UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

RESEARCH TOPIC:

A STRATEGY TO REDUCE IT RISKS IN TECHNOLOGY-BASED SMALL AND MEDIUM-SIZED ENTERPRISES

BY

ELIUD KIBET CHOGE

A PROJECT REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT OF THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT OF THE UNIVERSITY OF NAIROBI

AUGUST 2020

DECLARATION

I declare that this research project report is my original work and has not been presented for any award in any other university.

Signed: …… Date: ……

Eliud Kibet Choge

P54/11583/2018

SUPERVISOR'S DECLARATION

This project report has been approved for presentation for the award of the degree of Master of Science in Information Technology Management of the University of Nairobi, by me as the University Supervisor.

Signed: ……..…… Date: ……

Prof. Elisha Toyne Opiyo

ACKNOWLEDGEMENT

I want to give my sincere appreciation to my supervisor for the guidance, suggestions, and corrections that you gave me in all the steps I took in coming up with this project report. Your insightful thoughts were much appreciated and helpful. I am also grateful to the school administration for its continued support in terms of provision of resources. The school enabled me to be in a good environment where working was simple and easy. Also, through the provision of library resources and a conducive environment, it was convenient to do my research with a lot of interest and peace. All the friends, colleagues and fellow classmates who contributed to the success of my work stand to be pillars in the whole journey. May God truly bless you and provide for you in all your endeavors.

DEDICATION

I wish to dedicate this research project to my beloved family who have supported me during this project. May the Almighty bless and be with them.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

SMEs – Small and Medium-sized Enterprises

GDP – Gross Domestic Product

ICT – Information and Communication Technology

IT – Information Technology

IS – Information Security

PwC-UK – PricewaterhouseCoopers United Kingdom

RMF – Risk Management Framework

FAIR – Factor Analysis of Information Risk

NIST – National Institute of Standards and Technology

COBIT – Control Objectives for Information and Related Technologies

ITIL – Information Technology Infrastructure Library

KRI – Key Risk Indicators

SPSS – Statistical Packages for Social Sciences

LIST OF TABLES

LIST OF FIGURES

Definition of Key Terms

ICT/ IT: The unification of communications or integration of telecommunication channels such as internet, software, wireless networks, and audiovisual systems for the transmission and manipulation of information.

ICT Risks: Refers to any crisis such as software failure, virus infections or malicious attacks resulting from the use of ICT equipment.

ICT Risk Reduction: The application of proper risk management strategies to mitigate occurrence during operation.

ICT Risk Reduction Strategy: Refers to a preferable means of dealing with or managing any likely ICT risks.

ABSTRACT

SMEs in Kenya contribute greatly to the country's growing economy. However, they face numerous challenges in sustaining their growth. A number of these SMEs are Technology-based, having technology and computing at the center of their operations and performance. Hence, they face myriads of risks, throwing them into the drawing board to seek ways of managing such IT risks in their operations. The purpose of this paper is to identify a comprehensive risk management strategy, which will help in the mitigation of potential IT risks in technology-based SMEs. This would involve determining the key IT risks faced by the SMEs and recommending the implementation of proper IT risk assessment and management methodologies. The study used a descriptive research design, with a target population of 120 employees from Compulynx Limited, 15 employees from Conquest Capital and 5 employees from Faculty Solutions. From the expected respondents, only 80 participated fully in the study causing a response rate of 87%. The method of data collection included the use of questionnaires. The data analysis was done using SPSS with descriptive statistics and other inferential statistics. From the data analysis, the researcher concluded that technology-based SMEs are implementing risk reduction as the most comprehensive way of mitigating the risks, which they are exposed to. The companies employ strongly valid risk management practices in protecting businesses against risks.

Chapter 1: Introduction

1.1 Background

The SMEs in Kenya, which are the greatest contributors to the growing Kenyan economy, face numerous challenges that impede their growth; hence, a domino effect on the revenue earned from such establishments. A conducted economic survey by the government of Kenya revealed that 75% of the businesses operating in the country are SMEs, which contributes to 18.4% of the total GDP and 87% of the employers' population in Kenya (Mutwiri, 2018). The establishments are critical due to the creation of employment opportunities, especially for the youth who miss the few formal employment opportunities. Given the height of the contribution made by the firms, it is evident that modern economic progression in the country is wholly dependent on the success of the small enterprises, which form the focal point of every operation.

While the firms bear the potential to perform better, challenges such as constrained markets, administration issues, restricted access to information beneficial for improvement, and problems with implementing innovations impede full capacity performance. One of the key areas considered by various leadership in a bid to improve the current performance is the adoption of technology for various production purposes including sales and marketing to ensure that the firms compete favorably in the currently e-commercialized markets (Migiro, 2006; Wamuyu & Maharaj, 2011; Chale & Mbamba, 2015). Besides this, the adoption streamlines the processes to ensure uniformity in the acquired product.

Performance of Technology-Based SMEs

The adoption of technology for use in the production processes of many industries depends much on the financial affordability and the level of adaptability of staff to ascertain a higher-level service delivery. 84.3% of the SMEs use manual technology, with only a small 5.7% having

adopted computerized technology. Further, 10% using intermediate technology are often ready to shift to higher-level computerized technology provided the availability of resources (Gathogo & Ragui, 2014).

When comparing the height of performance of individual firms concerning the technology adoption, firms operating in a computerized environment seemed to experience entrepreneurial burnout at a later year than others did. Their continued operations and excitement arose from the new opportunities inspired by continued innovation. The firms comprised the entire 8.5% population of SMEs that considered their businesses as highly successful (Gathogo & Ragui, 2014).

Besides those mentioned above, the adoption of technology has equally been instrumental in boosting the quality of products sold by the companies while also enjoying the higher rates of production. The use of computerized technology further enables cost-cutting due to the lean workforce employed in managing the affairs of the company effectively. In 55.7% of the organizations, technology adoption improved the profitability values by more than 30%; hence, serving as an indication that when applied effectively, its use is effective for firm improvement and, by extension, economic development.

Challenges Experienced by the Technology-Based SMEs in Kenya

While adopting technology to better the process of production seems like a grand idea, it comes with numerous challenges the organization must handle in a bid to ascertain the eventual success of the transition. Some of the experienced challenges include the rapidly changing technology that will require the firm to ensure a continued upgrade of its systems for better performance; the increasing level of information insecurity due to the heightened techniques of illegal data access; the lacking human capital to implement and monitor the use of the acquired techniques in

production accordingly, and the risk caused by glitches and insufficient backup likely to tamper with the expected output. The challenges bear the potential of impeding the process of production much more than the anticipated improvement in performance and other anticipated benefits (Xia, 2009). Further, the heightened standards and the enacted legislations to oversee the implementation and use of certain technology in the firm, the lacking customer response, and the infrastructure of the business are other issues that could contribute greatly to the impediments to business performance.

Risk Management in IT-based Organizations

The contemporary world economy currently is under fundamental structural changes due to globalization in business and the volatility witnessed in the field of information and communication-based technology (Dutta & McCrohan, 2002). The interaction of the two characteristics causes the evolution of complex business structures dictated by the availability of high-level technology for the process of production. The intensive but lean application of ICT frameworks improves the performance of the organization to the point of competition with the larger enterprises in terms of the revenue and profitability (Bodin, Gordon, & Loeb, 2008). Despite the many opportunities available for growth, numerous risks arise due to the continued use of technology by the firms. First, the growing use of technology predisposes many firms to cybercrimes as third parties are using various mechanisms to gain the information they would like for malicious use. Secondly, the likely loss of data, mismanagement due to lacking human capital, and identity theft are some of the identifiable risks likely to impede the functioning of the technology-based SMEs.

1.2 Statement of the Problem

With the increasing use of technology in various production processes, various organizations suffer the risk of cybercrime and other forms of related ICT risks that impede proper functioning and the achievement of firm objectives. When taking the example of the technology-based SMEs in Kenya, many seem too dependent on e-commerce, especially for the newly founded that use it as a means to market their produce, which exposes them to the heightened insecurity in the worldwide network. While the number of institutions grow due to the continued innovation and inventions of process improvement techniques, almost half of those firms already in business suffer because of the failure of machines or the dangers of third party access.

By 2018, 62% of the companies worldwide were likely to experience cybersecurity attacks. One notable case manifesting the intensity of IT security include the case of Adobe in 2013, where personal information of about 7.5M of the Adobe Creative Cloud users were exposed to the public while Yahoo!'s unprecedented incident of breach in September 2016 affected close to 500M consumers of the products (Thielman, 2017; Morris, 2013). In the first half of 2019, more than 4.1B records of personal information was exposed as a result of cybercrimes such as hacking. Such occurrences are detrimental to the business, as customers become more worried about the safety of their personal data than the quality of services they could receive. For this reason, it is essential to identify an important means by which the arising issue should be corrected through proposed risk management techniques.

1.3 Research Purpose

The purpose is to determine a strategy for mitigating IT risks in the technology-based SMEs while investigating the role of risk assessment, risk identification and risk management on risk reduction in institutions.

1.4 Objectives

1.4.1 General Objective

To determine a comprehensive strategy for use in mitigating IT risks in the technology-based SMEs.

1.4.2 Specific Objectives

i. To determine the influence of IT risk identification on the reduction of IT risks

ii. To determine the influence of IT risk assessment on the reduction of IT risks

iii. To determine the influence of IT risk management on the reduction of IT risks

1.5 Research Questions

The research questions for use in the study are dependent upon the objectives defined above. The four research questions are as follows.

RQ1. Is there a comprehensive strategy for use in mitigating IT risks in the technology-based SMEs?

RQ2. What are the key IT risks faced by SMEs in Kenya using and developing technology-based solutions?

RQ3. What are the commendable and most applicable IT Risk Assessment and IT Risk Management best practices/ methodologies that will improve the situation in the SMEs today?

RQ4. Are there any strategies in place to reduce IT Risks in technology-based SMEs?

1.6 Significance of the Research

The research identifies a better ICT risk management framework that will help in managing the risk faced by the technology-based SMEs in the contemporary business environment. The

research is beneficial in introducing an improved service delivery framework addressing the important variables in ICT risk management frameworks for the IT managers. Besides this, it will also benefit the academic fraternity by enabling them to have a much better understanding and the underlying significance of risk control in the service industry. The information presented will be of help to the researchers by developing a better and more improved service delivery framework hence adding value in terms of knowledge.

1.7 Expected Contributions of the Study

1.7.1 Expected Outcomes

i. The propositions for better ICT risk assessment and management strategies beneficial for improving the situation on the ground

ii. A recommendation for the adoption of a risk management framework basing on properties such as adaptability and effectiveness

1.7.2 Expected Impact

i. The recommendations made from the research will inform policy formulation and decision-making strategies to ascertain the mitigation of potential threats and an improvement in the risk assessment frameworks adopted by various organizations

1.8 Scope of the Study

The type of risks an organization becomes exposed to is dependent on factors such as operational frameworks and the level of technology applied in the production processes. Further, the risk is also likely in cases where the team members in the relevant departments are unaware of the details regarding the operationalization of the adopted risk management frameworks in the firm. The existing risks bear different extremes of harm; hence, treated at different degrees. The study,

however, will be limited to the aspect of risk management frameworks that are currently employed in taming some of the potential ICT threats.

1.9 Delimitations of the Research

Some of the limitations existing for the research include the limited resources in terms of financial capability to conduct the research effectively. While there are millions of employees in the industry, the study only chose 150, which may not be statistically representative. With a higher financial base, it would be reasonable to use a higher sample size to ensure the validity and reliability of the obtained conclusion. Secondly, the inadequate time allocated for the study may make it difficult to gain the expected respondents since they are employees also working on other matters. The respondents also may not give accurate information due to the sensitivity of the type of information the study will be collecting. Although certain that the information is for research, some of the employees may not trust the researcher enough to reveal the framework in use out of fear of exposure to non-users.

1.10 Research Outline

Chapter 1 focuses on putting the research in order by identifying its purpose, significance, scope, and limitations associated with the research. When basing on the information provided in the background study, there is much information revealing just how much the ICT environment has become risky for small organizations, which hopes to use better infrastructure to boost sales and improve the quality of their production. Chapter 2 is the literature review and the conceptual framework giving details about the ICT risks and frameworks for the risk reduction strategies. Chapter 3 comprises the research methods used in the research, the data collection tools, and the considered ethical considerations for the research. Chapter 4 consists of the results obtained from conducting the analysis of the collected data and a discussion of the results. Chapter 5 looks into

the limitations of the research, the conclusion, and the recommendations made following the results and the discussion in relation to the topic of study.

Chapter 2: Literature Review

2.1 ICT Related Risks

The changing corporate environment requiring a reliable use and interpretation of business information causes many firms to realign their processes to suit the current dynamic business environment. The adoption and use of lean techniques aim to raise the companies' comparative advantage by ascertaining high-level profitability and improved efficiency. While boosting the capability to improve their customer services through fast and reliable business transactions, the adoption of the ICT applications introduces probable downfall through financial risk, operational risks, and technological risks (Bodin, Gordon, & Loeb, 2008).

ICT risks refer to any potential threats to the business operations arising from the use, ownership, operation, or involvement with any of the IT infrastructure within the company. Some of the likely identifiable risks include the likelihood of under or overprovisioning for the system, network issues and outages, hardware incompatibility, downtime, vendor reliability, migration issues, disaster recovery, and security breaches (Ahmad, Maynard, & Park, 2014). The risks are likely sources of unexpected costs likely to thwart the growth or expected improvement in the business performance.

While it is in the interest of various organizations to shield themselves from the adverse effects resulting from the risks, many fail due to the incapability to realize the underlying connection between the need for cooperation between the operational and management level activities in identifying and mitigating the risks (Dutta & McCrohan, 2002). Such a collaboration improves the decision-making processes that inspire the management policies and strategy implementation to ensure the achievement of a secure working environment.

2.2 ICT Risk Management

Upon the identification of the capability of the risks to occur, the IT based organizations must consider the establishment of worthwhile risk management practices for better operationalization of the company procedures. According to Speklé et al. 2007, ICT risk reduction strategies form part of the internal control and auditing that limits managerial risks within an organization. In emphasizing the managerial risks, the firm can support its requirement and governance issues through advanced policies, processes, systems, and skill collaboration to mitigate any likely negative effects. In forming part of the internal control, there is a chance of better security through the provision of guidance on risk management to other staff within the organization. Besides this, it gives independent assurance of adequacy and efficiency of the risk control practices to the management (Pickett & Pickett, 2005).

Because of the enormous role played in polishing output to achieve the company's objectives, ICT risk management should be the responsibility of the high-ranking management with expertise in providing strategy and strategic direction (Buckby, Best, & Stewart, 2005; Kumsuprom, Corbitt, & Pittayachawan, 2008). One of the key responsibilities in managing such risks is ascertaining information security through developed frameworks to increase the predictability of such incidences while establishing a firm and effective foundation for process improvement.

Given that many of the technology-based SMEs in Kenya consider e-commerce as the main approach to the exchange of goods and services, cybercrime becomes a common risk the companies must overcome. In a survey conducted by PwC-UK in 2015, 74% of the reported cases were from the small and medium enterprises and were targets due to their underdeveloped infrastructure that provided leeway for most of the attackers (Bougaardt & Kyobe, 2011; PwC-

UK, 2015). The lacking human capital and sufficient financial resources make the adoption of full-scale prevention quite impossible. The government of Kenya has put in regulations regarding corporate risk management that requires the institutions to establish a program that includes identification, assessment, measuring and reporting, and proper guidelines on mitigation to improve security and the possibility of proper risk management (RISHAD, 2019). Employing cost-effective and technologically sufficient policies is one sure way of mitigating the likely negative experiences resulting from insecurity.

2.3 Frameworks and Methodologies for ICT Risks

2.3.1 Risk Management Frameworks

According to Bougaardt & Kyobe, in 2011, the primary approach to ensuring proper ICT risk management is establishing properly structured approaches regarding Information Security (IS) and ICT governance. while information security focuses on prohibiting third party access to company data, ICT governance facilitates a top-down methodology to perform the evaluation and minimizing of potential threats (RISHAD, 2019).

A risk management framework defines a structured process necessary for identifying possible dangers to the organization and to define strategies for eliminating or curtailing the impact of the risks for effective monitoring and evaluation (Jones, 2007). The risk management frameworks preferred in employing ICT governance are as discussed below.

2.3.1.1 Factor Analysis of Information Risk (FAIR) Framework

FAIR is a taxonomy concerned with evaluating risks based on how they can affect each other. It attempts to establish accurate probabilities of the occurrence of potential threats and the magnitude of the losses the company is likely to incur. In practice, the FAIR approach can strengthen working procedures; hence, no need to replace the system in operation.

The capability to perform the complementary roles betters the achievement of the goals by bringing in process improvement (OpenGroup, 2010). Due to this, the company incurs less cost in terms of skilled human capital and investment in a completely different infrastructure. While the approach is cost-effective and friendly to the employees due to the need for an only limited appraisal, the approach can fail in the absence of compatibility and a failed definition of the improvement the company should make.

2.3.1.2 NIST Risk Management Framework

The recently developed NIST framework, which comprises the framework profile, the core, and the implementation tiers, functions to improve the critical infrastructure necessary for ascertaining cybersecurity for IT-based companies (Enocson & Söderholm, 2018). The framework is considered advantageous due to its cost-effectiveness in implementation and the lacking limitation to the size of an organization; hence, the applicability in handling the challenges experienced in the SMEs (RISHAD, 2019). Further, the flexibility in operationalization makes it attractive for both established and young businesses by promoting the institution of mature cybersecurity programs.

The NIST framework consists of five basic modules identified the Identify, Protect, Detect module, respond module, and the recover module. The first module Identifies functions to develop an understanding of how the organization can conduct internal management of the likely occurrence of cybersecurity risks. The second, which is the protected module, relies on the assessment in the identity module to develop and implement proper security controls that are vital for the delivery of core services necessary for the infrastructure (Shen, 2014). The detect module concerns itself with reviewing the functioning system to identify the source of the occurring problem promptly for better control. Identifying the occurring anomalies and events

furthers the detection process that provides a sufficient backdrop for the functioning of the responding module.

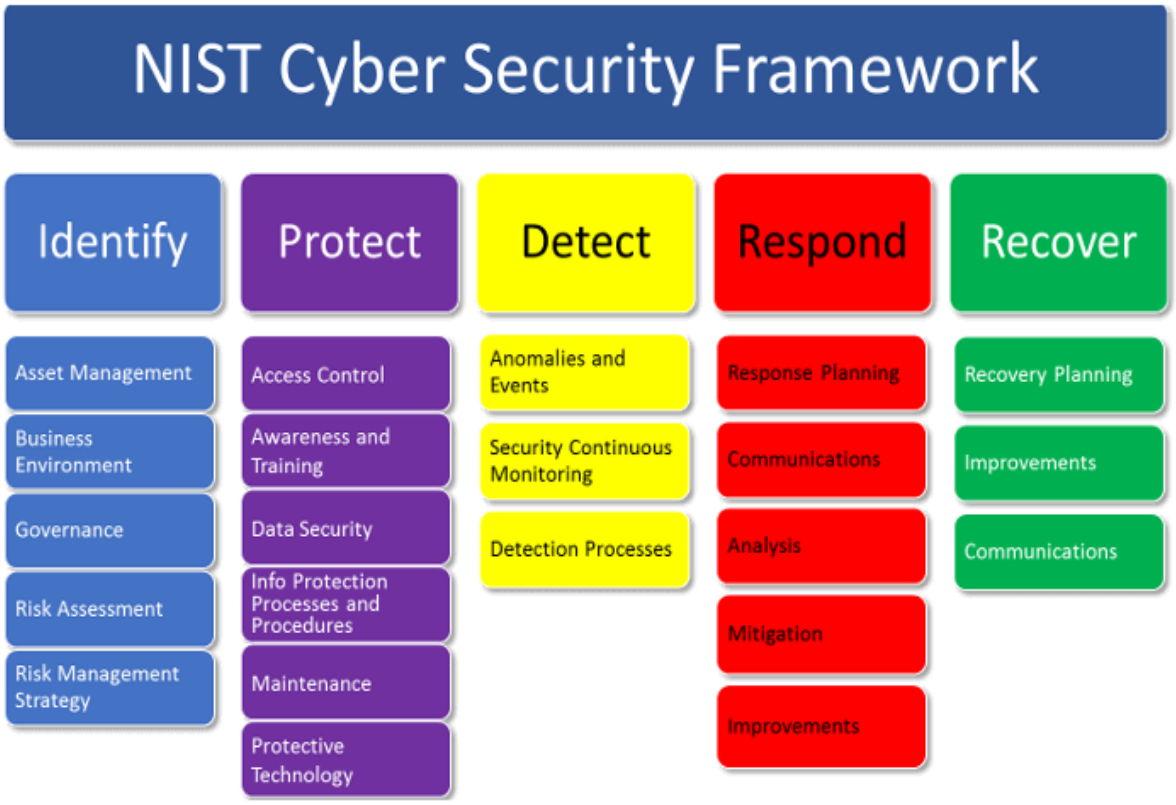

Figure 1: NIST Cybersecurity Framework

At the response stage, various processes, which include response planning, communication, analysis, mitigation, and suggestion of improvement to the process, occur to ascertain that the observed challenge is nipped at the root (Shen, 2014). Once done, the recovery module monitors the implementation process basing on the set objectives of the organization and functioning effectively to mitigate the challenge initially identified.

2.3.1.3 Control Objectives for Information and Related Technologies (COBIT) Framework

COBIT is renowned for its capability to an organized set of ICT controls that form a logical framework of various ICT related processes to enable the development of a well-defined process that allows for policy development and best practices for ICT management. Secondly, the framework also emphasizes on the need for compliance with the set regulatory procedures (Kumsuprom, Corbitt, & Pittayachawan, 2008). This allows for proper functionality in the identification and mitigation of any observed or potential risks.

In its functionality, COBIT looks into four basic domains that involve organizing and planning, acquiring and implementation, delivering and support, and monitoring. The full performance of the framework ascertains that the implementation process runs successfully from the point of ideation to the implementation and diagnostic checks for compatibility to the organization's objectives (Khther & Othman, 2013). The plan and organize domain involves the identification and usage of particular tools, evaluating its relevance, possible benefits, and the likely drawbacks basing on the potential risk. The domain enables the organization to realize early enough whether the approach to be employed is sufficiently feasible.

The second domain, acquire and implement, stems its responsibility from the perfect completion of the functions of the first domain. Upon identifying and choosing to implement a specific type of technology, the next step is to develop a maintenance plan for the systems and components. Establishing such processes provides the necessary avenue to establish the policies required to oversee the successful maintenance and functioning of the system (Ridley, Young, & Carroll, 2004). The delivery and support domain handles the management of the delivery of the services obtained from implementing the new system. The domain is important due to its capability to ascertain the eventual success of the process.

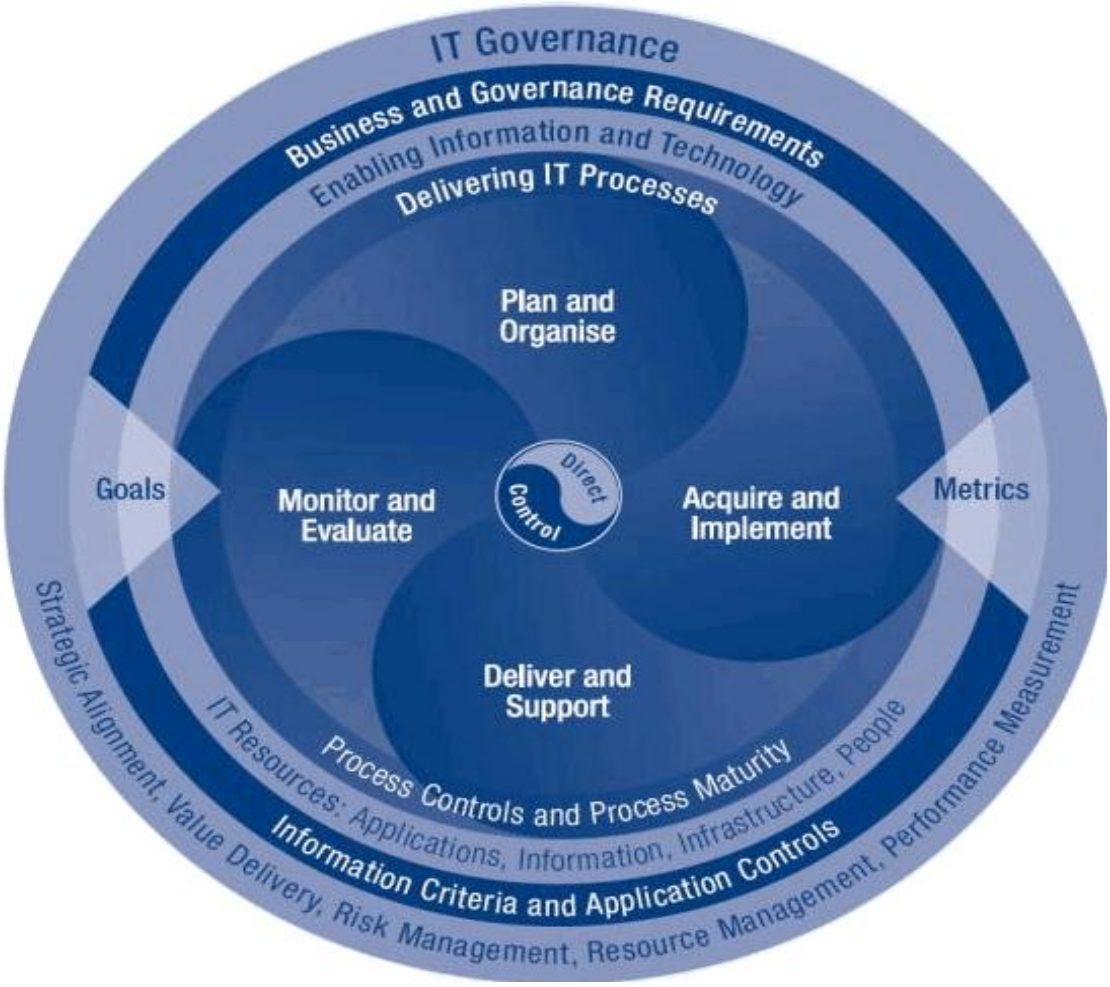

Figure 2: Components of the COBIT Cybersecurity Framework

During use, the company, through the monitor and evaluate domain, can successfully identify challenges and unforeseen drawbacks for better implementation. An assessment strategy is also necessary to check the implementation process versus the laid down procedures and other set standards to ascertain that the ICT risk management practices of the firm are highly compliant (Ridley, Young, & Carroll, 2004). Compliance will enable the firm to avoid any controversies with the regulatory authorities.

2.3.1.4 Information Technology Infrastructure Library (ITIL) Framework

ITIL functions to improve performance, especially for businesses with unique needs. The framework effectively identifies the principal elements and the necessary action points that, if implemented, will ensure the delivery of services performing beyond the minimum competency levels (Palilingan & Batmetan, 2018). While the frameworks mentioned above are technology and organization specific, ITIL offers a sort of general user approach that enables any institution to label the baseline determining the nature of implementation and measurement of system performance. Due to the nature of its operations, the framework is capable of meeting any organizational objectives irrespective of the organizational structure in place.

The framework functions in five service-oriented domains identifiable basing on design, strategy, operation, transition, and continual improvement. In the strategy service, the framework operates based on the information provided about the implementation, design, and development of the organization-specific management service. Capability, which looks into the possibility of matching the company objectives, is an essential aspect for consideration at this point. The service design comprises stipulated guidelines for the nature of services offered and the processes for service management to ensure the proper functioning of both processes (Mokhsin et al., 2018). The service transition domain is important to enable the organization to acquire new or other services that function to improve the processes within the company. The transition process ascertains that what is in place is adaptable and working towards the achievement of the set objectives.

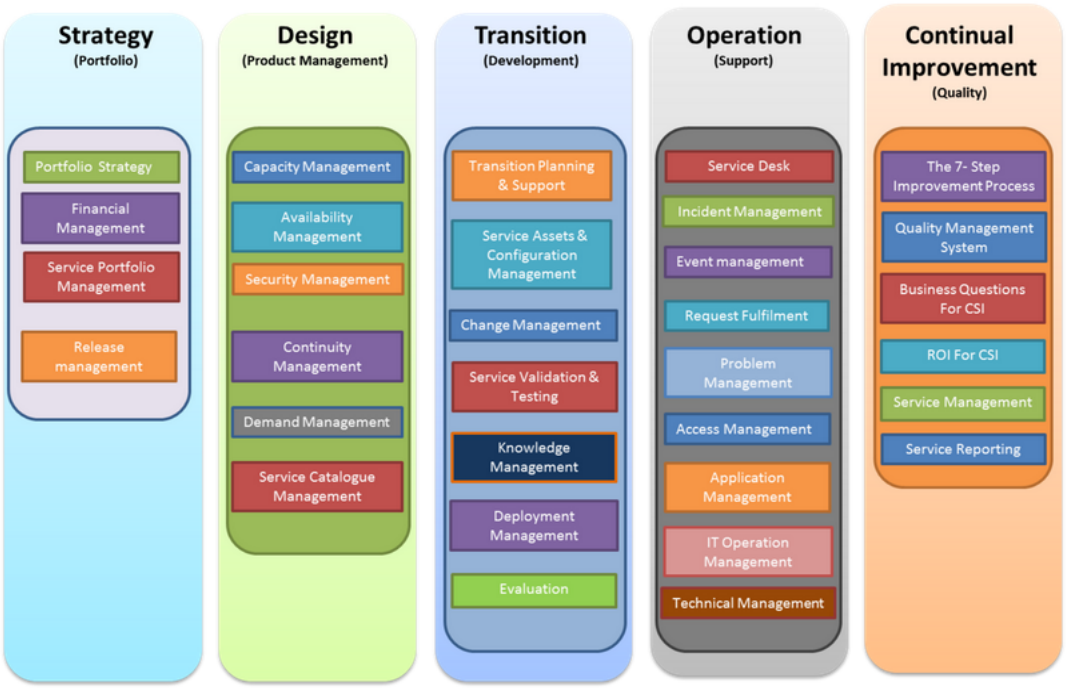

Figure 3: ITIL Framework

2.3.1.5 ISO/IEC 27001: 2013

The ISO / IEC 27001:2013 standard specifies the various criteria for the creation, implementation, maintenance and continuous development of the IS management system for organizations. In addition, it sets guidelines for evaluating and managing IS risks intended to achieve the organizational goals. The versatility of the standard allows it to be applied to various organizations, regardless of size. (Pardo, Pino, & Garcia, 2016). Despite outlining efficiently the details of what it requires of firms in operation, the standard does not define to the user how to achieve the requirements.

2.3.2 COBIT Framework in an IT-Based SME

Many IT-based companies recognize COBIT for use due to the capability to provide general guidelines relevant for managing ICT assets while also facilitating processes for effective ICT risk management. The framework in categorizing its roles basing on the domains as stated in the

previous section, coincides with the organizational processes relevant to many SMEs (Kumsuprom, Corbitt, & Pittayachawan, 2008). Some of the relevant aspects include clear allocation of duties and tasks, external persons, and the consistency in measurement practices, better processes and policies description, and improved communication, among others. In measuring the effectiveness of the COBIT framework, Solms et al. identify the capability of the framework to remain true to the objective of the process by remaining true to the instruction on what is necessary concerning information technology management (Krisanthi, Sukarsa, & Bayupati, 2014). The research further identifies the framework as having the capability to align perfectly with objectives with eventual success in business and technological control within the organization. The achievement of the two is a sure step to ascertaining process improvement and steering the development of mature ICT risk management processes.

While the framework seems effective in improving ICT governance, some of the identified drawbacks include its lacking in detail of the "how" when conducting the implementation process. Risk management, especially in an institution, should be in a systematic and technical-oriented manner for the firm to achieve every one of the objectives in place effectively. The absence of the definition of the nature of implementation distorts the uniformity of the results achieved in the end. Besides this, the ineffective application of the framework will have a significant effect on technical planning; hence, subjecting the entire process to failure.

2.3.3 COBIT vs. Other Frameworks

When considering the different risk management frameworks discussed above, many have redundant features while each lacks in one feature than the other. COBIT, for example, has its strength in the global acceptability of the standard and the capability to grow with a change in technology (White, 2019). Besides this, any organization choosing to use the system can

implement it without having to commit to a full-spectrum analysis as with other frameworks. The domains under which the system works make it easier for the user to follow through with the implementation plan to the point of success, especially because of the diagnostic checks available at every point. Other frameworks such as ITIL, ISO 27001:2013, and FAIR are equally advantageous in implementation due to the capability of the user to customize the frameworks to function according to the needs of the organization (ISO, 2019). The frameworks are efficient and economical, especially due to the limited need for human capital development in the use of FAIR and the minimal economic resource requirement for NIST. One notable disadvantage of using the NIST framework is the incapability for the user to make any modifications in an attempt to customize it for use. Other frameworks are not sufficiently wide in terms of scope, and further lack concise details on how the implementation process should occur to ascertain a successful outcome. The general nature of COBIT widens its scope of operationalization; hence, making it a preferable choice. However, the width could also serve as a detractor during implementation (Ridley, Young, & Carroll, 2004). The lacking limitation to a single area of use can cause some gaps in coverage; this could cost the organization by supplementing its use with other frameworks for effective use.

2.3.4 Proposed COBIT Risk Management Strategy

2.3.4.1 Key Risk Indicators (KRI)

A KRI refers to measures that can be used to determine how risky undertaking an activity can be. They formulate the key metrics used by the organization to quantify the increase in risk exposures in different areas of the enterprise. In implementing the COBIT framework, the key risk indicators are included, and the relevant service design discussed based on the process required for improvement in the table as shown.

Process	Potential Risk	Key Risk Indicator (Measurable)	Strategic Response	Source
Strategic management	Defining an amorphous strategy	Recorded fluctuations in customer satisfaction levels.	Defining and the documentation of better objectives using input from customers and suppliers for suitability	Market Investigation
Service portfolio management	Creating services outside the company's operating strategies resulting to no satisfaction	Recorded fluctuations in customer satisfaction levels, number of customers, and unprotected systems.	Analyze the effects on current services and the organization's development of new services and identify the resources needed to deliver the service.	Investigation
Demand Management	Incapability in identifying customer needs for specific services	Reduction in positive feedback from consumers Recorded fluctuations in customer count	Researching customer requirements (questionnaires, surveys).	Market surveys
Financial management	Inaccurate Budgeting	Variation between the actual spending and the drawn budget	Use of better forecasting techniques and enhanced priority setting	Research
Risk Management	Incapability to classify and control risks occurring during functioning	Poor decision making regarding risk management activities An increase in the identified risk gaps following losses	Improved corporate decision-making through efficient risk exposure communication across the organization; An open and supportive approach to identifying, analyzing and communicating danger and improving understanding of the cost and benefit consequences of their actions in all staff.	M_o_R (Douw & Mark , 2010).

Table 1: Table of Key Risk Indicators and Strategies for Improvement

2.3.4.2 Risk Management Improvement

The need to conduct effective ICT risk management arises from the organization's need to achieve its objectives despite the challenges faced. Given the identified key risk indicators, some of the improvement mechanisms likely to be employed in handling the risk management include continuous monitoring upon implementation, staff development, and maintenance and support

activities to ensure the system operates according to the set guidelines. In the displayed table, there are identified key strategies that, if employed, will improve the management of risk through the spotted key risk indicators.

Process	**Potential Risk**	**Key Risk Indicator (Measurable)**	**Strategic Response**	**Source**
Supplier management	Expensive but poor services No value for money	Agreed users versus available services Number of reviews of contracts per term Supplier number (in DB) with full data about them	Development of database containing supplier information for contract management while capturing every agreed information	Research
Information Management	Lack of adequate data regarding plans and policies	Incomplete designs for disaster management plans Longer time taken before implementing proposed solutions Number of gaps detected during simulations of the disaster plan.	Register and document the main business requirements. Get sponsor buy-in (Analysis and supporting documents) Create a Business Continuity Strategy Create Disaster Recovery plan and Invocation Guideline	Research
Availability Management	Systems Unavailability	Number of Denial of service attacks	Implement the minutest security yardsticks	COBIT (Wim & Steven, 2005).

Table 2: Risk Management Improvement

2.3.4.3 Risk Management Integration in COBIT

Besides risk management practices, the system must perform governance satisfactorily by identifying business assets and the threats related to them. Additionally, the identification should enable the planning, mitigation, and monitoring of the performance to ascertain that the objectives of the business are attained (Tuttle & Vandervelde, 2007). Upon implementation, various players within the business should work to ensure that the framework runs effectively to meet the required standard. Including various members of the organization in a role, especially if well trained, encourages cooperation among the staff while also improves the organizational culture of the institution. The level of technology used by the firm influences the effective running and management of the organization.

Figure 4: Risk Management Integration in the Organization

Given that upgrading the technology in use could be a challenge due to the challenges in affordability and adaptability, the use of the COBIT framework will be essential to ascertain that the firm can overcome the challenges it faces at an affordable cost (Lainhart IV, 2000). Besides

this, the capability to adapt easily to the framework will mitigate any incidences occurring due to the lacking knowledge during implementation.

2.4 Empirical Review

Abdulrahim (2017) aimed at examining major cybersecurity risks that SMEs in Kenya face in their daily operations. The research revealed that investment in cybersecurity, training and awareness creation, cybersecurity management, policies and programs on cybersecurity, vulnerability, management of incidences and realtime monitoring were key in cyber-risk management among SMEs. The study concluded that implementing strategies can provide a roadmap to assist in managing cybersecurity risks.

Makumbi, Miriti and Kahonge (2012) analysed IT security practices used SMEs in the financial sector in Kenya. The study established that the in SMEs setup, the risk posed by failure of IT security was of concern. The study further revealed that some of the attempts by SMEs to secure IT assets were largely uncoordinated. The IT security role, most of the time, was unassigned, and the staff tasked with the role lacked appropriate qualifications. Further conclusions were that most SMEs lacked formal IT security budget although some security related expenditures were made. Due to revelations of uncoordination of IT assets within SMEs, the current study sought to establish a strategy that can limit exposure of SMEs to IT risks, an enhance coordination of IT investments/assets.

Githii, Kamau, Muthoni and Maina (2014) investigated the faced risks and possible moderation strategies employed by SMEs in Kenya. The study established the existence of over fifteen different categories of risk in the Kenyan small and medium enterprises. The study recommended an investigation into the factors influencing the mitigation strategies chosen by

different firms. The current study limited its scope to IT risks, and the strategy adopted to reduce such risks across Technology based SMEs.

The current study adds to the existing gaps, contributing to reduction of IT Risks in Technology-based SMEs, through strategy. Nugroho, Susilo, Fajar and Rahmawati (2017) explored SMEs technology adoption readiness factors in Yogyakarta. The study established that IT had been adopted by companies but SMEs still dragged behind in the adoption. They added that IT contributed to competitive advantage but many factors affected SMEs' readiness to adopt information technology. The study however, did not address the aspect of mitigating risks faced as SMEs pursue competitive advantage through adoption of IT. The current study adds to the existing gaps in IT adoption by researching on a strategy to reduce it risks in technology-based SMEs

2.5 Conceptual Framework

A conceptual framework is a presentation model where one may provide a diagrammatic representation of the relationships between the study variables. As stated in the literature review, the conceptual structure of the paper focuses on defining the COBIT paradigm. The plan and organize domain covers the identification and use of a particular technology, evaluating its relevance, possible benefits, and the likely drawbacks basing on the potential risk. The domain enables the organization to realize early enough whether the approach to be employed is sufficiently feasible. In this domain, the company can establish the probable source of the risk, which can arise even from the business environment then organize strategies for implementation with the likelihood to mitigate the underlying uncertainties. Besides these, the company also conducts training and continues to create awareness about the new infrastructure in use to make it easier for the various concerned departments to adapt faster.

The second domain, acquire and implement, stems its responsibility from the perfect completion of the functions of the first domain. Upon identifying and choosing to implement a specific type of technology, the next step is to develop a maintenance plan for the systems and components. Establishing such processes provides the necessary avenue to establish the policies required to oversee the successful maintenance and functioning of the system. In this section, the company ensures limited control to limit any potential alterations to the original plan of operation.

The delivery and support domain handles the management of the delivery of the services obtained from implementing the new system. The domain is important due to its capability to ascertain the eventual success of the process. During use, the company, through the monitor and evaluate domain, can successfully identify challenges and unforeseen drawbacks for better implementation. The organization at this point places its concern more on elements such as data security, improvement in the protective technology in use, and ascertains that the human capital in use is well versed with the infrastructure in use. In so doing, the company ascertains that the implementation process is on point.

An assessment strategy is also necessary to check the implementation process versus the laid down procedures and other set standards to ascertain that the ICT risk management practices of the firm are highly compliant. Compliance will enable the firm to avoid any controversies with the regulatory authorities. The monitoring and evaluation process enables the company to realize any events and anomalies that could arise with the continued operation. Besides these, continued analysis allows for the implementation of mitigation strategies for process improvement.

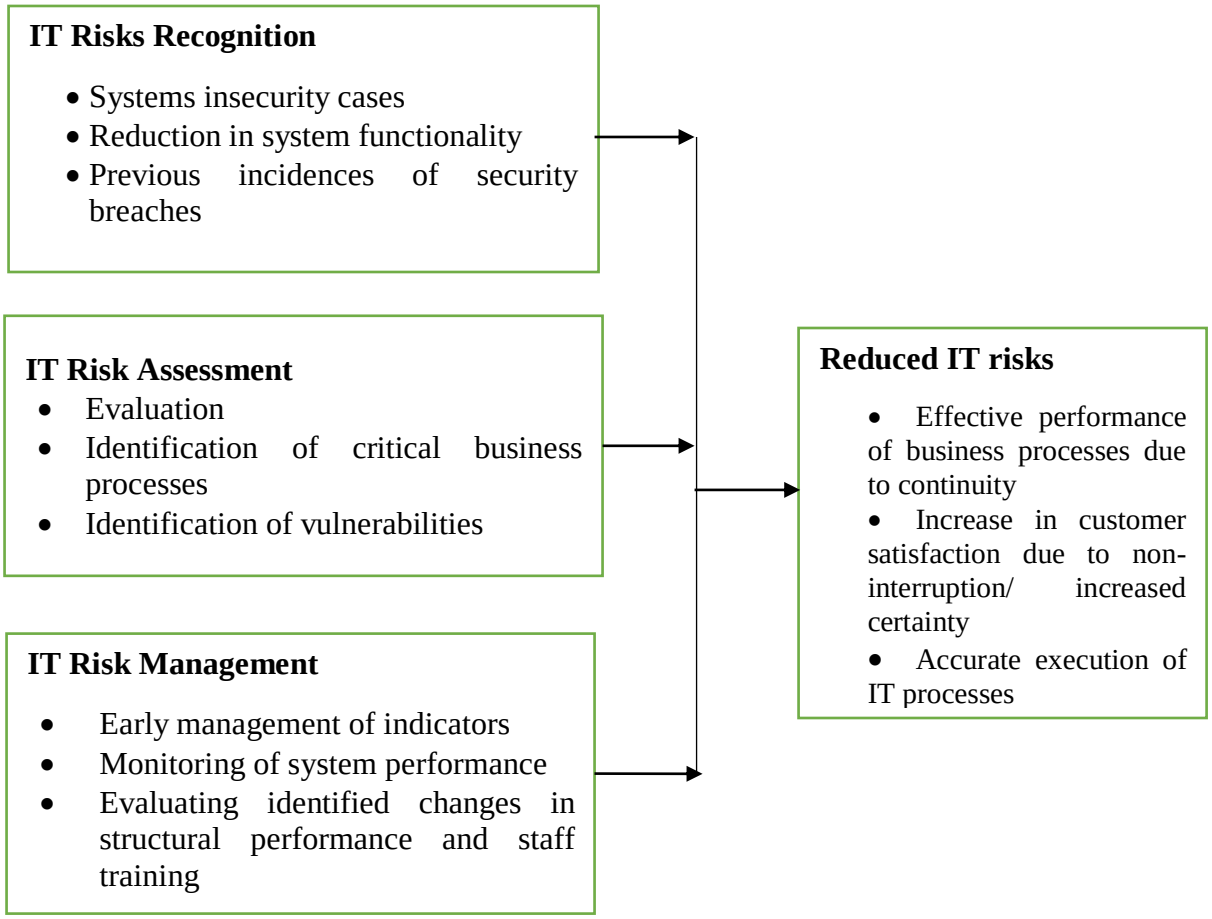

Figure 5: Conceptual Framework

2.6 Chapter Summary

The adoption and use of lean techniques aim to raise the companies' comparative advantage by ascertaining high-level profitability and improved efficiency. While boosting the capability to improve their customer services through fast and reliable business transactions, the adoption of the ICT applications introduces probable downfall through financial risk, operational risks, and technological risks. Upon the identification of the capability of the risks to occur, the IT based organizations must consider the establishment of worthwhile risk management practices for better operationalization of the company procedures. Employing various risk management frameworks such as COBIT, ITIL, FAIR, and ISO/IEC 27001:2013 provides the company with a

better direction in handling any potential threats likely to impede proper organizational performance. The comparison made of the different frameworks reveals COBIT as appropriate for implementation due to the wider scope of operation. The key risks indicators in implementing the COBIT framework include the occurrence of any incident regarding IS breaches post the implementation of the system, failure of the system to perform ICT governance as defined in the four different domains as discussed, and an increase in the number of potential threats after the adoption of the COBIT framework. Undertaking training and performing continued evaluation, maintenance, and support activities is one sure way of mitigating risks and ensuring higher predictability to increase the chances of better performance.

Chapter 3: Research Methodology

3.1 Introduction

Research methodology describes the used research and sampling design, data collection approaches, and the statistical techniques used during data analysis. The focus of this section of the research is the method used and sample design, the subject studied, the production, and administration of questionnaires and measurements used in data analysis. Besides these, ethical considerations will also be reviewed for a better administration of the research process.

3.2 Research Design

The study intends to use a descriptive research design, which will enable the analysis and prediction of the environment based on the current state of affairs. Additionally, the capability of the design to communicate effectively on the current condition of the technology-based SMEs makes it beneficial for use in the research. In employing a case study approach to the research, it will enable the making of inferences for other firms likely to be undergoing similar problems (Xu, 2018). The study will consider the use of both qualitative and quantitative information; that

is essential since the variables under consideration are of both natures. Quantitative research measures the quantifiable data, while qualitative approach looks into the immeasurable aspects of the study.

3.3 Target Population

The target population in research refers to those targeted by the research and is always the greatest beneficiaries upon the implementation of any recommendations made following the research. For the research, the target population comprises 120 employees in the IS of Compulynx Limited, 15 employees from Conquest Capital and 5 employees from Faculty Solutions, who will respond to questions regarding the risks faced and the employed techniques to assess their performance and capability to overcome the challenges experienced. The employees will include senior managers that are directors and heads of departments, managers, and the non-management staff currently working in the organization. Compulynx is a top software solutions company, with Conquest Capital and Faculty Solutions being among upcoming companies in the IT industry in Kenya.

3.4 Sampling Procedure

The sampling procedure uses a bi-phase sampling technique, which involved stratified sampling that was useful in identifying the ICT staff basing on hierarchy. For the risk management, the senior management becomes a point of focus due to their capability to understand the process better and offer insight that will be helpful for the research process. The support staff will also be necessary for evaluating risk management using the bottom-top approach; hence, provide more information to enrich the gathered information. Once stratified, the samples will be drawn from the groups using simple random sampling, which will give an equal chance of participation to

every staff member until the desired 120 participants are achieved (Guerrero, 2019). Giving equal chances to the participants minimizes bias by being more inclusive.

3.5 Sample Size

Calculating an exact sample size is necessary to ascertain that the results obtained from the study are representative of the population. This study applies the Slovin formula in determining the sample size. The formula is highly accurate given its dependence on the sampling error to estimate the required sample size (Slovin, 1960). The formula used for calculating sample size is given as below.

$$n = \frac{N}{1 + N(e)^2}$$

For n sample size, N population size, and e sampling error

When it comes to dealing with Conquest Capital and Faculty Solutions companies, it was impossible to do a sample. Rather, the researcher opted for Conquest Capital and Faculty Approaches to use the entire population of 15 employees and 5 employees respectively. Hence the projected respondent population for this study was 112.

1. Compulynx Limited

Strata	Target Population	Sample Size
Senior Managers	8	6
Managers	16	12
Support Staff	96	74
Total	120	92

2. Conquest Capital

Strata	Population
Senior Managers	2
Managers	3
Support Staff	10
Total	15

3. Faculty Solutions

Strata	Population
Senior Managers	1
Managers	1
Support Staff	3
Total	5

Table 3: Sample Size (Respondents) Determination

The required sample size which could be used in this research was determined as follows for a population (N) of 120 people with 95 percent confidence and sampling error at 0.05;

$$= \frac{120}{1 + 120(0.05)^2} = 92$$

3.6 Research Variables

COBIT is a cycle-based framework which includes various performance measures. An effective COBIT system depends on four basic domains, which are preparing and coordinating, obtaining and implementing, delivering and supporting, and tracking and evaluating.

3.6.1 Dependent Variable

The primary interest of the research is to determine the effectiveness of the implementation of the COBIT framework in mitigating IT risks for the technology-based SMEs. For this reason, the dependent variable in the study is reduced IT risks.

3.6.2 Independent Variables

Given that the integration of COBIT as a risk management strategy in the organization, the independent variables will be about the different stages of implementation to ascertain eventual success. The independent variables are therefore IT risks identification, IT risk assessment and IT risk management

The different independent variables will be in the categorical variables with various levels classifiable on a Likert Scale depending on the extent of performance communicated by the respondents. The four levels applicable are 1 as strongly agree, 2 as agree, 3 as disagree, and 4 as strongly disagree. The levels of the Likert Scale communicate the different degrees to which the opinions of the respondents reveal the reliability of the COBIT framework.

3.7 Methods of Data Collection

Data collection procedures employed in the process of research has a significant influence on the response communicated following a conducted study. The collection techniques viewed as necessary for the research are the use of questionnaires and the provision of an interview outline to assist in the group interviews conducted.

3.7.1 Questionnaires

The research will use semi-structured questionnaires, which will be necessary for minimizing the bias by encouraging the respondents to include their opinions of the performance upon completing the structured questions. The preparation of the questionnaire will be dependent on the extensive review of the information provided in the literature review section of this paper on the COBIT frameworks. Every recorded question will assist in the evaluation of the COBIT framework to determine its actual effectiveness when compared to the theoretical data. The administration of the questionnaires will be mainly by email to ensure that every selected

individual can successfully view and respond at their time of convenience. For those confirming availability, the help of a research assistant will be meaningful to ascertain the completion and selection of relevant responses of the required information. In the design, the questionnaire will comprise three specific parts that collect demographic, framework-specific, and suggestions for improvement questions to include the option of giving recommendations to improve the implementation of the framework in the SMEs.

3.7.2 Validity and reliability of the instrument

In research, measurement validity refers to the degree to which the instrument is true to the intended measurement. Proper validity ascertains a higher degree of fit between the operational and conceptual definitions of the construct (Nascimento-Ferreira, et al., 2016). In determining the validity of the instrument, it is necessary to conduct a pilot test involving at least 15 members in the population, which is counted as representative of the likely results of the study since it is approximately 10% of the population. The results of the pilot study will be used to adjust the initially designed questionnaire to ensure higher validity.

The reliability of the data collection instruments is identified from the capability to display consistency in the obtained results. The reliability of the instrument is expressed as a correlation coefficient, whose value ranges from 0-1, calculated as indicated below. A value above 0.5 is an indication of a high level of reliability.

3.7.3 Interviews

The essence of the interviews is to provide an opportunity for the respondents to explore the workings of the COBIT framework basing on their individual experiences and the opinions expressed within their circles of interaction. To ensure the effectiveness of the discussions, it is necessary for the moderator to ensure the inclusion of only relevant questions and proper

management of the interaction using effective communication skills. Other researchers have considered the use of interviews in managing IS issues due to the need to gather many opinions especially from knowledgeable individuals (Nascimento-Ferreira, et al., 2016). Six groups consisting of 6 participants, will be used for the research. The groups will also be drawn from the larger population of employees participating in the study within the involved departments of Compulynx Limited, Conquest Capital and Faculty Solutions. The questions for use in the discussions will originate from the questionnaire so that it acts as a mirror to confirm the information provided by the respondents.

3.8 Data Analysis

The basis for the interpretation of the gathered information will be the goals identified and the research questions outlined in the paper's first chapter. Various methods of analysis will be used for the data forms used in the report. First, the quantitative information obtained using semi-structured questionnaires will be analyzed using SPSS with descriptive statistics, such as central trend and dispersion metrics, which form the basis for a performance comparison.

Unlike the quantitative data obtained from the questionnaires used at Compulynx Limited, the qualitative data will result from the interactions made during the interviews. The notes made will result from the transcription of the ongoing discussions to ensure no form of information is lost in the process. The qualitative analysis will also be done in SPSS with further testing of hypotheses to ensure that one can draw correct inference from the obtained information.

3.9 Ethical Considerations

In conducting this study, some of the ethical considerations will include:

The identity of all the participants in this study will remain confidential for the entire period of the research. No third party that is beside the participants, and the researcher will have access or knowledge of any of the events during the research study. Despite recording their information for reference purposes and the availability of email addresses for communication with the participants, no critical information such as phone numbers, private identification, will be availed to the researcher to ensure the safety of the participants. Every submitted detail will be handled with the utmost care to ascertain that no other party can access them even after the period of research ends.

The researcher ascertains every person was willingly participating in the study that no sort of harm will be inflicted upon them. In case of any injuries, especially during the interviews, will be catered for by the researchers provided sufficient evidence relating the incident to the activities of the research come forth. Before engaging in the process as respondents, the researcher will inform every member of the team of the project details and the necessary information regarding the timelines and the information to be collected to ensure that they make an informed choice to either participate or not. No respondent will participate in the study forcefully or through any form of coercion.

3.10 Chapter Summary

The key focus of the chapter is the study methodology, which involves the design of the sample, the population, the sampling procedure and the necessary data techniques. Qualitative and quantitative research methods will be merged to balance each other to aid in the implementation of a mixed-mode research approach. Study design, population and sampling techniques have been explored. The key method of data collection was highlighted as questionnaires and further group discussions were conducted to assess the reliability of the decisions taken in the research

process. The data collected using these methods will be analyzed using SPSS statistical tools and will be interpreted in the different measures of central tendency and dispersion, depending on the particular aspects that the study wishes to compare. Ethical considerations are necessary in order to lay the groundwork on which elements are legally and morally permissible when working with the participants.

Chapter 4: Results

4.0 Introduction

This chapter presents the study findings. Frequency tables and descriptive statistics are presented. The focus group discussion outcome is also presented in thematic form.

4.1 Demographic Information

The demographic attributes of the study respondents are presented in this section. Out of the expected 92 respondents, only 80 participated in the study with the response rate standing at 86.97%. The response rate was sufficient for representation; thus, used in the analysis.

4.1.1 Work Experience

As indicated in Table 4.1, the majority of the study participants 81.3% cited that they had worked in the IT industry for 0 to 4 years while the least 5% cited that they had worked for more than ten years. 13.8% of the respondents indicated having worked for between 5 to 9 years in the different organizations.

Table 4.1 Work Experience of the study participants

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	>10 years	4	5.0	5.0	5.0
	0-4 years	65	81.3	81.3	86.3
	5-9 years	11	13.8	13.8	100.0
	Total	80	100.0	100.0	

4.1.2 Role in the organization

Results in Table 4.2 presents the role of study participants in the organization. Majority 41.3% indicated that they were the support staff while the least 26.3% are in the administrative role. The intermediate managers were 32.5%.

Table 4.2 Role in the organization

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Administrative	21	26.3	26.3	26.3
	Intermediate Manager	26	32.5	32.5	58.8
	Support Staff	33	41.3	41.3	100.0
	Total	80	100.0	100.0	

4.3 *Objective 1: Determining the influence of IT risk identification on the reduction of IT risks*

4.3.1 Possibility of facing a threat due to technology use

80% of the respondents associated the occurring threats with the technology used at the company, while 20% indicated that they do not face threats with the technology they use.

Table 4.4 Possibility of threat due to technology use

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	16	20.0	20.0	20.0
	Yes	64	80.0	80.0	100.0
	Total	80	100.0	100.0	

4.3.2 Key IT risks faced by SMEs that are developing technology-based solutions.

The study participants gave the information technology risks that they encounter when they are developing technology-based solutions. This they attributed to the fact that there are too many

developers of the technology-based solutions that make the technologies developed very cheap. The business does not make profits at all. Another risk faced by the SME is the employee loss risk because big companies that offer better pay poach the employees. Another risk is that of continuity in that the technology used gets outdated very fast. The loss of employees due to death and poaching also poses the challenge of continuing with the development of the technology-based solution. Other risks faced include that of customer relation risk, branding risk, capital market risk, and economic risk.

Table 4.5 Risks faced by SMEs

Risk	Frequency	Percent
Economic risk	70	71.7
Capital market risks	31	33.6
Branding risks	48	50.9
Customer relation risk	32	40.0
Continuity risk	75	79.1
Employee loss risk	70	75.4
Competition risk	80	86.8

In comparing the capability to identify risk and the capability of facing risks, more than 70% of the population of respondents confirmed that they could prevent the risks due to the proper understanding of their sources.

4.2 *Objective 2: To determine the influence of IT risk assessment on the reduction of IT risks*

All the respondents in the study responded that the company is faced with various risks, which affect the operations of the company to a certain level. The respondents also agreed that the following risk mitigation strategies could be incorporated in mitigating the IT risks: risk avoidance, risk sharing, risk reduction, and risk transfer. Their capability to identify the risks and

assess their effects on the company performance at different stages caused them to identify better the risk management practices to undertake. The results of the response are as follows:

Table 4.3 A Comprehensive strategy for use in mitigating IT risk

Risk mitigation strategy	Frequency	Percent
Risk Avoidance	13	11.6
Risk Sharing	22	19.6
Risk reduction	52	46.4
Risk transfer	25	22.3

From the above table, 11.6% of the respondents believe that the IT risk within their companies and other SMEs can be avoided, 19.6% believe that the risks can be shared, 46.4% believe that the risks can be reduced, and 22.3% believe that risks can be transferred. From these results, the majority of the respondents believe that risk reduction can work better in mitigating the IT risks. Therefore, it is concluded that a comprehensive strategy for mitigating the IT risks within the company is risk reduction using commendable frameworks such as COBIT and NIST.

4.4 *Objective 3: To determine the influence of IT risk management on the reduction of IT risks*

4.4.1 Presence of risk management practices put in place to manage the occurrence of the identified risks

66.1% indicated that they employ strongly valid risk control practices in the business, while 33.9% indicated that they employ weakly valid risk management practices at a place to manage the occurrence of the identified risks. With weak validity, risk management practices do not yield an expected result because they are not fully effective. With strong validity, the risk management practices are much effective, hence yielding successful results. From this result, it would mean

that a smaller percentage of the respondents do not believe in the risk management practices which the organization employs. Hence, the company ought to educate and sensitize its staff on the use of such risk management practices and make them aware of the various risks the company is exposed to.

Table 4.6 Presence of risk management practices

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Weak	21	26.3	26.3	26.3
	Strong	57	71.3	71.3	97.5
	Intermediate	2	2.5	2.5	100.0
	Total	80	100.0	100.0	

4.4.2 Main challenges preventing the establishment of proper risk management plans

The organization presented the challenges that prevent the establishment of proper risk management plans. As indicated in Table 4.6, the majority 77.7% cited financial constraint as the main challenge, 65.2% indicated leadership as the challenge, and 54.5% indicated staff adaptability as the challenge.

Table 4.7 Challenges preventing the establishment of proper risk management plans

Challenge	Frequency	Percent
Financial	87	77.7
Leadership	71	63.4
Staff adaptability	61	54.5

4.4.3 Ways you think the system in place can be improved for better risk management.

The study sought to review and recommend the implementation of information technology risk assessment and information risk management best practices.

4.5 Main Objective: To determine a comprehensive strategy for use in mitigating IT risks in the technology-based SMEs

The study sought to develop an implementation strategy on how to manage and reduce IT risks. From the study participants, they proposed the following strategies to help manage and reduce IT risks, as shown in Table 4.8. As indicated in Table 4.8, the Majority of the respondents indicated diversification as the major strategy to manage and reduce IT risks. Besides, collaboration with other stakeholders and having insurance was also stated as a strategy to manage and reduce IT risks. Therefore, it would be concluded that both collaboration, diversification, and having insurance can be implemented to manage and reduce risks, with much emphasis and interest being on collaboration. The three strategies are effective because, from the respondents, these strategies surpass the 50% average score of interview adoption.

Table 4.8 Strategies on how to manage and reduce IT risks

Strategy	Frequency	Percent
Collaboration	62	77.50
Diversification	69	86.25
Having Insurance	56	70

COBIT framework as a solution for risk reduction

Understanding the COBIT framework

The study investigated whether the organization understood the COBIT framework. The results are presented in Table 4.9. More than half of the participants indicated that they understood the COBIT framework, which is an indication of firsthand experience in its use.

Table 4.9 Understand the COBIT framework

1. Are you familiar with the COBIT framework?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	33	41.2	41.2	41.2
	Yes	47	58.8	58.8	100.0
	Total	80	100.0	100.0	

Duration working with the framework

The length of working with the framework is presented in Table 4.10. The majority of the respondents, 28.7%, have worked with it for less than one year, while the least 10.1% have worked it for more than 4 years.

Table 4.10 Understand COBIT framework

2. How long have you worked with the framework (including the time outside your current place of work)?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	< 1 year	23	28.7	28.7	28.7
	>6 years	1	1.3	1.3	30.0
	1-3 years	16	20.0	20.0	50.0
	4-6 years	7	8.8	8.8	58.8
	Not Relevant	33	41.3	41.3	100.0
	Total	80	100.0	100.0	

Level of knowledge on the COBIT framework

Out of the 80 respondents, 54.8% reported as being knowledgeable of the functioning of the COBIT framework. The remaining 45.2% reported lacking knowledge or the experience not being relevant to them.

Table 4.11 Level of knowledge on the COBIT framework

3. Describe your level of knowledge on the COBIT framework basing on the measures indicated below by only checking one box that applies to you.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	1.3	1.3	1.3
	Expert level	3	3.8	3.8	5.0
	Highly knowledgeable	2	2.5	2.5	7.5
	Knowledgeable	15	18.8	18.8	26.3
	Not knowledgeable	29	36.3	36.3	62.5
	Not Relevant	9	11.3	11.3	73.8
	Slightly knowledgeable	21	26.3	26.3	100.0
	Total	80	100.0	100.0	

Use of other ICT risk management frameworks

The majority of 83.7% indicated that they had worked with other ICT risk management frameworks before, while 16.3% indicated that they have not worked with them before.

Table 4.12 Working with other ICT risk management frameworks before

		Frequency	Percent
Valid	No	13	16.3
	Yes	67	83.7
	Total	80	100.0

Expertise on the frameworks used

The majority of the participants, 24.1%, indicated that they were slightly knowledgeable, while 15.2% indicated that they were highly knowledgeable.

Table 4.13 Expertise on frameworks used

		Frequency	Percent
Valid	Not knowledgeable	15	18.8
	Slightly knowledgeable	22	27.5
	Knowledgeable	21	26.3
	Highly knowledgeable	12	15
	Expert level	10	12.5
	Total	80	100.0

Comparison of COBIT with other frameworks used previously

Of the total respondents, 46.2% reported having used the framework for some time, thus able to tell the existing differences in use. From the 46.2%, 64.9% reported that the COBIT framework performed better than other frameworks such as NIST.

Table 4.14: Comparison of COBIT with other frameworks

4. c. How does COBIT compare to other frameworks used previously?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Extremely better	6	7.5	7.5	7.5
	Extremely poor performance	1	1.3	1.3	8.8
	No difference	12	15.0	15.0	23.8
	Not Relevant	43	53.8	53.8	77.5
	Slightly better	18	22.5	22.5	100.0
	Total	80	100.0	100.0	

Hypothesis testing for effective risk reduction using the COBIT framework

Given that both the dependent and independent variables are categorical variables, the hypothesis testing will rely on the F test to draw conclusions on the reliability of the COBIT framework. The obtained results are as plotted in the table below.

Tests of Between-Subjects Effects

Dependent Variable: 1. Does your organization face numerous threats due to the technology in use?

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	3.404[a]	15	.227	1.511	.029
Intercept	12.691	1	12.691	84.476	.000
Level of knowledge	1.374	5	.275	1.829	.055
Familiar COBIT	.016	1	.016	.108	.744
COBIT effective performance	.296	2	.148	.985	.069
Level of knowledge * Familiar COBIT	1.078	2	.539	3.587	.034
Level of knowledge * COBIT effective performance	.959	3	.320	2.129	.106
Familiar COBIT * COBIT effective performance	.591	2	.295	1.965	.149
Level of knowledge * Familiar COBIT * COBIT effective performance	.000	0	.	.	.
Error	9.314	62	.150		
Total	62.000	78			
Corrected Total	12.718	77			

a. R Squared = .568 (Adjusted R Squared = .322)

The dependent variable being risk reduction (measured using the number of risks faced by the organization), the aim of the hypothesis test is to estimate the influence of the knowledge and practice of the COBIT frameworks in an organization. The fitted model was significant at 5%. Besides this, being knowledgeable on the COBIT framework and having practiced it had a significant effect unlike people who just stated their familiarity with the framework. With further testing, an interaction between the level of knowledge and familiarity with the COBIT

framework improved the probability of reducing the risks faced in the organization. This serves as further evidence of the reliability of the framework for IT risk reduction.

4.6 Chapter summary

The analysis chapter provides the findings as analyzed using descriptive statistics and the frequency tables. Using the sample size of 80 for this study, the majority of them have been working in the organization for at most four years, and a superficial number serves at the support staff level. In mitigating the IT risk, 46.4% believe that risk reduction is the best mitigation strategy for the companies. Hence, it means that many of the employees do not believe in risk reduction, but when compared to other mitigation strategies, risk reduction proves the most comprehensive. Also, the majority of the respondents face threats based on the technology they use. When considering the various types of risk, competition is the most experienced risk in the company. With the presence of risk management practices within the company, the majority of the respondents believe that such practices are powerfully effective, hence strengthening the organization. With various challenges affecting the organization, financial constraints remain the main challenge. The majority of the workers in the organization indicated that they understood COBIT, with 26.7% having worked with it for one to three years. Conclusively, the majority of the respondents have worked with other ICT risk management frameworks, with 24.1% being slightly knowledgeable. The respondents indicated that the COBIT framework performed slightly better.

Chapter 5: Conclusion and recommendation

5.1 Answer to main research objective

The research project aimed to identify and implement an attractive risk management framework, which would help in mitigating the IT risks. The general objective was to determine a comprehensive strategy for mitigating IT risks in the IT risks in the technology-based SMEs. This objective was fulfilled. It involved determining the key IT risks faced by the SMEs, as well as recommending that implementing the IT risk assessment and management technologies. In addition, it aimed towards developing the implementation strategy in managing and reducing the risks. For instance, from the data results, 46.4 percent of the respondents were positive that risk reduction is the best mitigation strategy, which can be used to reflect to the SMEs in the IT industry. Though this shows that many employees do not believe in risk reduction, but when compared to other mitigation strategies, then risk reduction proves to be the most comprehensive mitigating strategies. Therefore, this is enough evidence that the objective of this research had been achieved, based on the data collected and analyzed to address the main aim of the project.

In conducting the research, the primary aim was to determine a comprehensive strategy for use in mitigating IT risks in the technology-based SMEs. Answering the question relies on the series of qualitative analysis conducted for each specific objective determining the effective use of the COBIT framework above others like NIST. From the analysis, it is evident that only half of the population of respondents confirmed having used COBIT frameworks as an IT risk reduction strategy. Checking experiences confirmed that 43% of the population had a positive report of the COBIT framework; stating that the continued use reduced the experienced risk to cybersecurity attacks. Those incorporating the use of multiple frameworks confirmed that COBIT still outperformed the others. The larger part of those experiencing the greater challenges had never

incorporated the framework in their system, which is sufficient evidence to conclude that the COBIT framework is the most comprehensive strategy in mitigating the IT risks in technology-based SMEs.

5.2 Methodological Reflection

The study had various limitations. First, the limited resources, especially in financial capability to conduct the research effectively. This made it difficult to conduct the interview, transport and preparation of the analysis and presentation. Secondly, the population selected for the research was not enough. In an industry with hundreds of employees, only 80 could be used in the research. With enough resources, this population could be increased to at most 500 – 1000 for a more accurate and generalized results. Therefore, with a higher financial base, it would be reasonable to use a higher sample size to ensure the reliability and validity of the obtained result. Thirdly, the occurrence of the COVID-19 pandemic could not allow for the interviews to take place as scheduled initially. Most of the targeted respondents were unavailable due to the work-from-home procedures stated by the government.

5.3 Conclusion

SMEs in Kenya experience serious risks, especially the technology-based SMEs. This research concludes that the SMEs implement risk reduction as the most comprehensive way of mitigating the risks within the technology-based companies, for it seems tricky to assume that risk avoidance, risk sharing, and risk transfer is possible within the companies, and if they are possible, then to lower efficiency. Since the technology-based companies face threats in the use of technology, they are automatically exposed to the IT risks, including the branding risks, economic risks, capital market risks, continuity risks, employees' risks, and competition risks.

All these risks are attributed to either the internal or external factors of the technology-based SMEs.

The research also affirms that IT-based SMEs employ strongly valid risk management practices to protect the businesses, hence yielding effective production results and income. However, financial constraints prove to be the primary challenge when preventing the establishment of proper risk management plans. In addition, the adaptability of staff is another challenge, as well as leadership management. Also, the research affirms that the major implementation strategy for managing and reducing IT risks is collaboration, with others being diversification and having insurance. Therefore, addressing and mitigating IT risks in technology-based SMEs is a responsibility for both the employees and the management.

5.4 Policy Recommendations

The outcomes of the research project directly and indirectly relates to the industry. For instance, when addressing the objectives of mitigating IT risks within the industry, risk reduction can be the best mitigating procedure to reduce and control such risk. This is practical in many of the IT firms. Some of the recommended policy changes include training the employees on the COBIT framework to improve its adoption among smaller businesses. Currently, about 43% indicated that they have not interacted with the platform before. The adoption of the framework will help in mitigating risks to enhance customer satisfaction and data security. Secondly, small and medium enterprises should consider increasing the accessibility of resources for risk management to the knowledgeable employees to enable them mitigate their occurrence. Given that most companies reported for issues for such as phishing, better knowlegeability and the availability of resources can enable them to counter that.

5.5 Research Recommendations

The research sought to determine the strategies for use in the mitigation of IT risks within the technology-based SMEs. This means that the researchers determined the key IT risks faced by the SMEs, the implementation strategies of the IT risk assessments, and management as well as developing an implementation strategy for managing the risks in general. Therefore, it is proposed that further research be conducted to assess the factors contributing to such risks. Such factors would consider the association between IT risks and other related businesses in other industries. Secondly, it is proposed or recommended that various exposure to IT-based SMEs be determined. With full knowledge and recognition of such exposures, it would be significant to understand the relationship between the It risks and the various SMEs within the IT industries.

Thirdly, when such research is done, the qualitative design of analysis ought to be incorporated, especially when the researcher is concerned with giving observational summaries of the respondents. This would mean that quantitative design covers the statistical analyses and inferences, while the qualitative design would deal with observational analysis. Such conglomeration of the two designs is essential, especially when the researcher decides to focus on various exposures to IT risks, which my research did not explore.

Fourth, it is recommended that other future research to consider IT simulation-related analysis when exploring various IT-based companies for data analysis. Such simulation would be essential, especially when dealing with cross-company data collection and analysis. With various data, it would be more reliable to give inferences and a reliable conclusion.

Lastly, I recommend that future research studies be funded with resources for the benefits and efficiency of conducting deep data collection in various IT companies within the SMEs. Proper

and diversity in data collection with different companies would improve the accuracy of the analysis and interpreted data is more dependable, as compared to single-company analysis.

References

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 357-370.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM, 51*(4), 64.

Bougaardt, G., & Kyobe, M. (2011). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa. *In ICIME 2011-Proceedings of the 2nd International Conference on Information Management and Evaluation: ICIME 2011 Ryerson University* (p. 62). Toronto, CA: Academic Conferences Limited.

Buckby, S., Best, P., & Stewart, J. (2005). The Role of Boards in Reviewing Information Technology Governance (ITG) as part of organizational control environment assessments. *In Cusack, B., Eds. Proceedings 2005 IT Governance International Conference*, (pp. 1-14). Auckland, NZ.

Chale, P., & Mbamba, U. (2015). The role of mobile money services on growth of small and medium enterprises in Tanzania: Evidence from Kinondoni District in Dar es Salaam Region. *Business Management Review*, 171.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

Enocson, J., & Söderholm, L. (2018). Prevention of Cyber Security Incidents within the Public Sector: A qualitative case study of two public organizations and their way towards a sustainable cyber climate.

Gathogo, G., & Ragui, M. (2014). Effects of Capital and Technology on the Performance of SMEs in the Manufacturing Sector in Kenya-Case of selected firms in Thika Municipality. *European Journal of Business Management, 6*(7), 308-311.

Guerrero, H. (2019). Inferential Statistical Analysis of Data. *In Excel Data Analysis*, 179-224.

ISO. (2019, August 28). *ISO/IEC 27001:2013 [ISO/IEC 27001:2013]*. Retrieved February 2020, from ISO: https://www.iso.org/standard/54534.html

Jones, A. (2007). A framework for the management of information security risks. *BT technology journal, 25*(1), 30-36.

Khther, R. A., & Othman, M. (2013). Cobit framework as a guideline of effective it governance in higher education: a review. *International Journal of Information Technology Convergence and Services, 3*(1), 21.

Krisanthi, G. A., Sukarsa, I. M., & Bayupati, I. P. (2014). Governance audit of application procurement using COBIT framework. *Journal of Theoretical and Applied Information Technology*, 342-351.

Kumsuprom, S., Corbitt, B., & Pittayachawan, S. (2008). ICT risk management in organizations: Case studies in Thai business. *ACIS 2008 Proceedings*, 98.

Lainhart IV, J. W. (2000). COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems*, 21-25.

Migiro, S. O. (2006). Diffusion of ICTs and E-commerce adoption in manufacturing SMEs in Kenya. *Journal of Libraries and Information Science*, *72*(1), 35-44.

Mokhsin, M., Zainol, A. S., Haihom, S. N., Som, M. H., & Abdul, A. J. (2018). Applying ITIL Framework to Analyze Problem Management Key Performance Indicator (KPI): a Case Study of Malay Owner Company (Mesiniaga Berhad). *International Journal of Engineering & Technology*, 80-86.

Morris, M. W. (2013). Breaching of earth embankments and dams. *The Open University*.

Mutwiri, G. (2018). EFFECT OF TECHNOLOGY INNOVATION ON ACCESS TO MARKETS BY SMALL MEDIUM ENTERPRISES IN NAIROBI COUNTY. *UoN Repository*, 18.

Nascimento-Ferreira, M. V., Collese, T. S., de Moraes, A. C., Rendo-Urteaga, T., Moreno, L. A., & Carvalho, H. B. (2016). Validity and reliability of sleep time questionnaires in children and adolescents: A systematic review and meta-analysis. *Sleep medicine reviews*, 85-96.

OpenGroup. (2010). *Technical Standard: Risk Taxonomy.* The Open Group. Retrieved February 18, 2020

Palilingan, V. R., & Batmetan, J. R. (2018). Incident management in academic information system using ITIL framework. *In IOP Conference Series: Materials Science and Engineering*, 12110.

Pardo, C., Pino, F. J., & Garcia, F. (2016). Towards an Integrated Management System (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2 Standards. *International Journal of Software Engineering and Its Applications*, *10*(9), 217-230.

Pickett, S., & Pickett, J. (2005). Auditing for Managers. *The Ultimate Risk Management*, 147.

PwC-UK. (2015). *2015 INFORMATION SECURITY BREACHES SURVEY.* London: Crown Copyright. Retrieved February 18, 2020

Ridley, G., Young, J., & Carroll, P. (2004). COBIT and its Utilization: A framework from the literature. *In 37th Annual Hawaii International Conference on System Sciences* (pp. 8-12). Hawaii: IEEE.

RISHAD, A. N. (2019). MANAGING CYBERSECURITY AS A BUSINESS RISK IN INFORMATION TECHNOLOGY-BASED SMES. *Doctoral Thesis, University of Nairobi*, 13-99.

Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer, 10*(4), 16.

Slovin, E. (1960, March 13). Slovin's formula for sampling technique. p. 22.

Spekle, R. F., Van Elten, H. J., & Kruis, A. M. (2007). Sourcing of internal auditing: An empirical study. *Management Accounting Research, 18*(1), 102-124.

Thielman, S. (2017). Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian*, 15.

Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting information systems*, 240-263.

Wamuyu, P. K., & Maharaj, M. S. (2011). Factors influencing successful use of mobile technologies to facilitate E-Commerce in small enterprises: The case of Kenya. *USIU Repository*, 1-12.

White, S. (2019, January 5). *What is COBIT? A framework for alignment and governance*. Retrieved January 2020, from CIO: https://www.cio.com/article/3243684/what-is-cobit-a-framework-for-alignment-and-governance.html

Xia, J. (2009). Factors influencing Chinese suppliers' quality performance: A supplier selection model for small and medium enterprises (SMEs) to ensure their Chinese suppliers' ability to provide quality products. *Indiana State University*.

Xu, M. (2018). Inferential Statistical Analyses on Information Network Generation. *Doctoral Dissertation*.

APPENDICES

Appendix A: Interview Outline

1. How have you been involved in the use of the COBIT framework? If yes, how long?
2. What influenced your choice to purchase the system currently in use?
3. What are some the advantages experienced in the use of the framework?
4. Have you experienced any disappointing situations since the first time of use?
5. Let's list these on the flip chart. If you had to pick only one factor that was most important to you, what would it be? You can pick something that you mentioned or something that was said by others.
6. Have you ever used other frameworks prior to or after choosing to use the framework?
7. What do you think are some of the functions that require improvement to ensure the system functions effectively?
8. Suppose that you were in charge and could make one change that would make the program better. What would you do?
9. What would be the influencing factors of the choice made in Q8 above?
10. What do you think about merging COBIT and other frameworks such as NIST and ITIL in the function process? Could it be a game changer in ICT risk management?

Appendix B: Questionnaire

A. Contact Details

The information entered in this section is purely for reference and communication with the researcher. Any filled in content will remain highly confidential.

Name of Organization	
Position in the Organization	
Email address	
Phone number	

B. Work Experience

1. How long have you been working at your organization?

0-4 years [ ] 5-9 years [ ] > 10 years [ ]

2. How long have you been working in the field of information technology?

0-4 years [ ] 5-9 years [ ] > 10 years [ ]

3. What is your role in the organization?

Administrative [ ] Intermediate manager [ ] Support staff [ ]

C. ICT Risk Management Practices

1. Does your organization face numerous threats due to the technology in use?

Yes [ ] No [ ]

2. Mention some of the risks faced by (or have been experienced in the past)

……

……

……

……..……

3. Are there any risk management practices put in place to manage the occurrence of the identified risks?

Yes [ ] No [ ]

4. What are the main challenges supporting (or preventing) the establishment of proper risk management plans?

Attribute	Yes	No
Financial		
Leadership		
Staff adaptability		

If other, specify and explain in the section below.

……

……

……

……..……..

……

……..……..

5. Mention any ways you think the system in place can be improved for better risk management.

……

……

……

……

……

D. Understanding of the COBIT framework

1. Do you understand how the COBIT framework operates?

   Yes [ ] No [ ]

2. How long have you worked with the framework (including the time outside your current place of work)?

< 1 year [ ] 1-3 years [ ] 4-6 years [ ] >6 years [ ]

3. Describe your level of knowledge on the COBIT framework basing on the measures indicated below by only checking one box that applies to you.

   Not knowledgeable [ ]

   Slightly knowledgeable [ ]

   Knowledgeable [ ]

   Highly knowledgeable [ ]

   Expert level [ ]

4. Have you worked with other ICT risk management frameworks before?

Yes [ ] No [ ] (If yes, please indicate which ones in the space provided and proceed with question 4b)

……

……..……..

……

……..……..

4b. Rate your expertise on other framework (s) used as checked in Q4 above.

Not knowledgeable [ ]

Slightly knowledgeable [ ]

Knowledgeable [ ]

Highly knowledgeable [ ]

Expert level [ ]

4c. How does COBIT compare to other frameworks used previously?

Extremely poor performance [ ]

Poor performance [ ]

No difference [ ]

Slightly better [ ]

Extremely better [ ]

4d. What influences your classification above?

Attribute	Yes	No
Affordability		
Maintenance		
User friendliness		
Adaptability		

5. Do you think COBIT is effectively performing its functions basing on the set organizational goals?

   Yes [ ] No [ ]

6. Kindly mention any failures witnessed during use that affected your performance in the role largely.

   ……

   ……

   ……..……

7. Give any suggestions for improvement that will help in ascertaining better performance of the software in the organization.

   ……

   ……

   ……

❖ END

APPENDIX C: WORK PLAN

Activity	January	February	March	April	May	June
Desktop Research: identifying topics and possible methodologies						
Literature Review						
Feasibility Study						
Proposal Development: Aligning the provided information						
Progress Report						
Final Presentation of findings						

APPENDIX D: BUDGET

Item	Description	Quantity	Total Cost (Kshs)
Proposal	Printing copies of proposal and binding	6	3,000
Stationery	Pens	7	6,500
	Notebook	3	
	Flash Disk	1	
	Questionnaires	100	
Collecting data and Analysis	Travel and subsistence expenses		50,000
Report	Printing copies and hard cover binding	6	10,000
Internet	Weekly internet bundles @ 500	12 GB	5,400
Publishing	Publishing of paper		12,000
Total Cost			**85,900**