration activities for services affected by cybersecurity events. It includes:

1. Recovery Planning – Execution and maintenance of recovery processes is done to ensure restoration of systems that have been affected cybersecurity incident within the SME.
2. Improvements – Lessons learnt are incorporated to recovery planning processes in order to improve them.
3. Communications – Both the internal and external parties are involved in restoration within the SME.

CHAPTER THREE

RESEARCH METHODOLOGY

This chapter contains the research philosophy, research design, case background, data collection methods, data analysis methods, validity testing and ethical considerations that were used to assess the management of cybersecurity as a business risk in Kenyan Information Technology based SMEs.

3.1 Research Philosophy

This research adopted the pragmatic philosophy which advocates the use of mixed methods in research, sidesteps the contentious issues of truth and reality and focuses instead on ‘what works’ as the truth regarding the research questions under investigation. Using this approach, any of the methods, techniques and procedures associated with quantitative or qualitative research were able to be used. It recognizes that every method has its limitations and that different approaches can be complementary.

3.2 Research Design

The study adopted a descriptive research design through which the existing state of affairs was able to be depicted. The major purpose of this is description of the state of affairs as it exists at present (Kothari, 2004).

The research was a case study. It focused on in depth understanding of the cybersecurity risk management practices within the selected SME. Both quantitative and qualitative research was done. Quantitative research is based on the measurement of quantity or amount. It is applicable to phenomena that can be expressed in terms of quantity. Qualitative research, on the other hand, is concerned with phenomena relating to or involving quality or kind (Kothari, 2004).

3.3 Case Background

The organization is a leading technology services provider that develops, supplies and manages software solutions and services. It has a 20 years’ presence in the market and is a fully Kenyan owned company. The organization has 45 clients cutting across seven countries including Kenya, Uganda, Ethiopia, Zambia, Nigeria, Ghana and South Africa. It offers services to both mainstream and distributor segments. The organization's staff complement of 130 plus comprising of permanent, fixed term and contract workers in the Kenya, Nigeria and Ghana country offices. Over the last four years the firm has grown significantly in both a technological and people perspective. This is evident from the increase in product ranges and market segment. This has therefore increased the need for them to have adequate cybersecurity risk management practices.

3.4 Data Collection Methods

The data collection was done using two phases. The first phase included obtaining survey data which was collected from 118 respondents country-wide to determine the state of cybersecurity within Kenya. The data relevant to the conceptual framework of the study was selected for further analysis.

The second phase included generating open ended questions to collect qualitative data based on the NIST framework. Interview sessions were held with the Chief Technology Officer, ICT manager, finance team, Business Process Owners, sales and marketing lead, network manager, HR manager as well as general users. Secondary data sources including policies and procedures as well as control implementation evidence were also used to gather information and evidence regarding the research problem.

Table 4 Data Collection Methods

Data Source	Type of Data	Use of data collected
Questionnaires	Quantitative Data	To give background information about the state of cybersecurity within organizations.
Interviews with CTO, Business Process Owners, finance team and sales and marketing lead.	Qualitative Data	To understand the decision-making process with regards to cybersecurity within their organization.
Interviews with ICT Personnel and General Users	Qualitative Data	To gain in depth understanding of key cybersecurity concern areas in day to day processes.

In carrying out the risk assessment, the following steps were used as defined by the NIST framework:

Prioritization and scoping: This included identifying and determining the organization's mission and objectives. It also involved a high level analysis of the organization's priorities.

Orientation: This involved the identification of the in scope systems and information assets as well as the risk approach.

Creation of a current profile: This involved identifying the controls that have currently been implemented within the SME.

Conduction of a risk assessment: This involved an analysis of the operational environment and overall risk management practices. This was done through personal opinion with bias to best practice standards based on the NIST controls.

Creation of a target profile: This involved defining the target cybersecurity posture of the SME.

Determination, analysis and prioritization of gaps: This involved creation of a prioritized action plan, in this case the cybersecurity strategy to achieve the outcomes in the target profile.

Implementation of action plan: This involved defining timelines and stakeholders tasked with implementation of the defined action points.

3.5 Data Analysis Methods

Deductive content analysis approach (Kothari, 2004) was used based on the conceptual framework. The quantitative data obtained was classified numerically for it to be analyzed. The qualitative data collected from primary sources was systematically organized to facilitate analysis. It involved collected data editing, coding, classification and tabulation (Kothari, 2004).

Editing: This involved scrutinizing the data collected from interviews to detect errors and omissions so that they can be corrected. This ensured that the data accuracy and consistency.

Coding: Coding was done at interview questionnaire level. The NIST coding method was adapted.

Classification: Data was classified according to its attributes and analyzed into the NIST functions to identify any similarities and differences.

Tabulation: Data collected was arranged into concise and logical order for further analysis. This facilitated comparison and provided a basis for statistical computation to determine the organization’s current risk profile.

3.6 Validity Testing

Validity is establishing whether the instrument content is measuring what it is supposed to measure (Mugenda, 2003). For this study, respondent validation technique was used so as to determine whether the respondents acknowledge that the results are authentic. This was done once the results were analyzed and condensed. The data obtained was also analyzed against cybersecurity risk management practices in the context of other SMEs to determine how they have been adopted within the organization.

3.7 Ethical Considerations

The research purpose was clearly communicated to those responding to the questionnaires and interviews. Privacy and anonymity was maintained and this was assured to the respondents. Consent was also sought by the target respondents before carrying out the research.

CHAPTER FOUR

DATA ANALYSIS, RESULTS AND DISCUSSION

This chapter contains data analysis approach used, presentation of the cybersecurity risk management findings, cybersecurity strategy and discussion of study.

4.1 Data Analysis

Data analysis was done using a combination of primary and secondary data. The Primary data was obtained by use of an interview guide in line with the NIST framework. The targeted population was seven key individuals, all of which were available. This population consisted of the Chief Technology Officer, ICT manager, finance team, Business Process Owners, sales and marketing lead, network manager, HR manager as well as general users. The criteria for selecting these individuals include; their current position, the duration at which they have worked in the organization and their qualifications. The target population have served the organization for more than five years and include heads of departments within the organization. They have undergraduate qualifications in relation to their areas of expertise as well as professional certifications. This therefore made them suitable audience in providing the necessary information needed for this study.

Secondary data sources including policies and procedures as well as control implementation evidence were also used to gather information and evidence related to the research problem. The qualitative data was edited, coded, classified and tabulated according to the NIST framework.

4.1.1 Control Mapping to Target Population

4.1.1.1 Core Function: Identify (ID)

This tables below present a summary of the mapping of the controls under the identify core function to the person(s) interviewed within the SME.

Table 5 Asset Management Target Population

Sub-Category	**Person Interviewed**
ID.AM-1: Physical devices and systems within the organization are inventoried	ICT Manager
ID.AM-2: Software platforms and applications within the organization are inventoried	ICT Manager
ID.AM-3: Organizational communication and data flows are mapped	ICT Manager
ID.AM-4: External information systems are catalogued	ICT Manager
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	ICT Manager
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	ICT Manager

Table 6 Business Environment Target Population

Sub-Category	**Person Interviewed**
ID.BE-1: The organization’s role in the supply chain is identified and communicated	CTO
ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated	CTO
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	CTO
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	CTO
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	CTO

Table 7 Governance Target Population

Sub-Category	**Person Interviewed**
ID.GV-1: Organizational cybersecurity policy is established and communicated	CTO
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	CTO
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	CTO
ID.GV-4: Governance and risk management processes address cybersecurity risks	CTO

Table 8 Risk Assessment Target Population

Sub-Category	Person Interviewed
ID.RA-1: Asset vulnerabilities are identified and documented	ICT Manager
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	ICT Manager
ID.RA-3: Threats, both internal and external, are identified and documented	ICT Manager
ID.RA-4: Potential business impacts and likelihoods are identified	ICT Manager
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	ICT Manager
ID.RA-6: Risk responses are identified and prioritized	ICT Manager

Table 9 Risk Management Strategy Target Population

Sub-Category	Person Interviewed
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Business Process Owner
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	Business Process Owner
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	Business Process Owner

Table 10 Supply Chain Risk Management Target Population

Sub-Category	Person Interviewed
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Business Process Owner
ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber-supply chain risk assessment process	Sales and Marketing Lead
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Sales and Marketing Lead
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	Sales and Marketing Lead
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	CTO

4.1.1.2 Core Function: Protect (PR)

This tables below present a summary of the mapping of the controls under the protect core function to the person(s) interviewed within the SME.

Table 11 Identity Management, Authentication and Access Control Target Population

Sub-Category	Person Interviewed
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	ICT Manager
PR.AC-2: Physical access to assets is managed and protected	ICT Manager
PR.AC-3: Remote access is managed	ICT Manager
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	ICT Manager
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	ICT Manager
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	ICT Manager
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	ICT Manager

Table 12 Awareness and Training Target Population

Sub-Category	Person Interviewed
PR.AT-1: All users are informed and trained	ICT Manager General Users
PR.AT-2: Privileged users understand their roles and responsibilities	ICT Manager
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	ICT Manager
PR.AT-4: Senior executives understand their roles and responsibilities	ICT Manager
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	ICT Manager

Table 13 Data Security Target Population

Sub-Category	Person Interviewed
PR.DS-1: Data-at-rest is protected	ICT Manager
PR.DS-2: Data-in-transit is protected	ICT Manager
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	ICT Manager
PR.DS-4: Adequate capacity to ensure availability is maintained	ICT Manager

PR.DS-5: Protections against data leaks are implemented	ICT Manager
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	ICT Manager
PR.DS-7: The development and testing environment(s) are separate from the production environment	ICT Manager
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	ICT Manager

Table 14 Information Protection Processes and Procedures

Sub-Category	Person Interviewed
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	ICT Manager
PR.IP-2: A System Development Life Cycle to manage systems is implemented	ICT Manager
PR.IP-3: Configuration change control processes are in place	ICT Manager
PR.IP-4: Backups of information are conducted, maintained, and tested	ICT Manager
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	ICT Manager
PR.IP-6: Data is destroyed according to policy	ICT Manager
PR.IP-7: Protection processes are improved	ICT Manager
PR.IP-8: Effectiveness of protection technologies is shared	ICT Manager
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	ICT Manager
PR.IP-10: Response and recovery plans are tested	ICT Manager
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	HR Manager
PR.IP-12: A vulnerability management plan is developed and implemented	CTO

Table 15 Maintenance Target Population

Sub-Category	Person Interviewed
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	ICT Manager Finance Team
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	ICT Manager

Table 16 Protective Technology Target Population

Sub-Category	**Person Interviewed**
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	ICT Manager
PR.PT-2: Removable media is protected and its use restricted according to policy	ICT Manager
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	ICT Manager
PR.PT-4: Communications and control networks are protected	ICT Manager
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	ICT Manager

4.1.1.3 Core Function: Detect (DE)

This tables below present a summary of the mapping of the controls under the detect core function to the person(s) interviewed within the SME.

Table 17 Anomalies and Events Target Population

Sub-Category	**Person Interviewed**
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Network Manager
DE.AE-2: Detected events are analyzed to understand attack targets and methods	Network Manager
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	Network Manager
DE.AE-4: Impact of events is determined	Network Manager
DE.AE-5: Incident alert thresholds are established	Network Manager

Table 18 Security Continuous Monitoring Target Population

Sub-Category	**Person Interviewed**
DE.CM-1: The network is monitored to detect potential cybersecurity events	Network Manager
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Network Manager
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Network Manager
DE.CM-4: Malicious code is detected	Network Manager
DE.CM-5: Unauthorized mobile code is detected	Network Manager
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	ICT Manager

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	ICT Manager
DE.CM-8: Vulnerability scans are performed	ICT Manager

Table 19 Detection Processes Target Population

Sub-Category	**Person Interviewed**
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	ICT Manager
DE.DP-2: Detection activities comply with all applicable requirements	ICT Manager
DE.DP-3: Detection processes are tested	ICT Manager
DE.DP-4: Event detection information is communicated	ICT Manager
DE.DP-5: Detection processes are continuously improved	ICT Manager

4.1.1.4 Core Function: Respond (RS)

This tables below present a summary of the mapping of the controls under the respond core function to the person(s) interviewed within the SME.

Table 20 Response Planning Target Population

Sub-Category	**Person Interviewed**
RS.RP-1: Response plan is executed during or after an incident	ICT Manager

Table 21 Communications Target Population

Sub-Category	**Person Interviewed**
RS.CO-1: Personnel know their roles and order of operations when a response is needed	ICT Manager
RS.CO-2: Incidents are reported consistent with established criteria	ICT Manager
RS.CO-3: Information is shared consistent with response plans	ICT Manager
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	CTO
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	CTO

Table 22 Analysis Target Population

Sub-Category	**Person Interviewed**
RS.AN-1: Notifications from detection systems are investigated	ICT Manager
RS.AN-2: The impact of the incident is understood	ICT Manager

RS.AN-3: Forensics are performed	ICT Manager
RS.AN-4: Incidents are categorized consistent with response plans	CTO
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	CTO

Table 23 Mitigation Target Population

Sub-Category	**Person Interviewed**
RS.MI-1: Incidents are contained	ICT Manager
RS.MI-2: Incidents are mitigated	ICT Manager
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	ICT Manager

Table 24 Improvements Target Population

Sub-Category	**Person Interviewed**
RS.IM-1: Response plans incorporate lessons learned	ICT Manager
RS.IM-2: Response strategies are updated	ICT Manager

4.1.1.5 Core Function: Recover (RS)

This tables below present a summary of the mapping of the controls under the recover core function to the person(s) interviewed within the SME.

Table 25 Recovery Planning Target Population

Sub-Category	**Person Interviewed**
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	ICT Manager

Table 26 Improvements Target Population

Sub-Category	**Person Interviewed**
RC.IM-1: Recovery plans incorporate lessons learned	ICT Manager
RC.IM-2: Recovery strategies are updated	ICT Manager

Table 27 Communications Target Population

Sub-Category	**Person Interviewed**

RC.CO-1: Public relations are managed	CTO
RC.CO-2: Reputation is repaired after an incident	CTO
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	CTO

4.2 Cybersecurity Risk Management within the SME

The interview respondents were asked questions in relation to their areas of expertise based on the NIST framework. The objective of this was to establish the current profile of the organization and determine the desired target profile. The comparison of the profiles was done with the purpose of identifying gaps to be addressed which would contribute to the cybersecurity strategy developed. The tiers defined by NIST are partial, risk informed, repeatable and adaptive. The results below represent the findings as per the framework's core functions. Further details have been provided in appendix four.

4.2.1 Core Function: Identify (ID)

4.2.1.1 Asset Management (ID.AM)

The organization's ICT asset management policy which defines ICT asset management processes to ensure IT assets are identified, inventoried and maintained was reviewed. Every employee at the organization has a responsibility for protecting the confidentiality of the company's information. The organization has implemented an ICT asset management tool which is able to track physical devices and systems as well as software applications. From a functional perspective, organizational data flows and communication have been mapped. These have been documented data classification standard document. Classification is done indicating the need, priorities and degree of protection needed.

While these are good controls which have been implemented there are also areas of concern with regards to asset management. A formal process for updating the asset inventory currently lacks within the organization. A hardware resource classification standard that prioritizes hardware assets based on criticality currently lacks.

4.2.1.2 Business Environment (ID.BE)

The organization has identified its role within the supply chain. Prioritization of organizational goals and objectives have been documented and are communicated to the relevant stakeholders who are in charge of implementation. The organization is highly dependent on selected service providers such as the two identified Internet Service Providers.

4.2.1.3 Governance (ID.GV)

The respondent pointed out that an organizational cybersecurity policy has been established. The cybersecurity policies which seek to establish and maintain comprehensive protection and clear accountability for the organization's information assets and resources were reviewed. This includes information assets that are proprietary to the organization, private to the organization's customers and all other private and proprietary information assets and resources that, if subject to inadvertent or unauthorized disclosure, would likely cause financial, legal, regulatory, or reputation damage to the organization. Cybersecurity management is currently outsourced to a third party who provides services when need occurs. Legal and regulatory requirements applicable to the organization are addressed within their cybersecurity risk management practices.

However, it was noted that not all policies are regularly updated. Cybersecurity policies need to be regularly updated to provide relevant direction within the organization.

4.2.1.4 Risk Assessment (ID.RA)

It was clear that vulnerability assessments and penetration testing is carried out within the organization both at complete network level and application specific assessment. These are carried out by an independent third party cybersecurity services provider. The results of these assessments are well inventoried and documented. Cyber threat intelligence is received from third party security provider.

Stand up meetings are done on a regular basis where the organization discusses their various products and potential business impacts are documented. Any issues identified are remediated by the internal ICT team.

The organization's main challenge in this area is that there lacks a formal process of distributing threat intelligence information to other members of the organization. In addition, an accountability process for tracking on closure of assessment findings currently lacks.

4.2.1.5 Risk Management Strategy (ID.RM)

The information security risk and compliance management standard document was reviewed. This policy breaks down the core activities of risk management which include; identification assessment and monitoring. It was noted that risks are looked at in three perspectives which include; product risks, project risks and customer risks. Cybersecurity risks are addressed as part of product and customer risks. Organizational risk tolerance is addressed through a consultative approach between the organization and its customers.

However, there are areas of concern with regards to risk management strategy. The information security risk and compliance management standard document currently lacks a formal review and updating process.

4.2.1.6 Supply Chain Risk Management (ID.SC)

In terms of supply chain risk management, the respondent explained that risk thresholds are determined and operationalized internally. Risks are minimized through a methodology of constant evaluation. Contracts are developed for all clients which address issues of protection and confidentiality of data which meet objectives of the SME's cybersecurity program. Initial due diligence is done on clients however it was clear that there lacks a routinely process for assessing third party vendors.

4.2.1.7 Breakdown of Controls Assessed in the Identify Core Function

The table below represents a summary of the controls that were assessed under the identify core function.

Table 28 Identify analysis

CATEGORY	CONTROLS ASSESSED	PASSED	FAILED
Asset Management (ID.AM)	6	3	3
Business Environment (ID.BE)	5	2	3
Governance (ID.GV)	4	3	1
Risk Assessment (ID.RA)	6	3	3
Risk Management Strategy (ID.RM)	3	2	1
Supply Chain Risk Management Strategy (ID.SC)	5	3	2
Total	29	16	13

Source: Research data, 2019

4.2.2 Core Function: Protect (PR)

4.2.2.1 Access Control (PR.AC)

The respondent pointed out that the organization has an Active Directory for management of user identities and credentials. A user access management policy has been developed which states guidelines on the management of user access to information systems. A data centre walk through was done to confirm that physical access to the critical servers is managed. Data centre access is limited to the CTO and ICT team. Of importance to note is that for remote access, a change management process has to be followed which has to be signed off by both the client and the organization. VPN connections and remote desktop sessions are used. The network has been segmented into VLANs. There is a data centre VLAN, User VLAN, management VLAN. LDAP has been setup for access management. In addition, two factor authentication has been implemented for their corporate email and helpdesk. However, these controls need to be improved by having all machines integrated to the Active Directory. Processes need to be put in place to manage remote desktop sessions. Two factor authentication should be implemented for other systems as well.

4.2.2.2 Awareness and Training (PR.AT)

Cybersecurity sensitization programs have currently no within the organization is currently work in progress. is within the organization. Privileged users and senior executives understand their roles and responsibilities in relation to cybersecurity. These have been defined in the job descriptions as well as the ICT policies. The respondent pointed out that for third parties as well as cybersecurity personnel, the responsibilities are defined both in the contracts and SLAs. These were noted to be regularly reviewed.

4.3.2.3 Data Security (PR.DS)

Data at rest is secured through Transparent Data Encryption, masking of data as well as object wrapping. Data in transit is protected through secure transfer channels such as VPN. A tool for ICT monitoring, network monitoring, server and applications monitoring has been deployed within the organization to ensure maintenance of availability of critical assets. A good control put in place is that development and testing environments have been separated. The respondent also pointed out that a disk diagnostic tool is used for data integrity checking.

However, in terms of data security an asset management process currently lacks. There is need for a Data Loss Prevention solution.

4.3.2.4 Information Protection Processes and Procedures (PR.IP)

The respondent pointed out a baseline configuration of ICT system currently lacks within the organization. The organization has adopted agile software methodology which allows for cross-functional teams. It was also noted that configuration changes go through a change management process. Sign-offs are done by both the organization and the client if it’s an external change however if it’s an internal change sign offs are done by management before changes can be applied on the production environment. The data backup standard which defines the backup schedule was reviewed. Backups are done based on the sensitivity of data; highly sensitive data is done twice a day whereas less sensitive data is done twice in a week. An end of week backup is also scheduled. The respondent also pointed out that testing of the backups is done on a biweekly basis. Physical environment for information assets policies are met within the organization.

The ICT recovery plan which enables the recovery of critical services in a time effective way to reduce the effect of IT disruptions and to maintain resilience before, during, and after a disruption was reviewed. Component testing is done to test recovery within the organization. A vulnerability management plan is developed for the various critical applications. Assessments are done before implementation. It was noted that cybersecurity is included in human resource practices. Reference checks are done using referees, organizations or previous networks. Reference checks are done using referees, organization or networks. The induction process includes a section where the ICT department trains on the various policies.

While these are good controls implemented, there organization lacks a formal process for documenting results of backup testing. Data destruction methods currently lack. It was noted that there lacks an effective way to measure effectiveness of protection technologies.

4.3.2.5 Maintenance (PR.MA)

Assets repair and maintenance is done internally however it isn't logged. An asset aging policy currently lacks within the organization.

4.3.2.6 Protective Technology (PR.PT)

The organization’s logging and monitoring standard which defines the baseline requirements for logging and monitoring security events within the organization was reviewed. This standard has currently not been fully implemented within the organization. Communication and control networks are protected through the use of secure data transfer mechanisms. Load balancing has been implemented for both the on premise infrastructure and cloud infrastructure to achieve resilience requirements.

However, the organization currently lacks controls to protect and restrict use of removable media.

4.3.2.7 Breakdown of Controls Assessed in the Protect Core Function

The table below represents a summary of the controls that were assessed under the protect core function.

Table 29 Protect analysis

CATEGORY	CONTROLS ASSESSED	PASSED	FAILED
Access Control (PR.AC)	7	3	4
Awareness and Training (PR.AT)	5	3	2
Data Security (PR.DS)	8	4	4
Information Protection Processes and Procedures (PR.IP)	12	6	6
Maintenance (PR.MA)	2	1	1
Protective Technology (PR.PT)	5	2	3
Total	39	19	20

Source: Research data, 2019

4.2.3 Core Function: Detect (DE)

4.2.3.1 Anomalies and Events (DE.AE)

When asked about the event detection process, the respondent pointed out that the organization relies on the firewall and system log files to analyze attack targets and methods. An incident report is generated once an incident is noted. In addition, it was noted that there includes a section where the impact is noted.

Despite these controls put in place, a formal network baseline currently lacks. Incident alert thresholds have also currently not been fully established.

4.2.3.2 Security Continuous Monitoring (DE.CM)

Network monitoring is done on a need basis using the firewall. Real time network monitoring has currently not yet been implemented. The physical environment is monitored for detection of any cybersecurity events. Vulnerability scans are done when need occurs. The organization is yet to implement a vulnerability management program.

4.2.3.3 Detection Processes (DE.DP)

With regards to processes for detection, the respondent pointed out that roles and responsibilities for detection purposes have been defined but not yet fully implemented. Requirements for detection activities are still being developed internally. The CTO and ICT manager receive alerts from the detection systems. It is however of importance to note that discussions for improvement of detection processes are done at managerial level.

4.2.3.4 Breakdown of Controls Assessed in the Detect Core Function

The table below represents a summary of the controls that were assessed under the detect core function.

Table 30 Detect analysis

CATEGORY	CONTROLS ASSESSED	PASSED	FAILED
Anomalies and Events (DE.AE)	5	1	4
Security Continuous Monitoring (DE.CM)	8	3	5
Detection Processes (DE.DP)	5	2	3
Total	18	6	12

Source: Research data, 2019

4.2.4 Core Function: Respond (RS)

4.2.4.1 Response Planning (RS.RP)

The organization has developed information security policies, standards and guidelines. These are implemented to protect the organization against current and emerging security threats that could cause a cybersecurity incident. The incident management standard was reviewed and it was noted that specific security controls have been defined to reduce the likelihood and impact of incidents However, the policies currently lacks a formal updating process.

4.2.4.2 Communications (RS.CO)

A crisis management team currently lacks within the organization. Incidents are escalated to the CTO and ICT manager within the organization however consistency of reporting and establishment of incident criteria currently lack within the organization. It was noted that response information is shared on need basis.

4.2.4.3 Analysis (RS.AN)

As explained by the respondent, the organization, the notifications received from the firewall are investigated by the CTO and ICT manager. The impact of the incident is analyzed together with their third party cybersecurity services provider. Formal processes to receive, analyze and respond to incidents have currently not been documented but appropriate remedial action is taken for identified issues.

4.2.4.4 Mitigation (RS.MI)

When asked about incident mitigation, the respondent pointed out that upon identification of an incident, it is investigated and appropriate remedial actions are taken. Majority of the vulnerabilities identified are mitigated through patch management.

4.2.4.5 Improvements (RS.IM)

Lessons learnt are incorporated into the response plan on a need basis. In addition, the response strategies currently lack a formal updating process.

4.2.4.6 Breakdown of Controls Assessed in the Respond Core Function

The table below represents a summary of the controls that were assessed under the respond core function.

Table 31 Respond analysis

CATEGORY	CONTROLS ASSESSED	PASSED	FAILED
Response Planning (RS.RP)	1	1	0
Communications (RS.CO)	5	2	3
Analysis (RS.AN)	5	2	3
Mitigation (RS.MI)	3	2	1
Improvements (RS.IM)	2	1	1
Total	16	8	8

Source: Research data, 2019

4.2.5 Core Function: Recover (RC)

4.2.5.1 Recovery Planning (RC.RP)

The organization’s ICT recovery plan which is to enable the recovery of critical organizational services to reduce the effect of IT disruptions and to maintain resilience before, during, and after a disruption was reviewed. It was however noted that the incident response procedure is more reactive. A crisis management team to manage and communicate information in the event of a disaster currently lacks within the organization.

4.2.5.2 Improvements (RC.IM)

The respondents pointed out that recovery strategies are updated based on their various clients. Each client has its own unique scenarios identified. Lessons learnt are retrieved from the incident reports. Incident reports are generated upon identification of an incident. The report contains a section for recommendations which is used to update the recovery strategy.

4.2.5.3 Communications (RC.CO)

The organization's incident management standard document was reviewed. The communication procedures are both short-term counter-measures and longer-term action plans used to eliminate the current threat to the organization's business assets as per the investigation results. It was however noted that this policy has currently not yet been fully implemented within the organization. The organization is yet to define an escalation tree for communication of cybersecurity incidents.

4.2.5.4 Breakdown of Controls Assessed in the Recover Core Function

The table below represents a summary of the controls that were assessed under the recover core function.

Table 32 Recover analysis

CATEGORY	CONTROLS ASSESSED	PASSED	FAILED
Recovery Planning (RC.RP)	1	1	0
Improvements (RC.IM)	2	1	1
Communications (RC.CO)	3	0	3
Total	6	2	4

Source: Research data, 2019

4.2.6 Breakdown of the Core Functions Assessed

The table below represents a summary of the controls that were assessed under the NIST core functions.

Table 33 Core Functions Summary

CORE FUNCTION	CONTROLS ASSESSED	PASSED	FAILED
Identify (ID)	29	16	13
Protect (PR)	39	19	20
Detect (DE)	18	6	12

Respond (RS)	16	8	8
Recover (RC)	6	2	4
Total	108	51	57

Source: Research data, 2019

4.3 Cybersecurity Strategy

4.3.1 Introduction

This cybersecurity strategic plan seeks to establish an implementation roadmap for improving cybersecurity resilience within the organization in the next one year. It outlines a roadmap for protection of information assets to ensure alignment to the business goals and objectives. This strategy is a living document and should be reviewed on an annual basis or when major changes occur to ensure that it remains relevant to the organizational and technological changes.

The strategy is divided into the following thematic areas: Identify, Protect, Detect, Respond and Recover. Further details have been provided in appendix one.

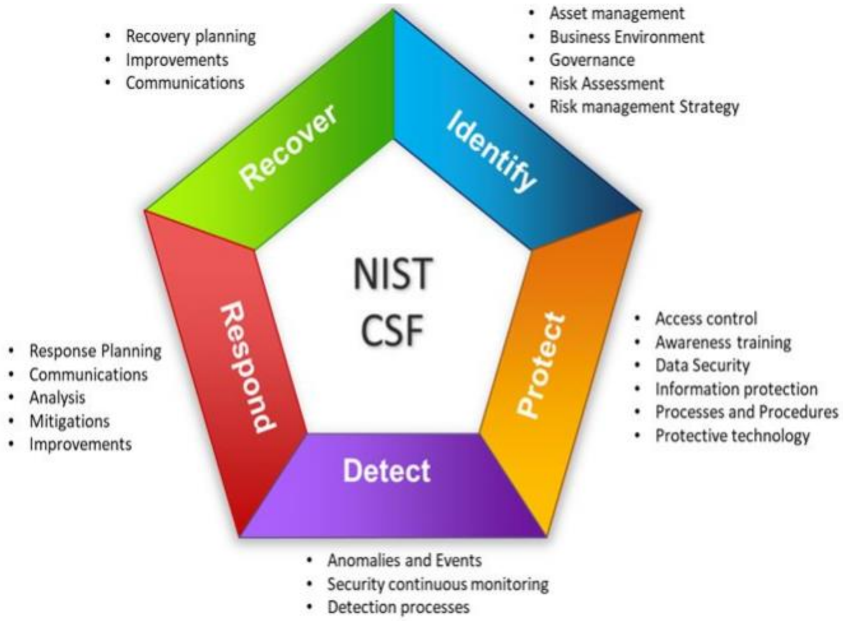


Figure 9 NIST Cybersecurity Framework

Source: SOGETILABS

4.3.2 Purpose

The purpose of this strategy is to ensure:

i. Confidentiality of organizational data
ii. Resilience of organizational systems
iii. Protection of client’s confidential data
iv. Adequate response to cyber threats against information assets
v. Compliance with appropriate cybersecurity standards and regulator requirements

4.4 Discussion of Findings

4.4.1 Current and target profile

Based on analysis of the five core functions assessed, the organization is tier two (2) which is risk informed as they scored an average of 47%. The characteristics of a risk informed organization as per the NIST framework are as below:

1. Management approves the risk management practices.
2. A cybersecurity risk management approach that can be used organization wide has currently not been established but there is awareness around cybersecurity risk. Integrated risk management program.
3. The role in the larger ecosystem is understood however not to both dependencies or dependents.

The target profile is tier (3) which is repeatable.

4.4.2 Analysis of gaps identified

The study clearly indicates that there is need to improve cybersecurity risk management practices within organizations, specifically SMEs. There is a growing concern around cybercrime. In the context of SMEs this finding correlates with a previous study which found that the SMEs have become a target for cybercriminals to gain access to sensitive company information as a result of their increasing technology dependence (Sammut, 2017).

4.4.2.1 Identify

In terms of cybersecurity investment, the study shows that it there is still need for improvement in allocation of resources for cybersecurity initiatives. From a governance perspective, cybersecurity budgeting should be included in the ICT budget. Fielder, König, Panaousis, Schauer, & Rass (2018) found that the majority of SMEs have limited resources for cybersecurity investment. The lack of adequate cybersecurity mechanisms in place could result to significant cybersecurity attacks on their core systems and network infrastructure. SMEs need to include cybersecurity related expenses and tools in their budgeting process.

Policy management was a key issue noted. The results show that there lacks an efficient policy management program. This finding relates to a study by Banham (2017) who found that small firms typically don’t have a cybersecurity policy. SMEs need to form policy oversight committees comprised of key stakeholders across the departments is key in cybersecurity policy management.

This will help in setting a tone for enterprise wide respect for policy practice. ICT asset management also needs to be streamlined so as to ensure adequate decision management on hardware and software purchasing or distribution.

4.4.2.2 Protect

Vulnerability management programs were also observed to have not been clearly defined. Javaid & Iqbal (2017) found that cybersecurity risk management in SMEs is still a challenge primarily because of lack of budget and expertise. Choosing the right cybersecurity risk management frameworks still remains a weak link. SMEs need effective vulnerability management programs to enforce accountability of closure of issues reported. Audit reports of high risk vendors should be regularly reviewed to ensure adequate due diligence is done. In addition, SMEs need to align their assessment techniques according to the evolving nature of cyber threats based on the nature of their organization.

4.4.2.3 Detect

Another challenge noted was the lack of real time visibility on network activity. No and Vasarhely (2017) found that real-time cybersecurity visibility monitoring and ongoing assessment by automated tools are key to a cybersecurity assurance model. SMEs need real time visibility on network activity monitoring which will help in monitoring of any anomalous activity within the organization’s network.

4.4.2.4 Respond

Cybersecurity incident management also came out as a key area of concern. This finding is similar to a previous study which found that small businesses are more highly affected by cybersecurity incidents as they are less prepared due to limited resources (Eilts & Levy, 2018). SMEs need to develop appropriate actionable activities to be taken regarding a cybersecurity event that has been detected.

4.4.2.5 Recover

SMEs need to develop internal and external communication procedures. In addition, the study found that cybersecurity training and awareness is still an area of improvement. Based on the data analysed, majority of the organizations carry out training on a yearly basis. Sadok & Bednar (2016) note that SMEs will need to implement effective cybersecurity awareness programs to improve resilience capabilities.

4.4.3 Cybersecurity Strategy

The cybersecurity strategy developed clearly brings out the need for people, process and technology management for comprehensive cybersecurity risk management within SMEs. It outlines initiatives, KPI's, timelines and responsibility in maturing the cybersecurity posture of the organization. The study found out that people are one of the weak links in the organizational cybersecurity chain. Conteh and Schmick (2016) note that employees need to attend initial and regular trainings to build on cybersecurity awareness to the common social engineering attacks.

The Kenyan SME regulatory body has defined their role in the national agenda and this includes embracing ICT within the authority. This should be aligned to a cybersecurity guideline tailored for SMEs within Kenya.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

This chapter outlines the summary findings based on research objectives as well as alignment to the research assessment framework. Research conclusions are further drawn from the study.

5.1 Summary of Findings

Objective 1: To determine the key cybersecurity risks being faced by SMEs that are developing technology-based solutions

Through review of related literature and analysis of collected data, key cybersecurity risks being faced include the lack of adequate controls put in place within their network environment due to limited budgets. SMEs face the same cybersecurity threats as large organizations. Their processes and controls are however still not as mature. In addition to the deficiencies in technology and process controls, people are also a source of cybersecurity threats within SMEs. Majority of the organizations carry out cybersecurity training once a year. Most SMEs have been affected by social engineering and phishing attacks. This can be addressed through regular training and sensitization.

Objective 2: To review cybersecurity standards and recommend that which will be most applicable to SMEs that are developing technology-based solutions

From the literature review it was established that frameworks have been developed for cybersecurity risk management and have been applied in different contexts and yielded results. CIS controls is not as broad compared to other frameworks as it provides prioritized controls that first need to be implemented to yield results (Gerberding, 2017). The COSO framework provides a formalized structure for evaluating the effectiveness of controls implemented (Leal, 2016). The ISO 27001 provides details on what needs to be achieved however it lacks specifics on what needs to be done to implement the defined controls (Leal, 2016). The ITIL philosophy often requires organizations to change their culture in order to embrace the new processes (Iden & Eikebrokk, 2014). COBIT has detailed its processes however it still lacks the specific technical information that is required for implementation. The ISSA (UK) has defined recommendations for SMEs in terms of cybersecurity controls however it currently has not been actively established (Ponsard, Grandclaudon & Dallons, 2018). Mijnhardt, Baars & Spruit (2016) found that currently a large number of organizations use more complicated guidelines which are hard to adopt within SMEs leaving them without an easily understandable guideline for their cybersecurity needs. NIST cybersecurity framework was found to be most applicable to SMEs that are developing technology-based solutions. The framework has been designed to be used and adopted by various organization regardless of size, including SMEs.

Objective 3: To undertake a cybersecurity risk assessment in a selected SME.

This focused on in depth understanding of the cybersecurity risk management practices within the selected SME based on the controls defined in the NIST framework. The five core functions of the framework were assessed and analyzed and the organization is currently tier two (2) which is risk informed as they scored an average of 47%. From a governance perspective, cybersecurity budgeting should be included in the ICT budget. The lack of adequate cybersecurity mechanisms in place could result to significant cybersecurity attacks on their core systems and network infrastructure. Policy management was a key issue noted. The results show that there lacks an efficient policy management program. ICT asset management also needs to be streamlined so as to ensure adequate decision management on hardware and software purchasing or distribution.

Vulnerability management programs were also observed to have not been clearly defined. Lack of real time visibility on network activity and cybersecurity incident management also came out as key areas of concern. SMEs need to develop internal and external communication procedures. In addition, the study found that cybersecurity training and awareness is still an area of improvement.

Objective 4: To develop an implementation strategy which will provide a roadmap for managing cyber-risk as a business risk.

Based on the gaps identified within the environment, a cybersecurity implementation plan was developed outlining a roadmap to increase the organization's cybersecurity resilience and posture within the next one year. The aim of the plan is to protect information assets to ensure alignment to the organization's objectives and business goals. The plan is broken down into the five core functions of the NIST framework. Each initiative of the implementation plan has Key Performance Indicators, timelines and the stakeholder(s) responsible.

5.2 Research Assessment

Using (Whetten, 1989) an evaluation of this research work is presented below.

What is new? Does the thesis make a significant, value-added contribution to the current thinking?

This study brought out that key cybersecurity challenges facing SMEs in Kenya and agrees with Twisdale (2018). The key cybersecurity risks being faced include the lack of adequate controls put in place within their network environment. In addition to the deficiencies in technology and process controls, people are also a source of cybersecurity threats within SMEs. Cybersecurity investment continues being an issue within the SMEs but they are in a position to become more resilient even with limited resources (Dahlberg & Guay, 2015). There is need for active engagement of internal stakeholders in the risk management process concurring with (Ponsard, Grandclaudon & Dallons, 2018) who recognize the importance of management commitment. Kenya should formulate policies on the use of BYOD in SMEs to avoid employees thinking that their personal devices were being used without due consideration to personal costs. BYODs have been successfully adopted in Tanzania as a means of bypassing the investment required in organizational ICT resources (Kabanda & Brown, 2014).

So what? How will the research change the current thinking and practice?

In addition to technology and process controls, the research brings out the need to address people as a source of cyberthreats within SMEs and agrees with Aldawood & Skinner (2018). It also emphasizes on the need for improvement in allocation of resources for cybersecurity initiatives concurring with Hills & Atkinson (2016) who found that many SMEs have limited resources for cybersecurity investment.

Are the underlying logic and supportive evidence compelling?

The study established that various frameworks have been developed for cybersecurity risk management and have been applied in different contexts and yielded results. CIS controls is not as broad compared to other frameworks as it provides prioritized controls that first need to be implemented to yield results (Gerberding, 2017). The COSO framework provides a formalized structure for evaluating the effectiveness of controls implemented (Leal, 2016). The ISO 27001 provides details on what needs to be achieved however it lacks specifics on what needs to be done to implement the defined controls (Leal, 2016). The ITIL philosophy often requires organizations to change their culture in order to embrace the new processes (Iden & Eikebrokk, 2014). COBIT has detailed its processes however it still lacks the specific technical information that is required for implementation. The ISSA (UK) has defined recommendations for SMEs in terms of cybersecurity controls however it currently has not been actively established (Ponsard, Grandclaudon & Dallons, 2018).

The NIST cybersecurity framework was adapted for this study. It was found to be most suitable for the SME environment concurring with Gerberding (2017) who found that it is a detailed risk management framework with flexible controls. The results proved that the framework can be used by an organization that have currently not yet matured their cybersecurity program and have a smaller budget.

How thorough was the study

Through the use of descriptive research design, the existing state of affairs was able to be depicted. It was highly qualitative in nature and quality sampling was done. The assessment was done based on the 108 controls defined under the five core functions as per the NIST cybersecurity framework. Interviews were conducted with respective stakeholders to generate information, facts and evidence as per the NIST controls. The control gaps were identified and prioritized which formed the key initiatives of the cybersecurity strategy.

Why now? Is it of interest to the people?

SMEs provide numerous employment opportunities and contribute a large percentage of the national income of African countries. In Kenya they account for approximately 81.1% of the employment opportunities within the country (KNBS, 2016). Given their economic contribution and the role they play in the country’s vision 2030 program, investing in cybersecurity has become a key priority in ensuring that they protect themselves against cyberattacks that could lead to financial and reputational damage.

Who else including academic researchers are interested in this study?

SMEs in Kenya can use the research findings to establish a common cyber-risk management strategy to combat cybercrime, the Government to assess the adequacy of the current legislations in addressing cybersecurity risks, regulatory bodies on which key cybersecurity risk areas to focus on, and assist technology service providers to adapt a culture of cybersecurity that encourages safe use of the cyberspace.

5.3 Conclusion

This study applied and found the NIST cybersecurity framework to be suitable for cybersecurity risk management within the SME environment. Application of this framework in similar scenarios will depict a strategic view of the SMEs cybersecurity risk management practices. This will position an organization in establishing a target profile for the desired cybersecurity posture. The application of the developed cybersecurity strategy will provide a roadmap for protection of information assets to ensure to ensure alignment to the organization’s objectives and business goals.

5.4 Limitations of the Study

This study was conducted in the context of SMEs specifically developing technology based solutions and therefore may not adequately capture the processes within SMEs that are adopting technology based solutions. It is also biased towards an SME that uses a third-party service provider for cybersecurity services.

5.5 Recommendations for Further Research

A multi-level model can be used to understand cybercrime impacts within the financial sector. The findings indicate that that strong dynamic relationships affect the cost of cybercrime and arise at different levels of society and value network (Lagazio, Sherif & Cushman, 2014). In addition, Bayesian networks can be used in a cybersecurity risk management framework to enable quantification of network compromise attempts. This information can be used to develop a security management plan (Poolsappasit, Dewri & Ray, 2012). The Kenyan SME regulatory body should also consider developing a cybersecurity guideline tailored for SMEs within Kenya.

REFERENCES

Accenture (2017). Cost of Cyber Crime Study (2017)

Aldawood, H., & Skinner, G. (2018, December). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*(pp. 62-68). IEEE.

Almeida, F., Carvalho, I., & Cruz, F. (2018). Structure and Challenges of a Security Policy on Small and Medium Enterprises. *KSII Transactions on Internet & Information Systems*, *12*(2).

Antonescu, M., & Birău, R. (2015). Financial and non-financial implications of cybercrimes in emerging countries. Procedia Economics and Finance, 32, 618-621.

Azmi, R., Tibben, W., & Win, K. T. (2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.

Banham, R. (2017). Cybersecurity threats proliferating for midsize and smaller businesses. *Journal of Accountancy*, *224*(1), 75.

Bell, S. (2017). Cybersecurity is not just a'big business' issue. *Governance Directions*, *69*(9), 536.

Candiwan, C. (2014). Analysis of ISO27001 implementation for enterprises and SMEs in indonesia. In *The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)* (pp. 50-58). The Society of Digital Information and Wireless Communication.

Carlton, M., & Levy, Y. (2015, April). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. In *SoutheastCon 2015* (pp. 1-6). IEEE.

CBK (2018). Guidelines on Cybersecurity for Payment Service Providers. https://www.centralbank.go.ke/wp-content/uploads/2018/08/DRAFT-CYBER-SECURITY-GUIDELINES-FOR-PSP-AUGUST-2018.pdf. Accessed on 30 April 2019.

Chak, S. K. (2015). *Managing Cybersecurity as a Business Risk for Small and Medium Enterprises* (Doctoral dissertation).

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31.

CSO (2017). State of Cybercrime Report

Cyber Security Ventures (2017). 2017 Cybercrime Report

Dahlberg, R., & Guay, F. (2015). Creating resilient SMEs: is business continuity management the answer?. *WIT Transactions on The Built Environment, 168,* 975-984.

Eilts, D., & Levy, Y. (2018). Towards an Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses.

Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk assessment uncertainties in cybersecurity investments. Games, 9(2), 34.

Gartner (2017). Business Impact of Security Incidents and Evolving Regulations Driving Market Growth.

Gerberding, K. (2017). NIST, CIS/SANS 20, ISO 27001 – Simplifying Security Control Assessment

Hayes, J., & Bodhani, A. (2013). Cyber security: small firms under fire [Information Technology Professionalism]. Engineering & Technology, 8(6), 80-83.

Henson, R., & Garfield, J. (2016). What Attitude Changes Are Needed to Cause SMEs to Take a Strategic Approach to Information Security?. *Athens Journal of Business and Economics*, *2*(3), 303-318.

Hills, M., & Atkinson, L. (2016). Towards cyber-resilient & sustainable SMES: the case study of added value from a large IT reseller.

Iden, J., & Eikebrokk, T.R. (2014). Using the ITIL process reference model for realizing IT governance: An empirical investigation. *Information Systems Management*, 31., p. 37-58.

IRA (2014). Guidelines to the Insurance Industry on the Business Continuity Management. https://www.ira.go.ke/images/docs/Guideline_on_Business_Continuity_Management.pdf. Accessed on 30 April 2019.

ISSA-UK 5173 (2011). Information Security for Small and Medium Sized Enterprises

Javaid, M. I., & Iqbal, M. M. W. (2017, April). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). In 2017 International Conference on Communication Technologies (ComTech) (pp. 78-90). IEEE.

Karali, Y., Panda, S., & Panda, C. S. (2015). Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India. *International Journal of Engineering and Management Research (IJEMR)*, *5*(2), 43-48.

Kabanda, S., & Brown, I. (2014). Bring-your-own-device (BYOD) practices in SMEs in developing countries–the case of Tanzania. ACIS.

Karim, S. S. (2016). Cyber-Crime Scenario in Banking Sector of Bangladesh: An Overview. *Vol-44*, 12-19.

Kaur, S., Sharma, S., & Singh, A. (2015). Cyber security: Attacks, implications and legitimations across the globe. *International Journal of Computer Applications*, *114*(6).

KNBS (2016). Micro, Small and Medium Establishment (MSME) Survey, Basic Report.

Klaper, D., & Hovy, E. (2014, June). A taxonomy and a knowledge portal for cybersecurity. In Proceedings of the 15th Annual International Conference on Digital Government Research (pp. 79-85). ACM.

Kluitenberg, H. (2014). Security risk management in it small and medium enterprises. In *Proc. 20th Twente Student Conf. IT*.

Kothari, C. R., & Garg, G. (2014). Research Methodology - Methods and Techniques

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. Computers & Security, 45, 58-74.

Leal, R. (2016). How to integrate COSO, COBIT, and ISO 27001 frameworks

McAfee (2018). Economic Impact of Cybercrime –No Slowing Down

Mierzwa, S., & Scott, J. (2017). Cybersecurity in Non-Profit and Non-Governmental Organizations. *Institute for Critical Infrastructure Technology, February*.

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational characteristics influencing SME information security maturity. *Journal of Computer Information Systems*, *56*(2), 106-115.

Mugenda, O. M. (2003). Research Methods: Quantitative and Qualitative Approach

Mwasambo, L. M., & Moturi, C. A. Experience in Social Engineering by eCommerce Platforms in Kenya.

Nilsen, R., Levy, Y., Terrell, S., & Beyer, D. (2017). A Developmental Study on Assessing the Cybersecurity Competency of Organizational Information System Users.

NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity

No, W. G., & Vasarhelyi, M. A. (2017). Cybersecurity and continuous assurance. Journal of Emerging Technologies in Accounting, 14(1), 1-12.

Osborn, E. (2015). Business versus technology: Sources of the perceived lack of cyber security in SMEs.

Pathak, P. B., & Nanded, Y. M. (2016). A dangerous trend of cybercrime: ransomware growing challenge. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume, 5.

Polkowski, Z., & Dysarz, J. (2017). It Security Management In Small And Medium Enterprises. *Scientific Bulletin-Economic Sciences*, *16*(3), 134-148.

Ponsard, C., Grandclaudon, J., & Dallons, G. (2018). Towards a Cyber Security Label for SMEs: A European Perspective-. In *ICISSP* (pp. 426-431).

Poolsappasit, N., Dewri, R., & Ray, I. (2012). Dynamic security risk management using bayesian attack graphs. IEEE Transactions on Dependable and Secure Computing, 9(1), 61-74.

Radunović, V., & Rüfenacht, D. (2016). *Cybersecurity Competence Building Trends*. Research Report. DiploFoundation. https://www. diplomacy. edu/sites/default/files/Cybersecurity% 20Full% 20Report. pdf (3 December 2017).

Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk management. In Cyber-Risk Management (pp. 33-47). Springer, Cham.

Sadok, M., & Bednar, P. M. (2016). Information Security Management in SMEs: Beyond the IT Challenges. In *HAISA*(pp. 209-219).

Sammut, V. (2017). Cyber-attacks against small and medium-sized enterprises (SMEs): the situation in Malta (Bachelor's thesis, University of Malta).

Santos-Olmo, A., Sánchez, L., Caballero, I., Camacho, S., & Fernandez-Medina, E. (2016). The importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet*, *8*(3), 30.

SASRA (2015). Guideline on Risk Management Practices for Deposit-Taking Sacco Societies. https://www.sasra.go.ke/index. Accessed on 30 April 2019.

Serianu Limited (2017). Africa Cybersecurity Report 2017, Demystifying Africa's Cybersecurity Poverty Line

Smith, K., Smith, M., & Smith, J. (2010). Case studies of cybercrime and its impact on marketing activity and shareholder value.

Sullivan-Taylor, B., & Branicki, L. (2011). Creating resilient SMEs: why one size might not fit all. International Journal of Production Research, 49(18), 5565-5579

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks.

Topping, C. (2017). The role of awareness in adoption of government cyber security initiatives: A study of SMEs in the UK

Twisdale, J. A. (2018). *Exploring SME Vulnerabilities to Cyber-criminal Activities Through Employee Behavior and Internet Access* (Doctoral dissertation, Walden University).

Valli, C., Martinus, I. C., & Johnstone, M. N. (2014). Small to medium enterprise cyber security awareness: an initial survey of Western Australian business.

van Ommen, B. (2014). IT Security in SMEs: Necessary or Irrelevant?. In *21stTwente Student Conference on IT*.

Verbano, C., & Venturini, K. (2013). Managing risks in SMEs: A literature review and research agenda. *Journal of technology management & innovation*, *8*(3), 186-197.

Watkins, B. (2014). The impact of cyber attacks on the private sector. no. August, 1-1

Whetten, D.A. (1989) 'What constitutes a theoretical contribution?'; Academy of management Review, 14(4), p. 490 – 495. The framework outlines 7 points which you can use to evaluate your research work.

Yeboah-Boateng, E. O. (2013). *Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA)*. Institut for Elektroniske Systemer, Aalborg Universitet.

APPENDICES

APPENDIX 1 – DETAILED CYBERSECURITY STRATEGY THEMATIC AREAS

Thematic Area: Identify

Identify Initiatives

Strategies/ Initiatives	Outcomes	KPI's	Timelines				Responsibility
			Q1 (January - March)	**Q2 (April - June)**	**Q3 (July - September)**	**Q4 (October - December)**	
Strategy 1: Core function Identify	Organizational understanding within the organization to manage cybersecurity risks.						
Key Initiatives:							
1. Development of a policy management program which will entail a clear process of drafting, reviewing and approving the organization's policies.		Formation of a policy oversight committee comprised of key stakeholders across the departments.	20%	50%	30%		CTO
2. ICT asset management streamlining which will involve tracking and managing ownership of all organization's data.		Prioritization of assets based on classification, criticality and business value.	10%	40%	50%		CTO ICT Manager
3. Coordination of threat intelligence information sharing practices.		Sharing of information on threat intelligence to all employees	50%	50%			ICT Manager
4. Implementation of a formal process for tracking on		Assigning roles and responsibilities for closure	30%	60%	10%		CTO

closure of vulnerabilities identified. This will help in accountability of closure of issues reported.		on vulnerabilities identified.					
5. Development of a third party due diligence activity program. This will ensure efficient security.		Review of audit reports of high risk vendors.	10%	20%	60%	10%	CTO ICT Manager

Thematic Area: Protect

Protect Initiatives

Strategies/ Initiatives	**Outcomes**	**KPI's**	**Timelines**				**Responsibility**
			Q1 (January - March)	**Q2 (April - June)**	**Q3 (July - September)**	**Q4 (October - December)**	
Strategy 2: Core function Protect	Proper security controls vital for the delivery of core services related to infrastructure.						
Key Initiatives:							
1. User access management streamlining.		Integrating all users to the Active Directory.	10%	60%	30%		ICT Manager Networks Manager
2. Development of a remote desktop access management process.		Limiting remote desktop sessions to administrators that need it. Lockout sessions should be used to strengthen access controls.	40%	50%	10%		ICT Manager Networks Manager

3. Implementation of two factor authentication for other critical business systems.		2FA implementation for critical business systems.	10%	50%	40%		CTO Business Process Owners ICT Manager
4. Provision of regular cybersecurity training and awareness.		Develop an annual cybersecurity training plan and budget. Training should be based on specific target groups.	30%	60%	10%		CTO HR Manager
5. Data Loss Prevention Management		Implementation of a Data Loss Prevention solution.	10%	20%	60%	10%	CTO ICT Manager
6. Development of a baseline configuration of ICT systems.		Attributes of the ICT systems should be documented at a point in time which should serve as a basis for defining change.	20%	50%	30%		CTO ICT Manager
7. Documentation of results of backup testing.		A formal process for documentation of results and lessons learnt during backup testing should be developed.	50%	40%	10%		CTO ICT Manager Networks Manager Business Process Owners
8. Provision of a data destruction tool.		A data destruction tool will ensure permanent wiping of sensitive data on partitions and disk volumes preventing recovery of data.	10%	30%	50%	10%	CTO ICT Manager
9. Effect a logging process for maintenance of organizational assets.		Maintenance logs for assets should be maintained and signed off.	30%	50%	20%		CTO ICT Manager
10. Development of an asset aging policy.		Implementation of asset aging policy	20%	40%	20%	20%	CTO ICT Manager

Thematic Area: Detect

Detect Initiatives

Strategies/ Initiatives	**Outcomes**	**KPI's**	**Timelines**				**Responsibility**
			Q1 (January - March)	**Q2 (April - June)**	**Q3 (July - September)**	**Q4 (October - December)**	
Strategy 3: Core function Detect	Appropriate steps taken to establish the source of occurrence of a cybersecurity event in a timely manner.						
Key Initiatives:							
1. Development of formal baseline of network operations and data flows.		Documenting network baseline operations and data flows.	20%	50%	30%		CTO ICT Manager Network Manager
2. Implementation of incident alert thresholds.		Analyzing incidents to determine patterns and develop thresholds.	10%	40%	50%		CTO ICT Manager Network Manager
3. Effect real time network activity monitoring.		Investment in a real time log analysis tool.	10%	50%	40%		CTO
4. Documentation of requirements for detection activities.		Develop roles and responsibilities for detection activities	30%	60%	10%		CTO

Thematic Area: Respond

Respond Initiatives

Strategies/ Initiatives	**Outcomes**	**KPI's**	**Timelines**				**Responsibility**
			Q1 (January - March)	**Q2 (April - June)**	**Q3 (July - September)**	**Q4 (October - December)**	
Strategy 4: Core function Respond	Appropriate actionable activities are taken regarding a cybersecurity event that has been detected.						
Key Initiatives:							
1. Regular updating of the incident management standard		Documenting incident management standard.	20%	60%	20%		CTO ICT Manager
2. Development of a crisis management team		Develop roles and responsibilities for crisis management team.	10%	40%	50%		CTO
3. Development of a reporting process		Documenting incident reporting standard.	10%	50%	40%		CTO
4. Incident sharing process		Developing incident escalation call tree.	30%	60%	10%		CTO

Thematic Area: Recover

Recover Initiatives

Strategies/ Initiatives	Outcomes	KPI's	Timelines				Responsibility
			Q1 (January - March)	Q2 (April - June)	Q3 (July - September)	Q4 (October - December)	
Strategy 5: Core function Recover	Maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.						
Key Initiatives:							
1. Defining of internal and external communication procedures.		Documenting escalation and communication procedures.	20%	60%	20%		CTO

APPENDIX 2 – BACKGOUND INFORMATION QUESTIONNAIRE

This research is purely for academic purposes and is meant to get your opinion on cyber risk management Please answer these questions as precisely and as honestly as possible. Kindly complete by placing a tick in the appropriate box or fill in the spaces provided. The information provided will be kept confidential.

1. What type of organization do you work in?
   Public sector ( )
   Banking ( )
   Telecommunication ( )
   Financial Services Provider ( )
   Professional Services Provider ( )
   Academia ( )
   Cyber Security Services Provider ( )
   Healthcare Services Provider ( )
   Legal Services Provider ( )
   Insurance ( )
   Private Sector ( )
   Manufacturing ( )
2. How concerned is your organization about cybersecurity?
   Extremely concerned ( )
   Very concerned ( )
   Moderately concerned ( )
   Slightly concerned ( )
   Not at all concerned ( )
3. In terms of cybersecurity management, how is it carried out within your organization?
   By an Internet Service Provider ( )
   I manage my own cybersecurity ( )
   In house by someone who is tasked as a secondary role ( )

In house Computer Emergency Response Team ( )

Outsourced to an independent specialist or organization ( )

Not sure ( )

4. Which security testing techniques are used within your organization?

   Penetration testing ( )

   Vulnerability assessments ( )

   Audits ( )

   Don’t know ( )

5. How often are cybersecurity trainings done:

   On a weekly basis ( )

   On a monthly basis ( )

   On a yearly basis ( )

   Never ( )

   Only when there is a problem ( )

6. Does your organization allow the use of mobile devices?

   Yes ( )

   No ( )

7. What is the approximate annual cybersecurity budget?

   USD 0 ( )

   USD 1 – 1000 ( )

   USD 1001 – 5000 ( )

   USD 5001 – 10000 ( )

   USD 10000+ ( )

   Don't know ( )

APPENDIX 3 – RESEARCH INTERVIEW GUIDE (CTO)

TOPIC: CYBER RISK MANAGEMENT

SECTION A: BUSINESS ENVIRONMENT

1. Has the organization's role in the supply chain been identified and communicated?
2. Has the organization's place in critical infrastructure and its industry sector been identified and communicated?
3. Have priorities for organizational mission, objectives, and activities been established and communicated?
4. Have dependencies and critical functions for delivery of critical services been established?
5. Have resilience requirements to support delivery of critical services been established for all operating states?

SECTION B: GOVERNANCE

1. Has the organizational cybersecurity policy been established and communicated?
2. Have cybersecurity roles and responsibilities been coordinated and aligned with internal roles and external partners?
3. Have legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations been understood and managed?
4. Do governance and risk management processes address cybersecurity risks?

SECTION C: INFORMATION PROTECTION PROCESSES

1. Has a vulnerability management plan been developed and implemented?

SECTION D: COMMUNICATIONS

1. Does coordination with stakeholders occur consistent with response plans?
2. Does voluntary information sharing occur with external stakeholders to achieve broader cybersecurity situational awareness?
3. How are public relations managed?
4. How is reputation repaired after an incident?
5. Are recovery activities are communicated to internal and external stakeholders as well as executive and management teams?

APPENDIX 4 – DETAILED CYBERSECURITY RISK MANAGEMENT FINDINGS WITHIN THE SME

1. Core Function Identify

1.1 Asset Management (ID.AM)

Sub-Category	Finding	Informative References
ID.AM-1: Physical devices and systems within the organization are inventoried	An ICT asset management policy which defines ICT asset management processes to ensure ICT assets are identified, inventoried and maintained was reviewed. The organization has implemented an open source ICT asset management tool. This is able to track the physical devices and systems. It was however noted that a formal procedure for updating the asset inventory has currently not been implemented therefore leading to lack of an updated physical asset inventory.	i. CIS CSC 1 ii. COBIT 5 BAI09.01, BAI09.02 iii. ISA 62443-2-1:2009 4.2.3.4 iv. ISA 62443-3-3:2013 SR 7.8 v. ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
ID.AM-2: Software platforms and applications within the organization are inventoried	The tool is also used to maintain the software and application inventory within the organization. However, due to the lack of formal policies and procedures, the software asset inventory is currently not updated.	i. CIS CSC 2 ii. COBIT 5 BAI09.01, BAI09.02, BAI09.05 iii. ISA 62443-2-1:2009 4.2.3.4 iv. ISA 62443-3-3:2013 SR 7.8 v. ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
ID.AM-3: Organizational communication and data flows are mapped	From a functional perspective, organizational data flows and organizational communication has been mapped. However, from a functional perspective, it is yet to be updated as the organization has shifted to a new software development methodology.	i. CIS CSC 12 ii. COBIT 5 DSS05.02 iii. ISA 62443-2-1:2009 4.2.3.4 iv. ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
ID.AM-4: External information systems are catalogued	At client level, the external information systems have been catalogued however there exists a gap in inventory management.	i. CIS CSC 12 ii. COBIT 5 APO02.02, APO10.04, DSS01.02 iii. ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their	Resources have currently not yet been prioritized based on classification, criticality and business value.	i. CIS CSC 13, 14 ii. COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 iii. ISA 62443-2-1:2009 4.2.3.6

classification, criticality, and business value		iv. ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	The organization uses a third party for managing cybersecurity needs when need occurs both internally and with third party stakeholders.	i. CIS CSC 17, 19 ii. COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 iii. ISA 62443-2-1:2009 4.3.2.3.3 iv. ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

1.2 Business Environment (ID.BE)

Sub-Category	Finding	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	The organization has identified its niche in software development and is communicated to clients through scope of works.	i. COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ii. ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 iii. NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	The organization has identified itself as a software development company.	i. COBIT 5 APO02.06, APO03.01 ii. ISO/IEC 27001:2013 Clause 4.1 iii. NIST SP 800-53 Rev. 4 PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Prioritization of organizational mission, objectives and activities have been documented and are communicated to the relevant stakeholders who are in charge of implementation.	i. COBIT 5 APO02.01, APO02.06, APO03.01 ii. ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 iii. NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Dependencies have been established however they are not formally documented and updated.	i. COBIT 5 APO10.01, BAI04.02, BAI09.02 ii. ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 iii. NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Resilience requirements have been established however they are not formally documented and updated.	i. COBIT 5 BAI03.02, DSS04.02 ii. ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 iii. NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA14

1.3 Governance (ID.GV)

Sub-Category	Finding	Informative Reference

ID.GV-1: Organizational cybersecurity policy is established and communicated	An organizational cybersecurity policy has been established however it lacks a formal updating process.	i. CIS CSC 19 ii. COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 iii. ISA 62443-2-1:2009 4.3.2.6 iv. ISO/IEC 27001:2013 A.5.1.1 v. NIST SP 800-53 Rev. 4 -1 controls from all security control families
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	Cybersecurity management is currently outsourced to a third party who provides services when need occurs.	i. CIS CSC 19 ii. COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 iii. ISA 62443-2-1:2009 4.3.2.3.3 iv. ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 v. NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Legal and regulatory requirements applicable to the organization are addressed within their cybersecurity risk management practices.	i. CIS CSC 19 ii. COBIT 5 BAI02.01, MEA03.01, MEA03.04 iii. ISA 62443-2-1:2009 4.4.3.7 iv. ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 v. NIST SP 800-53 Rev. 4 -1 controls from all security control families
ID.GV-4: Governance and risk management processes address cybersecurity risks	Governance and risk management practices currently address cybersecurity risks.	i. COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02 ii. ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 iii. ISO/IEC 27001:2013 Clause 6 iv. NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM9, PM-10, PM-11

1.4 Risk Assessment (ID.RA)

Sub-Category	Finding	Informative Reference
ID.RA-1: Asset vulnerabilities are identified and documented	Vulnerability assessments and penetration testing is carried out within the organization, both at complete network level and specific software. These are carried out by an independent third party cybersecurity services provider.	i. CIS CSC 4 ii. COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 iii. ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 iv. ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 v. NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	Cyber threat intelligence is received from third party security provider.	i. CIS CSC 4 ii. COBIT 5 BAI08.01 iii. ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 iv. ISO/IEC 27001:2013 A.6.1.4

		v. NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16
ID.RA-3: Threats, both internal and external, are identified and documented	There lacks a formal process for documentation of both internal and external threats.	i. CIS CSC 4 ii. COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 iii. ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 iv. ISO/IEC 27001:2013 Clause 6.1.2 v. NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM16
ID.RA-4: Potential business impacts and likelihoods are identified	Stand up meetings are done on a regular basis where the organization discusses their various products and potential business impacts are documented.	i. CIS CSC 4 ii. COBIT 5 DSS04.02 iii. ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 iv. ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 v. NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM9, PM-11
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	There lacks a formal process of distributing threat intelligence information to other members of the organization.	i. CIS CSC 4 ii. COBIT 5 APO12.02 iii. ISO/IEC 27001:2013 A.12.6.1 iv. NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
ID.RA-6: Risk responses are identified and prioritized	An accountability process for tracking on closure of assessment findings currently lacks.	i. CIS CSC 4 ii. COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 iii. NIST SP 800-53 Rev. 4 PM-4, PM-9

1.5 Risk Management Strategy (ID.RM)

Sub-Category	Finding	Informative Reference
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Risks are looked at in three perspectives which include; product risks, project risks and customer risks. Cybersecurity risks are addressed as part of product and customer risks. The information security risk and compliance management standard document currently lacks a formal review and updating process.	i. CIS CSC 4 ii. COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 iii. ISA 62443-2-1:2009 4.3.4.2 iv. ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 v. NIST SP 800-53 Rev. 4 PM-9
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	Organizational risk tolerance is addressed through a consultative approach between the organization and its customers.	i. COBIT 5 APO12.06 ii. ISA 62443-2-1:2009 4.3.2.6.5 iii. ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 PM-9
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical	Their determination of their risk tolerance is also influenced by regulator requirements.	i. COBIT 5 APO12.02 ii. ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 iii. NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM11

infrastructure and sector specific risk analysis		

1.6 Supply Chain Risk Management (ID.SC)

Sub-Category	**Finding**	**Informative Reference**
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Risk thresholds are determined and operationalized internally. Risks are minimized through a methodology of constant evaluation.	i. CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ii. ISA 62443-2-1:2009 4.3.4.2 iii. ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 iv. NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9
ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Currently suppliers and third party partners aren't assessed using a cyber supply chain risk assessment process however the processes are designed to meet the objectives of the organization's cybersecurity program.	i. COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ii. ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 ii. ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 iv. NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA14, SA-15, PM-9
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Contracts are developed for all clients which address issues of protection and confidentiality of data.	i. COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ii. ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 iii. ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 iv. NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM9
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	Initial due diligence is done on clients however based on the feedback, it was clear that there lacks a routinely process for assessing third party service providers.	i. COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ii. ISA 62443-2-1:2009 4.3.2.6.7 ISA 62443-3-3:2013 SR 6.1 iii. ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 iv. NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU16, PS-7, SA-9, SA-12
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	Response and recovery planning are done based on client requirements.	i. CIS CSC 19, 20 COBIT 5 DSS04.04 ii. ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 iii. ISO/IEC 27001:2013 A.17.1.3 iv. NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

2. Core Function Protect

2.1 Identity Management, Authentication and Access Control (PR.AC)

Sub-Category	Finding	Informative Reference
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	The organization has an Active Directory for management of user identities and credentials. It was however noted that not all user machines (End points) have been integrated as they are currently not running compatible operating systems. There is therefore need to migrate them to enterprise or professional.	i. CIS CSC 1, 5, 15, 16 ii. COBIT 5 DSS05.04, DSS06.03 iii. ISA 62443-2-1:2009 4.3.3.5.1 iv. ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 v. ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 vi. NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
PR.AC-2: Physical access to assets is managed and protected	There is an on- site data centre which stores physical assets. There is limited access to the data centre, only the ICT department (3) and security team have access.	i. COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ii. ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 iii. NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
PR.AC-3: Remote access is managed	For remote access, client sessions are either through VPN or remote desktop sessions. A change management form is used for this which is signed off by the client and the organization.	i. CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ii. ISA 62443-2-1:2009 4.3.3.6.6 iii. ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 iv. NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	User Access Matrices have been defined for critical systems. User access rights are reviewed by the Database Administrator and System administrator on a weekly basis.	i. CIS CSC 3, 5, 12, 14, 15, 16, 18 ii. COBIT 5 DSS05.04 iii. ISA 62443-2-1:2009 4.3.3.7.3 iv. ISA 62443-3-3:2013 SR 2.1 v. ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 vi. NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC5, AC-6, AC-14, AC-16, AC-24
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	The network has been segmented into VLANs. There is a data centre VLAN, User VLAN, management VLAN. Both primary and secondary links pass through the firewall however this hasn't been fully	i. CIS CSC 9, 14, 15, 18 ii. COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 iii. ISA 62443-3-3:2013 SR 3.1, SR 3.8 iv. ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3

	effected. There are plans to change the environment to a hybrid one and incorporate cloud backup.	v. NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	LDAP is used for identity management. User email address credentials are tied to LDAP.	i. CIS CSC, 16 ii. COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 iii. ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 iv. ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 v. ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 vi. NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Two factor authentication has been been incorporated for corpoarate emails, and the helpdesk system.	i. CIS CSC 1, 12, 15, 16 ii. COBIT 5 DSS05.04, DSS05.10, DSS06.10 iii. ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 iv. ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 v. ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 vi. NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

2.2 Awareness and Training (PR.AT)

Sub-Category	Finding	Informative Reference
PR.AT-1: All users are informed and trained	Cybersecurity training and awareness programs is still novice within the organization.	i. CIS CSC 17, 18 ii. COBIT 5 APO07.03, BAI05.07 iii. ISA 62443-2-1:2009 4.3.2.4.2 iv. ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 v. NIST SP 800-53 Rev. 4 AT-2, PM-13
PR.AT-2: Privileged users understand their roles and responsibilities	Privileged users understand their roles and responsibilities in relation to cybersecurity. These have been defined in the job descriptions as well as the ICT policies.	i. CIS CSC 5, 17, 18 ii. COBIT 5 APO07.02, DSS05.04, DSS06.03 iii. ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 iv. ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 v. NIST SP 800-53 Rev. 4 AT-3, PM-13
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	For third parties as well as cybersecurity personnel, the responsibilities are defined both in the contracts and SLAs. These were noted to be regularly reviewed.	i. CIS CSC 17 ii. COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 iii. ISA 62443-2-1:2009 4.3.2.4.2 iv. ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2

		v. NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16
PR.AT-4: Senior executives understand their roles and responsibilities	Senior executives understand their roles and responsibilities in relation to cybersecurity. These have been defined in the job descriptions as well as the ICT policies	i. CIS CSC 17, 19 ii. COBIT 5 EDM01.01, APO01.02, APO07.03 iii. ISA 62443-2-1:2009 4.3.2.4.2 iv. ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 v. NIST SP 800-53 Rev. 4 AT-3, PM-13
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	This has currently not been formally documented.	i. CIS CSC 17 ii. COBIT 5 APO07.03 iii. ISA 62443-2-1:2009 4.3.2.4.2 iv. ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 v. NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-1

2.3 Data Security (PR.DS)

Sub-Category	Finding	Informative Reference
PR.DS-1: Data-at-rest is protected	Data at rest is protected through methods such as Transparent Data Encryption, data masking and object wrapping.	i. CIS CSC 13, 14 ii. COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 iii. ISA 62443-3-3:2013 SR 3.4, SR 4.1 iv. ISO/IEC 27001:2013 A.8.2.3 v. NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-2
PR.DS-2: Data-in-transit is protected	Data in transit is protected through secure transfer channels such as VPN. A tool for ICT monitoring, network monitoring, server and applications monitoring has been deployed within the organization to ensure maintenance of availability of critical assets.	i. CIS CSC 13, 14 ii. COBIT 5 APO01.06, DSS05.02, DSS06.06 iii. ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 iv. ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 v. NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	The ICT asset management policy has currently not been fully implemented.	i. CIS CSC 1 ii. COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 iii. ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 iv. NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
PR.DS-4: Adequate capacity to ensure availability is maintained	A tool has been deployed for monitoring system uptime.	i. CIS CSC 1, 2, 13 ii. COBIT 5 APO13.01, BAI04.04 iii. ISA 62443-3-3:2013 SR 7.1, SR 7.2 iv. ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 v. NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5

PR.DS-5: Protections against data leaks are implemented	The organization currently lacks a Data Loss Prevention solution.	i. CIS CSC 13 ii. COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 iii. ISA 62443-3-3:2013 SR 5.2 iv. ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 v. NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Currently, there lacks integrity checking mechanisms to verify software, firmware and information integrity.	i. CIS CSC 2, 3 ii. COBIT 5 APO01.06, BAI06.01, DSS06.02 iii. ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 iv. ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 v. NIST SP 800-53 Rev. 4 SC-16, SI-7
PR.DS-7: The development and testing environment(s) are separate from the production environment	Development and test environments have been fully segregated.	i. CIS CSC 18, 20 ii. COBIT 5 BAI03.08, BAI07.04 iii. ISO/IEC 27001:2013 A.12.1.4 iv. NIST SP 800-53 Rev. 4 CM-2
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	A disk diagnostic tool is used for hardware integrity checking.	i. COBIT 5 BAI03.05 ii. ISA 62443-2-1:2009 4.3.4.4.4 iii. ISO/IEC 27001:2013 A.11.2.4 iv. NIST SP 800-53 Rev. 4 SA-10, SI-7

2.4 Information Protection Processes and Procedures (PR.IP)

Sub-Category	Finding	Informative Reference
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	A baseline configuration of ICT system currently lacks within the organization.	i. CIS CSC 3, 9, 11 ii. COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 iii. ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 iv. ISA 62443-3-3:2013 SR 7.6 v. ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 vi. NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM5, CM-6, CM-7, CM-9, SA-10
PR.IP-2: A System Development Life Cycle to manage systems is implemented	The organization has adopted agile software methodology which allows for cross-functional teams.	i. CIS CSC 18 ii. COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03 iii. ISA 62443-2-1:2009 4.3.4.3.3 iv. ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5

		v. NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI13, SI-14, SI-16, SI-17
PR.IP-3: Configuration change control processes are in place	Configuration changes go through a change management process. Sign-offs are done by both the organization and the client if it's an external change however if it's an internal change sign offs are done by management before changes can be applied on the production environment.	i. CIS CSC 3, 11 ii. COBIT 5 BAI01.06, BAI06.01 iii. ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 iv. ISA 62443-3-3:2013 SR 7.6 v. ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 vi. NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
PR.IP-4: Backups of information are conducted, maintained, and tested	The data backup standard which defines the backup schedule was reviewed. Backups are done based on the sensitivity of data; highly sensitive data is done twice a day whereas less sensitive data is done twice in a week. An end of week backup is also scheduled.	i. CIS CSC 10 ii. COBIT 5 APO13.01, DSS01.01, DSS04.07 iii. ISA 62443-2-1:2009 4.3.4.3.9 iv. ISA 62443-3-3:2013 SR 7.3, SR 7.4 v. ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 vi. NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	The ICT asset management has currently not been fully implemented.	i. COBIT 5 DSS01.04, DSS05.05 ii. ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 iii. ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 iv. NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE14, PE-15, PE-18
PR.IP-6: Data is destroyed according to policy	There lacks formal procedures for data destruction.	i. COBIT 5 BAI09.03, DSS05.06 ii. ISA 62443-2-1:2009 4.3.4.4.4 iii. ISA 62443-3-3:2013 SR 4.2 iv. ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 v. NIST SP 800-53 Rev. 4 MP-6
PR.IP-7: Protection processes are improved	There lacks formal documentation processes for protection processes.	i. COBIT 5 APO11.06, APO12.06, DSS04.05 ii. ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 iii. ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
PR.IP-8: Effectiveness of protection technologies is shared	Currently, there lacks an assessment methodology for effectiveness of protection technologies.	i. COBIT 5 BAI08.04, DSS03.04 ii. ISO/IEC 27001:2013 A.16.1.6 iii. NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	There is an ICT recovery plan which enables the recovery of critical services in a timely manner to minimize the effect of IT disruptions and to maintain resilience before, during, and after a disruption.	i. CIS CSC 19 ii. COBIT 5 APO12.06, DSS04.03 iii. ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 iv. ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 v. NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP13, IR-7, IR-8, IR-9, PE-17

PR.IP-10: Response and recovery plans are tested	Component testing is done to test recovery within the organization.	i. CIS CSC 19, 20 ii. COBIT 5 DSS04.04 iii. ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 iv. ISA 62443-3-3:2013 SR 3.3 v. ISO/IEC 27001:2013 A.17.1.3 vi. NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Cybersecurity is included in human resource practices. Reference checks are done using referees, organizations or previous networks. Reference checks are done using referees, organization or networks. The induction process includes a section where the ICT department trains on the various policies.	i. CIS CSC 5, 16 ii. COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 iii. ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 iv. NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
PR.IP-12: A vulnerability management plan is developed and implemented	A vulnerability management plan has been developed however it hasn’t been fully implemented.	i. CIS CSC 4, 18, 20 ii. COBIT 5 BAI03.10, DSS05.01, DSS05.02 iii. ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 iv. NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2

2.5 Maintenance (PR.MA)

Sub-Category	**Finding**	**Informative Reference**
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	Maintenance and repair of organizational assets is done internally however it isn't logged. An asset aging policy currently lacks within the organization.	i. COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05 ii. ISA 62443-2-1:2009 4.3.3.3.7 iii. ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 iv. NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Remote maintenance and repair of organizational assets is done internally however it isn't logged. An asset aging policy currently lacks within the organization.	i. CIS CSC 3, 5 ii. COBIT 5 DSS05.04 iii. ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 iv. ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 v. NIST SP 800-53 Rev. 4 MA-4

2.6 Protective Technology (PR.PT)

Sub-Category	**Finding**	**Informative Reference**

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	The organization's logging and monitoring has currently not been fully implemented within the organization.	i. CIS CSC 1, 3, 5, 6, 14, 15, 16 ii. COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 iii. ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 iv. ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 v. ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 vi. NIST SP 800-53 Rev. 4 AU Family
PR.PT-2: Removable media is protected and its use restricted according to policy	The organization currently lacks controls to protect and restrict use of removable media.	i. CIS CSC 8, 13 ii. COBIT 5 APO13.01, DSS05.02, DSS05.06 iii. ISA 62443-3-3:2013 SR 2.3 iv. ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 v. NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP5, MP-7, MP-8
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	The principle of least functionality has currently not been implemented.	i. CIS CSC 3, 11, 14 ii. COBIT 5 DSS05.02, DSS05.05, DSS06.06 iii. ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 iv. ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 v. ISO/IEC 27001:2013 A.9.1.2 vi. NIST SP 800-53 Rev. 4 AC-3, CM-7
PR.PT-4: Communications and control networks are protected	Communication and control networks are protected through the use of secure data transfer mechanisms.	i. CIS CSC 8, 12, 15 ii. COBIT 5 DSS05.02, APO13.01 iii. ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 iv. ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3 v. NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC38, SC-39, SC-40, SC-41, SC-43

PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Load balancing has been implemented for both the on premise infrastructure and cloud infrastructure to achieve resilience requirements.	i. COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 ii. ISA 62443-2-1:2009 4.3.2.5.2 iii. ISA 62443-3-3:2013 SR 7.1, SR 7.2 iv. ISO/IEC 27001:2013 A.17.1.2, A.17.2.1 v. NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP13, PL-8, SA-14, SC-6

3. Core Function Detect

3.1 Anomalies and Events (DE.AE)

Sub-Category	Finding	Informative Reference
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	A formal baseline of network operations and data flows currently lacks.	i. CIS CSC 1, 4, 6, 12, 13, 15, 16 ii. COBIT 5 DSS03.01 iii. ISA 62443-2-1:2009 4.4.3.3 iv. ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 v. NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
DE.AE-2: Detected events are analyzed to understand attack targets and methods	The organization relies on the firewall and system log files to analyze attack targets and methods. These events are analyzed by the CTO and ICT manager and escalated if there is need to.	i. CIS CSC 3, 6, 13, 15 ii. COBIT 5 DSS05.07 iii. ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 iv. ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 v. ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 vi. NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	The organization relies on the firewall and system log files to collect and correlate data.	i. CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 ii. COBIT 5 BAI08.02 iii. ISA 62443-3-3:2013 SR 6.1 iv. ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 v. NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
DE.AE-4: Impact of events is determined	An incident report is generated once an incident is noted. Based on the review of sample incident reports, it was noted that there includes a section where the impact is noted.	i. CIS CSC 4, 6 ii. COBIT 5 APO12.06, DSS03.01 iii. ISO/IEC 27001:2013 A.16.1.4 iv. NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
DE.AE-5: Incident alert thresholds are established	Incident alert thresholds haven’t been fully established within the organizations.	i. CIS CSC 6, 19 ii. COBIT 5 APO12.06, DSS03.01 iii. ISA 62443-2-1:2009 4.2.3.10 iv. ISO/IEC 27001:2013 A.16.1.4

		v. NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8

3.2 Security Continuous Monitoring (DE.CM)

Sub-Category	Finding	Informative Reference
DE.CM-1: The network is monitored to detect potential cybersecurity events	Network monitoring is done on a need basis using the firewall. Real time network monitoring has currently not yet been implemented.	i. CIS CSC 1, 7, 8, 12, 13, 15, 16 ii. COBIT 5 DSS01.03, DSS03.05, DSS05.07 iii. ISA 62443-3-3:2013 SR 6.2 iv. NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM3, SC-5, SC-7, SI-4
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	The physical environment is monitored to detect potential cybersecurity events.	i. COBIT 5 DSS01.04, DSS01.05 ii. ISA 62443-2-1:2009 4.3.3.3.8 iii. ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 iv. NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Real time network monitoring for personnel activity has currently not yet been implemented.	i. CIS CSC 5, 7, 14, 16 ii. COBIT 5 DSS05.07 iii. ISA 62443-3-3:2013 SR 6.2 iv. ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 v. NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-1
DE.CM-4: Malicious code is detected	There lacks processes for detection of malicious code.	i. CIS CSC 4, 7, 8, 12 ii. COBIT 5 DSS05.01 iii. ISA 62443-2-1:2009 4.3.4.3.8 iv. ISA 62443-3-3:2013 SR 3.2 v. ISO/IEC 27001:2013 A.12.2.1 vi. NIST SP 800-53 Rev. 4 SI-3, SI-8
DE.CM-5: Unauthorized mobile code is detected	There lacks processes for detection of unauthorized mobile code.	i. CIS CSC 7, 8 ii. COBIT 5 DSS05.01 iii. ISA 62443-3-3:2013 SR 2.4 iv. ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 v. NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	There lacks real time monitoring of external service provider activity within the organization.	i. COBIT 5 APO07.06, APO10.05 ii. ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 iii. NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
DE.CM-7: Monitoring for unauthorized personnel,	Monitoring of unauthorized connections is done using the firewall.	i. CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 ii. COBIT 5 DSS05.02, DSS05.05 iii. ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1

connections, devices, and software is performed		iv. NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
DE.CM-8: Vulnerability scans are performed	Vulnerability scans are done when need occurs. The organization is yet to implement a vulnerability management program.	i. CIS CSC 4, 20 ii. COBIT 5 BAI03.10, DSS05.01 iii. ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 iv. ISO/IEC 27001:2013 A.12.6.1 v. NIST SP 800-53 Rev. 4 RA-5

3.3 Detection Processes (DE. DP)

Sub-Category	**Finding**	**Informative Reference**
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	Roles and responsibilities for detection purposes have been defined but not yet fully implemented.	i. CIS CSC 19 COBIT 5 APO01.02, DSS05.01, DSS06.03 ii. ISA 62443-2-1:2009 4.4.3.1 iii. ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 iv. NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
DE.DP-2: Detection activities comply with all applicable requirements	Requirements for detection activities are still being developed internally.	i. COBIT 5 DSS06.01, MEA03.03, MEA03.04 ii. ISA 62443-2-1:2009 4.4.3.2 iii. ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 iv. NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA18, SI-4, PM-14
DE.DP-3: Detection processes are tested	Detection processes are currently not tested within the organization.	i. COBIT 5 APO13.02, DSS05.02 ii. ISA 62443-2-1:2009 4.4.3.2 iii. ISA 62443-3-3:2013 SR 3.3 iv. ISO/IEC 27001:2013 A.14.2.8 v. NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
DE.DP-4: Event detection information is communicated	The CTO and ICT manager receive alerts from the detection systems however there lacks a formal communication processes.	i. CIS CSC 19 ii. COBIT 5 APO08.04, APO12.06, DSS02.05 iii. ISA 62443-2-1:2009 4.3.4.5.9 iv. ISA 62443-3-3:2013 SR 6.1 v. ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 vi. NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA5, SI-4
DE.DP-5: Detection processes are continuously improved	Discussions for improvement of detection processes are done at managerial level.	i. COBIT 5 APO11.06, APO12.06, DSS04.05 ii. ISA 62443-2-1:2009 4.4.3.4 iii. ISO/IEC 27001:2013 A.16.1.6 iv. NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA5, SI-4, PM-14

4. Core Function Respond

4.1 Response Planning (RS.RP)

Sub-Category	Finding	Informative Reference
RS.RP-1: Response plan is executed during or after an incident	The organization has documented a security incident management standard and a response plan is executed during or after an incident.	i. CIS CSC 19 ii. COBIT 5 APO12.06, BAI01.10 iii. ISA 62443-2-1:2009 4.3.4.5.1 iv. ISO/IEC 27001:2013 A.16.1.5 v. NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8

4.2 Communications (RS.CO)

Sub-Category	Finding	Informative Reference
RS.CO-1: Personnel know their roles and order of operations when a response is needed	A crisis management team currently lacks within the organization.	i. CIS CSC 19 ii. COBIT 5 EDM03.02, APO01.02, APO12.03 iii. ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 iv. ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1 v. NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
RS.CO-2: Incidents are reported consistent with established criteria	Incidents are escalated to the CTO and ICT manager within the organization however consistency of reporting and establishment of incident criteria currently lack within the organization.	i. CIS CSC 19 ii. COBIT 5 DSS01.03 ISA 62443-2-1:2009 4.3.4.5.5 iii. ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 iv. NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
RS.CO-3: Information is shared consistent with response plans	It was noted that response information is shared on need basis.	i. CIS CSC 19 ii. COBIT 5 DSS03.04 iii. ISA 62443-2-1:2009 4.3.4.5.2 iv. ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 16.1.2 v. NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	It was noted that response information is shared on need basis.	i. CIS CSC 19 ii. COBIT 5 DSS03.04 iii. ISA 62443-2-1:2009 4.3.4.5.5 iv. ISO/IEC 27001:2013 Clause 7.4 v. NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	It was noted that response information is shared on need basis.	i. CIS CSC 19 ii. COBIT 5 BAI08.04 iii. ISO/IEC 27001:2013 A.6.1.4 iv. NIST SP 800-53 Rev. 4 SI-5, PM-15

4.3 Analysis (RS.AN)

Sub-Category	Finding	Informative Reference
RS.AN-1: Notifications from detection systems are investigated	The notifications received from the firewall are investigated by the CTO and ICT manager.	i. CIS CSC 4, 6, 8, 19 ii. COBIT 5 DSS02.04, DSS02.07 iii. ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 iv. ISA 62443-3-3:2013 SR 6.1 v. ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 vi. NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RS.AN-2: The impact of the incident is understood	The impact of the incident is analyzed together with their third party cybersecurity services provider.	i. COBIT 5 DSS02.02 ii. ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 iii. ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 iv. NIST SP 800-53 Rev. 4 CP-2, IR-4
RS.AN-3: Forensics are performed	Forensics is performed together with their third party cybersecurity services provider.	i. COBIT 5 APO12.06, DSS03.02, DSS05.07 ii. ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 iii. ISO/IEC 27001:2013 A.16.1.7 iv. NIST SP 800-53 Rev. 4 AU-7, IR-4
RS.AN-4: Incidents are categorized consistent with response plans	There currently lacks a formal incident categorization method within the organization.	i. CIS CSC 19 ii. COBIT 5 DSS02.02 iii. ISA 62443-2-1:2009 4.3.4.5.6 iv. ISO/IEC 27001:2013 A.16.1.4 v. NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Formal processes to receive, analyze and respond to incidents have currently been documented however not fully implemented.	i. CIS CSC 4, 19 ii. COBIT 5 EDM03.02, DSS05.07 iii. NIST SP 800-53 Rev. 4 SI-5, PM-15

4.4 Mitigation (RS.MI)

Sub-Category	Finding	Informative Reference
RS.MI-1: Incidents are contained	Upon identification of an incident, it is investigated and appropriate remedial actions are taken.	i. CIS CSC 19 ii. COBIT 5 APO12.06 iii. ISA 62443-2-1:2009 4.3.4.5.6

		iv. ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 v. ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 vi. NIST SP 800-53 Rev. 4 IR-4
RS.MI-2: Incidents are mitigated	Majority of the vulnerabilities identified are mitigated through patch management.	i. CIS CSC 4, 19 ii. COBIT 5 APO12.06 iii. ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 iv. ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 v. NIST SP 800-53 Rev. 4 IR-4
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	The process of updating newly identified vulnerabilities has currently not been streamlined within the organization.	i. CIS CSC 4 ii. COBIT 5 APO12.06 iii. ISO/IEC 27001:2013 A.12.6.1 iv. NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5

4.5 Improvements (RS.IM)

Sub-Category	Finding	Informative Reference
RS.IM-1: Response plans incorporate lessons learned	Lessons learnt are incorporated into the response plan on a need basis.	i. COBIT 5 BAI01.13 ii. ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 iii. ISO/IEC 27001:2013 A.16.1.6, Clause 10 iv. NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RS.IM-2: Response strategies are updated	The response strategies currently lack a formal updating process.	i. COBIT 5 BAI01.13, DSS04.08 ii. ISO/IEC 27001:2013 A.16.1.6, Clause 10 iii. NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

5. Recover

5.1 Recovery Planning (RC.RP)

Sub-Category	Finding	Informative Reference
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	The organization’s ICT recovery plan is executed after a cybersecurity incident. It is more of a reactive approach.	i. CIS CSC 10 ii. COBIT 5 APO12.06, DSS02.05, DSS03.04 iii. ISO/IEC 27001:2013 A.16.1.5 iv. NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8

5.2 Improvements (RC.IM)

Sub-Category	Finding	Informative Reference
RC.IM-1: Recovery plans incorporate lessons learned	Recovery strategies are updated based on their various clients. Each client has its own unique scenarios identified. Lessons learnt are retrieved from the incident reports.	i. COBIT 5 APO12.06, BAI05.07, DSS04.08 ii. ISA 62443-2-1:2009 4.4.3.4 iii. ISO/IEC 27001:2013 A.16.1.6, Clause 10 iv. NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RC.IM-2: Recovery strategies are updated	The recovery strategies are updated on an ad-hoc basis.	i. COBIT 5 APO12.06, BAI07.08 ii. ISO/IEC 27001:2013 A.16.1.6, Clause 10 iii. NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

5.3 Communications (RC.CO)

Sub-Category	Finding	Informative Reference
RC.CO-1: Public relations are managed	Currently, public relations are managed when need occurs.	i. COBIT 5 EDM03.02 ii. ISO/IEC 27001:2013 A.6.1.4, Clause 7.4
RC.CO-2: Reputation is repaired after an incident	The incident management policy contains both short-term counter-measures and longer-term action plans however it currently hasn’t been updated and is yet to be fully implemented.	i. COBIT 5 MEA03.02 ii. ISO/IEC 27001:2013 Clause 7.4
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	The organization is yet to define an escalation tree for communication of cybersecurity incidents.	i. COBIT 5 APO12.06 ii. ISO/IEC 27001:2013 Clause 7.4 iii. NIST SP 800-53 Rev. 4 CP-2, IR-4