UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

PROJECT REPORT

Information Security Management Toolkit for ISO/IEC 27001 standard, case of small-to-medium sized enterprises (SMEs)

Victor Wekesa Wanyonyi

P53/11737/2018

Supervisor: Dr. Elisha Abade

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

DECLARATION

Student

This project, as presented in this report, is my original work and has not been presented for any award in any other university.

Signed ..... Date .....

Victor Wekesa

P53/117737/2018

Supervisor

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

Supervisor: Dr. Elisha Abade

Signature: ..... Date: .....

DEDICATION

I dedicate this work to all out there who appreciate the importance of computer security and distributed systems.

ACKNOWLEDGEMENT

I am grateful to God for the good health and strength he grants me to learn and for providing priceless people who without their effort, collaboration and dedication, this project wouldn't have been a success.

I wish to personally thank the following people for their contributions to my inspiration and knowledge and other help in working through this project; my supervisor Dr. Elisha Abade for his unwavering support and guidance even where I thought it was beyond my capacity, and all my lecturers at the School of Computing and Informatics who helped me in many ways and made my education journey at the University of Nairobi pleasant and unforgettable.

Lastly sincere gratitude to caffeine and sugar, my companions through many long nights of writing, coding and research.

ABSTRACT

Information security has become an important aspect in today's business environment, where all operations are technology centered. Over the years lots of effort has been put to ensure that organizations manage information security in a standardized manner. There are several frameworks and standards such as COBIT, ITIL and ISO/IEC 27001 that have been proposed for this purpose. In this work the focus was on ISO/IEC 27001 which is an international standard that provides specification for an Information Security Management System (ISMS). The standard is designed to assist large and small enterprises to manage their information security processes in line with international best practice. Small and Medium-sized Enterprises (SMEs) usually find it difficult to comprehensively implement the prescriptive requirements of the standard. This study proposes a toolkit approach in helping SMEs implement the requirements of the standard. It proposes and develops an ISO/IEC 27001 information security toolkit as a prototype for guiding organizations in implementing information security controls. Apart from toolkit design and implementation, the study also assesses the toolkit and its usability. Results indicated that majority of SMEs would embrace the toolkit and that it can be of great importance in guiding them implement controls of the standard. Furthermore, the study found out that with further enhancement of the toolkit features, to incorporate all aspects of ISO 27001 standard, the toolkit can be used for both large enterprises and small enterprises in implementing the standard requirements.

Table of Contents

List of Abbreviations

ISMS – Information Security Management System

ISO – International Organization for Standardization

IEC – International Electrotechnical Commission

SMEs – Small and medium-sized enterprises

CIA – Confidential, Integrity and Availability

PCI DSS – Payment Card Industry Data Security Standard

ITIL – Information Technology Infrastructure Library

ITGI – IT Governance Institute

COBIT – Control Objectives for Information and Related Technology

IS – Information Security

DSR – Design Science Research

Definition of Important Terms

ISMS – An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process

ISO/IEC 27001:2013 – It is a standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

Software toolkit – This is a single utility program, a set of software routines or a complete integrated set of software utilities that are used to develop and maintain applications and databases.

Information Security – This is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

Availability – Property of being accessible and usable upon demand by an authorized entity.

Confidentiality – Property that makes information available or disclosed only to authorized individuals, entities or processes.

Integrity – Property of accuracy and completeness.

CHAPTER 1: INTRODUCTION

1.0 Context and Background Information

Information has become a very vital asset for large and small organizations in the current world. Over the past years, information has been increasingly recognized as an important raw material and for some it's the only asset. Economically, information and the ability to process information may have more impact on an organization's productivity than operational effectiveness or product innovation (Barlette & Fomin, 2009). In the world today where all operations are technology centered, information is often considered as the lifeblood of business, without which business cannot function (Sharma & Dash, 2012). Given the colossal value to organizations, it is important to secure information assets through a system of information security to ensure organizational competencies.

Expeditious development of technology has dramatically increased online business opportunities, but this has led to growing information security challenges (Soomro et al., 2015). Gordon and Loeb (2006), stated that information security relates to an array of actions designed to protect information and information systems. However, information security does not protect only the information, but also the whole infrastructure that makes its use easier. It covers hardware, software, and physical security. The more the number of applications, users and systems increase, the more the management of an organization's information security gets more complex and the vulnerability increases.

Information security concerning data breaches, consumer privacy issues, identity thefts, and other online threats is a major concern (Udo, 2001) for business enterprises. Unfortunately, no single formula guarantees absolute information security. In the last decade, information security risks have become a top priority on senior management agendas because of the increased incidence of security breaches and the direct and potential cost (IT Governance, 2019). The recent UK Government Information Security Breaches report indicates that security breaches are becoming more common for every type of business, regardless of its size. Apart from monetary penalties, inadequate security of information systems may result in regulatory non-compliance. Per the Sarbanes-Oxley Act (2002), organizations are legally responsible for the validity of reported financial data and the status of information systems where such financial data is stored and processed. Therefore, the importance of protecting information from being compromised has

become vital for a company's daily operations and survival (Fomin et al., 2008). Because of the continued escalation of cyber-attacks and the increasingly regulated data protection landscape, it is imperative for organizations to establish, implement, and maintain an effective Information Security Management System (ISMS) to manage critical information assets (IT Governance, 2019).

ISO/IEC 27001 (ISO/IEC 27001:2013) is the international, recognized standard that provides the specification for an information security management system (ISMS). The latest version was published in October 2015. The Standard is designed to help both large and small organizations manage their information security processes in line with international best practice while optimizing costs. It is technology and vendor neutral and is applicable to all organizations - irrespective of their size, type or nature. An Information Security Management System (ISMS) provides a structured way to managing information security. It comprises of guidelines, procedures and other controls involving people, processes and technology to help organizations protect and manage all their information assets. Confidentiality, availability and integrity (CIA) of corporate information assets and intellectual property is more important for the long-term success of organizations than traditional, physical and tangible assets. Complying to regulatory policies and procedures has an increasingly important role to play, and effectual information security is critical to regulatory compliance. It is a single entry point for everything to do with information security. It helps in identifying and accessing a wide range of information security-related advice and resources (IT Governance, 2019).

Thousands of large enterprises are certified against ISO/IEC 27001, and hundreds of others working per the principles provided by the standard. Organizations recognize the importance of implementing an Information Security Management System (ISMS). It helps them maintain legal and regulatory compliance, demonstrate credibility and trust to customers, reduce the likelihood of a security breach and many more advantages that are plain to see. However, small and medium sized enterprises find it difficult to work under those principles. As opposed to popular belief, the intricacies of information security involved in running small and medium-sized enterprises (SMEs) are often tricky. For one, formulation of information security management practices, which are primarily developed for bigger enterprises, has traditionally sidelined SMEs. In addition to that, the unique nature of the ways in which these businesses operate warrant customized approaches. Amusingly, the very unique traits of their operations have kept SMEs out of information security

management approach formulations. Furthermore, information security practices designed for larger corporates cannot be successfully implemented for SMEs. While regulatory responsibilities are as strictly applicable to SMEs as they are to corporate houses, a belief permeates that individual information security system failures of SMEs are too insignificant to be taken care of and that their contrasting nature will efficiently withstand any collective failure.

This study proposes a toolkit approach in guiding SMEs to implementing requirements provided by ISO/IEC 27001. A prototype toolkit has been develop and evaluated among selected group of SMEs.

1.1 Problem Definition

In contrast to multinational firms that adopt an information security management system (ISMS), it is often difficult for SMEs to comprehensively implement the prescriptive requirements of the ISO/IEC 27001:2013 standard. Most SMEs are vulnerable to a variety of information security risks that bring regulatory, operational and financial threats. They find it difficult to effectively put into practice necessary guidelines such as policies and procedures for mitigating information security risk. They also lack affordable software tools that they can leverage in identifying missing requirements/controls that they have not implemented.

In addition, small and medium-sized enterprises, are the most likely to manage their information security processes in house, getting ISO 27001 implementation right the first time is of utmost importance to the businesses and, of course, to their customers. They usually face some issues throughout the implementation process including having or recruiting the right staff to carry out the implementation; producing, controlling, and managing information; and correctly interpreting the requirements of the standard.

Organizations security is critical for business operations, as well as retaining credibility and earning the trust of clients. Many of the investors may also consider a boost in funding if provided with viable security controls plans. Thus, having a toolkit that provides a guide to implementing the necessary requirements provided by ISO/IEC 27001:2013 can give an enterprise a competitive advantage.

1.2 Goals and Objectives

1.2.1 Project goal

To develop a software toolkit that contains modules which represents the requirements of ISO/IEC 27001:2013 information security management standard and can be used by small and medium-sized enterprises as a guide to implement the requirements of the standard.

1.2.2 Objectives

1. To analyze ISO/IEC 27001:2013 standard and its requirements for establishing, implementing, maintaining and continually improving an information security management system.
2. To examine requirements provided by ISO/IEC 27001:2013 standard and determine how they can be transformed into software modules.
3. To design a software toolkit which consists of modules that guides an organization in implementing the requirements of ISO/IEC 27001 standard.
4. To implement, test and evaluate a software toolkit that validates an enterprise against the requirements of the standard.

1.3 Project Justification

As from Kenya Bureau of Standards information website there are only four organizations that are ISO/IEC 27001 certified. This is because, many organizations do not know the contents of the standard and the importance of managing information security. This is a gap that can be bridged. This research project seeks to bridge this gap by providing a tool that was meant to guide an organization on implementing the requirements of the standard.

Organizations security is vital for business operations, as well as retaining credibility and earning the trust of clients. Many of the investors also consider a boost in funding if provided with viable security controls plans. Thus, having a toolkit that provides a guide to implementing the necessary requirements provided by ISO/IEC 27001:2013 can give an enterprise a competitive advantage.

In addition, availability of new technologies that can enable development of a software tool which will enable organization manage their assets, processes and information is also a justification of conducting this study.

1.4 Scope of Study

This is project solely focused on implementing software modules that can be used to guide an enterprise against requirements provided by ISO/IEC 27001. The target organizations are the small-medium sized enterprises.

1.5 Assumptions and Limitation of Study

The requirements provided by the standard in Annex controls can be transformed into software modules and that the modules can be used to validate against an enterprise information security requirements implements.

The tool developed was limited to the requirements provided by the standard and that they could be converted into software modules.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

To determine the challenges faced by SMEs in getting certification for ISO/IEC 27001 standard and implementation of ISMS, a systematic review of existing literature on challenges and barriers of implementing ISMS was conducted. Therefore, this section explores related researches conducted on information security management systems on organizations. It also explores the concepts around ISMS and ISO/IEC 27001. The review aims at bringing out good insights into the concepts of information security, standards of information security, and effectiveness of utilizing an ISMS for by organization. The aim of the literature review is to build a foundation for the research questions identified for implementation of information security management system. Each step within the literature review is supported by searching existing literature and using the findings to aid logical reasoning.

2.2 Information Security

Information Security (InfoSec) refers to the processes and methodologies that are designed and enforced to safeguard print, electronic, or any other form of confidential, private and sensitive information from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption (Shirley P, 2006). InfoSec responsibilities embodies establishing a collection of business processes which will shield information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage.

A lot of huge organizations employ a dedicated information security group to implement and maintain the organization's InfoSec program. Normally, this group is led by a chief information security officer. The group is mainly responsible for conducting risk management, a process through which vulnerabilities and threats to information assets are continuously assessed, and the appropriate protective controls are decided on and applied. The worth of an organization lies within its information. Its security is crucial for business operations, along with retaining credibility and earning the trust of clients.

2.2.1 Principles of Information Security

A principle that is a key requirement of information security for proper and safe utilization, flow, and storage of information is the confidentiality, integrity, and availability (CIA) triad. They are the three major objectives of information security.

Figure (1) is an illustration of the CIA triad together with the four layers of information security. These four layers show the way systems communicate and how information flows among different systems. The layers illustrates that data communications and computer network protocols are designated to function in a layered manner, which transfers data from one layer to the next. Application Access Layer describes the notion that access to end-user applications must be constrained to business ought-to-know. The Infrastructure Access Layer describes the notion that access to infrastructure components should be constrained to business ought-to-know. he Physical Access Layer delineate the notion that the physical access to any system, server, computer, data center, or another physical object storing private information should be constrained to business ought-to-know. Data in Motion Layer outlines the notion that information ought to be secured while in motion. The little icon in the middle illustrates the center of information security and the reason for the emergence of the CIA principles; it represents information and the need to protect sensitive information.

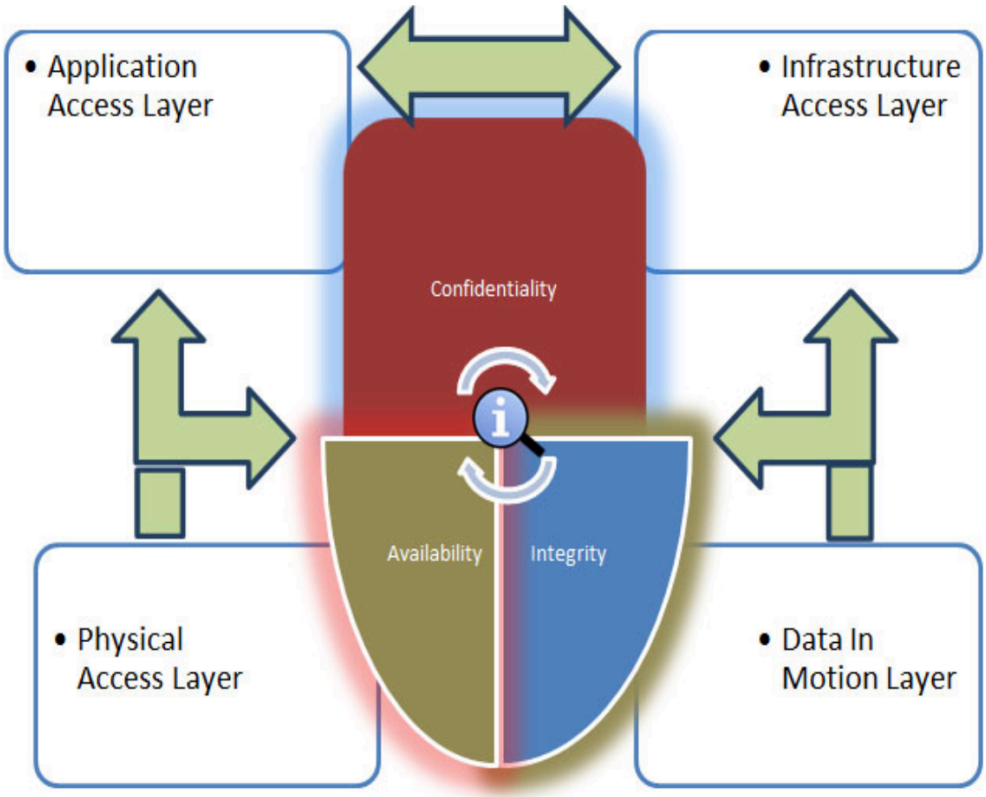


Figure 1 Principles of information security (source: https://resources.infosecinstitute.com/guiding-principles-in-information-security)

The goal of confidentiality is to make sure that information is concealed from people unauthorized to access it. Confidentiality principle decrees that information should exclusively be viewed by people with proper and correct rights. The science used to make sure information confidentiality is cryptography, which entails encryption and decryption techniques. Confidentiality can be easily breached therefore every employee in an organization should be aware of his responsibilities in maintaining confidentiality of the information delegated to them for the exercise of their duties.

Integrity involves maintaining accuracy and completeness of data. This means data cannot be modified in an unwarranted way. For instance, if an employee leaves an organization then in that case data for that employee in all departments like accounts, should be updated to reflect that the employee has let that role. This ensures that data is complete and accurate. In addition to this, only authorized individual should have rights to edit employee data.

Availability means information must be available when needed. For instance, if one needs to access all information of an employee, in that case it requires collaboration from different organizational teams like network team, development operations, incident response and policy/change management. Denial of service attack is one of the factor that can hamper the availability of information.

2.3 ISMS

An Information Security Management System (ISMS) is a set of policies and procedures defined by a company for systematically managing sensitive information to ensure that the principle of confidentiality, integrity and availability is adhered to (Cherdantseva & Hilton, 2013). The ISMS idea was first described by Edward Humphreys in his triumphant attempt to develop the first ISMS standard –BS 7799 issued in 1995 by the British Standard Institute (BSI) as a code of practice of information security management (Humphreys, 2011). Following on from this the UK launched the BS 7799 ISMS certification scheme to increase the awareness of this ISMS standard. Thus, by the end of 1999 more than 20 countries had adopted this standard and the number of certified organizations had been significantly increased (Humphreys, 2011).

Apart from BS 7799 standard, many ISMS standards and frameworks have been published. Some examples include ISO 27001, PCI DSS, ITIL and COBIT (Susanto et al., 2011). For each standard, there are many implementation guidelines for organizations to choose depending on the nature of

business, information security maturity level, company size and budget. However, ensuring organizational compliance with one of these standards or frameworks is challenging. Recent research indicates that some of these standards and frameworks are not well adopted (IT Governance, 2016). It is noted that, in a recent survey from 319 IT security decision makers at companies with more than 100 employees, only less than half have been compliant with ISMS standards for more than a year (Dimensional research, 2016). To help organizations effectively establish, implement and maintain ISMS, many studies (Rocha Flores et al., 2014; Barton et al.) have analyzed the key factors that may affect ISMS within organizations, such as information security awareness, effective risk analysis, positive management, knowledge sharing, and organizational culture. Barriers to ISMS implementation have been stated, such as low knowledge of applicable standards and frameworks, lack of management commitment, misconceptions on cyber-attack targeting SMEs, limited budget, standard complexity, resistance to change, lack of enough software tooling on the standards, and inadequate academic publications (Fomin et al., 2008).

2.4 ISMS Standards and Frameworks

This section gives an overview of most common ISMS standards and frameworks. The ones reviewed are ISO 27001, PCI DSS, COBIT and ITIL. The overview includes profile, purpose and function for each standard in implementing ISMS for organizations.

2.4.1 ISO/IEC 27001

The International Organization for Standardization (ISO) is a global body that collects and manages various standards for different disciplines. In today's world, with so many industries now reliant upon the internet and digital networks, more and more emphasis is being placed on the technology portions of ISO standards.

The ISO 27001 standard is designed to function as a framework for an organization's information security management system (ISMS). This includes all policies and processes relevant to how data is controlled and used. This standard does not mandate specific tools, solutions, or techniques, but instead functions as a compliance checklist.

This standard is applicable to all types of organizations, all sizes, all industries and markets (ISO, 2013). It introduces a series of security process based on the well-known "Plan-Do- Check-Act"

(PDCA) model (Figure 2), which is a continuous improvement process that requires organizations to review their ISMS regularly to ensure the effectiveness (Humphreys, 2011; Susanto et al., 2011).

The purpose of the standard of ISO/IEC 27001 is to provide an approach that "based on a business risk approach, to establish, implement, operate, monitor, review, maintain and ISMS was first introduced within the standard of BS 7799-1 written by the Department of Trade and Industry (DTI) in the late 80's and then issued by the BSI in 1995. The BS 7799-2 was published in 1999, titled "Information Security Management Systems – Specification with guidance for use". Following its approval for publication as ISO/IEC 17799 in October 2000, BS 7799-1 became a member of the ISO/IEC as a code of practice for information security management. It was then renumbered as ISO/IEC 27002 in 2006. This happened after the introduction of BS 7799-2, which was then published as ISO/IEC 27001 in November 2005 (Humphreys, 2011). The main difference between ISO/IEC 27001 and ISO/IEC 27002 is that ISO/IEC 27001 only provides a prescription of the features of an effective ISMS, while ISO/IEC 27002 gives instructions and guidance on how to conduct the standard (IT Governance, 2013).

This standard is applicable to all types of organizations, all sizes, all industries and markets (ISO, 2013). It introduces a series of security process based on the well-known "Plan-Do- Check-Act" (PDCA) model (Figure 2), which is a continuous improvement process that requires organizations to review their ISMS regularly to ensure the effectiveness (Humphreys, 2011; Susanto et al., 2011).

The purpose of the standard of ISO/IEC 27001 is to provide an approach that "based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security" (Calder, 2011). The effectiveness of complying with ISO/IEC 27001 for organizations is preventing or minimizing the exposure to information security threats.

The core of this standard is information security risks assessment and management (IT Governance, 2017). A quantitative study identifies that companies compliant with ISO /IEC 27001 gain an improved risk based approach to information security management (Sharma & Dash, 2012). Related study on the cost-benefit analysis of an ISMS based on ISO/IEC 27001 through a comparison of the Key Performance Indicators of effectiveness and efficiency showed that an ISMS based on ISO/IEC 27001 is equivalent to risk management (BOEHMER, 2009).

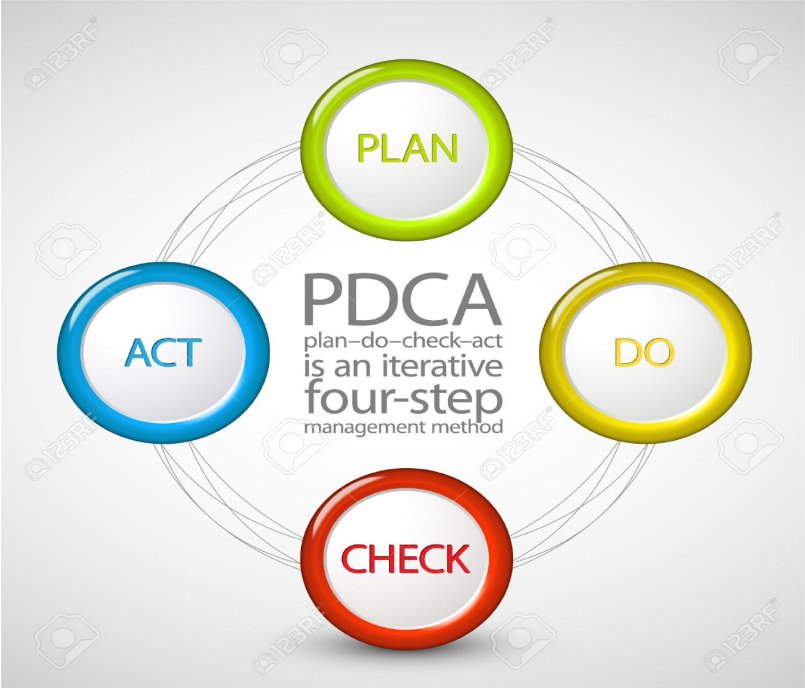


Figure 2: PDCA (source: https://www.123rf.com/photo_14226252_pdca-plan-do-check-act-diagram-schema.htm)

2.4.2 COBIT

The Control Objectives for Information and related Technology (COBIT) is a collection of best practices for information technology governance created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI).

COBIT gives information auditors, top management and general Information Technology users with a collection of generally accepted procedures, indicators, processes and best practices to help them in maximizing the benefits derived using information technology. It also helps in developing appropriate IT governance and control in a company. COBIT purpose is to investigate, come up with, reveal and foster an authoritative, up to date, global collection of by and large accepted information technology control objectives for everyday use by business stakeholders. These individuals benefit from the development of COBIT because it helps them understand their Information Technology systems and in making decisions on the level of security and control that is necessary to protect their companies' information assets through the development of an IT governance model. COBIT can be widely applied to various purposes. It covers security in addition to all the other risks that can occur with the use of IT.

COBIT has the following five main principles: Strategic alignment; Value delivery; Resource

management; Risk management; Performance measurement (Susanto et al., 2011). It also consists of 34 IT processes to contribute to effective internal controls over the reliability of financial reporting. An international survey of professionals indicated that some of these IT processes were critical for effectively governing internal IT environment via internal IT controls.

In 2012, the new version of COBIT was released by ISACA, called by COBIT 5. It helps organizations meet performance and compliance requirements. COBIT 5 is aligned with some well-known frameworks, such as ITIL, ISO/IEC 20000 and ISO/IEC 27001 (Radhakrishnan, 2015). It provides a comprehensive IT governance framework that "assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT" (Nugroho, 2015). It also has 5 key principles to improve the performance of IT to ensure that IT delivers business value (Radhakrishnan, 2015) (Figure 3).

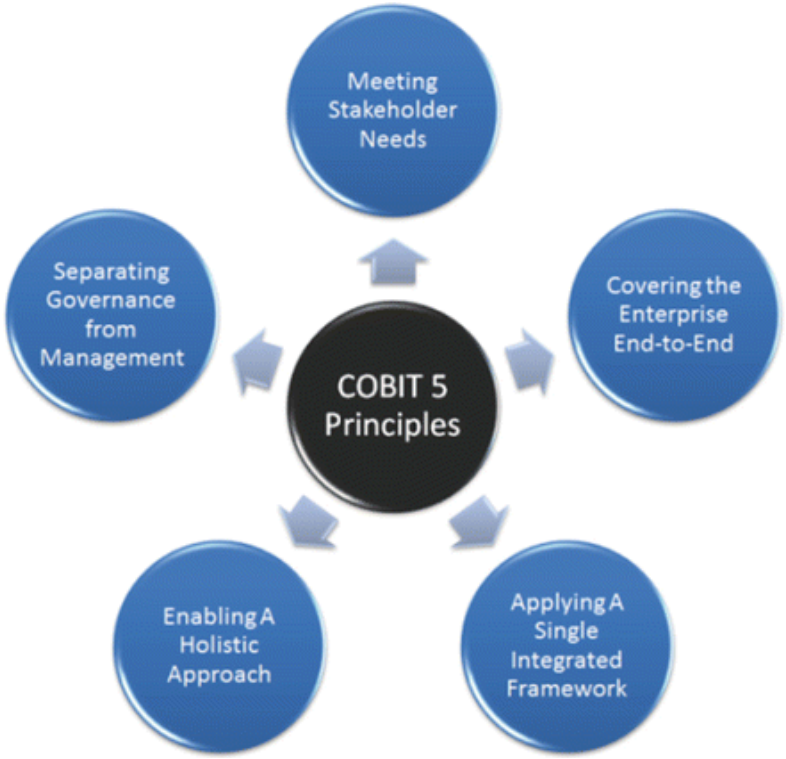


Figure 3 COBIT 5 Principles (Source: ISACA, COBIT 5, USA 2015)

2.4.3 PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted proprietary information security standard defined by the Payment Card Industry Security Standards Council

that is managed by major credit card brands (American Express, Discover, JCB, Visa, and MasterCard). PCI DSS is regarded as a key benchmark determining if a company has adequate security countermeasure to protect the cardholder data. Extensive industry rules are included in PCI DSS, which are updated regularly to reflect the latest best practices (Ramsey, 2016). These industry rules are related to the following main areas: Network and Systems; Protection of Cardholder Data, Vulnerability Management Program, Access Control, Monitoring and Testing of Networks, and Information Security Policy (Ukidve et al., 2017).

The purpose of this standard is to help entities process, store or transmit cardholder information in a secure environment, reduce the risk of compromised credit card data, protect the confidentiality of cardholder data, and to prevent credit card fraud (Ramsey, 2016).

2.4.5 ITIL

The Information Technology Infrastructure Library (ITIL), which was introduced by the Office of Government Commerce (OGC) in the UK in the late 1980s, is a set of concepts and practices for IT service management (ITSM) that focus on aligning IT services with the needs of the business. At present, it is the most widely accepted approach to IT service management in the world (AXELOS, 2017).

The ITIL framework consists of five service delivery processes, five service support processes and one service support function (service desk). The five service delivery processes are Service Level Management (SLM), Financial Management, Capacity Management, IT Service Continuity Management, and Availability Management. The five service support processes are Incident Management, Problem Management, Change Management, Release Management, and Configuration Management (Cater-Steel, 2006).

2.4.4 The ISF Standard of Good Practice for Information Security

The latest edition of the Standard of Good Practice for Information Security 2018 provides business-orientated focus on current and emerging information security topics. This entails supplemented coverage of the following interesting themes: Agile system development, alignment of information risk with operational risk, collaboration platforms, Industrial Control Systems (ICS), information privacy and threat Intelligence

Accompanied by its all-embracing coverage of information security controls and information risk-related enlightenment, it lays out business leaders and their teams with a globally recognized collection of good practices. If the standard is implemented properly, the organization will have the following benefits: helps the company to be agile and exploit new opportunities, ensuring that associated information risks remain inside bearable levels, responding to briskly evolving threats, encompassing complex cyber-attacks, using threat intelligence to increase cyber resilience and identify how regulatory and compliance requirements can best be met.

The Standard provides complete coverage of the topics set out in ISO/IEC 27002:2013, PCI DSS, NIST Cyber security Framework, CIS Top 20, and COBIT 5 for Information Security. ISF Benchmark and the ISF's comprehensive security control assessment tool also provide those benefits.

The Standard acts as a business enabler for individuals performing the following roles: CISOs, Information Security Managers, Risk Management Specialists, Business Managers, IT Managers and Technical Specialists, Internal and External Auditors, IT Service Providers, Procurement and Vendor Management teams.

2.3 Related Work

2.3.1 Information Security for SMEs based on Resource-Based View

Bleerton et al proposed an approach where the focus was to analyze implementation challenges, benefits and requirements in implementation of Information systems and managing information security in small and medium sized companies. The study tethers information security with the resource-based theory of firms, reason being, information security investments are considered as part of general ICT investments and therefore resource-based view being appropriate.

The study suggests that investing in security resources will improve business processes or may enable new ones. This is because the information security process is intended to protect businesses and their resources. Information and Communication Technology business value generation process, including resources, processes, business and security performances, directly impacts on organizational performance. The study also emphasizes on the fact that SMEs face barriers in IT adoption. SMEs are strongly influenced by standards and culture within the industry sectors when it comes to implementing information security. Some operate on the knowledge of few key

personnel and therefore the need for ISMS is not vital. However, for an organization to stay competitive then it is crucial for them to secure their valuable information about their product and divorce their practices from being closely intertwined with the presence of specific individuals.

For future work the study suggests that there is a need for SMEs to build their information security strategy and infrastructure. Building on the recommendations of their study, this study builds a toolkit which can be availed as a Software as a Service (SAAS) to help SMEs streamline their information security management programs in conformity with the requirements of ISO/IEC 27001 (ISMS) standard.

2.3.2 A toolkit for information security awareness and education

Peter K. et al in their study proposed an Information Security Toolkit that was geared towards providing security awareness and education. The main objective was to establish security knowledge and skills to all users of technology in organizations, especially among SMEs which cannot have adequate resources in terms of both financial and human capital to mount effective information security management system.

Towards the development of the toolkit, several learning theories were taken into consideration to create a piece that is user-friendly and at the same time achieves learning retention. The toolkit was created as a successful learning experience geared towards all generations by incorporating a variety of activities that utilize all learning styles.

Having developed a working prototype of the toolkit, the research could make an initial evaluation of its effectiveness. This was achieved by testing the toolkit using four representative groups of users, a group of students at different stages of their education cycle, a group of administrative staff, a group of experts involved in learning processes and a group of IT Experts. It is concluded that the security toolkit was a valuable resource to establish a sufficient level of security awareness amongst the online population.

There was a proposal to further enhance the toolkit by including additional topics so from a working prototype it evolves to a complete set capable of assessing and establishing an appropriate level of awareness.

2.3.3 Analysis of ISO 27001 implementation for Enterprises and SMEs

Candiwan did a survey on Implementation of information security management. The focus was to determine the readiness for both large companies and SMEs in obtaining certification of ISO 27001:2013 standard in developing countries.

Results showed that implementation of the standard main clause's requirements in large enterprises is more than in SMEs. Furthermore, the study found out that the number of controls that fulfil the requirements of ISO 27001:2013 for large enterprises are more than SMEs, however the number of controls that are partially compliant and not compliant for large enterprises are less than the number of controls for SMEs.

In summary, this study provided insights about the position of large organizations and SMEs on implementing controls provided by the standard. However, it has not provided ways in which these organizations can implement those requirements. Our study is hinged on bridging this gap by providing a toolkit that will assist SMEs to have a simpler way of implementing the required controls as well as being able to evaluate their level of compliance.

2.3.4 CertiToolKit for ISO 9001

ISO 9000 standard family addresses various quality management aspects. It includes some of the best-known standards of ISO. The standards provide recommendations and mechanisms for organizations that want to ensure that clients' requirements are consistently met by their products and services and that quality is improved consistently.

ISO 9001:2015 provides a collection of quality management system criteria and is the only family standard that can be certified to. However, it is not mandatory. Any enterprise, large or small, can use it irrespective of its field of activity.

The standard is based on various principles of quality management including strong customer focus, motivation and involvement of top management, process approach and ongoing improvement. The use of ISO 9001:2015 helps ensure that customers receive consistent products and services of good quality, which in turn brings many business benefits.

CertiToolkit for ISO 9001 is a set of customizable templates that industry experts have written to help organizations produce documentation that meets quality management system standard requirements.

2.3.5 ISO 9001:2015 Documentation Toolkit

This is a documentation toolkit provided by Advisera company. It aims at providing guidance on implementation of ISO 9001:2015 requirements. It provides access to all documents required by ISO 9001 certification, plus commonly used non-mandatory documents. The toolkit is provided at a fee to whoever is interested.

This is a proof that in deed a toolkit that consists of requirements of a standard can guide an organization in getting certified against that standard.

2.4 Summary of the literature and the Gap

Without information security small organizations are faced with various information risks resulting in financial loss, reputation damage, and regulatory noncompliance caused by ineffective information security management. In this literature review a summary of what information security entails is presented. A summary of most popular ISMS standards and frameworks, such as ISO 27001, PCI DSS, COBIT and ITIL, is also presented. Although all of them are information security related standards or frameworks aiming at protecting critical informational processes within organizations, functions and purposes of them are different: ISO 27001 is an information security framework based on business risks; PCI DSS is an information security standard released by the Payment Card Industry Security Standards Council to protect cardholders' data; COBIT is an IT governance framework which is created to map IT processes; ITIL is a good practice for IT service level management.

In line with the main objectives of the research, a systematic review of existing literature was conducted to explore the requirements provided by ISO/IEC 27001:2013 and the importance of information security to an organization. It was noted that many SMEs lack enough knowledge about information security standards and that they lack financial resources to implement necessary controls to protect themselves against cybercrimes. Some software tools exist but they are too expensive to them.

Since it has not been proved by existing literature whether these SMEs are willing to use a software tool that validates against the requirements of ISO/IEC 27001, this study will cover the gap to explore if a software tool with modules that addresses the requirements of the standard can be of importance to them.

2.5 Conceptual Framework

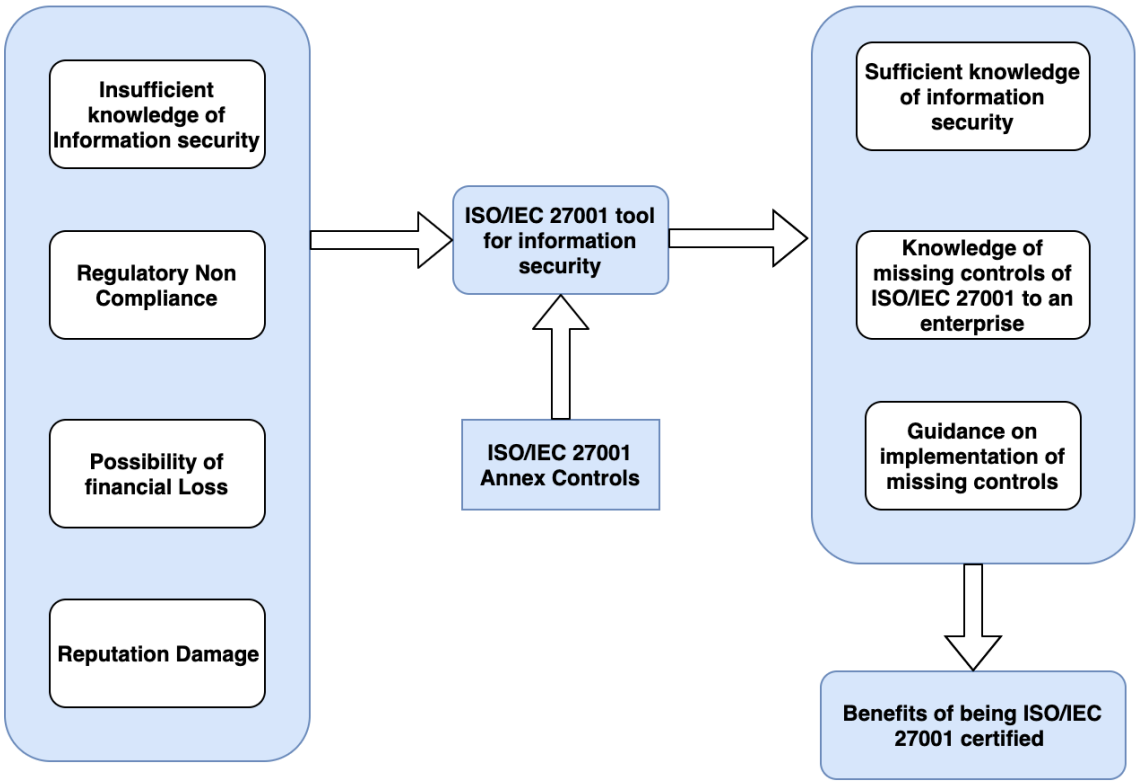


Figure 4: Conceptual framework

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

Research methodology is described as a systematic way of looking for solutions. It's a scientific way of doing an investigation that is aimed at arriving at some findings (Kothari, 2004; Rajasekar et al.., 2013). It indicates the pathway through which researchers construct their problem, objectives and present their result from the data obtained during the study period. Design science research on the other hand, is an outcome based information technology research methodology, that provides specific instructions for assessment and iteration within research projects. Its center of attention is on the invention and performance of artifacts with the explicit intention of improving the functional performance of the artifact.

The main goal of this research was to demonstrate that small and medium sizes enterprises can comprehensively implement the prescriptive requirements of the ISO/IEC 27001:2013 standard. The study sought to implement a software toolkit that consists of the requirements provided by the standard. Organizations were to use the tool to identify areas in which they have not adhered to the standard. Various reports are generated by the tool to give more insights of what has not been implemented, thereby, enabling an organization to be able to implement the missing pieces of information security practices that ISO/IEC 27001:2013 stipulates. Since the research was about designing a solution that can help organization in securing their information, design science research methodology will be adopted.

This section describes how the research was done to achieve the stated research objectives using design science methodology. It describes five steps of the design science methodology, together with activities that were conducted on each step.

3.2 Research Design

As mentioned earlier, a design science research (DSR) approach was adopted to design, build, and evaluate a software toolkit for ISO/IEC 27001. Therefore, this research used the DSR process model by (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007) to produce and present the research. This consisted of five process elements: 1. Identifying the Problem; 2. Defining Objectives of a Solution; 3. Design and Build; 4. Evaluation; 5. Communication. These process element titles are used to present the activities that were carried out in each section, with clear explanations of what they entailed.

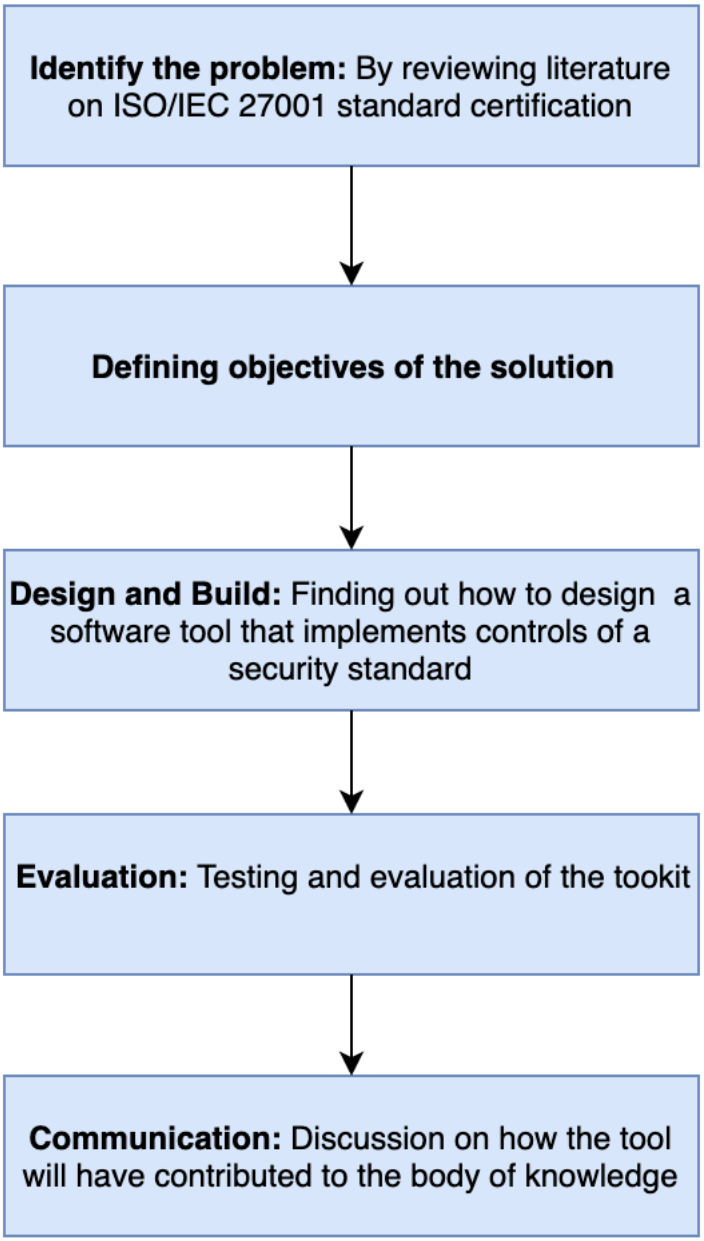


Figure 5: Research process based on DSR model

3.2.1 Identifying the problem

This phase involved reviewing the literature on information security standards and challenges faced by SMEs in getting certifications for those standards. Key outputs of this phase were;

i. Understanding of the challenges faced by SMEs in protecting their information

ii. Identified the standards which can guide organizations in protecting their information
iii. A problem statement of this study
iv. A review of ISO/IEC 27001 standard

3.2.2 Defining Objectives of the Solution

Stating the objectives for the research was necessary to provide focus (Peffers et al., 2007). Hence, this was the next phase of this research. It involved analyzing the problem identified and coming up with objectives that are specific, measurable, attainable, relevant and time-oriented. The output of this phase were the objectives defined on section 1.3.

3.2.3 Design and Build

In this phase the researcher designed and implemented the toolkit. During the designing process, the researcher first did an exploratory study, focusing on understanding the requirements of the ISO/IEC 27001 standard. This facilitated the scoping of the tool in terms of specifying the modules that were to be implemented.

During this cycle, prototyping development approach was used, described below;

3.2.3.1 Iterative Prototyping Development Approach

Software prototyping, refers to the process of developing a throw-away version of software application to validate the key functionality or idea of the system architecture. A prototype typically mimics only a main aspect of the application, avoiding bells and whistles and as such can use different, higher level implementation language than the final product.

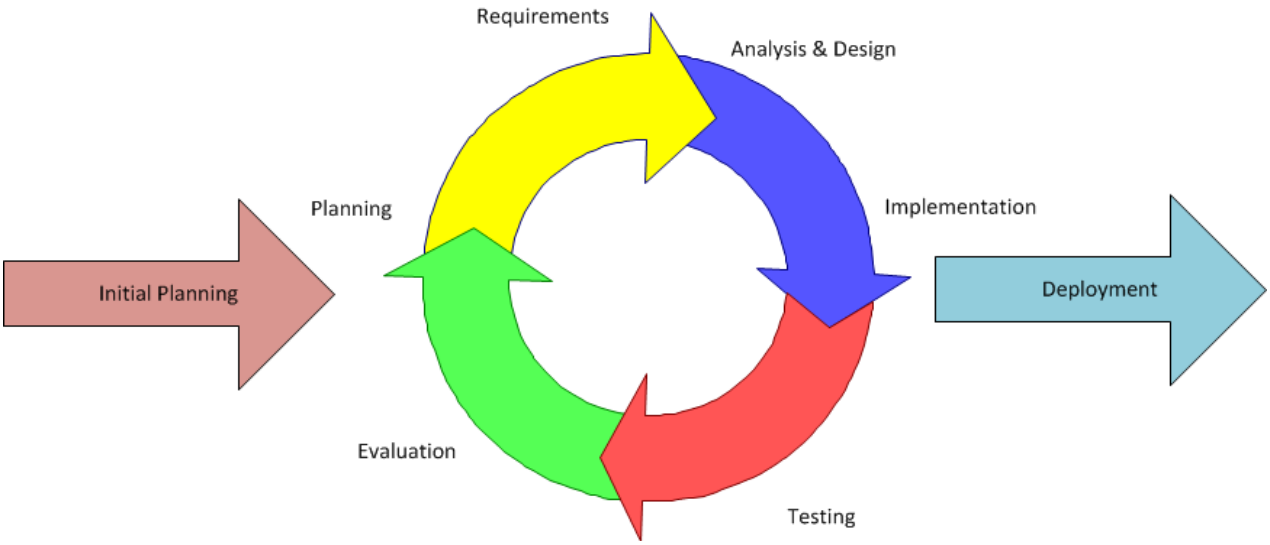


Figure 6: Prototyping process

This toolkit was developed using prototyping development process. This approach was preferred as it generates working software quickly and early in the software development life cycle, more flexible, and easier to test, debug and evaluate during a small iteration.

3.2.4 Evaluation and Testing of the toolkit

At this phase the developed tool will be tested and evaluated. During testing, both the integration and unit tests will be executed to determine whether the tool developed will be working as expected. Thereafter there will be user testing, whereby real users will have a chance to interact with the toolkit.

3.2.5 Communication

DSR needs to make contributions to both practice and the knowledge base for it to be considered DSR, and separate it from the mere task of developing artefacts (Hevner, 2007). The primary contribution of this research, to both the knowledge base and to practice, will be presented in terms of reports about how the tool will perform in guiding enterprises in implementing missing requirements for the standard.

3.5 Source of Data

Since the study was typically about developing a software tool that has requirements for ISO/IEC 27001:2013 standard, therefore there was need to get a genuine documentation that provides details about the standard. This was acquired from British Standards Institution (BSI). The institution provides a softcopy version of the standard's requirements at a fee.

3.6 Data Collection

There was physical interaction with the developed tool, thus data was gathered in person via observations. Testing of the tool and examining reports generated by it was also another way of data collection.

Data was also collected using google forms questionnaires. These questionnaires were send to individuals who had a chance to see how the toolkit works.

3.8 Data Analysis and Evaluation

The analysis of observed results was done manually, whereby the summarized recordings of the observer was analyzed. Observation paper templates which were used during data collection were key in providing the information needed to be analyzed.

3.9 Limitation of Data Collection and Analysis Methods

The main methods that were used during data collection were, doing an actual test of the tool and observation of the outputs. The limitations with these methods were checking validity of the output and personal bias. To avoid personal bias the researcher used several individual to test the tool. On checking validity of the output, the researcher wrote automated unit and integration tests that did validations.

CHAPTER 4: SYSTEM ANALYSIS AND DESIGN

4.1 Introduction

This chapter primarily describes processes that were carried out to come up with the software toolkit. These processes included doing system analysis, system design and coming with the architecture of the toolkit.

4.2 System Analysis

This is a process that decomposes a system into its component pieces for defining how well those components interact to accomplish the set requirements. The main activities that were carried out are outlined below.

4.2.1 Feasibility Study

Feasibility study was carried out to determine whether the project was worth undertaking by considering its benefits. A questionnaire was created and shared with information security specialists of different SMEs. Results of the questionnaire are analyzed below. Types of feasibility considered:

4.2.1.1 Operational Feasibility

Operational feasibility determined whether the system would adequately solve the problem being addressed. Here are some questions that needed to be answered in this feasibility:

i. What problem was the system trying to solve?
ii. To what extend would the system solve the problem?
iii. Is the solution acceptable?
iv. Are the system users willing to use the system?
v. Was the system going to achieve the research objectives of this study?

It was later established that the level to which the system tries to solve the problem and answer research questions was sufficient. It could not be conclusively established if users would be willing to use the system.

4.2.1.2 Technical Feasibility

Technical feasibility was carried out to determine whether the level of available software and hardware technology was sufficient for the development of the system. It also determined whether

the project team had sufficient knowledge of developing the system. Here are some questions needed to be answered in this feasibility:

i. What hardware and software tools are needed for the project?
ii. How would the tools be acquired?
iii. Was the level of knowledge and skills sufficient for the successful completion of the project?

It was later established that tools required in the development and deployment of this project were readily available. Some tools were provided freely on the internet while others were readily available.

4.2.1.3 Economic Feasibility

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

4.2.2 Requirement Elicitation

This section involved using the results of the domain problem to define the functional and non-functional requirements. The interviews, discussions and review of existing documents were all taken into consideration.

4.2.2.1 Functional Requirements

The system was meet the following functional requirements.

i. The toolkit should be able to provide information about the standard
ii. It should be able to capture details about an organization's implementation status of an annex control.
iii. The system should be able to do risk analysis of possible security threats posed by lack of implementing certain controls of the standard.
iv. The system should be able to keep vital information security assets' information.

4.2.2.2 Non-Functional Requirements

These requirements are not the core functionality of the system. However, they play a role in ensuring a better presentation of functional requirements. The system should meet the following non-functional requirements:

- Accuracy: This would ensure that the system can schedule and keep correct daily activities

- Speed: The system should have optimal speed.

- Efficiency: The system should be ensuring economical utilization of computer resources by its modules.

4.2.3 System Analysis Models

4.2.3.1 Use Case diagram

These are diagrams were used in analysis phase to identify and split functionality of the toolkit. There are made up of actors and use cases. An actor represents various external people or entities that interact with the system.

The use cases of the system consisted of several group of users; system admin and information security auditors.
Activities carried out by the system admin.

- Login
- Add annex controls
- Create organizations and assign users

Activities carried out by information security auditor.

- Login
- Validate annex controls for an organization
- Analyze risks and treatment activities
- View documentation

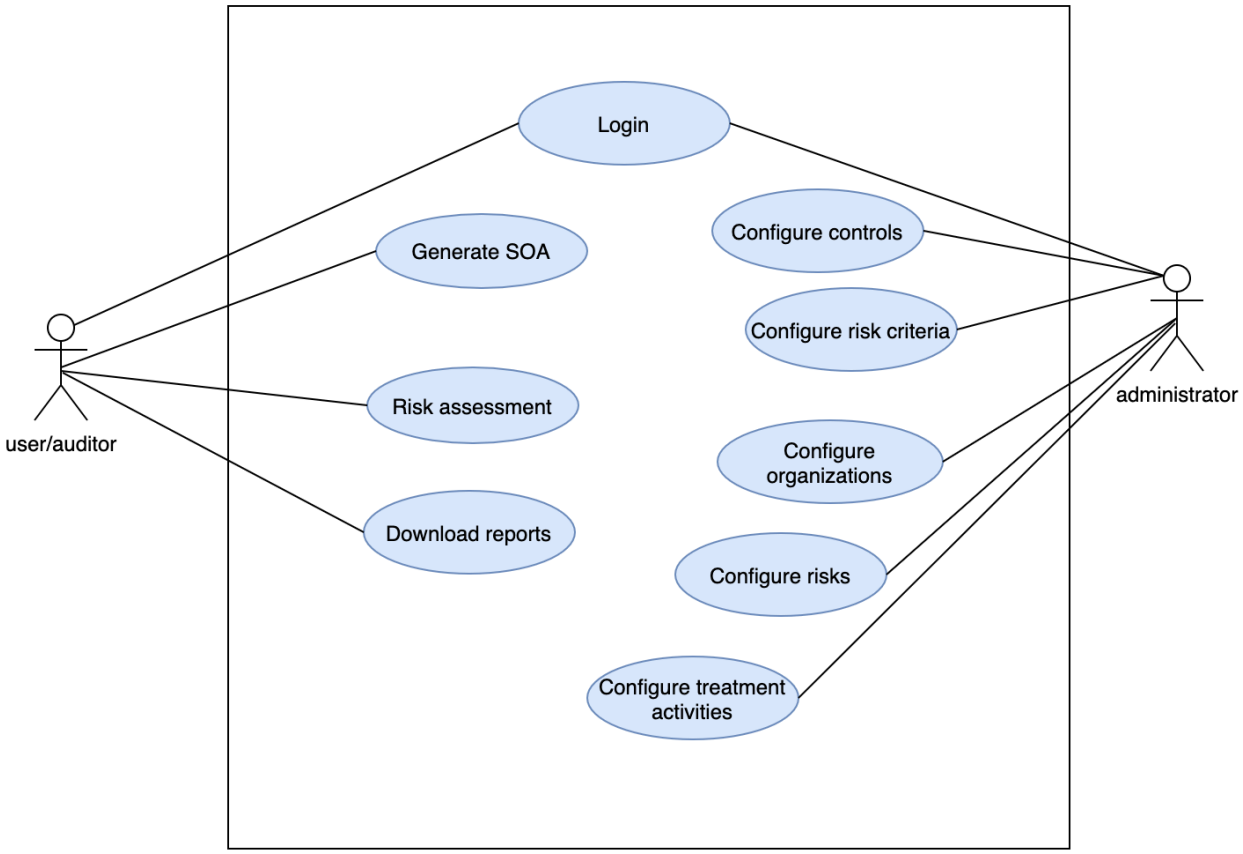


Figure 7: Use case diagram

4.2.3.2 Data Flow Diagrams

These diagrams show how data flow through the system and the processes that act on the data. They show how various data supplied by users are processes and finally stored in the database. The below diagrams show the process of data flow for this system.

i. Context Diagram

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

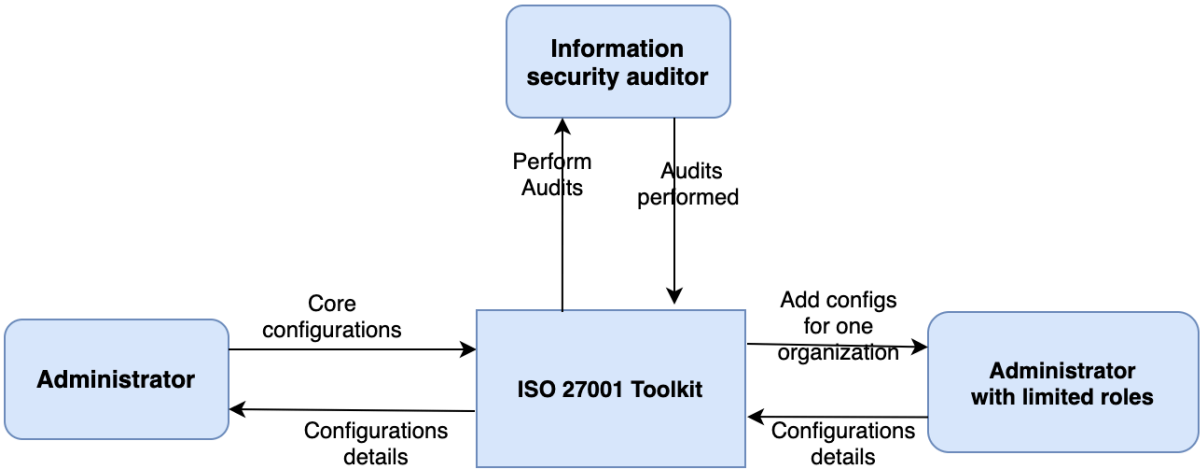


Figure 8: DFD Level 0

ii. DFD Level 1 Diagram

The figure below shows the decomposition of the toolkit usage processes. It shows some key data flow processes that takes place.

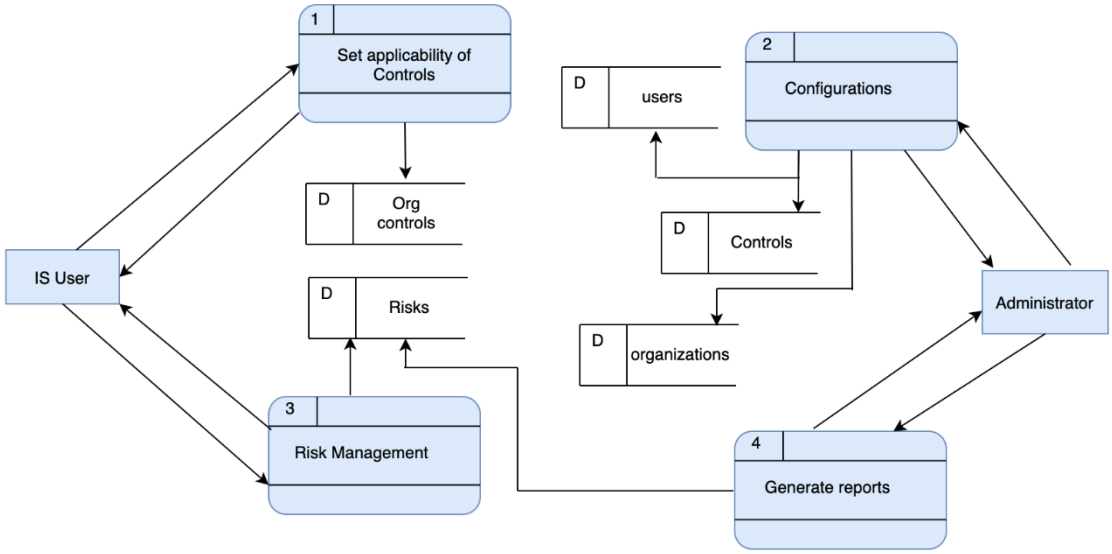


Figure 9: DFD Level 1 for toolkit

4.3 Toolkit Design

System design usually involves the process of designing the elements of a system such as the architecture, modules and components, the different interfaces of those components and the data that goes through that system. Its purpose is to provide sufficient detailed data and information about the system and its system elements to enable the implementation consistent with architectural entities as defined in models and views of the system architecture.

The aim of ISO/IEC 27001 certification is to effectively establish and manage an Information Security Management System (ISMS). The ISMS according to ISO/IEC 27001 standard is built around a Plan Do Check Action (PDCA) model which has an objective is a continual improvement of information security. Therefore, the toolkit was designed to conform to this model by providing modules that would enable an organization to plan for information security strategies, identify possible risks, come up with mitigation plans and acting on those plans. Moreover, the design also considered main clauses provided by the standard, and majority of those clauses were implemented as separate modules as shown in Figure 10.

The first module provided a summary of the standard. It highlighted all the ten sections of the standard and giving a summary of what each section required. Context of the organization was captured by the next module. It enables an organization to manage external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcomes of its ISMS. External and internal interested parties are also managed by this module. There was another module that handled planning and operation. It enabled an organization to determine its information risks and opportunities, do risk assessment and risk treatment planning.

Figure 10: Toolkit Modules

Statement of applicability module was designed to enable an organization to identify where it stands on the 114 controls provided by the standard. Internal Auditing module enabled an organizations to conduct internal audits at planned intervals to provide information on whether it conforms to the requirements provided by the standard and how far it stands on effectively implementing those requirements. Reporting feature on the toolkit was designed to generate reports on risks, management review reports and statistics of implemented controls.

A client-server model was leveraged. It is a popular model that is made up of a client and a server, whereby clients send requests while servers responds to those requests. Client-server system was chosen in this study because it increasingly minimizes application development time by dividing function of sharing information in both the client and the server. Data processing is majorly handled by the server and the results returned to the client

Several other activities were carried out during the design phase of this toolkit. These involved coming up with a toolkit architecture, database design, user interface design and infrastructural design.

4.3.1 Conceptual Toolkit Architecture

During this phase, the toolkit architecture was also designed. A system architecture usually a conceptual model that defines the structure, behavior and more views of a system. It is a formal description and representation of a system, organized in a way that supports reasoning about the structures of the system. The architecture was divided it into three tier design approach; presentation layer, business logic layer and data layer.

As shown in Figure 11, presentation layer is web based and we leveraged the use of material design, which is a modern software design language that provides principles and concepts of developing realistic and pleasing user interface components. It is platform and language independent. React JavaScript framework was also used to implement component based declarative views which are intuitive to users.

Business logic layer comprised of core logic of the toolkit. It exposed Application Programming Interface (APIs) for creating, updating and deleting records. This layer was developed using Python programming language and Django Model-View-Controller framework.

The data layer had Database Management System (DBMS). PostgreSQL was used because it provides a lot of features aimed to help developers build applications, administrators to protect data integrity and build fault-tolerant environments

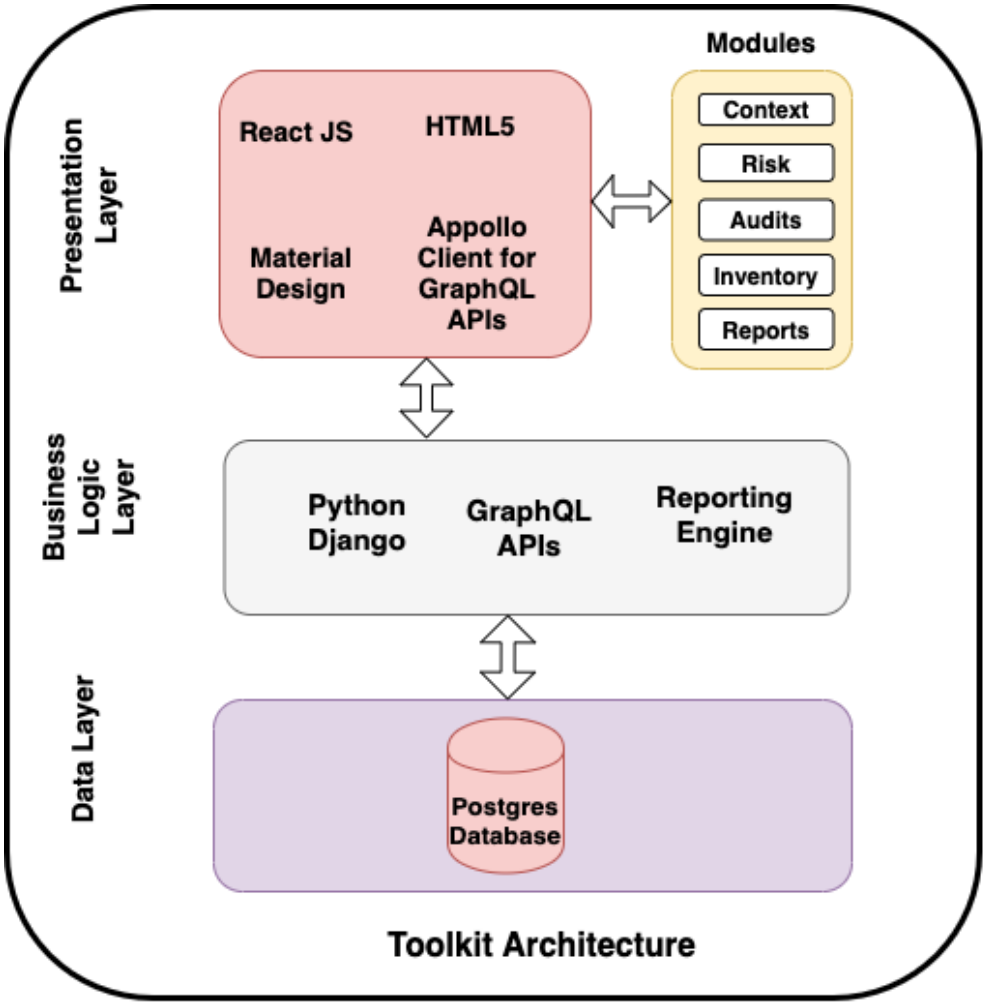


Figure 11: Conceptual Architecture

4.3.2 Database Design

Database design is the organization of data per a database model. The designer determines what data must be stored and how the data elements interrelate. With this information, they can begin to fit the data to the database model. Database management system manages the data accordingly. As shown on the conceptual design the database engine used on this toolkit was postgres relational database. Information about standard's controls, organizations, users, risks and inventories are stored in this database. Below is the entity relationship of the database.

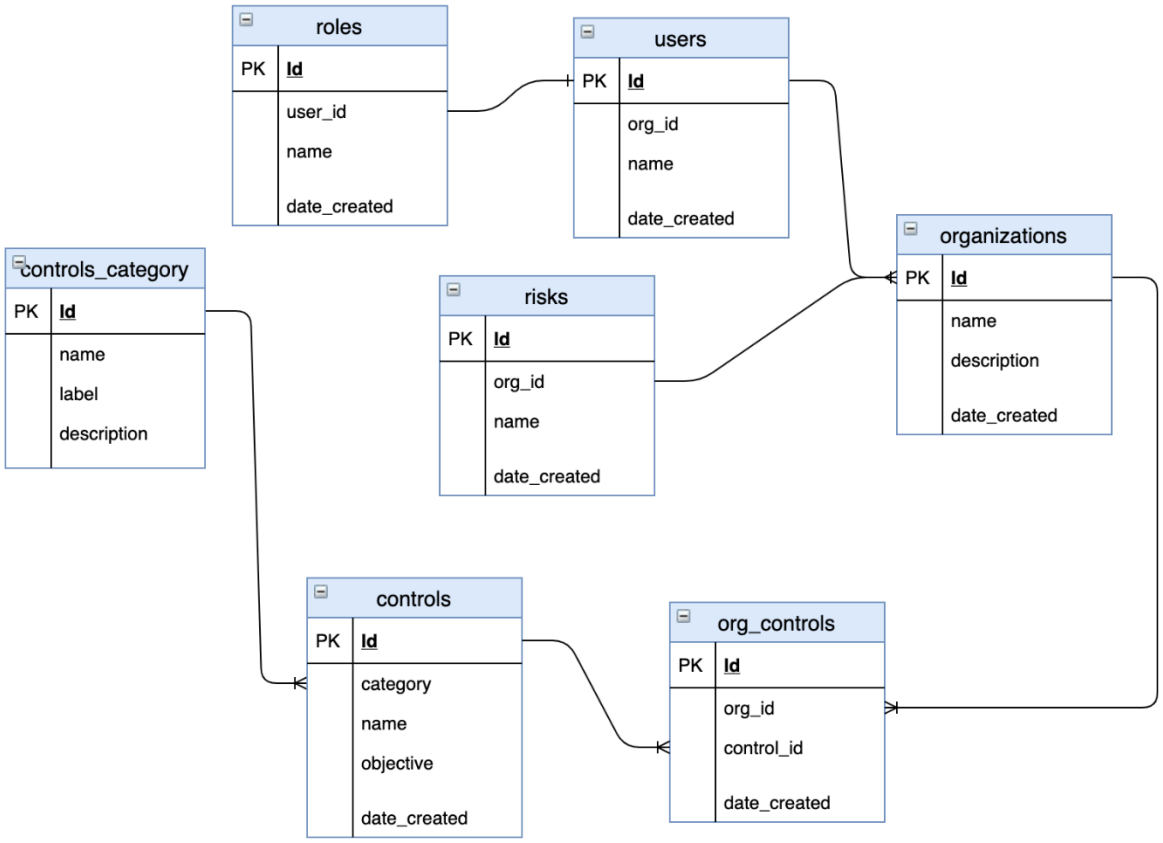


Figure 12: ERD Diagram

4.3.3 User Interface Design

User interface design more often than not have to do with the visual layout of the elements that users of a system might interact with in a technological system or product. This might be the input forms, tables, buttons or the visual structure of a webpage. These designs are meant not only to be appealing to potential users, but must also be functional and created with users in mind.

User interface design can extensively influence the usability and user experience of an application. If the design is too sophisticated or not tailored to targeted users, thy may not be able to find the information they are interested in. In web interface design, this might affect the number of users visiting it. The layout of a user interface design should also be clearly aimed to users so that interface components could be found in a logical position.

For this toolkit, the choice for user interface was based on a thorough investigation on usability and aspects that user like in a page. It was optimized so that user could operate on it quickly and

easily. Many experts believe that UI design should be simple and intuitive. Therefore, that was what was key on designing the toolkit interface. Below are the designs that were developed;

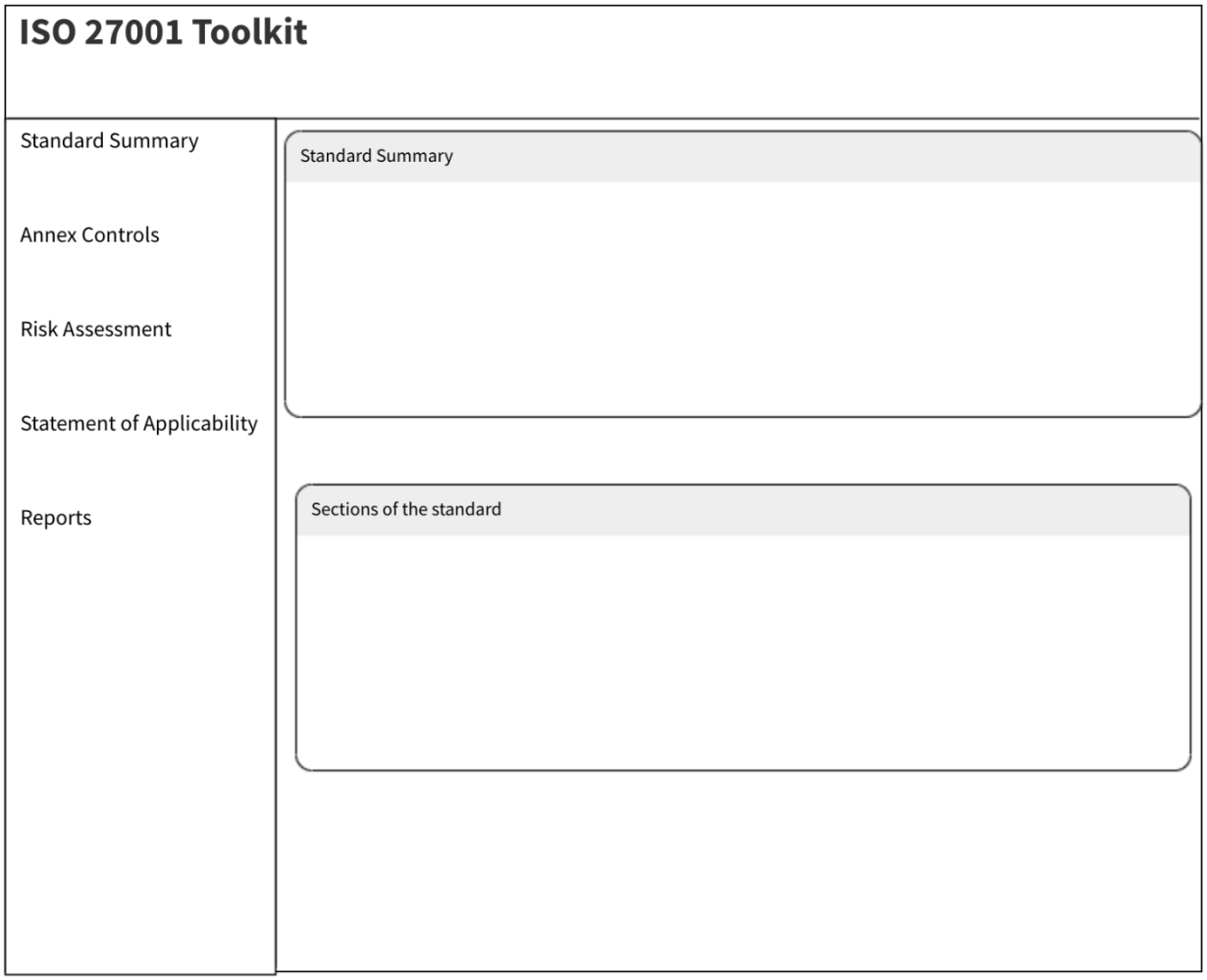


Figure 13: First Page

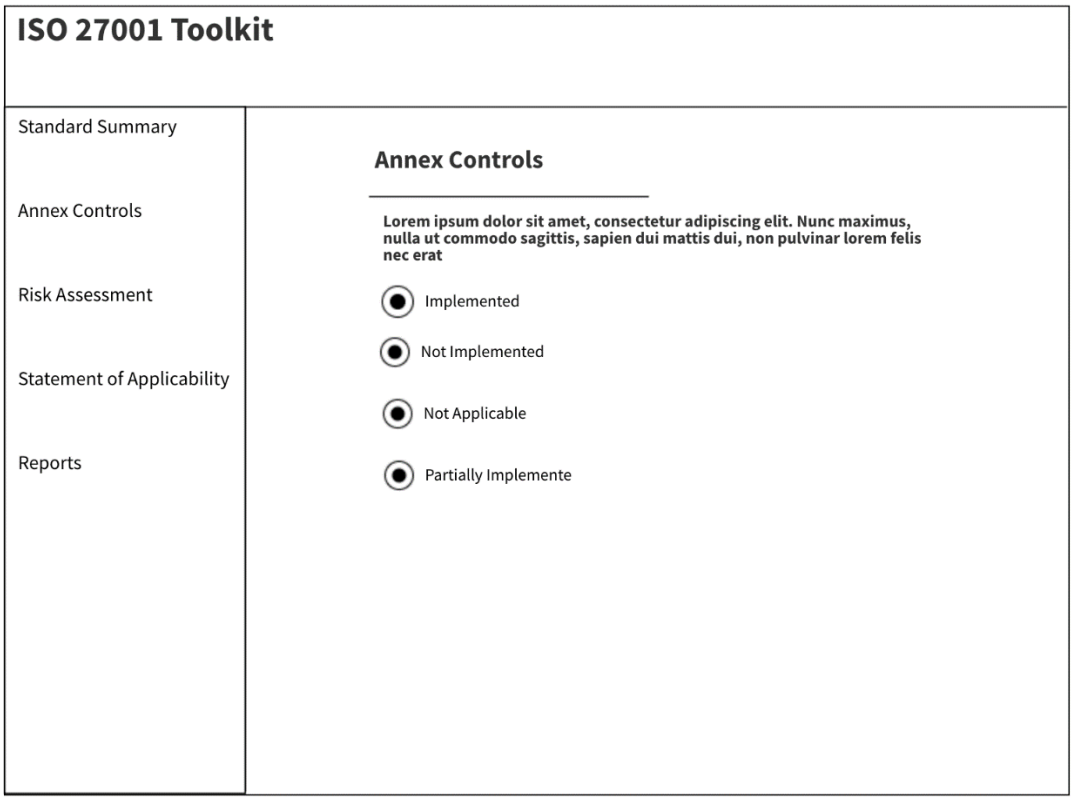


Figure 14: Annex Control page

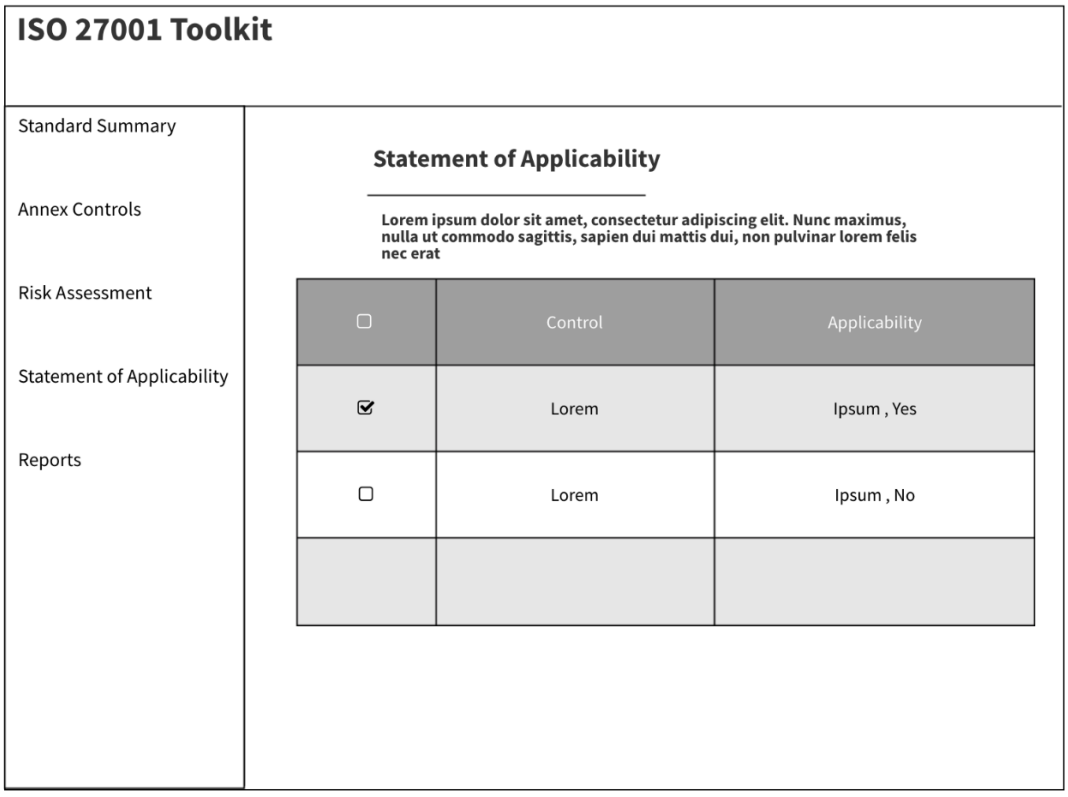


Figure 15: Statement of Applicability design

CHAPTER 5: IMPLEMENTATION AND TESTING

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

5.1 Hardware Resources

The hardware resources that were used during the implementation of this toolkit were as listed below;

- Personal Laptops with 8GB of RAM
- Cloud Server on Digital Ocean Platform

5.2 Software Resources

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

- Pycharm JetBrains programming IDE
- Postgres management for database.
- Language used –Python, JavaScript has an active community support on the web.
- Visio professional to draw diagrams
- Microsoft word for documentation
- Microsoft PowerPoint to do presentations
- Operating system: Mac OS and Linux (Mint)
- Docker for containerization

5.3 Choice of Programming tools, techniques and technologies

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

5.3.1 Python Django Framework

Django is a high-level Python Web framework that inspires fast development and clean, realistic design. It was implemented by experienced developers. The framework takes care of much of the hustle of Web development, thus a developer can focus on writing the application without needing to reinvent the wheel. The framework was chosen because of the following reasons;

- Incredibly fast. Django framework is designed to help developers take applications from concept to completion as quickly as possible
- Django is very secure. The framework takes security with extreme importance and it assists developers to avoid many known security mistakes
- Hugely scalable. Some of the widely used websites have leveraged the use of Django's ability to swiftly and flexibly scale.

5.3.2 React JavaScript Framework

This is widely used JavaScript library for building user interfaces. It makes it easy and painless to implement interactive user interfaces. React was chosen because of the following reasons;

- It is declarative. This implies that it facilitates designing of easy views for each state and efficiently updates and render components when data changes.
- It is Component-Based. Therefore, it enables building of encapsulated components that manage their own state, then compose them to make complex user interfaces.

5.3.4 GraphQL

This is a query language for Application Programming Interfaces (APIs) and runtime for delivering results for those queries with existing information. It delivers a fulfilled and comprehensible description of the data in an API. It provides clients with the mandate to request for exactly what they need and nothing more. It gives developers an opportunity to evolve their APIs over time. It also has powerful developer tools.

This language was used extensively in developing restful APIs for the toolkit. Below is an example of a request and data returned.

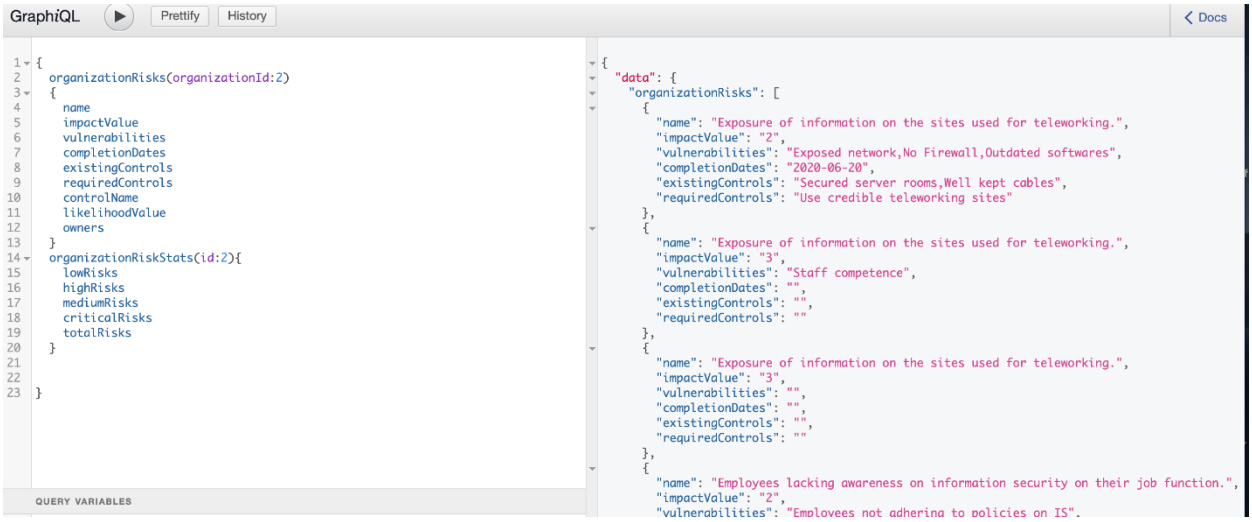


Figure 16: GraphQL sample data

5.3.4 Docker

This is a collection of platform as a service (PaaS) products that leverages on OS-level virtualization to provide software in packages called containers. It helps developers to package applications into containers. A container act as a standardized executable component that combine application source code with all libraries and dependencies required to run that code. Docker makes it easier, and safer to build, deploy, and manage containers. It's essentially a toolkit that enables developers to build, deploy, run, update, and stop containers using simple commands and automation scripts.

Since the toolkit consists of front-end, backend and Postgres database, Docker containers were set up to run each one of them. This tool was chosen because of the following reason;

- Improved and seamless portability: Docker containers run without modification across any desktop, data center and cloud environment.
- Light weight and more granular updates: With Docker, only one process can run in each container. This makes it possible to build an application that can continue running while one of its part is taken down for update.
- Automated container creation. It can automatically build a container based on source code.
- Container versioning: It can track versions of a container image, roll back to previous versions, and trace who built a version and how.
- Shared container libraries: Developers can access an open-source registry containing thousands of user-contributed libraries.

5.4 Testing

Software testing is a quality assurance undertaking. It represents the eventual review of specification, design and code generation. Several techniques were used to test this system and the final output was several test cases to exercise both internal logic and external requirements. Expected results were defined and actual results were documented. Several tests were carried out during the whole development cycle and some at the end of the development cycle. They are briefly outlined below.

5.4.1 Walkthroughs with Peers

This form of testing or technical review was continuous throughout the development cycle. It involved presentation of the presentation of a product at a point of time to fellow colleague or intended user or the project supervisor. We would then walk through the system functionality as a reviewer (student, user or supervisor) gave his/her comments while using the system. The developer also performed walkthroughs, to ensure that there were no flaws in the code in terms of programmatic errors such as semantic and syntactic errors.

5.4.2 Module Testing

The system was implemented module by module. Each module was tested on its own to ensure correctness in its functionality. Validation tests were carried out on all forms and verification tests carried out against the functional and non-functional requirements as described in the analysis section.

5.4.3 Integration Testing

Once the system was developed and deployed, there was need to verify that it was working correctly always and that it can be depended upon by project managers. To validate the application and guarantee its correctness, there was need to formalize the specifications and properties that were to be proven.

5.4.4 Validation Testing

After the above tests were completed, that ran during the development cycle, the validation of the whole system was performed. Validation succeeds when the application functions in a manner that can be reasonably expected by the end user. Each component of the application was confirmed to

work correctly when considered in isolation.

After these individual components were proven to work, they were integrated then run through rigorous black box testing to ensure they could correctly work together.

Finally, the eventual system was put to test to determine if it can serve the intended purpose i.e. enabling information security auditors of SMEs to work with the toolkit to validate its functionality.

5.4.5 Test Cases

Test cases involve the set of steps, conditions and inputs which can be used while performing the testing tasks. The main intent of this activity is to determine whether the software passes or fails in terms of its functionality and other aspects.

Sample test cases that were used are shown below:

Test No	**Module**	**Test**	**Expected Results**	**Actual Results**
1	Annex Controls	Verify user can select applicable controls for an organization and results to accurate SOA	A user can download SOA report based on the controls he/she had selected	The user could download accurate SOA report
2	Admin Configurations	Set configurations for an organization	An admin user can set configurations for an organization	An admin user could set configurations for an organization
3	Risk Assessment	Do risk assessment	A user can do risk analysis and assessment	A user could do risk analysis and assessment
4	Reports	View and Download reports	A user should be able to view and download	A user could download reports

			reports	
5	Risk treatment	Assign risk treatment activities	A user can allocate activities for risk treatment	A user could perform actions to treat risks

5.5 Sample Screen Shots of the Toolkit

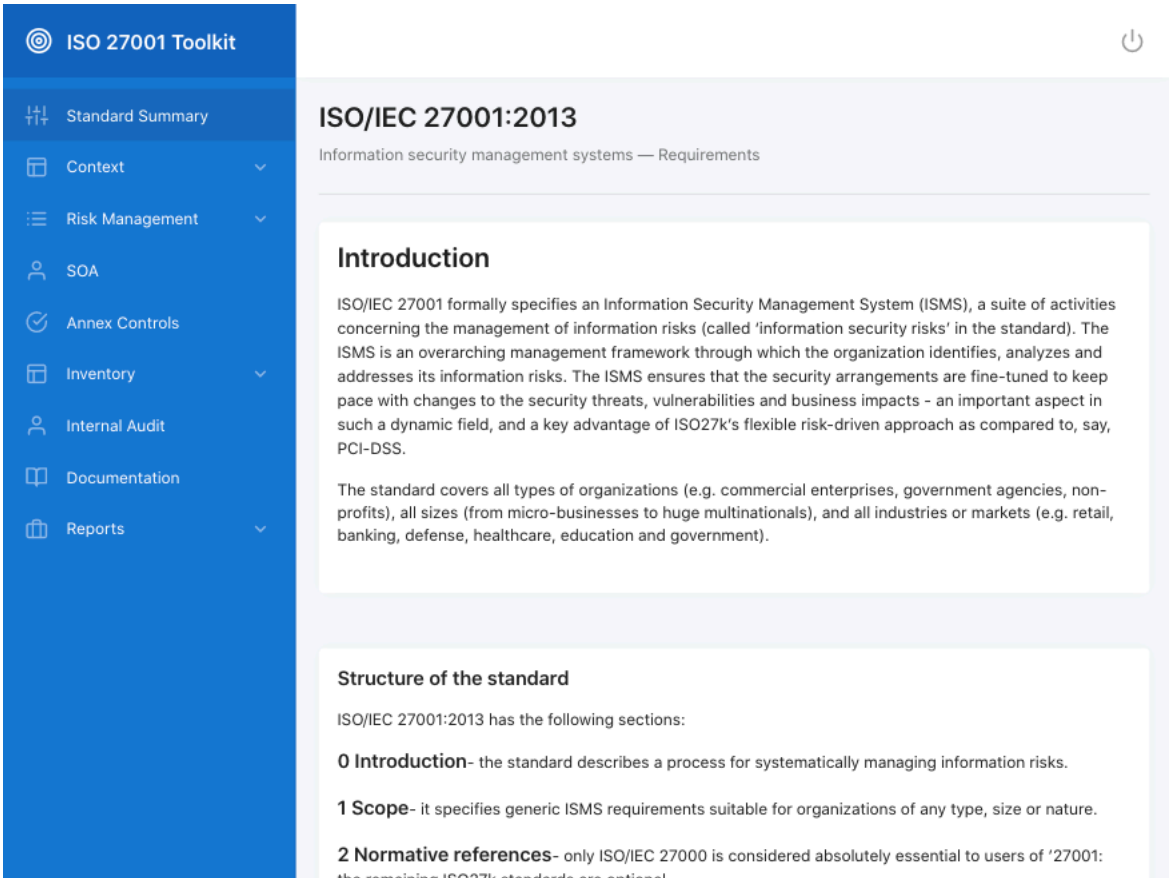


Figure 17: Standard summary view

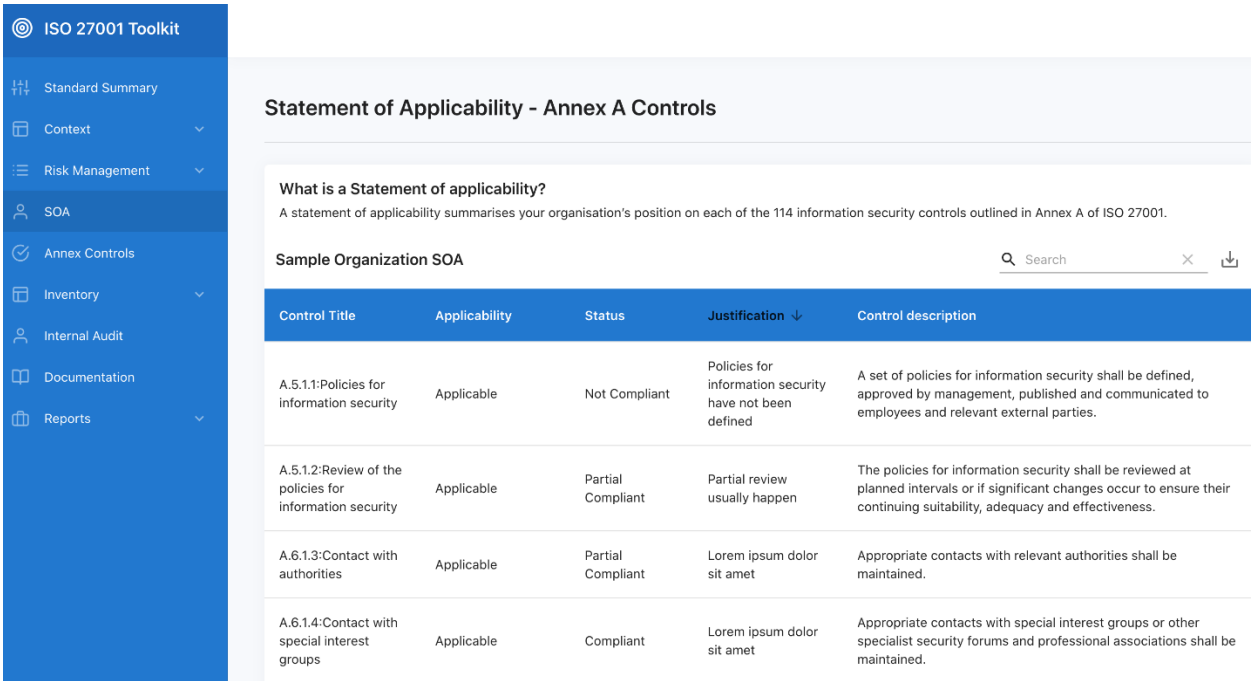


Figure 18: Statement of Applicability view

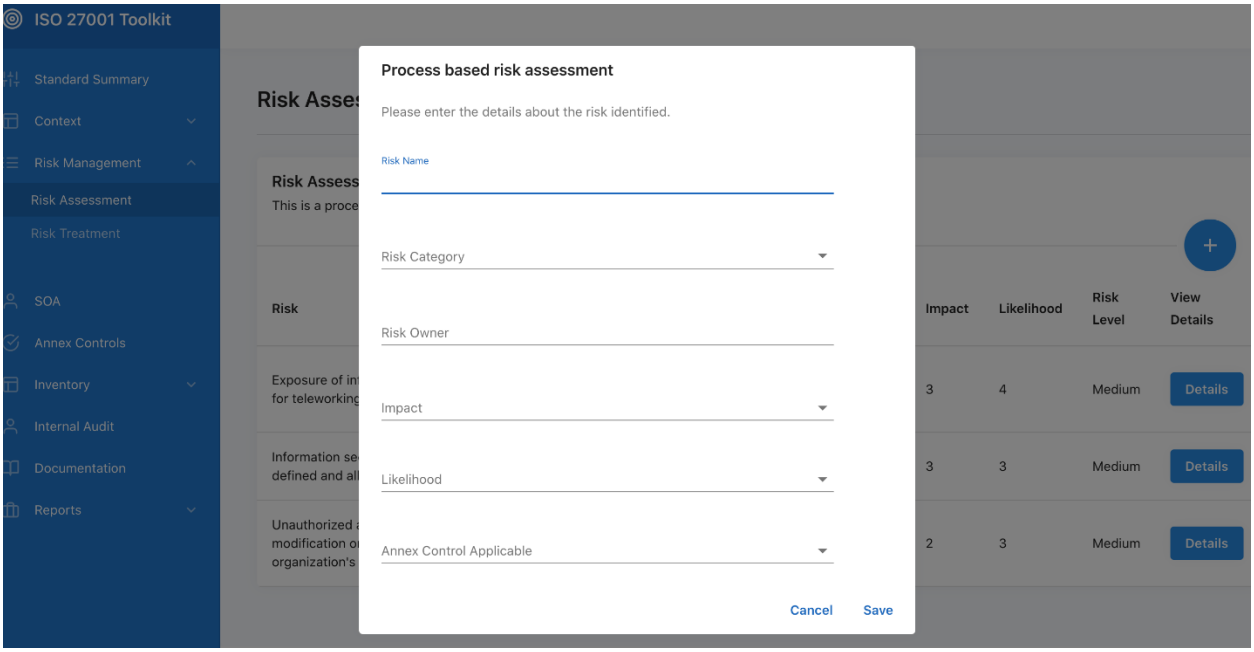


Figure 19: Risk management View

CHAPTER 6: RESULTS AND DISCUSSIONS

This chapter gives details on the findings and results after testing the toolkit with targeted users. It gives a comparison of the results obtained during the analysis phase when users were asked about the standard, and after testing the toolkit. It also gives an interpretation of the findings.

6.1 Toolkit Evaluation and Results

6.1.1 Functional Evaluation per module

The table below shows evaluation and results of various modules of the toolkit that was developed.

Module	Evaluation	Result
Statement of Applicability	Determining whether the module outputs correct statement of applicability for a given organization.	Given that the user does confirm annex controls provided by the toolkit, on whether the controls are implemented or not the toolkit was able to provide accurate statement of applicability.
Risk Assessment	Checking whether an information security expert can perform risk assessment with the toolkit.	The module enabled the user to add risks and evaluate them using Harm reference scale on impact and likelihood
Risk Treatment Planning	Evaluate whether risk treatment plan module enables IS expert to do planning for risk treatment.	The user could set a plan on treating the risks identified for a specific organization.
Admin Configuration	Determining whether the module facilitates configuration of standard requirements and other settings.	The module could perform all configurations properly
Reports	Evaluating whether the reports generated are relevant and accurate	The tool could generate reports about risk register, statement of applicability and risk treatment plan

6.1.1 User Testing

Testing of the toolkit took 2 months, from May 2020 to July 2020. Total number of organizations were 10 which were in Nairobi County Kenya. All organizations identified fall on the top 100 SMEs in Kenya. To provide a complete insight of the effectiveness of the toolkit, both quantitative data needed to be combined with qualitative data for determining whether the desired results had been achieved. Therefore, after testing the toolkit with target users, surveys were used to collect quantitative data while interviews were used to collect qualitative data. The key aspects that were considered included; usability of the toolkit, the extent to which the tool provided information about ISO/IEC 27001 standard, information security risk management, internal auditing functionality, statement of applicability generation and the extent of satisfaction of the reports generated.

Usability of the toolkit was the first aspect that the researcher was interested in getting feedback on. In respect to this aspect the feedback collected is shown in Table 1, whereby majority of respondents considered the application easy to use (90%).

Table 1: Usability Satisfaction

Aspect	Percentage
Ease of use	90
Information arranged in logical order	100
Readability of the content	100
Content keeps user engaged	100
Styling and colors of widgets	80

It shows that information was indeed arranged in a natural and logical order (100%) and presented in a clear and easy to read (100%). In general, participants were satisfied with the toolkit which kept them engaged with content that is relevant to what the aim of the toolkit was (100%). The only usability concern that was observed, had to do with the appearance of the toolkit widgets regarding colors, graphics and screen layouts (80%). This did not hinder us from coming up with

a conclusion that the usability of the tool was good because colors and graphics is something that can be improved on.

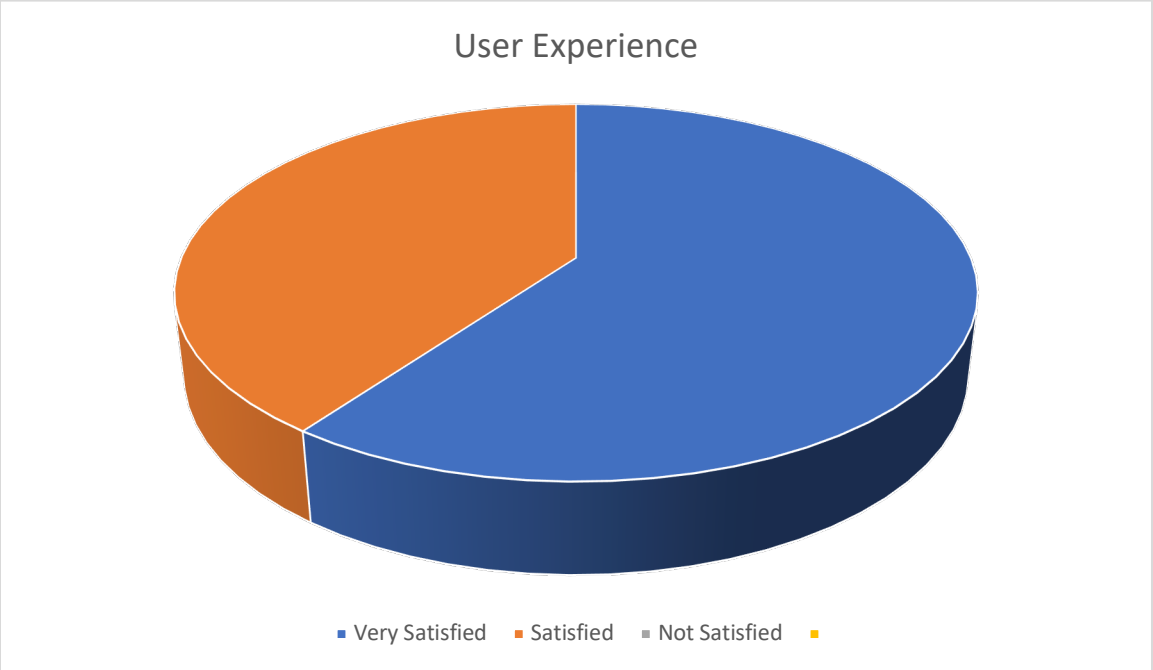


Figure 20: General Usability survey results

The extent to which the toolkit provided information about ISO/IEC 27001 standard was another aspect that the researcher were keen on. A huge number of respondents felt that the toolkit provided information security requirements as stipulated by the standard. Fig. 5 shows a summary of the results. Majority of the target users (70%) strongly agreed the toolkit was informative about the standard. 30% agreed that it was informative and none disagreed. Therefore, this showed that users from targeted organizations could gain knowledge about the standard and in return help organizations in protecting their information assets. Figure 21 shows the responses that was gotten.

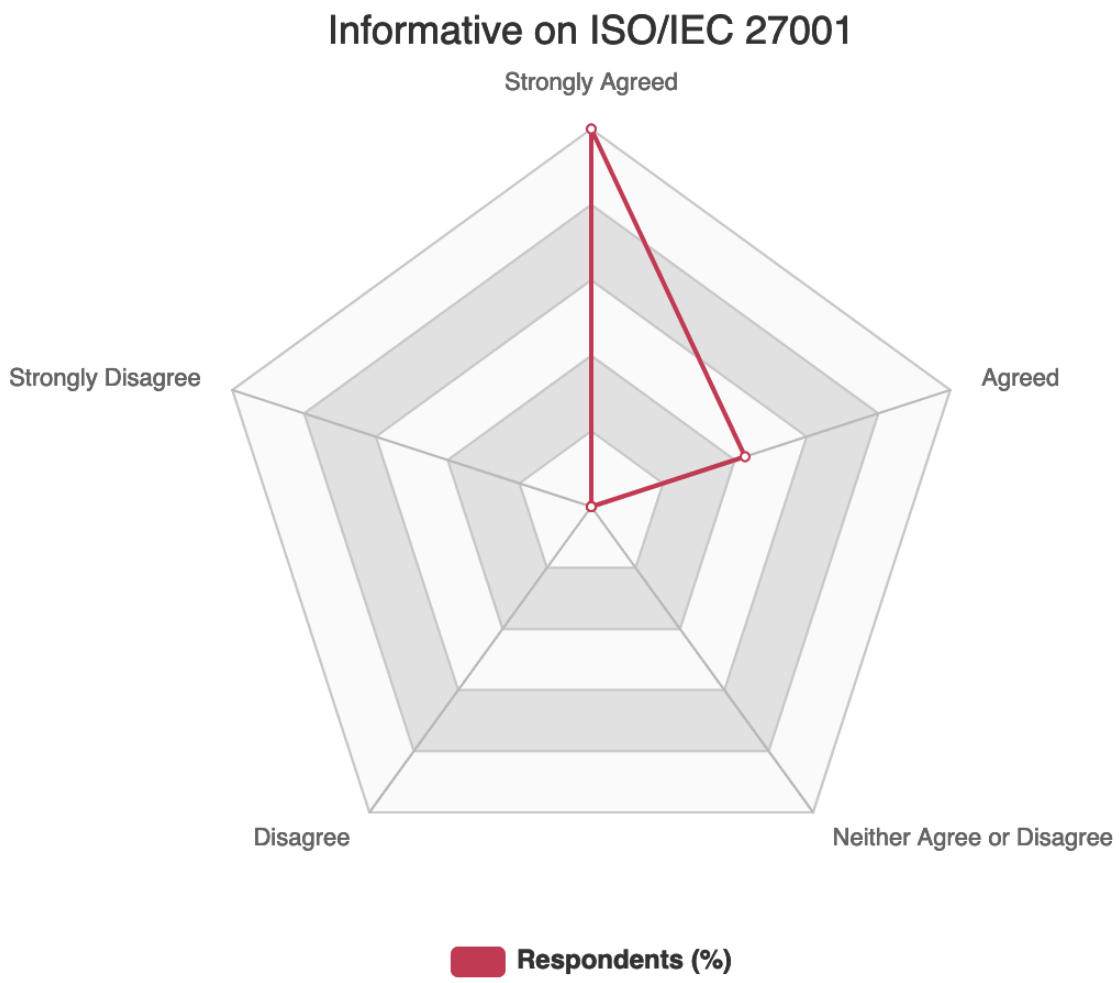


Figure 21: Feedback on how informative the toolkit was

Information security risk management is one of the key modules that the toolkit provided. Therefore, a survey was taken to determine how important it was in helping SMEs identify information risks, manage them and plan on how to treat or mitigate them. Table 2 shows results obtained. Majority of respondents strongly agreed that the toolkit provides a convenient way of managing information security risks (80%). Questions that were asked evolved around the aspects of information security risk management that are provided by the standard.

Table 2: Information Security Management Survey Feedback

Survey Question	Participants Answers				
	Strongly agree	Agree	Neither agree or disagree	Disagree	Strongly disagree
The toolkit provides a clear way of managing information security risks	80%	20%	0	0	0
Proper risk treatment planning	60%	40%	0	0	0
Informative, information security risk register.	70%	30%	0	0	0
Easy to link between standard control to a risk	50%	30%	20%	0	0
Treating identified risks can lead to ISO 27001 certification.	40%	50%	10%	0	0

As stated earlier, Statement of applicability summarizes an organization's position on each of the 114 information security controls outlined in Annex A of ISO/IEC 27001. The toolkit provided a way in which organizations can determine where they stand on those controls. An organization can either be Compliant, Partially Compliant or Non-Compliant to a control. A control can also not be applicable based on business processes carried by an organization. Out of 114 controls, an average of 21 controls were found to be compliant. An average of 38 were partially implemented, 39 were non-compliant and an average of 16 were not applicable to the business processes of those SMEs.

Table 3: Compliance Status of Annex Controls

Compliance Status	**Average Number of Controls**
Compliant Controls	21
Partially Compliant	38
Non-Compliant	39

Not Applicable Controls	16

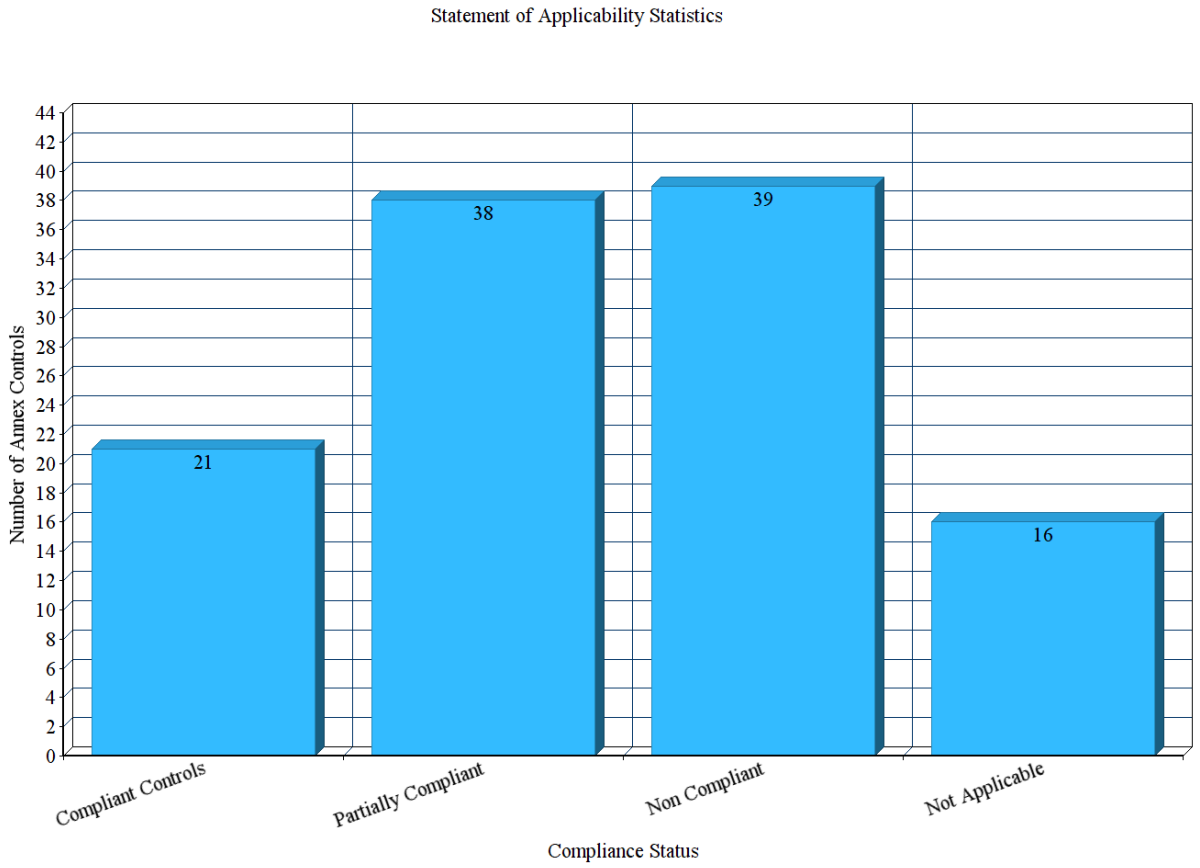


Figure 22: Compliance Status of Annex Controls

Interviews were conducted to determine whether internal auditing module had provided a mean in which an organization can conduct internal audits at planned intervals. Results showed that most of them will be willing to conduct internal audits at an interval of six months. They all seem to agree and understand the importance of doing frequent audits about their information security.

A questionnaire about the reports that are generated by the toolkit were send to the targeted users. Majority felt that the reports were sufficient and informative. However, a few of them felt that the toolkit could generate more reports. This feedback was taken to be as part of the toolkit improvement in future works.

6.3 Discussions

It is evident that the results shown above indicates that targeted users understand the importance of information security. Initially they did not know that there is a standard that can guide in protecting their organization information. They now acknowledge using the toolkit can help them understand the standard better and that it can guide them in implementing the requirements of the standard.

CHAPTER 7: CONCLUSIONS AND RECOMMENDATIONS

7.1 Conclusions

In this study, the researcher has demonstrated that it is indeed possible for SMEs to protect their information by complying with the requirements provided by ISO 27001. The researcher found out that most of these organizations were unaware of the importance of securing their information assets and lacked knowledge about the standard. They were therefore, vulnerable to cyber-attacks, manipulations from malicious people and exposure of their key information to the outside world. The myth about SMEs not having enough resources to protect their information assets can be misleading. With affordable toolkit, that provides requirements of ISO 27001, they can implement those requirements strategically.

Moreover, they can identify risks associated with unimplemented controls. This in turn enables them to create plans and dedicate resources into mitigating and treating those risks.
In addition to risk management, the toolkit enables organizations to monitor the progress of where they stand in implementing controls provided by the standard. It also provides insights to the management team on how vulnerable they are, and thus helping them to make key decisions in resolving those threats.

7.2 Challenges & Limitations

The key challenge of this study was converting some sections of the standard to software modules. Some sections are provided in terms of explanation of what need to be in place. For instance, there is a section that talks about management commitment to support the implementation of controls provided. It was challenging to convert that aspect of commitment into a software module.

In addition, getting willing users of the toolkit was a challenge. Most organizations were hesitant to provide details about their information security processes.

Lastly, the global pandemic that was experienced at the time of this study meant that one could not interact with users directly, thus data collection by observation method was hindered.

7.3 Contributions to the study

This study has demonstrated the ease of using current software development technologies in providing tools that can guide SMEs in protecting their information assets. New programming technologies such as GraphQL, ReactJS and containerization provide an elegant and efficient way of solving real world problems from any sector.

The study has also contributed knowledge to information security discipline as a whole. The objective was to help small and medium sized organization to protect their information via a ISO 27001 toolkit. The objective has been accomplished based on the results obtained. Therefore, toolkit approach has been discovered as a way of ensuring organization protect their information.

Web services can be leveraged on when implementing tools that are centered towards securing information.

7.4 Future Work

Future work should focus on exploring other technologies that can be used to implement toolkits for different security standards. Especially toolkits for ISO 27000's family of standards because they focus on different aspect of information security.

Additionally more features can be added to the developed toolkit to capture all the aspects provided by ISO 27001 standard. That can include;

- Management review module
- Continuous improvement module
- Monitoring and evaluation

REFERENCES

An approach to map COBIT processes to ISO/IEC 27001 information security management controls. Available from: https://www.researchgate.net/publication/292833500_An_approach_to_map_COBIT_processes_to_ISOIEC_27001_information_security_management_controls [Accessed: 11 December 2019].

Barlette, Y. & Fomin, V. V. 2009. *The Adoption of Information Security Management Standards: A Literature Review. Cyber Security and Global Information Assurance* (pp. 119–140). IGI Global. Available at: https://doi.org/10.4018/978-1-60566-326- 5.ch006 [Accessed: 11 December 2019].

Barlette, Y. & Fomin, V. V. 2009. *The Adoption of Information Security Management Standards: A Literature Review. Cyber Security and Global Information Assurance* (pp. 119–140).

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

Boehmer, W. 2009. *Cost-benefit trade-off analysis of an ISMS based on ISO 27001. International Conference on Availability, Reliability and Security*. 2009

Calder, A. 2009. *Implementing Information Security based on ISO 27001/ISO 27002: A Management Guide - Best Practice*. Van Haren Publishing.

Candiwan, 2017, *Analysis of ISO 27001 Implementation for Enterprises and SMEs in Indonesia*, pp. 50-57

Cherdantseva, Y., Hilton, J. 2013 *A Reference Model of Information Assurance & Security*. Available at: http://rmias.cardiff.ac.uk/

Gordon, L. and Loeb, M. (2006). Budgeting process for information security expenditures. Communications of the ACM, 49(1), 121-125.

IT Governance. 2019. ISO 27001 Global Report 2019. Available at: www.itgovernance.co.uk [Accessed: 20 December 2019].

Hevner, A. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems, 19*, 87–92.

Humphreys, E. 2011, *Information Security Management System Standards*.

Ivan, D. *Principles of information security*, Available from: https://resources.infosecinstitute.com/guiding-principles-in-information-security/

Kothari, C.R. (2004) *Research Methodology: Methods and Techniques. 2nd Edition*, New Age International Publishers, New Delhi.

Matthias, G, Tim s, A practical guideline for implementing an ISMS in accordance with the international standard ISO/IEC 27001:2013. Available at: https://www.isaca.de/sites/default/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf [Accessed: 20 December 2019]

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*, 45–77.10.2753/MIS0742-1222240302

Peppard, J. 2007. *The conundrum of IT management*. European Journal of Information Systems 16*: p.336–345. Available at: http://ai2-s2-pdfs.s3.amazonaws.com/fb46/bcf97dc64b6824e5f1a039f3df0c28424ec5.pdf [Accessed 11 December 2019].

Peter K, *A toolkit approach to information security awareness and education*, pp. 25-37

Radhakrishnan, S. 2015. *COBIT Helps Organizations Meet Performance and Compliance Requirements, COBIT Focus*, pp. 1-5, Business Source Complete, EBSCOhost

Ramsey, DB. 2016, *DATA SECURITY: EVOLVING LEGAL DUTIES AND CHALLENGES FOR FRANCHISE SYSTEMS*, Journal of Internet Law, 20, 3, pp. (3-17)

Reid, N., Petocz, P.& Gordon, S. (2008). *Research interviews in cyberspace. Qualitative Research Journal*.

Rocha Flores, W., Antonsen, E., & Ekstedt, M. 2014. *Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture*. Computers & Security 43: p.90–110.

Sarbanes-Oxley Act. 2002. Sarbanes-Oxley Act of 2002. Available at: http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302 .pdf. [Accessed: 28 December 2019].

Sharma, N., & Dash, P.K. 2012. Effectiveness of ISO 27001, as An Information Security Management System: An Analytical Study of Financial Aspects. Far East Journal of Psychology and Business 9(3): p.42–55.

Soomro, Z.A., Shah, M.H., & Ahmed, J. 2015. Information security management needs more holistic approach: A literature review. International Journal of Information Management 36(2), p.215–225.

Susanto, H., Almunawar, M.N., & Tuan, Y.C. 2011. *Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Science*s IJECS-IJENS 11(23).

Shirley P, 2006, Information Security Resources. Available from: https://www.sans.org/information-security/ [accessed: 20 December 2019]

Udo, G.J, Privacy and security concerns as major barriers for e-commerce: a survey study, Information Management & Computer Security 9/4 [2001] 165-174, MCB University Press.

The Graphql foundation. A query language for your API. Available at: https://graphql.org/ [Accessed: 18th May 2020].

Ukidve, A., Smantha, D.S., & Tadvalkar, M. 2017. Analysis of Payment Card Industry Data Security Standard [PCI DSS] Compliance by Confluence of COBIT 5 Framework. Journal of Engineering Research and Application www.ijera.com ISSN 7(11)

APPENDIX 1: CODE SAMPLE

Annex A Controls Schema

```
class Query(graphene.ObjectType):
    control_types = graphene.List(ControlObjectiveType)
    controls = graphene.List(ControlType)
    control = graphene.Field(ControlType, id=graphene.Int())
    non_compliant_controls = graphene.List(OrganizationControlsType, id=graphene.Int())
    organization_statement_of_applicability = graphene.List(OrganizationControlsType, id=graphene.Int())
    organization_report = graphene.Field(OrganizationReportType, id=graphene.Int())

    def resolve_non_compliant_controls(self,info, id=None):
        organization_instance = Organization.objects.get(pk=id)
        return OrganizationControls.objects.filter(
            organization=organization_instance, is_implemented=False, is_applicable=True
        )
    def resolve_control_types(self, info, **kwargs):
        return ReferenceControl.objects.all()

    def resolve_controls(self, info, **kwargs):
        return Control.objects.all()

    def resolve_control(self, info, id=None):
        if id:
            return Control.objects.get(pk=id)
        return None

    def resolve_organization_statement_of_applicability(self, info, id=None):
        organization_instance = Organization.objects.get(pk=id)
```

Risk Management GraphQL Schema

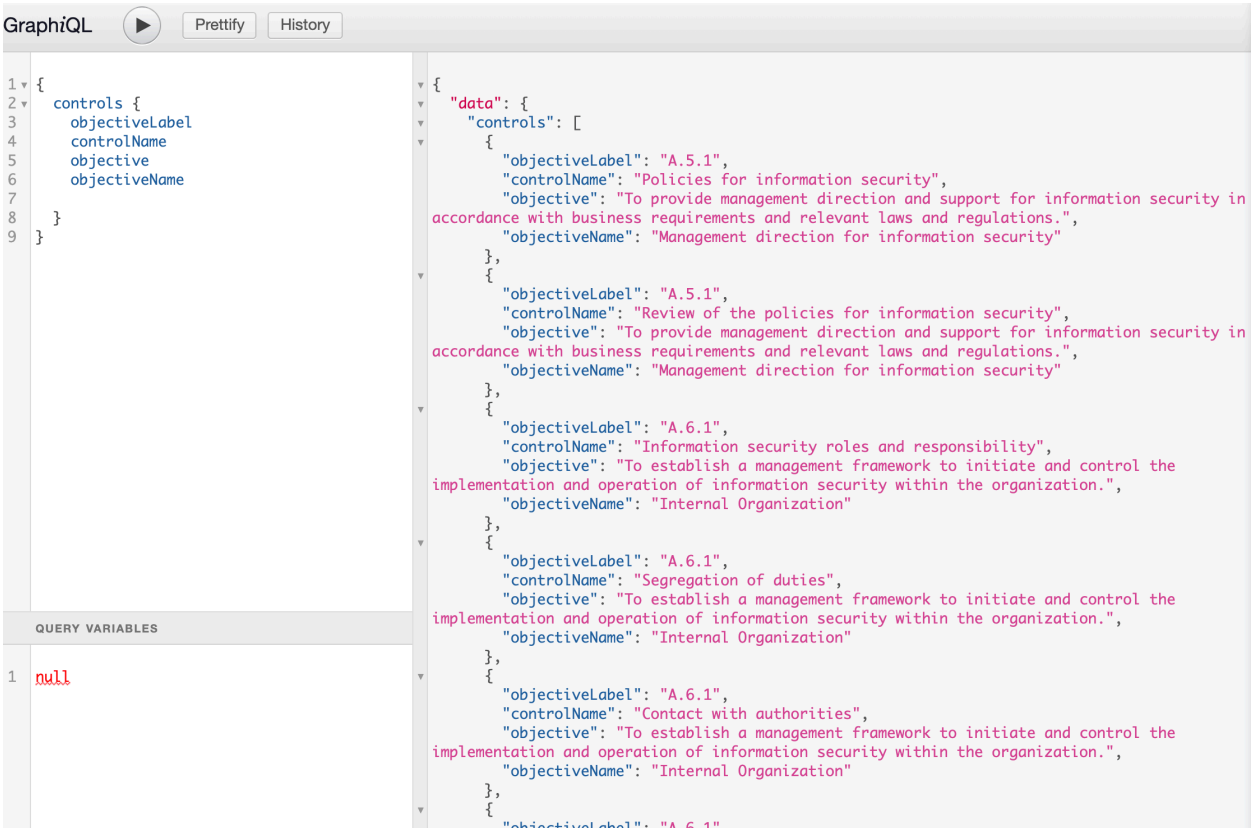
```
    class Arguments:
        name = graphene.String(required=True)
        impact = graphene.Int(required=True)
        likelihood = graphene.Int(required=True)
        organization = graphene.Int(required=True)
        control = graphene.Int(required=True)
        owner = graphene.String(required=True)
        category = graphene.String(required=True)

    def mutate(self, info, name, impact, likelihood, organization, control, owner, category):
        likelihood_ins = LikelihoodScale.objects.get(pk=likelihood)
        impact_ins = ImpactScale.objects.get(pk=impact)
        control_ins = Control.objects.get(pk=control)
        organization_ins = Organization.objects.get(pk=organization)
        organization_risk = OrganizationRisk(
            name=name, impact=impact_ins, organization=organization_ins,
            likelihood=likelihood_ins, control=control_ins, risk_category=category, risk_owner=owner
        )
        organization_risk.save()

        return OrganizationRiskMutation(
            name=organization_risk.name
        )


class VulnerabilityMutation(graphene.Mutation):
    name = graphene.String()
```

Frontend Sample Code

```
const Divider = styled(MuiDivider)(spacing);

const Paper = styled(MuiPaper)(spacing);

class AnnexControl extends React.Component {
    constructor(props) {
        super(props);

        this.state = {
            value: "Not Compliant",
            controlId: parseInt(props.controls[0].id),
            controlName: "",
            objectiveName: "",
            objective: "",
            label: "",
            referenceLabel: "",
            referenceName: "",
            objectiveLabel: "",
            isFinalControl: false,
            lastControlSaved: false,
            justification: ""
        }
    }

    static propTypes = {
        controls: PropTypes.array.isRequired,
        authData: PropTypes.object.isRequired
    };

    async componentDidMount() {
        const initialControl = await getControl(this.state.controlId);
        this.setState( state: {
            controlName: initialControl.controlName,
            objectiveName: initialControl.objectiveName,
            objective: initialControl.objective,
            description: initialControl.description,
```

APPENDIX 2: API SAMPLES

API query for Annex Controls



API Query for Organizations