UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

IMPACT ASSESSMENT METHODS FOR RISKS IN DATA PRIVACY: A CASE STUDY OF KENYAN IT-ENABLED SMEs

ROBERT WAFULA

REG NO. P54 / 35274 / 2019

SUPERVISOR: Dr. ANDREW MWAURA KAHONGE

A research project report submitted to the Department of Computing and Informatics in partial fulfillment of the requirements for awardarding a Master of Science in Information Technology Management from the University of Nairobi

August, 2019

DECLARATION

This project described in this report is my original work and to my knowledge this research project has never been submitted for any other university award.

Signature: R.Wafula Date: 24 August 2022

Robert Wafula
P54 / 35274 / 2019
Department of Computing & Informatics
University of Nairobi

The Project has been submitted in partial fulfillment of the requirements for the Master of Science Degree in Information Technology Management from the University of Nairobi with my approval as the University Supervisor

Signature: Date: 22/

Dr. Andrew Mwaura Kahonge
Department of Computing & Informatics
University of Nairobi

ACKNOWLEDGEMENT

I thank God for his mercy and kindness in guiding me through this research process. I also thank the Department of Computing and Information for giving me the opportunity to pursue my Master of Science degree in Information Technology Management. The professional guidance and time of all the staff in the department who have taught and challenged me, especially my project supervisor, Dr. Andrew Mwaura Kahonge. I also appreciate the tremendous encouragement from Mr. Christopher A. Moturi. Thanks also to Dr. Karim Omido, for taking the time to review my work and making an invaluable contribution. I would like to thank my family for their constant love and support during my research. Last but not least, I would like to thank my friends and colleagues who provided constructive feedback and supported me during my research.

May God Bless you.

DEDICATION

I dedicate this study to my loving wife who has been a beside me, to my mother who has been a great support even in illness, and to my brothers and their families who have continually accorded me their endless love and support.

ABSTRACT

Information has become a strategic commodity. Data-driven decision-making processes have been observed to lead to more efficient planning and usage of resources. Businesses have adopted their processes to collect data from their customers, in order to perform analyses from this data and obtain some useful information. The protection of data has become a key factor to the success of SMEs. The Government of Kenya enacted into law new data protection regulations that aims to ensure protection of individual personal data, and provided regulation on the handling of personal data. IT-enabled SMEs were therefore presented with new business risks in compliance to these new regulations. Therefore, there was a need to identify the key factors influencing compliance with data protection impact assessments in IT-enabled SMEs in Kenya and to identify applicable open source frameworks for managing data protection as a business risk.

The purpose of this study was to identify key data protection impact assessment factors facing IT-enabled SMEs in Kenya and to identify applicable open source frameworks for managing data protection as a business risk. This research was a case study focused on understanding privacy risk management practices among identified SMEs. A primarily qualitative study was performed to determine the data for this study, and the collected data were organized systematically to facilitate analysis.

The study found that Kenya has extensive legislation on data privacy. The study also highlighted the significance of Kenyan IT-enabled SMEs investing in the data privacy training and awareness, data privacy policy programs, data privacy vulnerability management programs and privacy by design plays a key role in management of data privacy as a business risk. The study also identified the use of OCTAVE-small as a framework that can be adopted by these SMEs. The study proved the viability of the OCTAVE-small Data Privacy Impact Assessment framework as suitable for IT-enabled SMEs in Kenya. This recommendation was guided by the proportionate regulatory framework which would ensure the SMEs maintain active risk management of data privacy related risks.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

4IR	Fourth Industrial Revolution
CMA	Capital Markets Authority
COBIT	Control Objectives for Information Technologies
DESA	Department of Economic and Social Affairs
DPIA	Data Privacy and Protection Impact Assessment
DPO	Data Protection Officer
EU	European Union
EY	Ernst & Young
GDP	Gross Domestic Product
GDPR	General Data Protection Regulations
GoK	Government of Kenya
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISF	Information Security Framework
ISO	International Organization for Standardization
ISRM	Information Security Risk Management
KICTANet	Kenya ICT Action Network
KNBS	Kenya National Bureau of Statistics
NIIMS	National Integrated Identity Management System
NIST	National Institute of Standard and Technology
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SMEs	Small and Medium Sized Enterprises
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development

DEFINITION OF TERMS

Assessment	The examining and/or evaluation of the administrative, operational, and technical controls in an information system or organization to resolve the extent to which the controls are implemented correctly.
Evaluation	The cross-examination of a system to determine its degree of compliance with a stated security model, security standard or specification.
Framework	A set of documented processes that define policies and procedures for the management and implementation of information security controls.
Impact	The magnitude of harm expected to result as a consequence of unauthorized disclosure, modification, destruction or loss of information or availability of an information system.
New Technology	Emerging technology that enhances or revolutionizes current technology.
Old Technology	Obsolete technology that is no longer widely used in favor of current technology.
Risk	A measure of the extent to which an entity is threatened by a potential situation or event.

CHAPTER ONE: INTRODUCTION

1.1. Background of the Study

Technology has proven to be an invaluable asset in the transformation and disruption of many industries. Technology, and industries driven by technology, have witnessed a revolution over the past few decades, as new digital solutions arise every day, phasing out old technology. The rate of technology change, in a study carried out in Germany on The Fourth Industrial Revolution by Schwab (2016) has forced businesses to reinvent their business processes to take advantage of technology to stay profitable, and even in some cases to stay relevant. Businesses and human resources have been forced to adopt this revolution, termed the Fourth Industrial Revolution (4IR) (Ibid.). This revolution has been characterized with the emergence, deployment and diffusion of new technologies in order to generate new opportunities to accelerate innovation, and increase production according to a Chinese study on Opportunities and Challenges of the Fourth Industrial Revolution (Xu, David and Kim, 2018). The EU Ecommerce Report denotes the uptake of new technologies as one of the determinants of a level playing field. This implies that a business that can embrace and adopt new technologies gains a competitive advantage in its respective domain and environment as compared to a business that does not adopt new technologies.

New technologies are perceived to be sources of contemporary information. Information has become a strategic commodity, and the protection of data has become a key factor to the success of SMEs in line with assertion from a Slovakian research entitled Data Protection and Security in SMEs under Enterprise Infrastructure (Hallova, Polakovic, Silerova, and Slovakova, 2019). Data-driven decision making processes have been observed to lead to more efficient planning and usage of resources (KICTANet, 2018). Businesses have therefore adopted their processes to collect data from their customers, in order to perform analyses from this data and obtain some useful information. This information plays a key role to reducing their business risks and maximizing their profitability. As businesses scramble to collect as much information as possible from their respective environments in order to obtain some advantage, regulatory bodies are needed to enact laws, policies and standards to govern how this information is collected, processed, stored and disposed. The Government of Kenya in 2019 enacted the Data Protection Act, 2019. This Act aims to ensure protection of individual

personal data, provide regulation on the processing of personal data, enshrine into law provisions for rights and responsibilities data subjects, data processors and data controllers and finally to establish the Office of the Data Protection Commissioner (Government of Kenya, 2019).

The Data Protection Act (Government of Kenya, 2019), defines responsibilities for those who collect personal data. This has a crucial implication to businesses that collect personal data. Such businesses become subject to the Data Protection Act, and breach of its provisions has punitive legal implications. The obligatory subjection to this Act implies that businesses have to carry out technological, legal and functional changes to ensure compliance with the law, presenting businesses with a new set of risks that they previously may not have accounted for. This can be especially risky to SMEs, who may not have the human and financial resources to ensure full compliance with the legislation. It has also been noted by Freitas and Mira-da-Silva, (2018) in their study in Italy on Compliance in SME's that in some instances, SMEs are unaware of their responsibilities in relation to data protection regulations. SMEs can also have less technically trained staff to handle data protection risks. The EY Global Information Security Survey notes that whereas 35% of larger companies have a threat intelligence program, only 25% of smaller organizations have a similar program. This implies data collected by SMEs could potentially be at greater risk as compared to larger companies. This risk becomes even more magnified when the staff are careless or unaware of their risk exposure, as this segment constitutes 34% of vulnerabilities with the most increased risk exposure between 2018 to 2019. (EY, 2019) The most commonly cited challenges for the general public and non-government actors in relation to data governance includes data privacy and the lack of understanding of data related policies (United Nations, 2020).

Statistics show that SMEs have provided a large percentage of employment opportunities within Africa, around 80% (World Economic Forum, 2010), and at 81.1% of employment opportunities within Kenya (Kenya National Bureau of Statistics, 2016). The importance of SMEs to the economy cannot be overstated, as they are key to job creation, poverty eradication and contribute significantly to the Gross Domestic Product (GDP). It is therefore relevant to establish the readiness of SMEs to the compliance requirements brought about by the new data protection regulations, and to establish a strategy that will serve as a guideline for managing business risks brought about from compliance to data protection and privacy regulations.

It is therefore relevant to establish the readiness of SMEs to the compliance requirements brought about by the new data protection regulations, and to establish a strategy that will serve as a guideline for managing business risks brought about from compliance to data protection and privacy regulations. The aim of this study was hence to establish the framework for evaluation of data privacy impact assessment methods in Kenyan IT-enabled SME's.

1.2. Problem Statement

The Fourth Industrial Revolution has enabled SMEs have easy access to digital tools and technologies that grant them capabilities to trade online through ecommerce. Ecommerce as a tool used through open-source software has the potential of allowing a greater number of SME's to engage in business; a process of which can eliminate expensive licensing fees courtesy of the contribution of developers. Developers of some of these tools have made them open source, removing the requirement for expensive licensing fees for new entrants into the e-commerce space (Schwab, 2016). SMEs have taken advantage of these open-source e-commerce platforms for conducting their business, and have inadvertently collected data from users both actively and passively. The data collected was for the purpose of obtaining commercial value from the information gained after analysing the data, which is one of the highlighting features of an evolving digital economy (United Nations, 2019).

The introduction of the Data Protection Act, 2019 introduced several concepts that governed how data controllers and data processors interact with data from data subjects. These new regulations were obligatory for all organizations that collect data within Kenya's jurisdictions (Government of Kenya, 2019). These new regulations placed responsibility of data collection, processing, storage, security, confidentiality and integrity with the organizations that collected the data. The Act also placed the responsibility of compliance with the regulations on the organization collecting the data. The breach of regulations defined in the Act was also denoted as a prosecutable offence, serving as a penalty for those who fail to adhere to the guidelines set in the Act. The establishment of this Act therefore exposed SMEs to the risk of non-compliance, and thus the need to set forth internal processes and procedures to ensure compliance to the Act.

The establishment of compliance procedures however requires resources. There is inadequate resources on how a data controller conducts and documents an impact assessment with regards

to data privacy regulations (Vallabhaneni, 2020). Despite the establishment of data privacy and protection regulations in many jurisdictions globally, the Global Information Survey highlighted there has been clear violation of data protection in the recent times as adduced by Ernst & Young (2019). There was therefore a gap in having a framework that guides the data privacy impact assessment, which is vital to identifying potential risks brought about by handling of user data, and also crucial to the privacy-by-design principle. This study hence aimed at identifying an open-source framework for evaluation of data privacy impact assessment methods in Kenyan IT-enabled SME's.

1.3. Research Objectives

The main objective of this research was to identify an open source assessment framework that is designed to conduct risk analysis and mitigation from breach of data privacy for Kenyan IT-enabled SMEs to benchmark their compliance to applicable data protection regulations. To achieve this, the researcher sought to meet the following objectives:

i. To investigate and identify applicable data protection regulations in Kenya
ii. To investigate and identify data protection compliance risks impacting Kenyan IT-enabled SMEs
iii. To investigate and identify information security frameworks that are relevant to impact assessment methods for risk in data privacy
iv. To identify an open source information security framework which will provide a roadmap for Kenyan IT-enabled SMEs to assess themselves in compliance to the data protection regulations in Kenya

1.4. Research Questions

This study was guided by the following research questions:-

i. What changes in data protection regulations have been enacted within the past three years, that are specifically applicable to Kenyan IT- enabled SMEs?
ii. What is the risk exposure for Kenyan IT- enabled SMES who fail to comply with the newly enacted data protection regulations?
iii. What existing information security frameworks exist to assess data privacy impact risks?

iv. What information security framework will best provide a roadmap for Kenyan IT-enabled SMEs to assess their data privacy impact risks as regards to the data protection regulations in Kenya?

1.5. Significance of the Research

Information is a strategic commodity in business, and SMEs make use of data in order to make informed decisions to boost their profitability, and sustain them in business. The findings in this research will provide a framework for IT- enabled SMEs in Kenya on privacy impact risk assessment relevant to data protection regulations as a component of their business risks. This is to enable the SMEs have a concise guide on how to carry out a comprehensive assessment of their compliance to the data privacy and protection regulations, with the aim of ensuring full compliance through corrective measures where they are deficient.

The findings in this research also aim to increase the body of knowledge on data protection compliance assessment for SMEs in other parts of the world, who can take applicable concepts from this document and tailor it to their specific environmental variables.

1.6. Scope of the Study

This research was intended to achieve the objective of identifying a feasible open source data privacy risk assessment framework. This study shall be limited to data privacy and protection risks in Kenya, and specifically IT- enabled SMEs because of time and resource constraints.

The scope of this research was limited to IT-enabled SMEs in Kenya. The research focused on proposing a feasible open source data privacy impact assessment framework applicable to these SMEs. A list of these SME's has been provided vide appendix 3. The researcher interviewed the ICT Manager at Takaful Insurance of Africa, the ICT Manager at Janice Medical & Cancer Hospital, and the Technical Director at Urban Kreative Limited. Takaful Insurance and Janice Medical & Cancer Hospital were representative of a balanced population in Kenya as they deal with clients from various walks of life. Urban Creative was chosen as it is an IT-enabled SME that specializes in providing digital services, in comparison with Takaful Insurance and Janice Medical & Cancer Hospital who use IT to enable operations in non-technology domains.

1.7. Assumptions and Limitations of the Study

The research made the following assumptions in this study:-

i. The technical jargon is clearly understood by the respondents.
ii. The respondents are able to fully interpret the questions without need for a research assistant.
iii. The respondents' answers are a truthful representation of their organization.

The researcher encountered the following limitations in the course of the research:-

i. The respondents were busy with their respective core functions and were unable to respond in the time allocated. The researcher mitigated this by allowing the respondents more time to complete the questionnaires.
ii. The respondents were unavailable for physical interviews due to COVID-19 risks. The researcher mitigated this by issuing the questionnaires by soft copy.

CHAPTER TWO: LITERATURE REVIEW

2.1. Introduction

Data protection is the process of guarding information from compromise, corruption, or loss. Data privacy focuses on the right of individuals, the reason for the collection and processing of the data, privacy inclinations, and the governing policies by which the data collector or processor handle personal data of the data subjects. Data protection and privacy has always played a key role in the business environment, as customers entrust their personal data to the businesses with the assumption that the business will protect their data, and not divulge it without their consent.

The adoption of e-commerce globally has empowered many SMEs to adopt new business models that allow them to reach consumers more directly at reduced cost. The growth of e-commerce adoption and usage has led to moving from self-regulation by e-commerce service providers to the current government-enforced regulations. The rise in new legislative measures has been to address issues around setting standards and policies that regulate e-commerce. The United Nations Conference on Trade and Development has made note of the increasing number of countries that have implemented e-transaction laws (79% of member states), consumer protection laws (52% of member states), data protection and privacy laws (58% of member states) and cybercrime laws (72% of member states) (UNCTAD, 2020).

This chapter highlights the impact that a breach on data privacy and protection can have to an organization, the concepts of risk management with regards to information security, the general concept of a data privacy and protection impact assessment, and an overview of existing model data privacy impact assessment frameworks.

2.2. The Impact of Data Privacy and Protection Breach

A data breach is the intentional or unintentional disclosure of confidential information to unauthorized parties (Cheng, Liu, and Yao, 2017). In this new digital age where data is of great commercial value, data breaches can pose existential threats to organizations. The cost of data breaches is not only viewed from the direct financial impact, but also to additional metrics such as consumer confidence, personal safety and social trust (Liu and Han, 2018).

Data breaches can be internal or external, and can also be as a result of intentional attacks or accidental exposure or revelation (Cheng et al., 2017). IBM Security conducts an annual Cost of Data Breach Study report, and in their 2019 report, they revealed the average total cost of a data breach being US $ 3.9 million. They also documented in the same report the average time to identify and contain a breach being 279 days (IBM Security, 2019). The report identifies a trend over the past 5 years, over which an increase in the global average cost of a data breach has increased by 12%. Figure 1 below shows this trend.

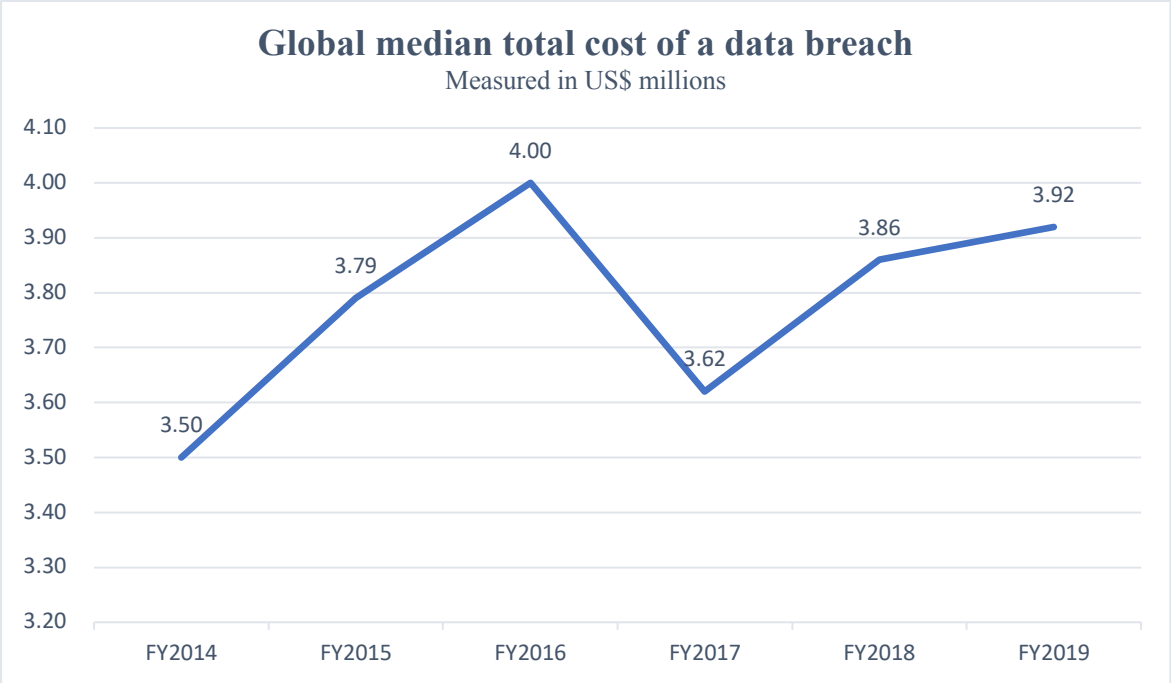

Figure 1: Global median total cost of a data breach

Source: IBM (2019) Cost of Data Breach Report 2019

These statistics are even more troubling when the comparing the cost of data breaches in large corporates versus smaller organizations. The report categorizes organizations into personnel size, and analyses the total cost of a data breach in each of these categories. Table 1 below shows these findings.

Number of Employees	Total Cost per Breach	Cost per Employee
	(US$ Millions)	(US$)
Less than 500	2.74	10,981.96
500 to 1,000	2.65	3,533.33
1,001 to 5,000	3.63	1,209.80

5,001 to 10,000	4.41	587.96
10,001 to 25,000	4.35	248.56
More than 25,000	5.11	408.80

Table 2.1: Cost of a data breach by organizational size
Source: IBM (2019) Cost of Data Breach Report 2019

A visual representation of these statistics is shown in figure 2 below

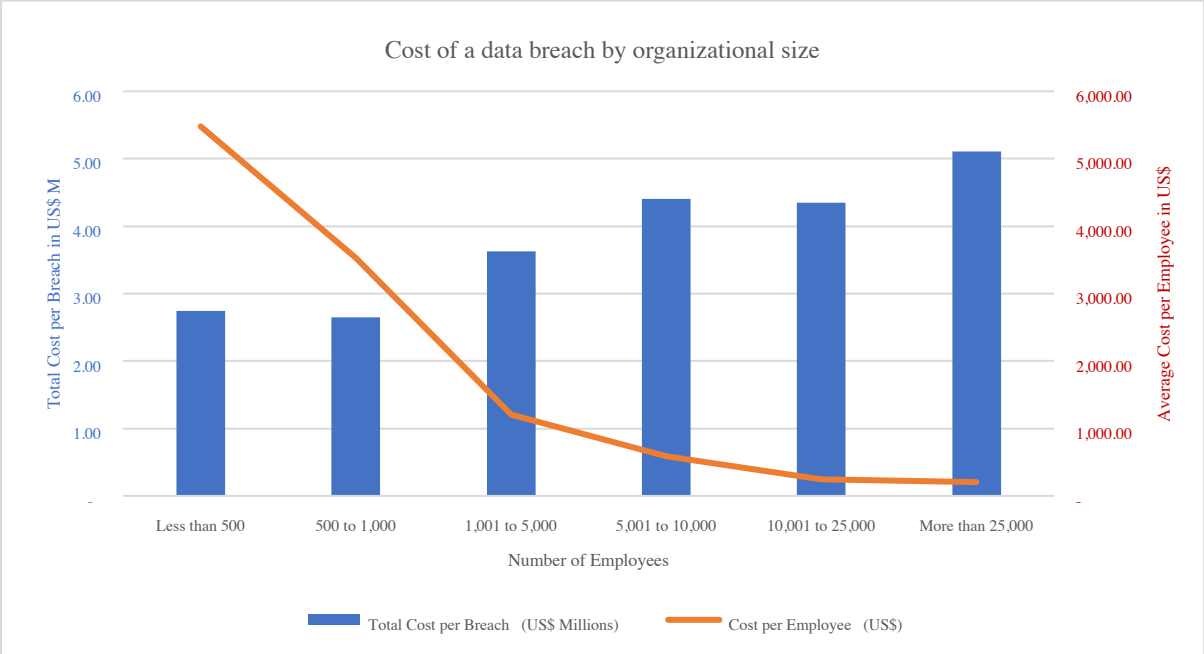

Figure 2: Cost of a data breach by organizational size
Source: IBM (2019) Cost of Data Breach Report 2019

An analysis of Figure 2 visual representation shows that generally the cost per employee of a data breach is inversely proportional to the total cost per breach. For instance, the total cost for the largest organizations large organizations with more than 25,000 employees had an average total cost of $5.11 million, which is $204 per employee. However, smaller organizations with 500 to 1,000 employees had an average total cost of $2.65 million, which is $3,533 per employee. This therefore shows that smaller organizations, in which SMEs are categorized, have higher costs relative to their size, and a breach poses a great threat to their ability to recover financially from an incident (IBM Security, 2019).

2.3. Information Security Risk Management

Risk can be defined as the probability of an event occurring and the consequences associated with that event. (Wangen, Hallstensen and Snekkenes, 2018). Risks should be identified, evaluated, analyzed, treated and reported. (Blakley, McDermott, and Geer, 2002). There are several standards and frameworks for information security risk assessment that have been developed. Information security risk management (ISRM) is defined as the practice of continuously identifying, evaluating, analyzing, treating and monitoring information security risks in order to achieve risk acceptance (Wangen et al, 2018). The figure below shows a typical risk management process, as defined on the ISO standard 31000.

Figure 3: Typical Risk Management Process (ISO 31000)

According to ISO 27000:2014, risk analysis is defined as the systematic use of information to identify potential sources of risks. It also further defines risk evaluation is a process comparing estimated risk against defined risk criteria to calculate the significance of the risk (ISO, 2014).

There are several elements that pose risks to information security, but this research will focus on data privacy as a component of information security risk. Data privacy focuses on the rights of data subjects, and data privacy and protection regulations exist to ensure enforcement of the rights of these data subjects. The processing of customer data has to be done in a secure manner, as breach of data privacy is an information security risk to the data processor. A data privacy risk assessment framework serves as a way for a data processor or controller to assess their adherence to observing the rights of data subjects, as defined in the Constitution of Kenya, 2010, and the Data Protection Act, 2019. The information security framework serves the purpose of identifying the potential risks, identifying the likelihood of occurrence, and identifying the severity of the consequences.

2.4. Data Privacy and Protection Risk Assessment

Privacy Risk Assessment is defined as a risk management approach to identify and allay privacy risks and to implement the principles of Privacy by Design so as to foster consumer trust (Oetzel and Spiekermann, 2014). In the instances where the processing of data has an impact on the fundamental rights and freedoms of data subjects, Section 31 of the Data Protection Act stipulates that a data controller or data processor must conduct a data protection impact assessment (Government of Kenya, 2019). A Data Protection Impact Assessment allows for stronger decision-making at the implementation stage and sidesteps the need for costly consequent ammendments or potential exposure of personal data (MacroSec, 2020). There is a need for a standardized framework for data management that will facilitate the recognition of potentially harmful data-processing activities, and provide guidance on existing risks (Alshammari and Simpson,2018).

A general flow diagram of a Privacy Impact Assessment is as shown in the following page:

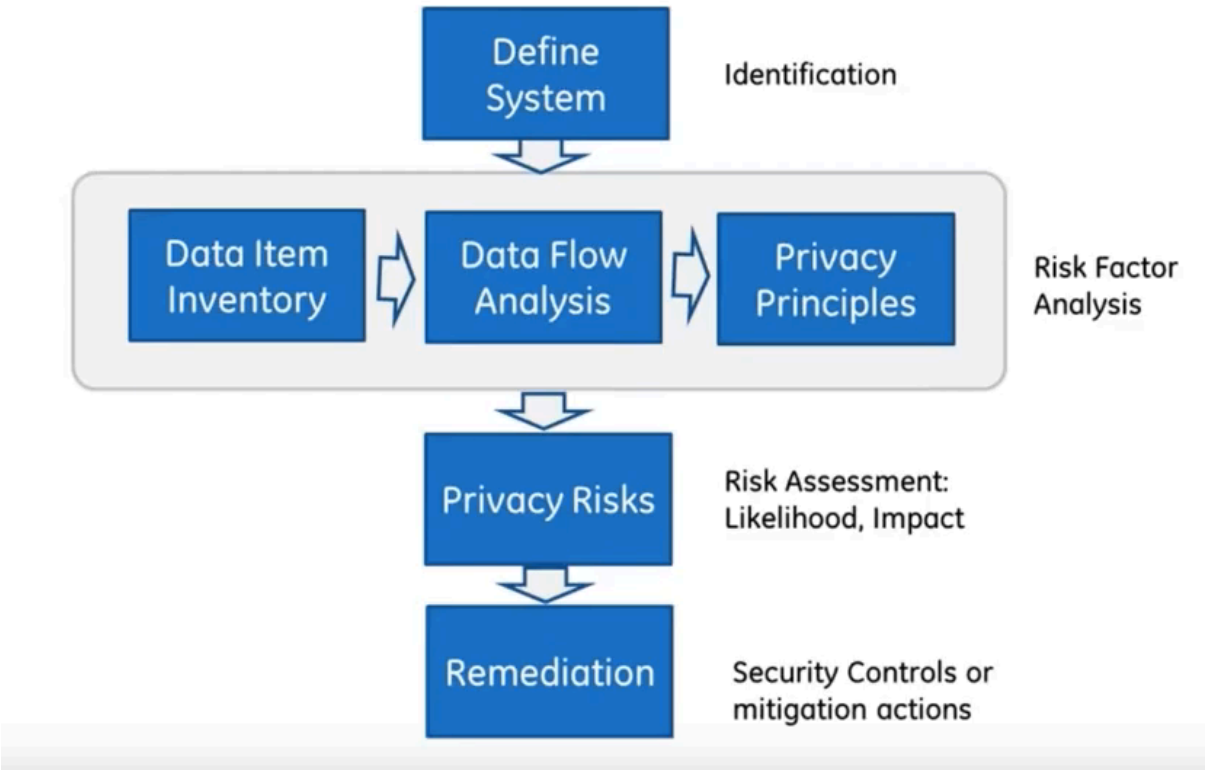

Figure 4: Flow of Privacy Risk Impact Assessment

Source: Databrackets Limited

The figure above is a general flow of a privacy impact assessment. The sequence of steps in this workflow is defined as:

i. ***System Identification***: The objective of this step is to define the system, and define what is within the boundary of the system
ii. ***Risk Factor Analysis***: The objective of this step is to understand the data items that are present in the system, what data flows are present in the system, what data items are present in each of the identified data flows, and then apply privacy principles to the data flows
iii. ***Privacy Risks***: The objective of this step is to associate identified privacy risks to the data items and data flows
iv. ***Remediation***: The objective of this step is to establish security controls to mitigate the identified privacy risks

2.5. Data Privacy Impact Assessment Frameworks

2.5.1. OCTAVE Allegro

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) methodology is an information security risk assessment methodology created by CERT. The OCTAVE Allegro methodology focuses on information assets, and considers other information containers as well (Ali and Awad, 2018). This methodology seeks to analyse how information is used by the users and devices in a system, as well as the information containers, and how this information is exposed to risks (Caralli, Stevens, Young and Wilson, 2007). This methodology is optimized to deliver efficient results with limited resources, and is best suited for smaller or mid-sized organizations (Duricu, 2019). The OCTAVE Allegro methodology contains guidance, questionnaires and worksheets for conducting the risk assessment process.

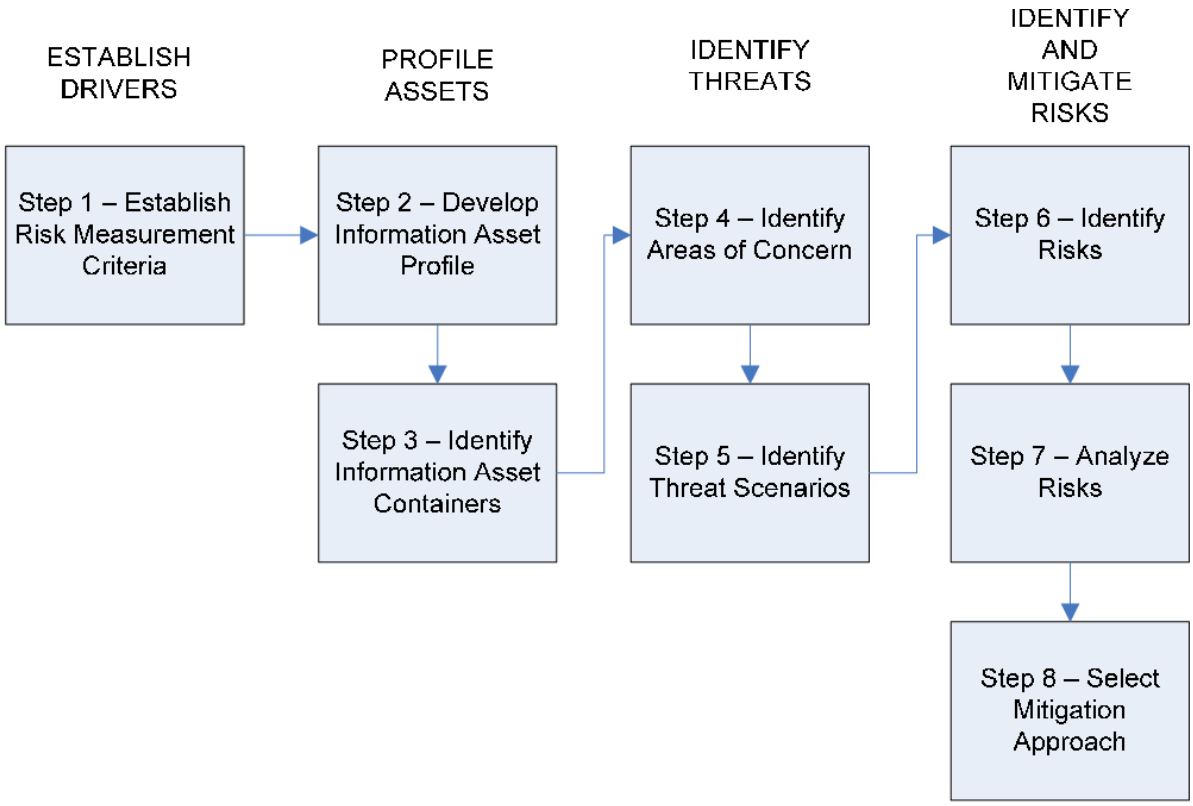

Figure 5: OCTAVE Allegro Methodology Flowchart

Source: Caralli et al., 2007

The OCTAVE Allegro methodology flowchart identifies eight steps that are categorized broadly into the following four phases:

i. ***Establish Drivers Phase***: The objective in this phase is to create a foundation for the risk assessment. This is done by developing a set of qualitative risk measurement criteria, and also by identifying business areas that are critical whereby the impact of risk is most significant.

ii. ***Profile Assets***: The objective in this phase is to identify and profile asset information inside the organization. The assets are stored in information asset containers, and these should also be identified and profiled. Any risks to the container are inherited by the assets within that container.

iii. ***Identify Threats***: The objective in this phase is to generate a list of potential threats, through the use of real-world scenarios. Each scenario is expounded upon, individually analysed and its inherent properties documented. Identified threats that are risky to the organization are clearly highlighted.

iv. ***Risk Mitigation Phase***: The objective in this phase is to identify the security risks to the information assets, analyse the impact and consequences of the identified threats, and develop a risk mitigation plan to contain the risk

2.5.2. ISO/IEC 27005:2018

The ISMS Family of Standards (ISO 27000 series) are information security standards that have been developed jointly by the ISO and IEC. These family of standards provide best practice recommendations on the management of information security risks (ISO/IEC, 2013). ISO/IEC 27005 is one of the standards in the ISMS family of standards, and specifically provides policies and methods for managing information security risks.

The ISO/IEC 27005:2018 is designed to aid the implementation of information security through a risk management approach (ISO/IEC, 2018). Whereas this standard does not identify a specific risk management method, it however outlines a sequence of structured activities that constitute the process. These activities are shown in the figure below, showcasing the sequence and relation of each sequence to the next:

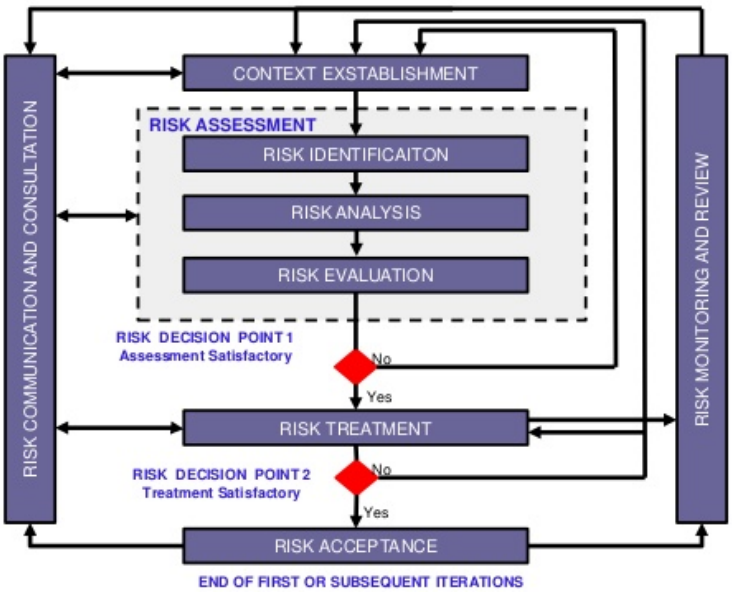

Figure 6: ISO 27005:2018 Information Security Risk Management Process

Source: Thomas Peng

The identified sequence of activities according to ISO 27005:2018 include:

i. ***Context establishment***: This activity refers to the information gathering phase, in which the risk assessment approach is defined. This includes the risk evaluation criteria, risk impact criteria, risk acceptance criteria and the scope of the information security risk management. A guidance standard on defining the scope of the information security risk management process is supplied in Annex A of ISO 27005:2018.

ii. ***Risk assessment***: This activity refers to identifying of risks and prioritizing them against the risk evaluation criteria generated in the context establishment activity. The risk assessment activity contains other sub activities that include identification of assets, threats, existing controls, vulnerabilities, consequences and risk estimation methodologies. It also includes the assessment of consequences, level or risk and likelihood of risk.

iii. ***Risk Treatment***: This activity refers to defining controls that are designed to reduce, retain, avoid or transfer the risks identified in the risk assessment activity. In this

activity, the activities undertaken include risk reduction, retention, avoidance or transfer

iv. ***Risk Acceptance***: This activity refers to ensuring that the remaining risks are explicitly accepted by the organization's leadership. In this activity, it is important that the risk acceptance is clearly documented to establish the risk acceptance standard.

v. ***Risk Communication***: This activity refers to the gathering of information on risks, and disseminating the findings of the risk assessments that are conducted.

vi. ***Risk Monitoring and Review***: This activity refers to maintaining regular observance of risks and their factors to ensure that a complete risk overview is maintained at all time. This is relevant at identifying contextual changes at an early stage and can treat risk early on.

2.5.3. NIST Privacy Framework

The National Institute of Standards and Technology (NIST) developed and published guidelines that aim to enable organizations adapt to progressively stringent data privacy requirements (NIST, 2020). The framework contains a set of voluntary procedures which can aid compliance with various data protection regulations globally (NetApp, 2020). This is done by enabling the organizations map their privacy requirements with distinct workflows and controls. The framework is designed to be flexible, scalable and extensible, making it suitable for use for all sizes of business, but especially helpful for small to medium organizations who may not have extensive knowledge on data privacy compliance.

NIST Privacy framework shares basic concepts and terminologies with the NIST cybersecurity framework (NetApp, 2020). The NIST framework structure is comprised of three foundational components:

i. ***Core***: This component is a set of five broadly based privacy protection activities known as functions. These functions are:
    a. *Identify (P)* – This component is concerned with identifying privacy risks through inventory, data mapping and risk assessments.

b. *Govern (P)* – This component relates to managing privacy risks through awareness training, monitoring, procedures, processes, policies, risk management strategies and reviews.

c. *Control (P)* – This component relates to data processing controls, processes, procedures, policies, and control of privacy risks from processing that does not belong to a device or individual.

d. *Communicate (P)* – This component refers to communication of privacy risks through data processing awareness and initiating communication policies, processes and procedures

e. *Protect (P)* – This component refers to protection against privacy risks through use of data policies, access control, authentication, data security, identity management, protective technology and system maintenance.

ii. ***Profiles***: This component is a set of specific functions that the organization can select from the framework based on what it determines to be its risk management priorities. The profiles are influenced by regulatory requirements in the jurisdiction in which they operate, the products and services the organization offers and the shared privacy responsibilities with external parties. This therefore implies one can pick a custom profile from the possible set of components in the core, as described by the figure below:

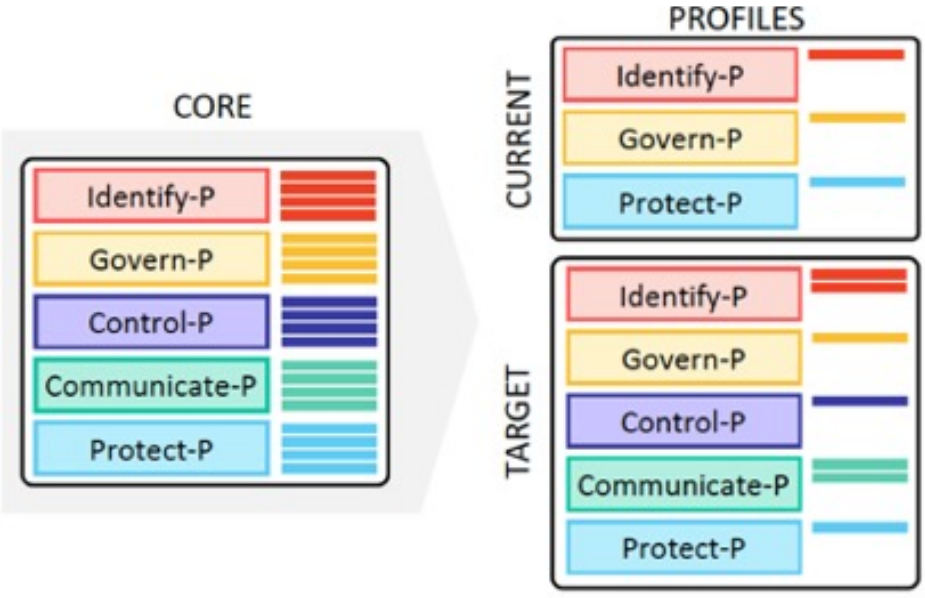

Figure 7: Relationship between Framework Core and Profiles

Source: NIST, 2020

iii. ***Implementation Tiers***: This component indicates the strength of the privacy measures the organization currently or projects to apply. It is ranked on a scale of Tier 1 up to Tier 4. These tiers allow the organization to benchmark its capacity to manage privacy risk

The NIST Privacy Framework 2020 also discusses in brief four approaches to risk management. These include

i. ***Mitigation*** – Including data privacy protections and measures in Information Technology business operations, products, and services.
ii. ***Transfer*** – Sharing accountability with data subjects by transferring power to third parties via permission channels.
iii. ***Avoidance*** – Stopping data collecting if there are more risks than advantages.
iv. ***Acceptance*** – Determining that, if the potential harm is low or negligible, no corrective action is necessary.

2.6. Summary of Frameworks

Framework Name	Source Organization	Description
OCTAVE Allegro	CERT	OCTAVE is focused on strategic, practice-related issues and is targeted at organizational risk. This framework works well for a knowledge-based risk assessment of a given process. Only organizational resources are allowed to implement the process. OCTAVE details the formation of an assessment team that is constituted of representatives of both business lines and IT personnel. Additionally, it employs a workshop-based methodology to acquire data and make choices.

		OCTAVE seeks to identify human resources that could be mission-critical, and its documentation is reliant on its three catalogues of information
ISO/IEC 27005:2018	ISO / IEC	ISO encompasses people, processes and technology. It is generally designed for higher-level management practices. It is clear in highlighting the right personnel are involved in the risk assessment. ISO makes use of system and network audit tools checking technical compliance, covering all the security controls as defined in the ISO 27005:2018 standard.
NIST Privacy Framework	NIST	NIST is a management system that is best suited for technology-related risk assessments and primarily allows third-party execution. In its approach, the NIST framework specifies duties, but it does not establish an assessment team. Common methods for acquiring information include surveys, interviews, and document reviews. Human resources are not mentioned by NIST as a possible organizational asset. It creates a Security Requirements Checklist for the management, operational, and technological security sectors.

Table 2.2: Summary of Frameworks

2.7. Theoretical Model

The theoretical model adopted for this study was the OCTAVE Small (OCTAVE-s). A simplified process model of the model is shown in figure 8 below:

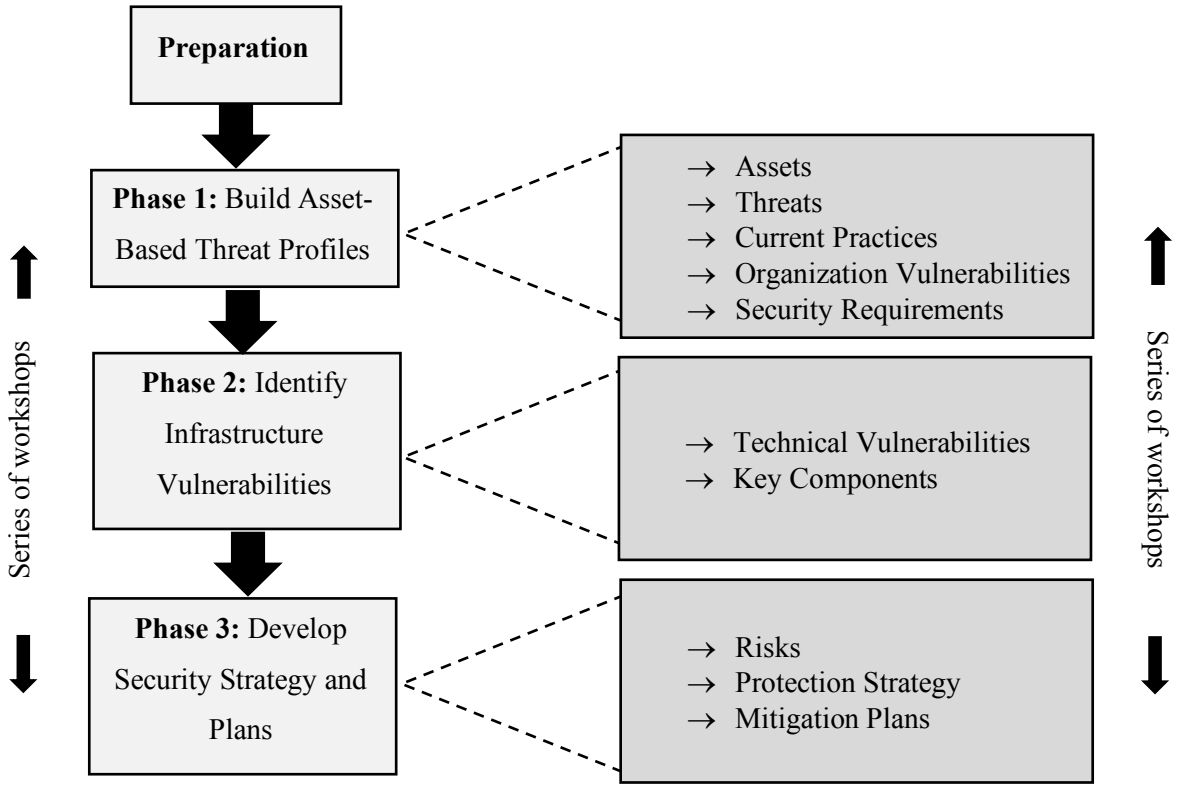

Figure 8: Data Privacy Impact Assessment process (OCTAVE-s)

Source: Pyka and Sobieski, 2012

The process model is divided into three main phases

i. *Phase 1 - Build Asset Based Threat Profiles*: This phase highlights the importance of data protection to the staff, and enumerates the potential risks that could emerge in the event of a data breach or loss.

ii. *Phase 2 – Identify Infrastructure Vulnerabilities*: This phase involves evaluates the information management systems technologies, with an aim to highlight data protection vulnerabilities, and a solution developed that is in line with the company's business model.

iii. *Phase 3 – Develop Security Strategy and Plans*: Using the information from phase 1 and 2, the risk analysis is conducted to classify threats based on probability, and a security strategy is developed to address the identified risks.

CHAPTER THREE: METHODOLOGY

3.1. Introduction

The chosen research approach is described in this chapter. It covers the research methodology, study design, context of the case, data collecting and analytic strategies, validation, and ethical concerns used to the execution of this study.

3.2. Research Philosophy

This study utilized the pragmatic research ethic, which acknowledges that there are several methods to do research and that no single viewpoint can provide an exhaustive picture (Saunders et al., 2012). With the help of this research philosophy, the researcher was able to combine several qualitative and quantitative research approaches, methods, and processes.

3.3. Research Design

The study utilized a descriptive research design, which is used to outline a population's characteristics. This is a method of scientific observation and description of a subject's characteristics without altering it in any manner. (Shields et al., 2013). The study's main goal was to comprehend how to control information security risk by evaluating compliance with data privacy laws using an evaluation methodology.

3.4. Case Background

The case study organization is a leading technology services provider that provides financial facilities, cross-border transactions through mobile services to individual and corporate customers. The organization has been in operation in the Kenyan market for 8 years, and has some relevant experience from its parent company that has been offering financial facilities within Europe. The organization has presence in 12 countries within Africa including Kenya, Tanzania, Uganda, Rwanda, Burundi, Zambia, Zimbabwe, Namibia, South Africa, Nigeria, Ghana and Egypt. They are also currently piloting their services Ethiopia and South Sudan.

Their business product requires them to actively collect user information to keep records on their customers, and in many of the jurisdictions they operate, it is also a legal requirement. With the growing information risks brought about by data breaches, they have voiced their

need for having a unified framework by which they can assess their compliance to data privacy and protection regulations within the jurisdictions they operate.

3.5. Data Collection Methods

The data collected during the first phase of the study was obtained through review of publicly accessible data available from Government agencies, and through corporate web portals. This was gotten primarily from the Kenya National Bureau of Statistics, with additional information collected from corporate websites. This phase of data collection established the source of quantitative data for the study.

The data collected during the second phase of the study was obtained through interview sessions with relevant staff at the case study organization. Key staff considered relevant for interviewing included senior management, business process owners and IT professionals. Additionally, secondary data sources were established that included policy and procedure documents. This phase of data collection established the source of qualitative data for the study.

Data Source	**Data Type**	**Data Use**
Publicly available data statistics	Qualitative Data	To establish a background on the state of information security risks arising from data privacy
Interviews with Senior Management	Qualitative Data	To understand the decision-making processes in the organization relevant to their data privacy concerns
Interviews with Business Process Owners	Qualitative Data	To understand the impact of data privacy concerns in their day to day execution of tasks
Interviews with IT professionals	Qualitative Data	To understand the technical implications of data privacy modifications to the overall stability of the system

Table 3.1: Data Collection Methods

3.6. Population and Sampling

The population consisted of Kenyan IT-enabled small and medium sized enterprises who make use of their IT systems to collect, process and store customer data. The researcher selected three SMEs to use for the case study as they are representative of the typical IT-enabled SME in Kenya. The researcher used random nonprobability sampling method used for this study, making use specifically of purposive and convenience-based nonprobability sampling.

Takaful Insurance of Africa is a company that provides insurance coverage services to a wide selection of customers, and are regulated by the Insurance Regulatory Authority. The collection of customer data is crucial to the delivery of their business products. The researcher interviewed four respondents until saturation was reached.

Janice Medical & Cancer Hospital is a medical facility that provides general medical services, as well as cancer specialist services. The collection of customer health data is crucial to the delivery of their business products. The researcher interviewed three respondents until saturation was reached.

Urban Kreative Limited is a digital solutions company that provides different digital and web solutions to clients over the web and physically. The collection of customer data was helpful to the delivery of their business products. The researcher interviewed three respondents until saturation was reached.

3.7. Data Analysis and Presentation Methods

Interpretive analysis method was used to analyze the data collected in this research. The interpretive analysis method constituted three key stages: deconstruction, interpretation and reconstruction (Sargeant, 2012). The deconstruction stage was conducted by carefully reading the survey and interview responses and breaking the data into categories through data coding that described the content. The interpretation stage involved purposefully looking for similarities and differences among data categories. The reconstruction stage involved contextualizing the findings within existing theories, evidence and practices.

3.8. Validity Testing

Validity defines the accuracy of a measurement by checking how well the result agrees with established theory and other measures of the same concept (Middleton, 2019). It is distinguishably different from reliability, which is purely a measure of consistency of results. This study adopted criterion validity methodology to benchmark data collected to existing data that is generally accepted as a valid measure.

3.9. Ethical Considerations

The research adopted key ethical considerations in conduction of the study. The first consideration was the clear communication of the research purpose to all respondents participating in the study. The second consideration was the acquisition of data was limited to data intended for publicly access and use, and where data was personal or had any form of restricted usage, explicit consent was sought from the owners of the data. The third consideration was the processing and storage of the data was subject to ensuring no personally identifiable information (PII) was acquired, processed or stored by the researcher during the conduction of the study.

CHAPTER FOUR: RESULTS AND DISCUSSION

4.1 Introduction

This chapter provides a presentation of the data privacy impact assessment data collected, the findings with respect to each objective and discussion of the study. The study analyzed each objective separately and presented these results as well as their interpretations in this chapter. The main method of analysis was qualitative, with the results presented in narrative form.

4.2 Applicable Data Protection Regulations in Kenya

On review of various empirical literature and other material on data protection regulations in Kenya, the study found that Kenya had in place various laws for protecting private data and especially for SMEs.

4.2.1 National Intelligence Service Act (2012)

This Act, No. 28 of 2012, which according to Omwenga (2019) states that in the case of a person accused of committing an offence, the right to privacy may be restricted. The privacy of a person's communications may be subject to investigation, monitoring, or other types of interference by the NIS. The Section further specifies that the Service must acquire a warrant before conducting any action. The act states that an officer of the Service has the authority to obtain any information, material, record, document, or thing in order to enter any location or gain access to anything, search for, remove, or return the information, material, record, document, or thing, or to examine, take notes from, make copies of, or otherwise record the information, material, record, document, or thing. The officer is able to install, maintain, or remove anything, as well as monitor communication.

4.2.2 Consumer Protection Act (2012)

This Act, No. 46 of 2012, calls for the disclosure of information about internet contracts. Before a consumer joins into an online arrangement, the provider must provide the customer with the required information. It is critical for the customer to understand the terms and conditions as well as how his or her personal data is handled. Before entering into the agreement, the provider must give the customer an express chance to accept or refuse it, as well as to remedy any mistakes. According to this regulation "*The discloser shall be accessible and available in a manner that ensures*".

The Consumer Protection Act of Kenya (2012) also guarantees the confidentiality of information obtained when exercising a power or performing a duty relevant to the administration of this Act. The person wielding the authority is not compelled to testify. It requires the provider to disclose information to the customer, and the information given to the consumer must be clear, complete, and in line with the Standards Act. Access to the data held by a data controller is necessary in order to determine how much information is released and the methods used to obtain it.

4.2.3 Computer Misuse and Cybercrimes Act (2018)

This Act, No. 5 of 2018, addresses the objectives, which include ensuring the availability, confidentiality, and integrity of computer systems, data , and programs. This includes rules that provide that a service provider is not responsible under this Act or any other law for disclosing any data or other information that the service provider reveals solely to the extent authorized by this Act. This safeguards the user's data further in that the service provider cannot divulge all of the data linked to a specific user that is not given under the Act.

4.2.4 Data Protection Bill (2018)

The 12th Parliament of Kenya drafted this Bill of 2018, which had many similar principles and guiding regulations to the European Union's GDPR. This proposed law was introduced in a Miscellaneous Amendments Act, and sought to put in a framework that allowed the Government of Kenya to establish a single source of truth of personal data on its citizens and residents. The justification for this process included the use of this tool as a national security asset that will enable the tracking down of terror suspects. The bill however was not unambiguous on the manner through which the government collects data in order to minimize data mishandling or targeted profiling by investigators. Privacy is a vital component of Kenya's Constitution; hence, adequate data protection laws must be implemented in order to hold data collectors of any kind liable for abuse of data acquired.

The Bill introduced data protection requirements that mandated how data must be handled in order to respect the privacy rights of data subjects. In addition, data should be treated lawfully, fairly, and transparently in regard to any data subject. It is gathered for clear, valid, and particular purposes and isn't processed further in a way that defeats those goals. According to the proposed legislation, the data must be sufficient, relevant, restricted to what is required for

processing, accurate, and, where necessary, maintained up to date. Inaccurate personal data must also be deleted or corrected without undue delay. Additionally, it must be made sure that personal information on data subjects is not kept longer than required or disclosed to a third party.

4.2.5 Data Protection Act (2019)

Onunda (2019) posed that Kenya, inspired by the General Data Protection Regulation (GDPR) developments, the worldwide standard for data protection, has embraced many of the guiding concepts and enacted the Data Protection Act (2019), which replicates the GDPR rules and principles (Coleman, 2019). The enactment of the Data Protection Act (2019) enabled the immediate protection of consumer data. The Data Protection Act took into considerations some of the concerns raised in the Data Protection Bill (2018), and provided guidance and limitations on how data can be collected, processed, stored and disposed.

The Government of Kenya introduced the National Integrated Identity Management System (NIIMS) digital population register in a bid to establish a centralized single source of truth containing personal data on all citizens and residents of Kenya. This registration process popularly became known as the Huduma Namba. The Government of Kenya aimed to obtain personal metadata, including biometrics, digital images and even genealogical information. This registration process garnered the attention of legal experts and civil society organizations who challenged the process on several grounds, among them being inadequate frameworks to guarantee data privacy and protection. The petition was brought before the High Court in Nairobi, which gave a landmark ruling stating among other things, the legal framework on data privacy was inadequate and totally wanting (Privacy International, 2020) and that the Government of Kenya hasn't appreciated the application of the Data Protection Act with respect to collection and processing of data under the National Integrated Identity Management System (Kenya Human Rights Commission, 2021). This ruling saw the first significant application of this Act in determining a petition with regards to data privacy.

4.2.6 Data Protection (General) Regulations (2021)

The enactment of the Data Protection Act (2019) brought to light the varied interpretations of the provisions in the Act. There was thus the immediate potential risk of misunderstanding of the Act by data processors as the Data Protection Act became enforceable immediately upon its enactment, unlike the European Union's GDPR which only became enforceable two years

after its adoption. The study established that this prompted the Data Commissioner to issue guidelines and regulations on the correct interpretations of the elements of the Data Protection Act, which is the Data Protection (General) Regulations of 2021.

4.2.7 Miscellaneous Regulations

The study also established that the Access to Information Act, the Banking Act, the Capital Markets Act, the Credit Reference Bureau Regulations, the Kenya Information and Communications Act (KICA), the Public Archives and Documentation Service Act, the Private Security Regulation Act, and the Elections (Technology) Regulations, 2017 are among the others. These regulations, in conjunction with professional ethics and judicial rulings, govern aspects of data processing in certain circumstances.

It was found that confidentiality provisions in the Banking Act, Credit Reference Bureau Regulations, and Capital Markets Act protect personal financial information. Laws requiring data release, such as the Access to Information Act and the Public Archives and Documentation Service Act, provide measures for protecting personal information. These include the anonymization of data, the suppression of sensitive personal information, and the concealing of the individual in issue. Intercepting messages is a violation of the Kenya Information and Communications Act. The Private Security Regulation Act prevents data gathered during building entrance from being utilized for other purposes. The Elections Act's ICT Regulations ensure the security of biometric data acquired during elections.

The study found that they do not, however, encompass all instances of data processing in our current environment. An example, individuals who utilize online platforms to access internet services, such as Facebook and Twitter, are not subject to data protection licensing terms under KICA. Although, these regulations are intended to ensure data protection, they had created policy concerns due to lack of framework to guide them. The main issue was that the government digitization effort lacked adequate policy or legal foundation. In the lack of a policy and legal framework outlining the reasons for which the data acquired may be used, the government gathers vast quantities of personal data. This information is already stored by third parties and used to validate identification papers. In other words, it has the ability to improve the efficiency with which individuals get services. However, this must be done in accordance with principles that safeguard and promote rights, highlighting the need of addressing fairness in data processing.

Long-term challenges in the data economy, such as internet access and strengthening Kenya's capability for the new economy, need state action. While big private organizations may already practice data protection and have the capacity to implement new standards once a data protection framework is in place, this may not be the case for IT-enabled SMEs. Interventions are thus necessary to guarantee that SMEs strengthen their capacity to advocate the highest levels of data protection.

4.3 Data protection compliance risks impacting Kenyan IT-enabled SMEs

4.3.1 Risk of Non-Uniform Application of Standards Guiding Data Privacy

Despite various data protection legislations in place, there are challenges in enforcing compliance. Kenya, like many other African nations, has limited data protection laws, and its constitution made no mention of the protection of private data. Without a comprehensive data protection framework, it is left to entities that collect personal data to use internal data protection measures. Failure to gather and use data appropriately exposes the entity to dangers such as identity theft, misuse of personal information, unlawful dissemination or sale of data, financial loss, and privacy erosion. Previous legislative initiatives to create a data protection law have likewise failed since they were not introduced in Assembly.

4.3.2 Risk of Violation of Human Rights

This is exposing IT-enabled SMEs to data protection compliance risk. The respondents indicated that The Kenyan legal system falls far short of protecting individual privacy rights and personal information rights, which holds that all human beings are born free and equal in dignity and rights. Lack of protection for these rights has resulted in a rise in cybercrime and other associated crimes that violate persons' privacy rights. This is due to the introduction of computers and the development of new telecommunications technology that is linked to the internet, which has increased the importance of information and enhanced the gathering and use of personal information.

According to literature reviewed and the respondents, although there is a necessity to safeguard human life, government monitoring has had a significant impact on private rights.

The government can access individuals' opinions based on their conversations through monitoring. It has the potential to be used for targeting people who spread negative information about the government. Coercion and blackmail might also result from this. Citizens may be discouraged from expressing themselves freely as a result of this, curtailing the democratic rights to free speech.

Terrorism warrants communication eavesdropping because of the harm it presents to people's lives. Mass monitoring has been justified in jurisdictions such as the United States on the grounds that it is the most effective means of averting terrorist attacks (Boussios, 2017). The Prevention of Terrorism Act only applies to communication channels. It does not safeguard against the interception of one's online activity or electrical equipment such as a computer.

The respondents also showed that totalitarianism, which results from a lack of adequate checks and balances, can allow for unrestricted surveillance, which may easily lead to exposure of personal data. This then foregoes privacy in exchange for security. According to the investigation, data protection is not identical with the right to privacy, but it is a developing right that has emerged in order to promote the right to privacy in the age of big data. Governments are infiltrating digital areas in order to obtain personal information, leading to intrusion of the citizen’s private lives.

The responses showed that the right to data protection is not explicitly stated in the Kenyan Constitution, but it does derive from Article, which prohibits needless disclosure or collection of one's personal information. This relates to the control and transfer of personal data, which is a key component of the right to data protection. However, existing legislation does not sufficiently secure data. The statutes that allow the government to intrude on people's privacy are excessively broad and do not fulfil constitutional requirements. They are deficient in terms of disclosure and judicial monitoring. The government is not required to reveal the type of monitoring or interception under judicial scrutiny. It just needs that the monitoring be directed at a specific individual. Judicial review is restricted to the first phase, not the process by which personal information unrelated to national security may be obtained while gathering pertinent data. The right to be forgotten is not adequately protected by either the existing law or the proposed legislation. Under clause 9 of the Data Protection Bill, the right to request the deletion of personal information that is inaccurate has been greatly expanded to include personal

information that is no longer required by the person who collected it, where consent has been withdrawn, and where the data was processed unlawfully.

4.3.3 Risk of Commercial and Reputational Loss to Businesses

Most of the respondents indicated that the most prevalent risk was information assets being illegally accessed. This was conducted either by people internal or external to the organization, for purposes other than why it was collected, either for profiteering in criminal activity or use of intellectual capital for other purposes. This unprecedented potential for cybercriminals has resulted in previously unheard-of patterns or behaviors that have had a significant impact on individuals, governments, and businesses (Qasim, 2010). They showed most business operations have been disrupted, leaving reputations in shambles and incurring additional costs such as identifying and correcting the situation, public relations costs to repair the damage done to reputation, and high legal costs, resulting in business closure, job losses, economic shrinkage, and instability.

The respondents indicated that majority of SMEs had weak data protection measures in place. In general, cybersecurity attacks towards SMEs had been on the rise with 43% of cyber-attacks worldwide targeting small businesses with majority being unprepared to deal with cyber-attacks. As Incidents of information breaches were increasingly being reported in various reports, it had led all countries worldwide to adopt new technologies or mechanisms to deter cybercriminals. They also had been a need to come up with reforms on information technology policy through the creation of new regulatory and legal frameworks to deal with this new form of criminal activity in cyberspace.

According to published research, data breaches have increased dramatically, exposing Kenyan SMEs with IT capabilities to threats including fraud, defamation, cyberbullying, and cyberattacks. Incidences of hacking have also been seen to be increasing. The protection of personal data has been jeopardized as the number of data breaches has grown. Inadequate legal frameworks generally result in ineffective data breach enforcement measures (Kinyanjui, 2018). The Kenyan Constitution guarantees the right to privacy, and the legislature is responsible for enacting legislation to provide complete data protection.

4.3.4 Risk of Non-Compliance to Standards

The study showed that only very few (7) firms were certified by KEBS in regards to information security management system (ISMS) which reflects the number of SMEs who have taken security policy implementation and compliance seriously. It is possible to examine the responses to organizational policies and tactics. The respondents said that they may have implemented data protection measures but it was not always linked to the organizational strategies and policies. When it comes to SMEs, organizational policy and compliance in terms of fulfilling external and legal standards is an area that requires attention and regular updating.

It was found that the problems that SMEs encounter appear to necessitate a more proactive effort on the part of both organizations and the government in terms of raising knowledge of data protection procedures and regulations. Proactive approaches include organizations improving governance in terms of strategies that use metrics to analyze data security risks within the organization, updating IT-enabled SME policies to include legal or regulatory requirements, and continuous training and education of personnel on cybersecurity issues and the implementation of security best practices within the organization.

4.3.5 Risk of Legal Exposure

The Communications Authority of Kenya has been accused of enabling direct access to private communications, according to the study's finding. This had enabled the Government of Kenya to perform mass monitoring on Kenyans. The right to privacy is obviously violated by bulk surveillance (Watt, 2017). Additionally, social media and internet service providers have been accused of engaging in extensive monitoring. Direct access to private communications provides a government unlimited authority, resulting in a violation of the fundamental foundations of the right to privacy.

4.4 Information security frameworks that are relevant to data privacy impact assessment

The most common security framework was found to include the; ISO/IEC Standard security frameworks, Control Objectives for Information and Related Technologies (COBIT), Committee of Sponsoring Organizations (COSO), Confidentiality, Integrity & Availability (CIA) Triad for Information Security, and Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE).

4.4.1 Common Principles in Data Privacy Risk Impact Assessment Frameworks

Various Data Privacy Impact Assessment frameworks have been established touching on; operations security, communications security as well system development, acquisition, and maintenance. Onunda (2019) indicated that the ISO 27002 Control 12 and ISO 27001 address operational security. Under the supervision of the Data Protection Officer or the Organization's information security adviser, well-defined and documented processes with responsibilities are assigned and made available to all involved personnel. Change management with any changes impacting information security in an organization, business processes, information processing facilities, application software, and systems are all covered by operation security. Capacity management in conjunction with system performance monitoring in terms of resource use.

Separation of the development, testing, and operational environments to reduce unauthorized access to or modification of the operating environment. Malware detection and prevention, as well as awareness training. Backup information, software, and system images on a regular basis in accordance with a defined comprehensive backup policy. The backup procedure is automated and takes place at a separate location from where the original data is kept.

It was found that security of communication largely affects the management and flow of information. Network security controls, network services security, and network service segregation that entails network security to ensure confidentiality of the information systems and applications, and to preserve availability of them and their integrity. Usually, this is assigned to the Network Manager and helps to define security procedures, standards and needs. Networks should be monitored continually to identify threats, tested for recovery and specified and enhanced security processes. Policies and procedures for information transmission should be explicitly established in order to secure all communication routes, and agreements should be created if third parties are involved. An organization utilizing electronic communications should identify, document, and regularly update confidentiality and non-disclosure agreements as part of its protective measures.

Meanwhile Information systems security requirements was found to include:

- Analysis and definition of information security needs,
- Security of service applications and protection from fraud, illegal divulgation, alteration and contracts in public networks,

- Protection from incomplete transmissions and misrouting, illegal communication and change of message of its application services,
- Security of information for development and support processes involves: Secure development policies are established and implemented.
- System change control processes, platform-based technical application review that can influence key business-critical applications
- Control of software package modifications and restriction
- Implementing, documenting, maintaining and applying the safe principles of system engineering.
- Create and secure system development and integration development environment
- Oversight and monitoring of the organization's outsourced system development.
- System security tests are performed to validate the safety functionality.
- Establishment of tests on system acceptability and new information system criteria or modifications to the existing versions.

4.4.2 ISO 27000 Series Framework

The ISO 27001:2013 provided an information security management standard that gave a framework for how businesses should mitigate risk associated with information security threats. This security management standard enabled organizations to protect their data assets from loss or unauthorized access (ISO, 2014). BSI (2005) indicated that if an organization is compliant with ISO/IEC 27001:2005, certain levels of compliance for each of the organizations can be guaranteed: access control, communication and operating management, compliance, incident safety management, business continuity management, information security policy, information security safety organization, asset management, physical and environmental management. It outlines how to apply the ISO/IEC 27001:2005 standard.

ISO/IEC 27005:2008, an internationally recognized standard for information security risk management, specifies a risk management process that includes creating the context, risk acceptance, assessment, communication, monitoring, treatment, and review (BSI, 2008). The procedure adheres to the PDCA paradigm and necessitates knowledge of the ISO/IEC 27001 and ISO/IEC 27002 standards. According to Singh and Lilja (2009), the standard is incapable of prioritizing controls and measuring the effect of security upgrades.

4.4.3 COBIT Framework

ITGI (2007) states the assurances of the COBIT framework; IT is business aligned; IT allows business and maximizes advantages; IT resources are used sensitively and IT risks are effectively handled. The COBIT framework allows managers to bridge the gap between needs for monitoring, the technological issues and operational hazards. COBIT is a framework for IT governance and a toolkit that helps managers bridge the gap between needs for control, technological problems and business dangers. The development of COBIT policy might include significant cooperation with the departments of Finance and Audit. (Rhodes-Ousley, 2013). In four corporate areas, the COBIT framework specifies 34 high-level control goals. This classification contains 318 detailed management objectives that address information requirements and resources. A quality control component that deals with quality, cost and delivery. fiduciary management components for effectiveness, efficiency, information reliability, and compliance; and security management components for confidentiality, integrity, and availability.

4.4.4 OCTAVE Framework

Assets, risks, and vulnerabilities are only a few of the risk components that the OCTAVE risk management approach considers (Alberts & Dorofee, 2001). It is a security framework for assessing risk levels and designing cyber-attack defenses. This framework describes techniques to help organizations minimize exposure to potential threats, determine the likely impact of attacks, and respond to successful attacks. OCTAVE is intended to capitalize on the knowledge and skills of individuals inside the company. The first stage is to create threat profiles based on the relative danger that they offer. The procedure continues with an organization-specific vulnerability assessment. OCTAVE is a complete approach to assess, analyze and apply internal organizational resources to evaluate and analyze threat/technology risk, using information technology and asset type (Storms, 2003).

Many studies on OCTAVE as a risk management technology on the security of information show the advantages of the use of that technology in many companies, independent of the technical capabilities of staff (Panda, 2009). One of OCTAVE's key benefits is its participation and its autonomy (Panda, 2009). OCTAVE generates an organization-wide perspective of current information security threats, giving a snapshot in time, or a baseline, on which to focus mitigation and improvement efforts (Alberts, Dorofee, Stevens & Woody, 2003). During OCTAVE, the team identifies and analyses the organizational information security risk to determine priorities and remediation plans by developing protection strategies for

organizational remediation and risk mitigation plans to reduce risk to critical organizational assets. The OCTAVE approach for Risk Management is autonomous since it encourages individuals in the same organization to work together to establish the Security Strategy of the organization (Tiwari, 2010). a finding that this study accomplished. OCTAVE method variations provide an organization with a variety of risk management approaches appropriate to an organization based on its information systems in size and layering (Panda, 2009)

4.5 Open-source DPIA frameworks for SMEs in Kenya

While this research suggests for OCTAVE-s framework for IT-enabled SMEs, Alberts and Dorofee (2002) and (Sosonkin, 2005) argue in favor of the organization's catalogue of practices, threat profile and catalogue of vulnerabilities through the implementation of the small risk management method of OCTAVE. These catalogues can serve as references for IT-enabled SMEs that choose to do risk management information security training with basic computer expertise people. OCTAVE-S features the same three phases: Build Asset-Based Threat Profiles, Identify Infrastructure Vulnerabilities, and Remediate Vulnerabilities. Organizational information is discovered and used to construct threat profiles for three to five important information-related assets during the asset-based threat profile development process. This includes gathering organizational data and developing threat profiles.

The Study Team identifies the organization's significant information-related assets, creates a set of impact evaluation criteria, and describes the present status of the organization's security policies when recognizing organizational information. The Analytics Team picks three to five essential information-related assets for creating threat profiles and specifies safety standards and threat profiles for these assets. They then examine the organization’s infrastructure and technological processes in order to improve the threat profiles, in order to discover infrastructure weaknesses. In this context, the Analytics Team analyses the access path in systems supporting the critical assets and assesses how well their technology-based procedures safeguard these assets in connection to key assets. When developing security strategies and plans, threats to significant assets are examined, and measures for risk mitigation and organizational protection are devised. The analysis team analyses all active hazards for effect and, optionally, likelihood in order to identify and evaluate risks. The team generates an organization-wide protection strategy and risk mitigation plans based on security practices, and

in such scenario, the team creates an organization-wide protection strategy and risk mitigation plans.

This research will take use of OCTAVE-small's versatility which can be tailored to meet the particular information systems risk settings, security, objectives, and skill levels available in the IT-enabled SMEs (Moyo, 2014). The Analytics Team picks three to five important information-related assets and specifies the security needs and threat profiles for those assets while creating threat profiles.

In order to fine-tune the threat profiles, the Analytics team performs a high-level examination of their infrastructure and technological processes when they find infrastructure flaws. In order to assess how successfully their technology-related policies are protecting these assets, the Analytics Team examines the computing infrastructure in relation to important assets, examines the access paths in the systems that support those assets, and so on. In this study, the OCTAVE-small approach will be utilized to pinpoint crucial organizational data, pinpoint threats to vital IT assets, pinpoint infrastructure vulnerabilities, pinpoint risks, and create mitigation and security strategies for IT-enabled SMEs. By doing this, research objectives will be met while also improving the risk management exercise for the workforce and making it more enjoyable.

OCTAVE provides a snapshot in time (baseline) that may be utilized to concentrate mitigation and enhancement actions by giving an organization-wide picture of current information security threats. Identifying an organization's information security risks, analyzing and prioritizing risks, and planning improvements through the development of organizational improvement protection strategies and risk mitigation plans to reduce risks to the organization's critical assets are all activities performed by the analytics team during OCTAVE. (Alberts, Dorofee, Stevens, Woody, 2003).

4.6 Discussion

The study established there have been changes in data protection regulations in Kenya, which are directly applicable to Kenyan IT-enabled SMEs. These regulations give guidance on the collection, processing, storage and purging of data, highlighting the roles and responsibilities of data processors, and also enumerating the rights and privileges accorded to data subjects.

The Data Protection Act was established to be enforceable immediately on its enactment, thus subjecting the Kenyan IT-enabled SMEs to potential risks from failure to comply with the new regulations. With this in mind, the study sought to establish data privacy impact assessment frameworks that are used to assess and mitigate potential data privacy risk. The study established several frameworks in place including the OCTAVE framework, The ISMS Family of Standards (ISO 27000 series) ISO 27005:2018 framework, and the NIST framework.

The basic principles observed with these frameworks included:

i. Definition of the data processing operation and its context. This stage identified the data being processed, the classification of the data, the purpose for which it is intended for, the technical means of processing the data, the physical location of the data processing, the categories of data subjects that provide data and the recipients of the data.
ii. Understanding and evaluating impact. This stage evaluated the potential impact to the data processor and data subjects that a potential security incident may result in. This involves using a qualitative approach to gain understanding of the organization's data processing operation. For the purpose of conducting this assessment by SMEs, the following needs to be considered: type of personal data, the criticality of the processing operation, the special characteristics of the data processor, and finally the special characteristics of the data subjects.
iii. Definition of possible threats and probability of their likelihood. This stage identified possible threats related to the overall data processing both internally and externally, and assess their probability of occurrence. This stage involved conducting a threat occurrence probability with expected results ranging from four (4) to twelve (12).
iv. Evaluation of risk. This stage was the final stage and involved establishing the final risk level is derived, guiding the SME what their risk exposure is, and they can now focus on mitigating potential risk at the highlighted areas.

The study established the OCTAVE-S variant of the OCTAVE framework as most appropriate for application by Kenyan IT-enabled SMEs to conduct their data privacy impact assessment as this framework was designed to analyze risk in SMEs. OCTAVE proved to be particularly viable as it considers the "People" as an asset in evaluation of information system risks. This framework also focuses on risk evaluation of information systems, and has formal procedures for risk acceptance. The adoption of this framework allows the SMEs to commence in

identifying their risk exposure with regards to data privacy, and as they grow in their capacity, they can then take on other frameworks more suited for larger, more structured, organizations such as the ISO 27005:2018.

The choice of this framework can be compared with researchers who conducted similar studies in trying to establish assessment frameworks with regard to data privacy. The first research highlighted is *the Guidelines for SMEs on the security of personal data processing* by the European Union Agency for Network and Information Security (ENISA, 2016). This guideline in the context of SMEs operating in Europe. This guideline proposes following the ISO/IEC 27000 family of standards, specifically the 27001:2013 standard. The study notes that the ISO 27000 family of standards is designed at organizations that are more mature, and also notes that the European Union's GDPR regulations only became enforceable two years after its adoption. This time frame allowed the EU-based SMEs to familiarize themselves with the provisions of the regulations, and have enough time to set themselves up to comply with regulations at the time of it becoming enforceable.

The study also further highlights the research conducted by Stephanus in *Implementation OCTAVE-S and ISO 27001 Controls in Risk Management Information Systems* (Stephanus, 2014). This research was conducted in Jakarta, the researcher concludes that by use of OCTAVE-S, a company can be able to map the risks and weaknesses of their information systems, they then can evaluate the scale of impact of the risks, threats and weaknesses identified, and thus establish their risk exposure level.

CHAPTER FIVE: CONCLUSION

5.1 Introduction

The research conducted sought answers the research questions and observed the following results:

5.1.1 Data Privacy Regulatory Changes Applicable to Kenyan IT-Enabled SMEs

The study found that the Government of Kenya has in place legislation on data protection and privacy which covers access, correction, the right to seek confirmation, update, rectify, and object to processing, as well as data portability. The enacted regulations however were found to have some limitations, such as unambiguity on constraints that are imposed on data

controllers. The ambiguous clauses have direct impact on Kenyan IT-enabled SMEs, such as being silent on constraints imposed on data controllers on collection and retention of data collected from these SMEs.

The study found that the primary risk is generally ensuring adequate compliance in privacy protection and its balance with national security. Personal information cannot be adequately protected in Kenya by data protection laws from both government and non-government organizations. The Data Protection Act (2019) and Data Protection (General) Guidelines regulations are very broad in terms of limits based on national security, and they allow the government unrestricted discretion when collecting personal data through surveillance. The study showed the existing danger of government surveillance, in which the government may acquire, store and erase personal data unrelated to national security or the commission of a crime. Although there are legal and constitutional arguments for restricting the right to privacy, the investigation concluded that there are some murky areas in its actual application. It concludes that the surveillance framework is inadequate. The study finds that data protection is an emerging right that has arisen to support the right to privacy in the big data era, not one that matches the right to privacy. The Kenyan Constitution does not specifically include the right to data protection, but it does result from the Article that forbids the gratuitous disclosure of or collecting of personal information. This has to do with the management and dissemination of personal data, which is essential to the right to data protection. Data security is, however, insufficient under current law.

5.1.2 Risk Exposure to Non-Compliant Kenyan IT-Enabled SMEs

The Data Commissioner issued the Data Protection (General) Guidelines (2021) in order to clarify the clauses contained in the Data Protection Act (2019), in order to limit the risk of ambiguous interpretation of the clauses. The Guidelines and the Act documents serve an important role for SMEs as prior to this, it was left to the SMEs to set and use their internally defined data protection measures. This approach led to failure to collect, process, store and dispose of data appropriately, leaving the IT-enabled SMEs to potential risks including identity theft, misuse of personal information, unlawful access, modification and dissemination of data, financial loss, privacy erosion and decreased customer trust. These regulations have brought to light the rights of a data subject, bringing in concepts such as data privacy awareness, data collection consent, transparency in the collection, processing and storage of data, and the ability of data subjects to request for their collected data to be purged amongst others.

5.1.3 Existing Frameworks to Assess Impact of Data Privacy Risks

The study identified several existing data privacy impact assessment frameworks. The three most popular frameworks that were referenced by researchers and technical experts included the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) framework, The ISMS Family of Standards (ISO 27000 series) ISO 27005:2018 framework, the National Institute of Standards and Technology (NIST) framework.

Other existing frameworks that the study found to be somewhat relevant to data privacy impact assessment included the Control Objectives for Information and Related Technologies (COBIT) framework, the Committee of Sponsoring Organizations (COSO) framework, and the Confidentiality, Integrity & Availability (CIA) Triad for Information Security.

5.1.4 Data Privacy Impact Assessment Framework best suited for Kenyan IT-Enabled SMEs

The study also found that in the face of dynamically changing IT environment, SMEs are turning to open source business solutions to run their systems. The study indicates that Open Source Business Solutions (OSS) are a cost-effective and dependable approach that SMEs in Kenya may use. This adoption aids SMEs in increasing their return on investment and allowing them to invest in business development and competitive strategy. Senior management prefers this method of cost cutting to retrenchment and expenditure reduction since it has no negative impact on the organization's structure and is long-term sustainable. The benefits of continuing community support for OSS are numerous. Due to the flexibility of OCTAVE-small, which can be adapted to the specific information systems risk settings, security, objectives, and degree of capabilities available in the Kenyan IT-enabled SMEs, this research recommended using it. Instead of the typical three phases, the OCTAVE-small strategy used in this study will be based on four separate processes. By delivering an organizational-wide view of the most recent information security risks, OCTAVE offers a snapshot in time (baseline) that may be used to focus mitigation and improvement measures. Identifying an organization's information security risks, analyzing and prioritizing risks, and planning improvements through the development of organizational improvement protection strategies and risk mitigation plans to reduce risks to the organization's critical assets are all activities performed by the analytics team during OCTAVE.

5.1.5 Summary

The strengthening of SME-centered data privacy impact assessment and data protection frameworks is highly desirable. Firstly, the study recommends that a data protection framework be created, which includes an independent institution to supervise fair and reasonable data processing while encouraging the data economy. Transparency should be emphasized as a good practice that should be embedded in the political and regulatory framework. This framework would address how IT-enabled SMEs acquire data, as well as how to promote and defend rights by obtaining informed consent from the data subject. Furthermore, it would provide the data subject with the ability to see, access, and request rectification of their data. Individuals would be shielded from choices made only through automated procedures and alerted in the event of a data breach.

Secondly, to limit the risks associated with processing personal information, the use of this personal information must be strictly regulated, monitored and enforced. Kenya should continue to implement and strengthen its data protection laws because it will provide individuals more control over their personal. This is especially significant given Kenya's growing potential to participate and be a global solutions provider in business processing outsourcing. As government monitoring evolves, and new technologies enable spying and infringing on the right to privacy, there is a need for the law to address such issues proactively. The technology should not be abused as a means of violating people's rights. All technologies and data protection legislation that the government wants to deploy on SMEs must be clearly disclosed, easily accessible and easily understandable. The Judiciary plays an important function in protecting the right to privacy. It acts as a check and balance on the executive. This helps to avoid misuse of authority. Non-state actors, such as corporations, should have a greater role in supporting the right to privacy. They should not reveal personal information to anybody, including the government, without first obtaining consent or a court order. Corporates should also take appropriate precautions, such as using contemporary encryption, to guarantee that personal information is not easily accessible to other parties.

The study proposes the OCTAVE-s framework based proportionate regulatory framework which would ensure that IT-enabled SMEs maintains active risk management with four stages;

The first stage involves an organizational effort to establish a dedicated group for IT-enabled SMEs to identify critical information assets and develop a collection of impact requirements and current security practices for IT-enabled SMEs. Contains definitions of confidential information. The information obtained is critical to creating a resource-based risk profile.

The second stage is to identify risks to critical information system resources. Evaluating the SME aspect gives the user of the data system a view of what is involved and what he is doing to protect these resources. A risk profile is then created for each asset by the project team after identifying the safety needs for important assets. A risk profile has to be established. I have to compile data that I've already collected from several CIS users. Threat profiles were generated for each of the identified key assets. The team must determine if the indicated threat causes: altering sensitive or important information Inability to access crucial information, technology, applications, or services; deletion or deterioration of essential information.

The third stage finds infrastructure vulnerabilities. Key components of vulnerabilities (technical vulnerabilities) that can contribute to unauthorized intrusion into critical assets are identified. This is a high-level study to improve the threat profile of your infrastructure and technology practices. Perform a physical scan of your computer's hardware and components to identify vulnerabilities that threats can exploit.

The fourth stage includes risk analysis and implementation of security controls and mitigation plans. The group must define and assess all risks to the company's core assets and make decisions. Based on the information gleaned from the research, this group should develop corporate security policies and mitigation strategies to address threats to critical assets. The impact and probability of occurrence of all identified risks are qualitatively evaluated in risk analysis. The results of the assessment lead to the development of organizational security policies and risk mitigation plans based on security practices.

5.3 Limitations of the Study

The researcher encountered the following limitations in the conduction of the research:-

i. This research may not be fully representative of all enterprises within SMEs. The research did not consider very small SMEs, with little to no knowledge of basic IT skills or infrastructure.

ii. The research is biased towards SMEs who use local IT infrastructure for collection, processing and storage of their data. The researcher notes there are SMEs who may use a third-party service provider whom these recommendations may not be applicable to.

5.4 Recommendation for further research

There are limitations to open-source adoption in SMEs, including the capacity of business users to cope with open source technology and escalation assistance, as open source is mostly supported by the community. Because the study focused solely on It-base SMEs, the impact is restricted to businesses having SMEs characteristics. Future study should be carried out to see if these findings hold true in large and public businesses.

REFERENCES

Alberts, C., Dorofee, A., Stevens, J. & Woody, C. (2003). Introduction to the OCTAVE Approach. Carnegie Mellon University. https://www.itgovernance.co.uk/files/Octave.pdf

Alberts, C. J. & Dorofee, A. (2002). *Managing information security risks: The OCTAVE SM approach. Addison-Wesley Anderson*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.461.7807&rep=rep1&type=pdf.

Alberts, C. J. & Dorofee, A. (2004). *Using Vulnerability Assessment Tools to Develop an OCTAVE Risk Profile*. Carnegie Mellon University. http://www.fish.com/satan/admin-guide-to-cracking.html.

Ali, B., and Awad, A.I. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors. 18. 817. 10.3390/s18030817.

Alshammari, M., Simpson, A. (2018): Personal data management: an abstract personal data lifecycle model. In: Teniente, E., Weidlich, M. (eds.) BPM 2017. LNBIP, vol. 308, pp. 685–697. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-74030-0_55

Blakley, B., McDermott, E., and Geer D. (2002). Information Security is Information Risk Management, ACM Digital Library.

Boussios , E. (2017). The Right to Privacy? - The Debate over the United States Government's Control over its Cyberspace. Athens Journal of Law, 2017, 222

Brodin, M. (2019). A Framework for GDPR Compliance for Small-and-Medium Sized Enterprises. *European Journal for Security Research.* https://doi.org/10.1007/s41125-019-00042-z.

Capital Markets Authority (CMA), Kenya National Bureau of Statistics KNBS (2020). SMEs Corporate Governance Survey Report: An Assessment of Level of Corporate Governance in SMEs. *Capital Markets Authority Research Papers*. Available at: https://www.cma.or.ke/index.php?option=com_phocadownload&view=category&download=554:cma-knbs-smes-corporate-governance-survey-report-april-2020&id=59:research-papers&Itemid=256

Caralli, R.A., Stevens, J.F., Young, L.R., Wilson,W.R. (2007) Introducing Octave Allegro: *Improving the Information Security Risk Assessment Process*; Technical Report CMU/SEI-2007-TR-012, ESC-TR-2007-012; Software Engineering Institute: Pittsburgh, PA, USA, 2007.

Cheng, L., Liu, F., and Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211.

Chin, R. W. K. (2012). A Security Control Framework for Consumerization of Mobile Devices in the Bank Sector.

Coleman, D. (2019). Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of data protection laws, Michigan Journal of Race and Law, 24(431).

DESA, United Nations (2020). Digital Government in the Decade of Action for Sustainable Development. *E-Government Survey 2020*. Available at: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

Duricu, A. (2019). Data Protection Impact Assessment (DPIA) and Risk Assessment in the context of the General Data Protection Regulation. Lulea University of Technology

Ernst & Young (2019). Is Cybersecurity More Than Protection. *EY Global Information Security Survey 2018-19*. Available at: https://assets.ey.com/content/dam/ey-sites/ey-

com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf. Date Accessed: 15-08-2021

European Union Agency for Network and Information Security (ENISA, 2016). Guidelines for SMEs on the security of personal data processing. DOI 10.2824/867415

Friedewald, M., Bieker, F., Hansen, M., Obersteller, H. and Rost, M. (2016). A Process for Data Protection Impact Assessment under the European General Data Protection Regulation. DOI 10.1007/978-3-319-44760-5.

Freitas, M. C. and Mira da Silva, M. (2018). GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management*, 3(4), 30. https://doi.org/10.20897/jisem/3941

Government of Kenya (2019). The Data Protection Act. *Kenya Gazette Supplement No. 181 (Acts No. 24)*. Retrieved from: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No 24of2019.pdf . Date accessed: 09-08-2020

Hallova, M., Polakovic, P., Silerova, E. and Slovakova, I. (2019). Data Protection and Security in SMEs under Enterprise Infrastructure, *AGRIS on-line Papers in Economics and Informatics*, Vol. 11, No. 1, pp. 27-33. ISSN 1804-1930. DOI 10.7160/aol.2019.110103.

IBM Security (2019). *Cost of a Data Breach Report 2019*. Available at: https://www.ibm.com/downloads/cas/RDEQK07R . Date accessed: 08-09-2020

Information technology, Security techniques, ISMS, Overview and vocabulary, International Organization for Standardization Norm, ISO/IEC 27000:2014.

IT Governance Institute (2007) COBIT 4.1. Rolling Meadows, IL: IT Governance Institute.

Kenya Human Rights Commission (2021). *Consortium Applauds Court Judgement Declaring Huduma Cards Illegal; Calls for Further Reforms*. Available at:

https://www.khrc.or.ke/2015-03-04-10-37-01/press-releases/754-consortium-applauds-court-judgement-declaring-huduma-cards-illegal-calls-for-further-reforms.html . Date accessed: 15-12-2021

Kenya ICT Action Network (KICTANet) (2018). *Data Protection in Kenya, Policy Brief*. Available at: https://www.kictanet.or.ke/download/data-protection-in-kenya/ . Date accessed: 16-08-2020

Kinyanjui A. W.. (2018). Data protection as a human right: balancing the right to privacy and national security in Kenya (University of Nairobi)

Liu, L., Han, M., Wang, Y., and Zhou, Y. (2018, June). Understanding data breach: A visualization aspect. In *International Conference on Wireless Algorithms, Systems, and Applications* (pp. 883-892). Springer, Cham.

MacroSec (2020). *Elements of a Data Protection Impact Assessment Under The Kenya Data Protection Act, 2019*. Available at: https://macrosec.tech/index.php/2020/01/17/elements-of-a-data-protection-impact-assessment-under-the-kenya-data-protection-act-2019/ . Date accessed: 24-02-2020

National Institute Standards and Technology (2020). NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management. Available at: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf . Date accessed: 19-08-2020

NetApp (2020). *NIST Data Privacy Framework: A Quick and Easy Introduction to the NIST Framework*. Available at: https://cloud.netapp.com/blog/ccs-blg-nist-data-privacy-framework-an-introduction . Date accessed: 07-05-2020

Ochieng, J. and Mbedi, M. (2019). What the Data Protection Act, 2019 Means for You. *Oraro & Company Advocates*. Available at: https://www.oraro.co.ke/2019/11/13/what-the-data-protection-act-2019-means-for-you/. Accessed on: 10th Sep 2020

Oetzel, M., and Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: A design science approach. *European Journal of Information Systems*. DOI: 10.1057/ejis.2013.18.

O'Harrow, R. (2004). No Place to Hide The Digital Person: Technology and Privacy In The Information Age (2004)

Omwenga, M. E (2019). Privacy and data protection in the digital age (Bachelor Dissertation, Jomo Kenyatta University Of Agriculture & Technology, Juja, Kenya)

Onunda, V. A. (2019). Small and Medium Enterprises and the 2019 Data Protection Act in Kenya: A Cybersecurity View (Bachelor's thesis, Tallinn University).

Qasimi, Z. K. S. A. S. L. A. (2010) Cyber Law and Cyber Security in Developing and Emerging Economies. Northampton, MA: Edward Elgar

Privacy International (2020). *Kenyan Court Ruling on Huduma Namba Identity System: the Good, the Bad and the Lessons*. Available at: https://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons. Date accessed: 21-05-2020

Pyka, M., and Sobieski, S. (2012). Implementation of the OCTAVE Methodology in Security Risk Management Process for Business Resources. *Internet - Technical Developments and Applications 2*. DOI: 10.1007/978-3-642-25355-3_21.

Rhodes-Ousley, M. (2013). Information Security. (McGraw-Hill, Ed.) (Second Edi). New York Chicago San Francisco Lisbon London Madrid Mexico City Milan New Delhi San Juan Seoul Singapore Sydney Tonronto. http://doi.org/10.15713/ins.mmj

Saunders, M., Lewis, P. & Thornhill, A. (2012) "Research Methods for Business Students" 6th edition, Pearson Education Limited

Sargeant J. (2012). Qualitative Research Part II: Participants, Analysis, and Quality Assurance. Journal of graduate medical education, 4(1), 1–3. https://doi.org/10.4300/JGME-D-11-00307.1

Schwab, K. (2016). The Fourth Industrial Revolution. *World Economic Forum*. Geneva Switzerland.

Shields, Patricia and Rangarajan, N. 2013. A Playbook for Research Methods: Integrating Conceptual Frameworks and Project Management. Stillwater, OK: New Forums Press. See Chapter 4 for an in-depth discussion of descriptive research.

Stephanus. 2014. Implementation OCTAVE-S and ISO 27001 Controls in Risk Management Information Systems. Information Systems Department, Binus University. Available at: https://journal.binus.ac.id/index.php/comtech/article/download/2225/1645&usg=AOvVaw1nXgCApFa2cNy_I1ujNez3 . Date accessed: 14-09-2020

Storms, A. 2003. Using vulnerability assessment tools to develop an OCTAVE risk profile, viewed 12 May 2012, from http://www.sans.org/reading_room

Turban, E., Outland, J., King, D., Lee, J., Liang, T., Turban, D. (2018). Electronic Commerce 2018: A Managerial and Social Networks Perspective. Ninth Edition. Springer International Publishing AG. Cham, Switzerland

UNCTAD, United Nations (2020). *Summary of Adoption of E-Commerce Legislation Worldwide*. Available at: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx . Date accessed: 16-08-2020

UNCTAD, United Nations (2019). Digital Economy Report 2019: *Value Creation and Capture - Implications for Developing Countries*. United Nations Publications, New York, United States of America

Wangen G., Hallstensen C., and Snekkenes E. (2018). A framework for estimating information security risk assessment method completeness, *Core Unified Risk Framework, CURF*, Springer, pp. 681-699

Watt, E. (2017). The Right to Privacy and the Future of Mass Surveillance. International Journal of Human Rights, 2017, 774

Xu, M., David, J.M., Kim, S.H. (2018). The Fourth Industrial Revolution: Opportunities and Challenges. *International Journal of Financial Research*. Vol. 9, No. 2; 2018 doi:10.5430/ijfr.v9n2p90

APPENDICES

APPENDIX 1 – AUTHORITY LETTER

ROBERT WAFULA
P.O. Box 173 - 00200
Nairobi, Kenya
12 April 2021

The CHIEF EXECUTIVE OFFICER,
TAKAFUL INSURANCE of AFRICA
P.O. Box 1811 – 00100
Nairobi, Kenya

Dear Sir/Madam,

RE: AUTHORITY TO CONDUCT AN ACADEMIC RESEARCH IN YOUR ORGANIZATION

I am a Master's student at the University of Nairobi, School of Computing, doing an academic research on Data Privacy Impact Assessment among IT-enabled SMEs in Kenya. I am drawn to your organization for two main reasons. Firstly, your organization is a leading medium-size business with clients spanning across different parts of the country and different walks of life. Secondly, your organization has embraced information technology in your service delivery and has become a core mode of service to your clients.

I hereby request availability of your IT Manager, Database Administrator and Lead Developer for the purpose of answering the attached questionnaire. The information collected shall be strictly confidential and anonymized, and a copy of the research shall be availed to your organization. Your support in this research will be greatly appreciated.

Yours truly,
Robert Wafula

APPENDIX 2 – DATA PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

This research is purely for academic purposes and is meant to get your opinion on data privacy impact assessment. 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

A. General Information

1. What type of organization do you work in?
   ( ) Public Sector
   ( ) Financial Services Sector
   ( ) Telecommunication Sector
   ( ) Academia Sector
   ( ) Health Sector
   ( ) Insurance Sector
   ( ) Other
   if Other, please describe _____

2. How concerned is your organization about data privacy?
   ( ) Extremely concerned
   ( ) Very concerned
   ( ) Moderately concerned
   ( ) Slightly concerned
   ( ) Not concerned
   ( ) I don't know

3. How many customers does your organization have?
   ( ) 0 – 50
   ( ) 51 – 100
   ( ) 101 – 500
   ( ) 501 – 2,000
   ( ) Over 2,000

4. How does your organization store confidential information (e.g. customer names, customer phone numbers, customer addresses) ?
   ( ) Electronic records
   ( ) Paper records
   ( ) Both

( ) I don't know

B. Data Policy Information

5. What is your level of understanding of the Data Protection Act, 2019?
   ( ) Extremely knowledgeable
   ( ) Very knowledgeable
   ( ) Moderately knowledgeable
   ( ) Slightly knowledgeable
   ( ) I don't know

6. Does your organization have a well-documented ***data protection and privacy*** policy?
   ( ) Yes
   ( ) No
   ( ) I don't know

7. If your answer is Yes in question 5, do you have access to your organization's ***data protection and privacy*** policy?
   ( ) Yes
   ( ) No
   ( ) I don't know

8. If your answer is Yes in question 5, how often is your organization's ***data protection and privacy*** policy reviewed ?
   ( ) More than once a year
   ( ) Once a year
   ( ) Once every 2 years
   ( ) Less than once every 2 years
   ( ) I don't know

9. Does your organization have a well-documented ***data access*** policy?
   ( ) Yes
   ( ) No
   ( ) I don't know

10. If your answer is Yes in question 8, do you have access to your organization's ***data access*** policy?
    ( ) Yes
    ( ) No
    ( ) I don't know

11. If your answer is Yes in question 8, how often is your organization's ***data access*** policy reviewed ?
    ( ) More than once a year
    ( ) Once a year
    ( ) Once every 2 years
    ( ) Less than once every 2 years
    ( ) I don't know

12. Does your organization have a well-documented ***data destruction*** policy?
    ( ) Yes
    ( ) No
    ( ) I don't know

13. If your answer is Yes in question 8, do you have access to your organization's ***data destruction*** policy?
    ( ) Yes
    ( ) No
    ( ) I don't know

14. If your answer is Yes in question 8, how often is your organization's ***data destruction*** policy reviewed ?
    ( ) More than once a year
    ( ) Once a year
    ( ) Once every 2 years
    ( ) Less than once every 2 years
    ( ) I don't know

C. Business Processes Information

15. Who conducts data privacy impact ***assessment*** in your organization?
    ( ) Internal assessment officer/team as their primary role
    ( ) Internal assessment officer/team as their secondary role
    ( ) External auditors
    ( ) Independent third-party expert
    ( ) I have never conducted a data privacy impact assessment
    ( ) I don't know

16. Who conducts ***training*** on data privacy in your organization?
    ( ) Internal training officer/team as their primary role

( ) Internal training officer/team as their secondary role
( ) Independent third-party expert
( ) I have never conducted a data privacy training
( ) I don't know

17. How often does your organization conduct data privacy training?
( ) More than once a year
( ) Once a year
( ) Once every 2 years
( ) Less than once every 2 years
( ) I don't know

18. Where does your organization's primary confidential information reside?
( ) On-site data storage
( ) Outsourced to off-site data storage
( ) Both
( ) I don't know

19. Where does your organization's backup confidential information reside?
( ) On-site data storage
( ) Outsourced to off-site data storage
( ) Both
( ) I don't know
( ) I don't have a backup

20. If you selected **Outsourced to off-site data storage** in either question 17 or 18, how does your organization monitor data privacy risks at outsourced service providers?

Tick all that apply	YES	NO
20.1. Our organization has an outsourcing policy that addresses data privacy risks	( )	( )
20.2. Our organization annually assess outsourced service providers	( )	( )
20.3. Our organization limits data access to outsourced service providers	( )	( )
20.4. Our organization vets outsourced service providers staff who handle the organization's data		

( ) ( )

21. Ticking either Yes or No, please assess if your organization has ever identified any issues with data privacy control. If you don't know, you can leave the respective question unticked

	YES	NO
21.1. My organization has identified data privacy issues	( )	( )
21.2. My organization has addressed all its data privacy issues	( )	( )

22. If you have further information that you believe would be useful, please document it below without divulging any confidential information.

C. Your Profile Information

23. Job Title:

APPENDIX 3 – LIST OF SMEs INTERVIEWED

The following SMEs were interviewed for this study.

1. Takaful Insurance of Africa
2. Janice Medical & Cancer Hospital
3. Urban Kreative Limited