
Electronic Theses and Dissertations

2017

An Information technology controls evaluation prototype for financial institutions in Kenya

Anthony Mwangi Muiyuro
Fuculty of Information Technology (FIT)
Strathmore University

Follow this and additional works at <https://su-plus.strathmore.edu/handle/11071/5626>

Recommended Citation

Muiyuro, A. M. (2017). *An Information technology controls evaluation prototype for financial institutions in Kenya* (Thesis). Strathmore University. Retrieved from <http://su-plus.strathmore.edu/handle/11071/5626>

An Information Technology Controls Evaluation Prototype for Financial Institutions in Kenya

Muiyuro Anthony Mwangi

Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in
Information Technology at Strathmore University

June, 2017

This thesis is available for Library use on the understanding that it is copyright material and that
no quotation from the thesis may be published without proper acknowledgement.

Declaration and Approval

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

© No part of this thesis may be reproduced without the permission of the author and Strathmore University

Anthony Mwangi Muiyuro

Reg No: 51287

Signature

Date

Approval

The research thesis of Muiyuro Anthony Mwangi was reviewed and approved by:

Dr. Bernard Shibwabo,

Academic Director, Faculty of Information Technology,
Strathmore University.

Dr. Joseph Orero,

Dean, Faculty of Information Technology,
Strathmore University.

Prof. Ruth Kiraka,

Dean, School of Graduate Studies,
Strathmore University.

Abstract

In today's dynamic and ever complex world, automation has become a competitive edge that many organizations have embraced. Introducing greater efficiencies and cutting edge capabilities, technology has become a key driver of business growth and innovation. Due to this high level of technology adoption, this rapid and ever changing business environment has become a breeding ground to some of the most detrimental threats, attacks and disruptive incidents. These emerging threats can only be managed by having relevant and effective IT controls that will maintain the confidentiality, integrity and availability of the information assets. The financial services sector has been at the edge of introducing new technology driven products and services that promise greater efficiencies, faster transaction processing and enhanced security. However, the financial services space is faced by ever-escalating IT risks from various threats. To effectively leverage on these technical capabilities and effectively manage the inherent IT risks, an effective and comprehensive risk driven control framework must be identified, established and enforced to commensurate the business' risk appetite and achieve the business goals. The current problem experienced by organizations is enforcing an effective IT controls framework with continuous evaluations to ensure control effectiveness and fit for purpose. This research explored an approach to rolling out an IT controls system based on the NIST 53-800 framework that would be subject to periodic assessments by control owners to gauge its effectiveness for onward improvements and optimization. This research explored quantitative methods in data gathering and analysis with a target study population of the Kenyan financial institutions. The researcher employed convenience sampling and selected seven key financial institutions with a mature controls environment. This study has proposed an evidence based IT controls framework tailored to improve the Governance and oversight within IT in Financial institutions. The prototype was developed using the Rapid development approach embedding the v-process in the iterative build. The prototype developed gives oversight and visibility of all the IT controls enforced in the organization(s) and provide a way to continually monitor control effectiveness, control deficiencies and the remedial actions. Data from the respondents was analyzed to deduce the conclusion to this research. The developed prototype attained a 98% accuracy level in assessing IT controls and provided management a platform for control evidence evaluation to determine control effectiveness.

Dedication

I dedicate this research to God for his grace, favor and faithfulness while doing this work. To my loving wife, for her encouragement and motivation to be at my best. To my dear parents, for believing in me and constant guidance and inspiration; to my siblings, family and friends; Thank you.

Acknowledgements

I wish to express my gratitude to the Almighty God for giving the inspiration, grace and determination of doing this work to the best of my ability. I am grateful to my supervisor Dr. Bernard Shibwabo for his unfailing guidance and candid feedback that has formed and shaped this work to its successful completion. I would also like to appreciate Prof. Ismail Ateya for his guidance throughout the thesis preparation sessions. To Prof. Reuben Marwanga, you have been a constant source of insight and direction on how my thesis can be relevant in solving a real world problem. Finally, my sincere gratitude goes to Mr. Preston Odera, President of the Information Systems Audit and Control Association (ISACA Kenya chapter) for his wonderful support.

Table of Contents

Abstract	iii
Dedication	iv
Acknowledgements	v
Table of Contents	vi
Table of Figures	x
List of Tables	xii
Abbreviations	xiii
Definition of Terms	xiv
Chapter 1: Introduction	2
1.1 Background	2
1.2 Problem Statement	3
1.3 Aim	4
1.4 Specific Objectives	4
1.5 Research Questions	4
1.6 Justification	5
1.7 Scope and Limitation	5
Chapter 2: Literature Review	6
2.1 Introduction	6
2.2 Key IT controls in Financial Services Institutions	6
2.2.1 Computer Operations Controls	8
2.2.2 Access to Program and Data	9
2.2.3 Program Changes	10
2.2.4 Program Development	10
2.2.5 Entity Level Controls	10
2.3 Approaches to IT Controls Selection and Assessments	10
2.3.1 IT Risk Analysis and Management	10
2.3.2 Best Practice Frameworks/ Benchmark Manuals	11
2.3.3 Information Security Checklists	14
2.3.4 Controls Desirability Functions	15
2.3.5 Information Security Control Attribute Profile	16

2.3.6	Information Security Risk-Control Assessment Model	16
2.3.7	Information Security Risk Management Model/ Approach.....	17
2.4	Strengths and Weaknesses of IT Controls Assessment Approaches.....	18
2.5	Proposed conceptual framework	20
2.5.1	IT Controls Assessment Prototype.....	20
Chapter 3: Research Methodology		21
3.1	Introduction	21
3.2	Research Design.....	21
3.3	System Development Methodology	21
3.3.1	The V-process Model Approach.....	22
3.4	Target Population	24
3.5	Sampling Procedure	24
3.6	Data Collection Methods.....	24
3.7	Data Analysis and Presentation.....	25
3.8	Research Quality	25
3.8.1	Reliability.....	25
3.8.2	Validity	26
3.8.3	Objectivity.....	26
3.8.4	Analysis of the methodologies.....	26
3.8.5	Ethical Considerations	26
Chapter 4: System Analysis and Design		27
4.1	Overview	27
4.2	Data Analysis and Findings.....	27
4.2.1	Cyber Incidents Caused by IT Control Gaps	27
4.2.2	Efficiency of The Current IT controls Assessment Methods.....	28
4.2.3	Visibility of In-effective IT Controls Through Manual Control Assessments	29
4.2.4	Subjectivity of The Current IT Controls Assessment Methods	30
4.2.5	Effectiveness and Accuracy of System Based Control Self-assessments.....	30
4.2.6	Confidentiality of IT Control Gaps Findings.....	31
4.3	Requirements for the proposed system	32
4.3.1	End-User Requirements.....	32
4.3.1	Functional Requirements	32

4.3.2	Non-Functional Requirements	33
4.3.3	System Requirements.....	33
4.4	System Process Modelling	34
4.4.1	Context Level Diagram.....	34
4.4.2	Use case Diagram	37
4.4.3	Sequence Diagram	43
4.4.4	Entity Relationship Diagram.....	45
4.4.5	Class Diagram.....	46
4.5	The Prototype Architecture	48
Chapter 5: System Implementation and Testing		51
5.2	Introduction	51
5.3	Controls Assessment Program Flow	47
5.4	System Server Requirements	51
5.4.1	Hardware Requirements.....	51
5.4.2	Server Requirements	51
5.4.3	Client Machine Requirements.....	52
5.5	System Users, Roles and Access Matrix.....	52
5.5.1	Control Owner Role.....	52
5.5.2	Process Owner Role.....	52
5.5.3	Assurance Managers	53
5.5.4	System Administrator	53
5.6	System Pseudo Code	54
5.7	Sample Forms Used	55
5.7.1	System User Management	55
5.7.2	Performing Controls assessment.....	55
5.7.3	Uploading Control evidence	58
5.7.4	Raise Deficiency log.....	58
5.7.5	Raise remediation plan.....	59
5.8	Prototype Validation	60
5.9	Testing of Prototype	62
5.10	Maintenance of the Prototype	63
Chapter 6: Discussions		64

6.1	Introduction	64
6.2	Findings	64
6.2.1	User Experience Findings	64
6.2.2	Prototype Accuracy.....	66
6.2.3	Prototype Performance.....	67
6.2.4	Adoption of Controls Assessment Prototype	68
6.2.5	Reliability of Controls assessment system.....	69
6.3	Limitation of this Prototype	69
Chapter 7: Conclusions and Recommendations		70
7.1	Conclusion.....	70
7.2	Recommendations for Further Research	71
References		72
Appendices.....		76
Appendix A: Turnitin Originality Report		76
Appendix B: User Requirements Questionnaire		77
Appendix C: System Usability Questionnaire		79
Appendix D: Interview Questions.....		82

Table of Figures

Figure 2.1: Nist Cybersecurity Program Controls	6
Figure 2.2: Cobit Framework	7
Figure 2.3: All State IT Control Framework	13
Figure 2.4 : Nist Risk Management Framework	14
Figure 2.5: Proposed Conceptual Framework	20
Figure 3.1: The V-Process Model.....	23
Figure 4.1 : Cyber Incidents Caused By IT Control Gaps.....	28
Figure 4.2 : Efficiency of Current Methods Of IT Controls Assessments.....	29
Figure 4.3 : Visibility of In-Effective IT Controls Through Manual Assessments	29
Figure 4.4: Subjectivity of Existing IT Controls Assessment Methods.....	30
Figure 4.5: Effectiveness and Accuracy of System Based IT Controls Self-Assessment	31
Figure 4.6 : Confidentiality of IT Control Gaps Findings.	31
Figure 4.7 : Context Level Diagram	34
Figure 4.8: Level 0 Diagram.....	37
Figure 4.9 : Use Case Diagram	38
Figure 4.10 :Sequence Diagram.....	44
Figure 4.11: Entity Relationship Diagram	45
Figure 4.12 :Class Diagram	46
Figure 4.13: Controls Assessment Prototype Architecture.....	50
Figure 5.1: IT Controls Assessment Program Flow.....	48
Figure 5.2: The Controls Assessment Pseudo Code	54
Figure 5.3 : Controls Assessment System Dashboard	56
Figure 5.4 : Control Assessment Details.....	57
Figure 5.5 : Assessment Control Details.....	57
Figure 5.6: Assessing A Control.....	58
Figure 5.7 : Creating A Deficiency Log	59
Figure 5.8: Raising A Remediation Plan	60
Figure 5.9: Prototype Validation (Username/ Password Required).....	61

Figure 5.10 Unsuccessful Log-In.....	61
Figure 6.1 : Controls Assessment Prototype User Friendliness.....	65
Figure 6.2 : Controls Assessment Prototype User Friendliness.....	66
Figure 6.3 : Accuracy Of Controls Assessment.....	67
Figure 6.4: Efficiency Of Using Prototype In Controls Assessment	68
Figure 6.5: Adoption Of System Based Control Assessment	68
Figure 6.6: Reliability Of System In Remediating Control Gaps	69

List of Tables

Table 4.1 : IT Controls Assessment System Main Use Cases	38
Table 4.2 : Manage Control Owners Use Case.....	39
Table 4.3: Assess Control Use Case	40
Table 4.4: Upload Control Evidence	40
Table 4.5 : Raise Deficiency Log Use Case	41
Table 4.6 : Raise Remediation Plan Use Case.....	41
Table 4.7 : Review Control Assessment.....	41
Table 4.8 : Accept Control Assessment.....	42
Table 4.9 : Reject Control Assessment.....	42
Table 4.10 :Verify Control Assessment.....	42
Table 4.11: View Reports	43
Table 5.1 : Hardware Requirements	51
Table 5.2 : Application Server Requirements.....	51
Table 5.3 : Client Machine Requirements	52
Table 5.4 : System Test Cases	62

Abbreviations/ Acronyms

COBIT	Control Objectives in IT
CSA	Controls Self-Assessment
GCC	General Computer controls
GUI	Graphical User Interface
IT	Information Technology
ISC	Information Security Control
ISCAP	Information Security Control Attribute Profile
ISRMM	Information Security Risk Management Method
IaaS	Infrastructure as a Service
RAM	Risk Assessment Methodology
RAD	Rapid Application Development
R&IS	Risk and Information Security
SaaS	Software as a Service
SLA	Service Level Agreement
SOD	Segregation of Duty Matrix

Definition of Terms

IT Controls - Procedures or policies that provides a reasonable assurance that the information technology used by an organization operates as intended, that data is reliable and that the organization is in compliance with applicable laws and regulations (ISACA, 2013).

General Computer Controls - These are control activities performed around the IT environment that organizations rely on for integrity, availability and confidentiality (NIST, 2013).

Information Security - This is the practice of the prevention, detection, response and recovery of information related incidents and events (ISACA, 2012).

IT Governance - The ability for the organization's IT investment to sustainably enable and extend the organization's strategies and objectives (ITGI, 2007).

Control Owner – This is the person(s) responsible for the day-to-day running of a control and the overall success or failure identified during testing for remediation (Da Veiga & Eloff, 2007).

Process Owner – This is the person who has the ultimate responsibility of the overall performance of a process in an organization (Da Veiga & Eloff, 2007).

Chapter 1: Introduction

1.1 Background

With the high adoption of technology to enable business processes, there is a high reliance on computers and information systems. This in effect has given rise to the proliferation of information security threats and incidents that have greatly impacted the confidentiality, integrity and availability of the information held by organizations.

Over the years, the financial institutions have been a constant target by cyber criminals with the intent to exploit vulnerabilities for financial gain. Instructively Serianu's Kenya Cyber Security Report (2015), the financial services sector lost KS. 4 Billion to cyber related fraud causing huge losses. These cyber-attacks were a mix of stealth tech savvy criminals and employees able to circumvent controls to commit fraud.

As noted by the Serianu's Cyber Security Report (2016), businesses have highly digitized their business processes and the move to the internet and cloud-based infrastructures has highly exposed them to cyber-attacks and information security incidents. With this new operating environment, financial institutions need to build their capacities and capabilities in anticipating, detecting, responding and containing cyber security attacks. According to the report, the estimated cost of Cyber-crime in Kenya in 2016 was \$ 175 Million (KS 17.5 Billion).

Further noted in the Serianu's Cyber Security Report (2016), businesses in Kenya are not investing in the right capabilities to make their IT environment more resilient. Case in point is the financial services sector, which lacks visibility of the effectiveness of their controls which gives them a false sense of security from cyber-attacks and incidents.

Lapse of IT controls is indicative of wrong investments in IT security infrastructure which to do not effectively anticipate, detect, respond and contain these information security incidences. One of the most critical challenge facing most organizations in Kenya is the lack of awareness of their risks, effectiveness of their controls and gaps in their IT security posture (Kenya Cyber Security Report, 2015).

According to a study performed by Bedard, Graham and Jackson (2008), 21 percent of all the audit issues noted in organization's audits were related to information security and the controls deficiencies thereof. In his study, Bedard et al. (2008) concluded that within the organizations in scope of his study, there were no adequate information security controls (ISC) and the ones in place were not operating effectively.

Most information security challenges in organizations are addressed by the deployment of Security tools and technologies such as access management, antivirus, firewalls, encryption and change management among others. (Volonino & Robinson, 2004; Bedard, Graham & Jackson, 2008). These tool are pivotal to ensuring the security of the IT estate, they cannot be deemed sufficient to address the information security challenges faced by organizations (Herath & Rao, 2009). Therefore to improve the overall information security posture, organizations have to implement appropriate controls that are fit for purpose and effectively safeguard against the various information security risks aligned to their security requirements.

1.2 Problem Statement

The effective and adequate assessment and evaluation of information security controls is key to protecting the information assets of organizations (Mather, Kumaraswamy, & Latif, 2009). The Kenyan Financial institutions do not have a structured approach to effectively evaluate their IT controls for adequacy and effectiveness. (Kenya Cyber Security Report, 2015).

Traditional control assessment methodologies entail manual checklists that do not evaluate the deployed IT controls based on their design adequacy and operating effectiveness with supporting evidence of the controls. (Institute of Internal Auditors, 2012)

Dhillon and Torkzadeh (2006) concludes that the current control evaluation methodologies are subjective based on dichotomous values (i.e. Yes or No answers) and are not based on any empirical data to support the control assessments. Furthermore, these IT controls evaluation are adhoc and do not provide a remediation and follow-up plan for all noted deficiencies.

There is a need for organizations to adopt a more robust controls self-assessment method that will be based on control evidence of effectiveness. An effective system for IT controls evaluation should be established to ensure control data is collected, deficiencies detected and remedial actions

agreed for onward tracking. Further visibility of control environment is desired to gauge the level of protection currents controls deliver.

1.3 Aim

The purpose of this research is to develop a system prototype that facilitates the process of organizations assessing their Information security controls based on their operational effectiveness and design adequacy. Unlike traditional assessment methodologies, the system based control assessments will evaluate the adequacy and effectiveness of controls and help organizations note the deficiencies and track the remediation strategies.

This proposed assessment approach will significantly minimize subjectivity by adopting an evidence based assessment approach where accountability of the control is assigned to control owners (1st Line Management) and ultimately benchmark controls performance to best practice. Evaluating the IT controls using the assessment tool could therefore lead to a thorough and more detailed approach to control testing by providing supporting evidence that will give management visibility on performing controls to effectively improve their information security posture.

1.4 Specific Objectives

- (i) To examine the key IT controls in financial institutions
- (ii) To evaluate approaches applied to IT Controls selection and assessments
- (iii) To analyze the weaknesses of the current methods of IT controls self-assessments
- (iv) To develop an IT controls self-assessment prototype
- (v) To test the developed prototype

1.5 Research Questions

- (i) What are the key IT controls in financial institutions?
- (ii) What are the approaches applied to IT controls selection and assessments?
- (iii) What are the weaknesses to the current methods of IT controls self-assessments?
- (iv) How will the IT controls prototype be developed?
- (v) How will the developed prototype be tested?

1.6 Justification

It is important for organizations especially in the financial services space to know the effectiveness of their IT controls in safe guarding their IT assets. In order to mature the organization's security level that aligns to the security goals, regular assessment of IT controls is paramount. Since there are numerous information security controls that are selected and implemented, organizations usually do not have visibility of the level of effectiveness in protecting the information assets.

Organizations must evaluate and prioritize their IT controls in order to meet their security objectives (Da Veiga & Eloff, 2007). It is the best interest of all organizations to embrace and effective controls assessment methodology to accurately reflect the how well they are protected against information security risks.

1.7 Scope and Limitation

The prototype embeds the process flow from 1st Line controls assessment, 2nd Line independent testing and 3rd Line assurance of the controls testing. In order to achieve the main objective, the research proposes an IT controls evaluation framework that will enable IT management to perform their self-assessment of their deployed IT controls.

The research proposes an IT controls assessment prototype that cover various IT application general controls, Database controls, Physical security controls and Network controls.

There is a reliance on the manual intervention to perform the assessment by the control owners and thus the assessments cannot be performed automatically without data input. The process flow incorporates the control owners to provide evidence based on their observations to assess and evaluate the controls.

The developed prototype will be tested in a secure testing environment that will simulate deployed IT controls to validate accuracy and fit to purpose. The population of this research is 50 financial institutions that have matured their IT estate. The researcher will sample and collect data from 7 institutions.

Chapter 2: Literature Review

2.1 Introduction

The intent and purpose of this chapter is to discuss and put in context the different IT controls assessments methodologies and evaluation approaches adopted by organizations as well as propose and IT controls assessment prototype that will be developed. This chapter will detail the different assessment methods that have been identified with a focus on their adequacy, strengths and weaknesses. The subsequent sections of this chapter will detail and critique all these IT controls assessment methodologies and draw out their inadequacies to build up on the proposed prototype assessment approach.

2.2 Key IT controls in Financial Services Institutions

According to the Security and Privacy Controls for federal information systems and organizations (NIST, 2013) the cybersecurity assessment program outlines key domains to mapping key IT controls as shown in figure 2.1

CPA Domains		NIST Controls	
POLICIES AND STANDARDS	Identity and Access Management	<ul style="list-style-type: none"> •AC-02 Account Management •AC-04 Information Flow Enforcement •CM-07 Least Functionality •AC-01 Access Control Policies and Procedures 	<ul style="list-style-type: none"> AC-03 Access Enforcement AC-05 Separation of Duties AC-06 Least Privilege
	Security Monitoring	<ul style="list-style-type: none"> •AU-02 Audit Events •AU-06 Audit Review, Analysis and Reporting Information •CA-07 Continuous Monitoring 	<ul style="list-style-type: none"> AU-03 Content of Audit Records AU-09 Protection of Audit
	Vulnerability Identification & Remediation	<ul style="list-style-type: none"> •CA-02 Security Assessments •CA-08 Penetration Testing •CM-04 Security Impact Analysis 	
	Host Security	<ul style="list-style-type: none"> •CM-02 Baseline Configuration •CM-06 Configuration Settings 	
	Data Protection	<ul style="list-style-type: none"> •SC-01 System and Comm Protection Policy and Procedures •SC-08 Transmission Confidentiality and Integrity 	
	Network Security	<ul style="list-style-type: none"> •SC-05 Denial of Service Protection •SC-07 Boundary Protection 	

Figure 2.1: NIST Cybersecurity Program Controls (NIST, 2013)

CobiT as an IT governance framework, prescribes various IT controls that aim to ensure that IT works as effectively as possible to minimize risk and maximize the value and benefits of technology investments. The CobiT framework stipulates to IT assurance professionals the generally accepted measures, processes and indicators to ensure that benefits are realized and risk mitigated in a tenable manner. It ensures alignment of IT with the business. (ISACA. 2012)

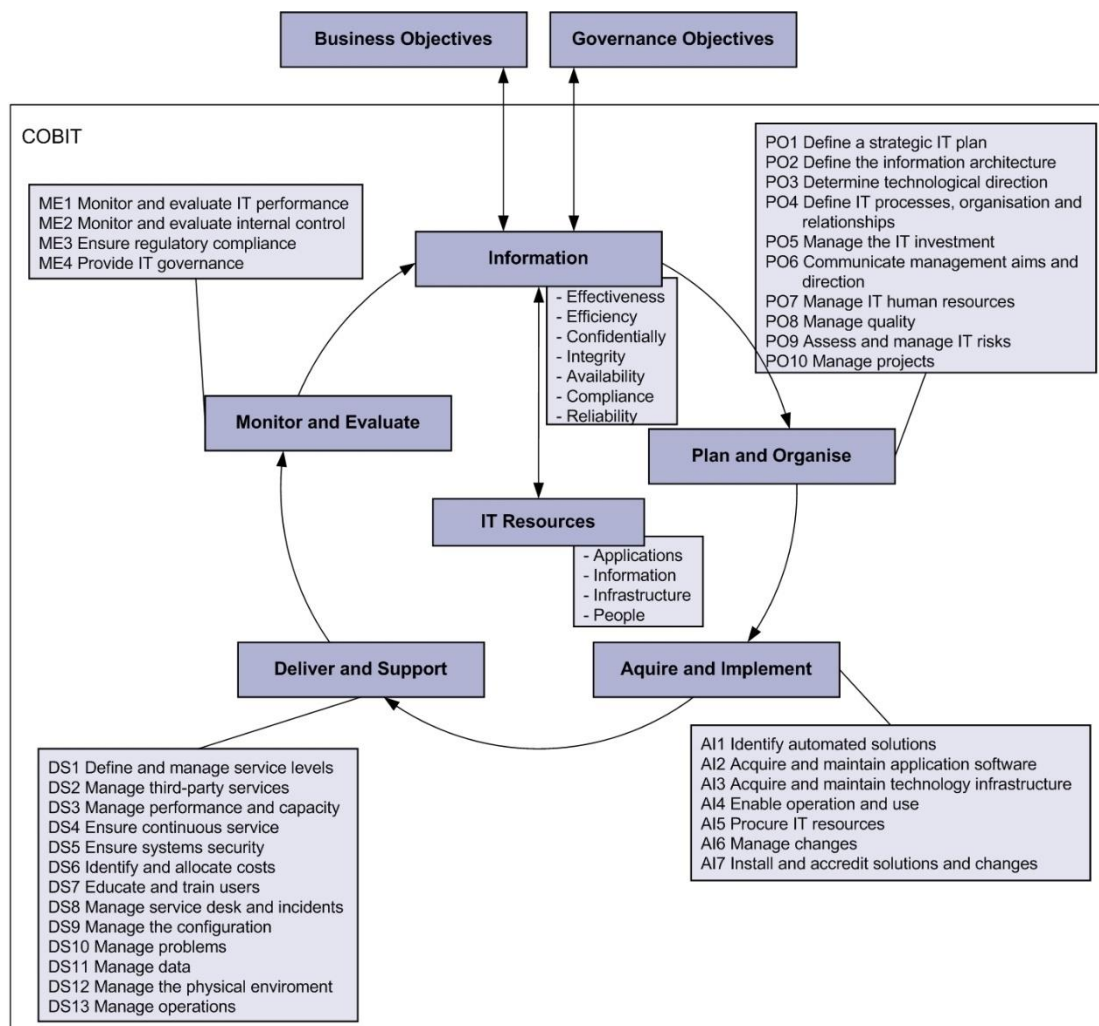


Figure 2.2: CobiT Framework (ISACA, 2012)

2.2.1 Computer Operations Controls (NIST, 2013)

- a) **Firewall configuration and changes** - IT should ensure that preventive measures are in place across the organization to protect information systems and technology from malware (Viruses, worms, spyware, and spam) and unauthorized access for malicious intent.
- b) **Malware and rogue device detection (server and desktop)** - IT should ensure that detective and corrective measures are in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (such as viruses, worms, spyware and spam) and unauthorized access for malicious intent.
- c) **Remote connections and 3rd party network access** - Remote connections and access to the network resources is governed to limit the risk of unauthorized access to financial and financial reporting applications from outside the network.
- d) **Vulnerability management services (VMS)** - Internal and external automated vulnerability scans are performed to ensure that financial applications are hosted in a secure network.
- e) **System security configuration validation** - Controls provide reasonable assurance that operating systems are well protected and that security configuration complies with approved security baselines. Security settings require at a minimum, but not limited to, that there is an authentication mechanism to maintain the effectiveness of the access security (password is required and changed periodically).
- f) **Data center access and environmental factors** - IT Must protect computer assets and business data to minimize the risk of business disruption
- g) **Data replication, back-up and back-up testing** - To ensure that infrastructure and applications used for financial reporting, are recoverable in the event of a localized or widespread disaster.
- h) **Infrastructure monitoring (capacity management)** - Capacity is monitored to ensure that systems don't run out of space causing failure.
- i) **Batch processing and monitoring** - IT management should ensure that the continuous scheduling of jobs, processes and tasks is organized into the most efficient sequence, maximizing throughput and utilization, to meet the objectives set in service level agreements. The initial schedules as well as changes to these schedules should be appropriately authorized.
- j) **Problem management** - The problem management system should provide for adequate audit trail facilities which allow tracing from incident to underlying cause and back. It should closely

interlock with change management, Risk management, capacity management and configuration management

- k) **Incident management** - There is a management system around incident management and incident reporting to ensure incidents are properly managed.
- l) **Contract management** - Changes to all contracts vendors are made in a formal, controlled and approved manner.
- m) **Vendor management** - Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements, SLAs, and that performance is competitive with alternative suppliers and market conditions.
- n) **Contracts with vendors and contractors** - IT management should ensure that all contractors and vendors have valid and authorized contracts in place that conform to universal business standards in accordance with legal and regulatory requirements and that contractors are not paid unless a signed contract is in place.
- o) **Asset Management** - Account for all IT assets (hardware & software) and ensure that they are managed to optimize the value provided by them.
- p) **Software License Management** - Account for all software licenses and ensure that software installed is in compliance with license agreements.

2.2.2 Access to Program and Data (NIST, 2013)

These are controls that relate to user administration of IT elements.

- a) **Termination of users** – Control Ensure that active user IDs exist only for valid employees.
- b) **Extraction of user IDs for revalidation (general users)** - Control to ensure that only users with a valid business need have access to systems.
- c) **User ID IMACD (Install, Move, Add, and Change & Delete)** – Controls to ensure that all authorized user access requests are processed in a timely manner.
- d) **Extraction of privileged user IDs for revalidation** – Control to ensure that only users with a valid business need have privileged access to systems.
- e) **Segregation of duties** – Control to implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process.

2.2.3 Program Changes (NIST, 2013)

Program Changes controls give oversight and guidance over the change management process.

- a) **Change Management** - IT management must ensure that the likelihood of disruption, unauthorized alteration and errors is minimized by a management system which provides for the analysis, implementation and follow-up of all changes requested and made to existing IT infrastructure and applications.

2.2.4 Program Development (NIST, 2013)

These are controls that govern the system development process

- a) **System development** - To ensure that development of new or major changes to existing business applications, meet business and information security requirements.

2.2.5 Entity Level Controls (NIST, 2013)

- a) **ELC.1** – Personal Development Plans and Performance Reviews for IT Staff - IT management has adequate skilled resource to deliver IT services to the business.**ELC.2** – Compliance to defined IT Frameworks - Management ensures that an appropriate IT framework is applied by the business.

2.3 Approaches to IT Controls Selection and Assessments

2.3.1 IT Risk Analysis and Management

The process of encompassing the identification, selection and prioritization of IT controls has posed a challenge in the past and attempts to come up with more effective ways have been made (Barnard & von Solms, 2000). Among the many methodologies and approaches is the Risk Analysis and Management (RAM). The RAM methodology constitutes of performing a business analysis and embedding a risks assessment to identify the risks in information security. The resulting identified risks are also perceived as the requirements according to Barnard & von solms (2000). In this RAM methodology, the information security requirements would be identified and the proposed information security controls be outlined for implementation to mitigate the identified risks from the assessment and analysis performed.

According to Haar and von Solms (2003), the pitfall to this RAM approach has been identified to be subjective and has a bottom-up approach and does not take into account the organizational context and constraints. For instance by performing a RAM an organization may outline 20 information security controls that may be relevant both from an operational efficiency and design adequacy perspective but may be limited in implementing the controls in their entirety effectively due to resource constraints (Staff, costs and time) among others.

The organization may not be adequately resourced to ensure that all the outlined controls have been effectively enforced to mitigate the identified IT risks. The organizations are left to subjectively select the controls they feel are critical to their environment based on their prioritized information assets they want to protect. The main determinant to this selective process would be a cost and benefit analysis that would be determinant for the controls they need to effect. This approach does not effectively evaluate the key controls to implement based on empirical data over their IT estate. Thus this prompts organization to come up with context specific ways and methodologies to evaluate the controls to employ based on evidence rather than subjectivity. This would effectively gauge the relevance of specific information security controls in meeting their control objectives.

Dhillon and Torkzadeh (2006) acknowledge that the RAM methodology has proven to be effective and useful in managing Risk and ensuring information security. This approach has proven to be practical in cases where there were reasonable cost implications on information security incidents that have occurred in the past. However the approach does not conclude to be the best means in achieving information security. Its adoption does not encompass all the success factors of an effective information security controls assessment and evaluation technique.

When organizations use the RAM approach, they baseline controls that can either be irrelevant, or have complexities that are beyond scope. The exclusive adoption of the RAM approach has been critiqued to be more ambiguous in optimizing information security controls rather than being of value.

2.3.2 Best Practice Frameworks/ Benchmark Manuals

Organizations widely use Best practice frameworks and benchmark manuals to introduce, mature and optimize their Information security controls (Barnard & von Solms, 2000). Best practice

frameworks and benchmark manuals assist organization to identify, select and deploy information security controls. Many of the frameworks are based on industry best practice and acknowledged by professional bodies with supporting certifications (Saint-Germain, 2005). The adopted best practice frameworks and benchmarks include

- i. COBIT (Control Objective for IT) by ISACA
- ii. ITIL (Information Technology Infrastructure Library) by AXELOS
- iii. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)
- iv. NIST (National Institute of Standards and Technology)
- v. ISO/IEC 177995
- vi. ISO/IEC 27001
- vii. ISO 27002
- viii. PROTECT
- ix. CMM (Capability Maturity Model)
- x. ISA (Information Security Architecture)
- xi. COSO (Committee of Sponsoring Organizations of the Treadway Commission)

The best practice benchmarking and baseline manual selection process was instituted to provide the data/ information owners with a guideline/ framework for selecting information controls that satisfy the information security and privacy legislation requirements as well as the control and protection objectives of the organization.

According to van der Haar and von Solms (2003), the process of identifying and implementing the most effective IT control from the baseline best practice frameworks and standards can be challenging. They further assert that the identification of the controls to effect is left to the users as per the best practice frameworks. They offer little or no guidance on the controls to implement based on the unique business and IT environment (Haar & von Solms, 2003). Organizational specific constraints and factors such as Staffing resources, budget constraints and time commitments among others are not considered with the direct adoption of the IT controls outlined in the best practice frameworks and benchmark manuals.

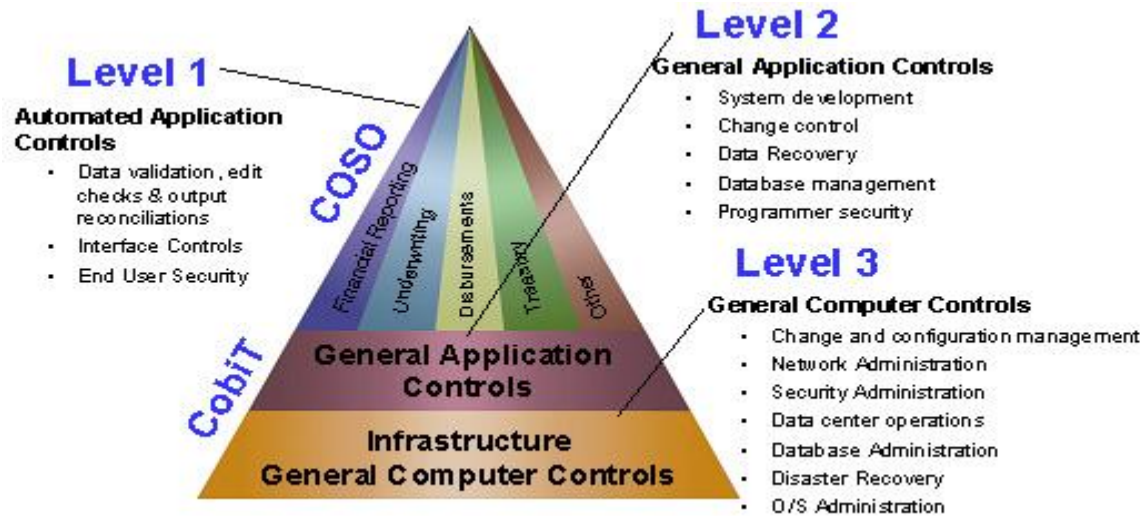


Figure 2.3: All State IT Cntrol Framework, (ITGI, 2010)

Barnard and von Solms (2000) argue that a random adhoc approach to implementing the IT controls stipulated in the Best practice frameworks and baseline manuals may lead to the inclusion of un-necessary, non-critical controls or worse the omission/exclusion of very critical controls required. The NIST Risk management framework embeds a controls life-cycle process from the selection, implementation up to the assessments of the controls. It however does not prescriptively define the controls selection and assessment criteria to be adopted.

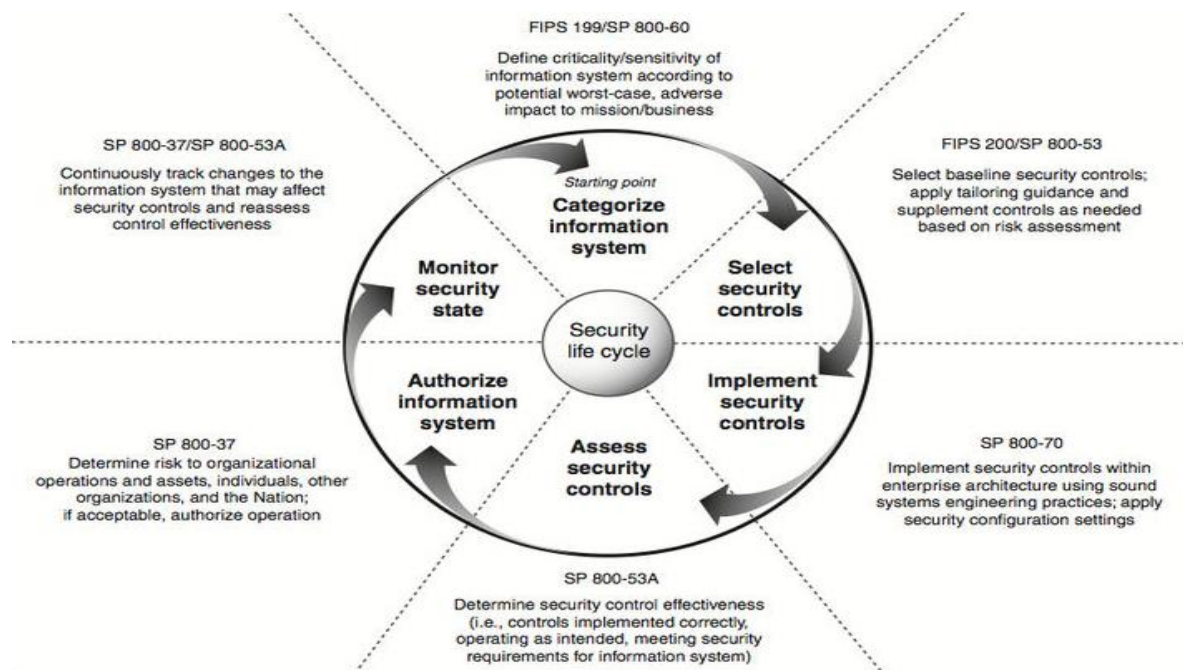


Figure 2.4 : NIST Risk Management Framework (NIST, 2012)

2.3.3 Information Security Checklists

Checklists are also used as a methodology to evaluate information security controls. Chen and Yoon (2010) employed checklists as a framework to identify, evaluate and assess common information security risks, controls in organizations that have employed cloud based infrastructures. The checklists were designed to be used by both Internal Auditors and External Auditor. The checklists outlined the success factors of an effective IT control to provide assurance over the computing environment. The checklists as proposed by Chen and Yoon (2010) were to assess the IT controls over the Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) public cloud delivery models. To base this study Chen and Yoon (2010) hold that check-listing controls for assessment is a popular method of evaluation since it's in-expensive, simple and easily customizable.

Various approaches to information security controls assessments through checklists have been proposed. According to Dhillon and Torkzadeh (2006), their significance has been focused on highlighting “all the possible threats that a computer system has and propose mitigating measures that would help in overcoming the threat”. The emphasis on using information security controls

checklists to assess the controls over the IT estate over the years has dimmed Dhillon and Torkzadeh (2006). This is simply because checklists provide very little analytical ability and are not verifiable based on empirical data. Based on their research and interviewing various Information Security Managers, Dhillon and Torkzadeh (2006) concluded that these checklists can be considered to identify, evaluate and assess IT controls and the very essence of information security controls assessments. Checklists can be used a good approach in evaluating information security controls but over-reliance on the can be flawed and potentially give a false sense of security by a blanket affirmation on a control effectiveness (Dhillon &Torkzadeh, 2006).

2.3.4 Controls Desirability Functions

An innovative approach to assessing and evaluating controls was proposed by Otero, Otero, and Qureshi (2010) to assist organizations choose the most effective and context specific controls with respect to resource constraints. This controls assessment and evaluation methodology employed desirability functions to rate controls based on their desired objectives and quantify them based on the benefits delivered and limitations to achieve the desired goals. While implementing the control, the metric would serve as an indicative of the control rating in satisfying the control requirements. The quality of the information security control would be benchmarked against the organizational goal. A case study was performed and this approach was proved to be successful and provided a way to gauge the quality of an information security controls in organizations. This evaluation was based on specific criteria centric on the organizations.

This approach to IT controls assessment by Otero et al. (2010) factored in relevant quality factors and attributes of effective IT controls to determine their relative significance. This paved way to an IT control prioritization technique that displayed how well the IT controls met the desired quality attributes, and how significant these attributes were to the organization in question. Desirability of the IT controls was defined by the different features inherent to the control to be either present or not. These features were all outlines and determined and the IT controls in questions would be subject to measure against the desired features. This would serve as the basis of this control assessment. Once these “desired” features were determined, each IT control would be evaluated against the feature using a Boolean (binary) scale (i.e. ..., 0 or 1). The IT control that had the higher level of quality as per the Boolean scale was ranked of higher priority as per that specific quality attribute.

Though this approach was able to prioritize IT controls based on their relevance and how well they were able to meet the quality attributes, and based on the organizations' priority of the attributes, the Boolean criteria to selection of the IT controls may not be considered to be the most precise approach to identifying, assessing and ultimately implementing IT controls in organizations.

2.3.5 Information Security Control Attribute Profile

In the study by Van der Haar and von Solms (2003), a model was proposed to derive the optimal set of key control attributes that would match key control objectives. This model was dubbed the Information Security Control Attribute Profile (ISCAP) and was envisioned to assist in the effective selection and subsequent assessments of ISC's. The researchers examined the attribute desired to match-select effective ISC in organizations. In this manner, the organizations in the study were required to outline all the attributes that all their IT controls should encompass before selection and implementation. To cite a few of these attributes were accurate installations, correctness, clearance, acceptance and rules and procedures. Before selecting and ISC for implementation, each of the ISC should have the attributes and characteristics that have been outlined above.

Further to this, Van der Haar and von Solms (2003) states that the identification of security characteristics that optimize control effectiveness is key to ensuring control effectiveness and continuous operation.

The ISCAP controls assessment methodology the organizations were able to determine if the controls were adequate based on the attributes sought by soliciting feedback from personnel and stating whether the attributes were present or not. The main improvement in this approach is formalizing the ISCAP model to one methodology that would address the subjectivity present in evaluating and assessing ISC in organizations to give a more robust and thorough assessment of ISC.

2.3.6 Information Security Risk-Control Assessment Model

To improve and further optimize the information security of organizations, Ou Yang, Shieh, and Tzeng (2011) proposed an Information Security Risk-Control Assessment Model (ISRCAM). This approach specifically combined the Compromise solution and the Multi-criteria optimization technique to assess how adequate the already implemented ISC were against performance. This

was to validate how effective already implemented controls were in safeguarding against various information related risks and incidents hence improving the overall security of organizations.

The model was based on aggregation of functions that represents proximity to the desired control features this was used to rank risk values and risk control areas (Ou Yang et al., 2011). Further stated by Ou Yang et al. (2011) this approach presented multicriteria ranking that was based on how well a control satisfied the desired attributes. Decision makers are assisted by this assessment methodologies by the having a set of choices in conflicting criteria thus selecting the best and most suitable control (Opricovic & Tzeng, 2007).

2.3.7 Information Security Risk Management Model/ Approach

An approach for Information Security Risk Management Model was developed to assess and quantitatively rank ISC by employing the PROMOTHEE methodology and also the GAIA plane (Lv, Zhou & Wang, 2011). This approach is a multi-criteria method of analysis based on pair wise comparisons (Lv et al. 2011). By established a group of decision models to assess and rank the ISC, the authors of this methodology proposed this approach in the Information Security field. From certain aspects of the decision maker's preferences (Line 1 and assurance professionals) this multi-attribute model was based on the PROMETHEE method to assess and evaluate the ISC against certain risks. A criteria based ranking was given accordingly, and a sensitivity analysis based on the GAIA module was brought forward.

The GAIA module considered organizations specific criteria and gave a graphical analysis tool to evaluate the ISC. The criteria used in this assessment included the cost of the information security measurement, how effective the solution is to mitigating risks, social ethical considerations, the demand of the organizational security and other requirements relative to the decision makers (Line 1 & Line 2).

This contribution by Lv et al. (2011) included a multiple criteria based ranking model for the controls that factored in the interests of the relevant decision makers for an information security control plan to be implemented. The authors however noted that though the common expectation for every decision maker is to identify ISC that would match and optimize all the criteria, there however would not be any best solutions and the selection based on this proposed methodology would result to the selection of unnecessary ISC or/ and the omission of the required ones.

Evidently, subjectivity was still a major hindrance to objectively selecting ISC in Lv et al. (2011) study. When employing the ISRMM there's is a high degree of subjectivity be decision makers and thus cannot objectively select relevant and effective ISC based on their adequacy for satisfy the control requirements to meet the objectives. Organizations need to explore better and more effective ways in selecting their ISC and ways for assess them to ensure that the continually meet their objectives.

2.4 Strengths and Weaknesses of IT Controls Assessment Approaches

Table 2.1 Strengths and Weaknesses of Information Technology Controls Assessment approaches

ISC Assessment Approach	Weaknesses/ Critical review
Risk Analysis & Management (RAM) (Dhillon & Torkzadeh, 2006; Barnard & von solms, 2000)	<ul style="list-style-type: none"> As described, RAM is subjective and has a bottom-up approach to controls assessments and does not take into consideration the organization-specific constraints (van der Haar & von Solms, 2003) Unnecessary ISC can be implemented or complex irrelevant controls can be employed when organizations perform RAM The excessive and exclusive reliance of the RAM assessment methodology has proven to be more trivial and problematic than beneficial in maximizing information security by mitigating risks (Dhillon & Torkzadeh, 2006)
Best practice frameworks/ Benchmark manuals (COBIT, NIST, ISO 27001, ITIL, OCTAVE, PROTECT, CMM and ISA) (Barnard & von Soms, 2000; Da Veiga & Eloff, 2007; Siougle & Zorkadis, 2002)	<ul style="list-style-type: none"> Best practice frameworks and baseline manuals leave the selection of ISC at the discretion of the users and offers little guidance on the best controls to adopt as per the particular business situation (van der Haar & von Solms, 2003) The do not account for constraints which are specific to organizations such as costs, resource constraints, time etc. (Barnard & von Solms, 2000).

Information Security Checklists (Dhillon & Torkzadeh, 2006; Baskerville, 1993; Chen & Yoon, 2010)	<ul style="list-style-type: none"> • The provide little analytical stability and thus this approach has significantly declined (Dhillon & Torkzadeh , 2006) • The exclusive dependence on checklists could result in a flawed information systems security strategy (Dhillon & Torkzadeh, 2006). • They do not address the task that the user may have of accurately understanding the substantive questions (Backhouse and Dhillon, 1996) • Checklists focus on what can be done against what has not been done and do not have any analytical stability to the actions that have been identified (Baskerville, 1993).
Control desirability functions (Otero et al.,2010)	<ul style="list-style-type: none"> • This assessment method of determining which ISC to select using a Boolean criteria may not be precise enough since it also has some degree of productivity (Otero et al., 2010)
Information security Risk-Control Assessment model (Ou Yang et al.,2011)	<ul style="list-style-type: none"> • This model focused on assessing the effectiveness of selected and already implemented controls and does not give guidance on implementing new controls. (Ou Yang et al., 2011)
Information Security Risk management model approach (Lv et al.,2011)	<ul style="list-style-type: none"> • Selection of the ISC is solely dependent on the preferences of the decision maker and not objective enough (Lv et al., 2011)

2.5 Proposed conceptual framework

2.5.1 IT Controls Assessment Prototype

The proposed conceptual prototype will have the control owners perform the controls assessment that will be defined by the system with matching controls evaluation criteria. These evaluated controls will then be reviewed by a supervisor (process owner) who will validate and ratify the assessments. All control with noted deficiencies will be stored in the system where they will be tracked for remedial actions to close the gaps. The system will have a reporting capability that the oversight assurance team will be able to extract reports to get visibility of the controls performance.

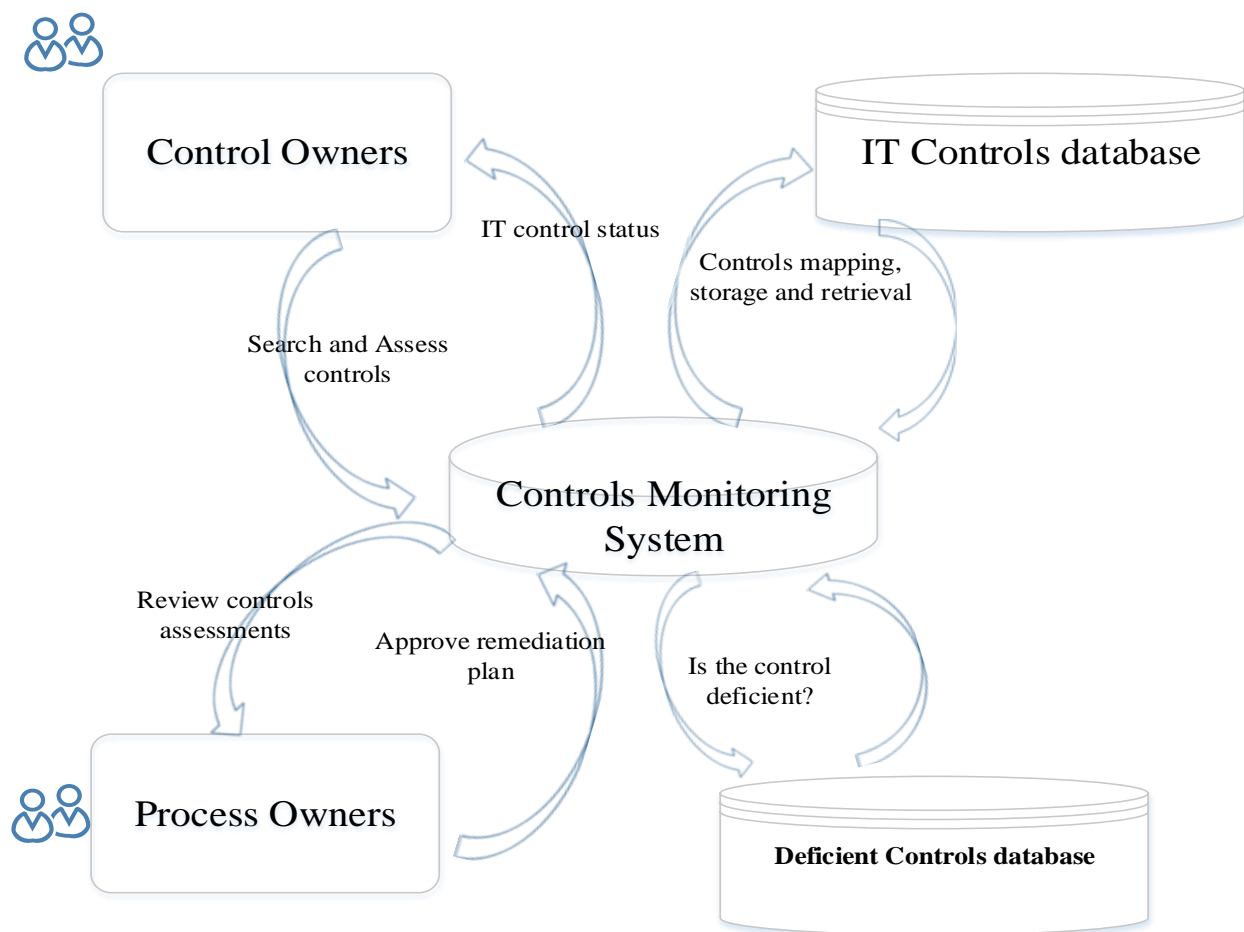


Figure 2.5: Proposed Conceptual Framework

Chapter 3: Research Methodology

3.1 Introduction

This chapter outlines the research methodology that was adopted in this study. It discusses the research design, population of study, data collection, data analysis techniques and presentation methods used in this study.

The main goal of this research was to design and develop a practical and relevant controls assessment prototype that can be used in assessing IT controls in Kenyan financial institutions. The prototype will be used by management and assurance professionals to determine if controls are effective by assessing and evaluating IT controls based on the control objectives that are quantitatively reviewed. The control assessment prototype will outline the methodology and process flow that will be embedded to review and assess the implemented controls to ensure that they continually perform against the expected control goals. In-effective IT controls can pose a risk to organizations since they give a false sense of security.

3.2 Research Design

This was an applied research and used quantitative methods to examine the relationships between variables. These relationship were analyzed and represented mathematically by using statistical analysis. The findings gathered from this research approach formed the basis to develop the controls assessment prototype that was used to assess the IT controls. This prescriptively attempts to propose a solution to the problem of assessing IT controls. In the context of quantitative research, the goal of the researcher was to gain a deep, intense and 'holistic' overview of the topic under study. Since this approach allowed the researcher to contact the experts in the field, it is regarded as a good approach.

3.3 System Development Methodology

According to the Centre for Medicare and Medical services (2008), a systems development methodology is the process framework for planning, designing and development of an application

system. In this work, the researcher adopted a systems development methodology. The prototype of the proposed solution was developed using the Rapid application development methodology (RAD).

Due to the researches limitation on time and other resources, this development approach was the most suitable due to its iterative nature. This development approach yields optimal quality software builds at a relatively low price and enables the developer to rapidly effect changes due to its iterative nature. According to Nashawaty (2015), the development approach enables the researcher to reduce the overall risk since the prototype development is broken to small sub-tasks which are easy to manage. After determining the high level requirements of the overall system, the RAD approach was employed to demonstrate the proof of concept of the functionality as well as to define additional requirements. This iterative process continued until the system interface was delivered to the users for user acceptance testing.

The user requirements needed for the design and development of the prototype was clear and the need for a simultaneous verification exercise was high. This study applied the V-process model to develop the system while testing and verifying interpretively. The V-process model is a model for verification and validation. It enables the developer to incrementally develop while validating the software build. It also follows a sequential process of execution (Khan & Beg, 2013; Khan, Parveen & Sadiq, 2014).

3.3.1 The V-process Model Approach

For the development of the prototype the various stages of development will have a corresponding test plan that will be simultaneously be created. These are detailed as below;

- i. **Requirements** – The researcher solicited the user requirements for the prototype while creating a test plan to ensure that the system meets the specified functionality articulated in the requirements gathering phase.
- ii. **The high-level design (HLD)** - The researcher worked on the system architecture and design. This provided an overview of the solution, platform, system, product and process. The researcher also created an integration test plan that would aim to test the different components ability to work together.

- iii. **The low-level design (LLD)** - In this phase, the actual software components were designed. The actual logic for each component of the system was defined. In this phase, the Class diagram was created detailing all the methods and relation between the classes comes. Simultaneously, the component tests were also created.
- iv. **Implementation** – This is where the system build and coding was done by the researcher. Once coding was completed, the software test plans were created to be performed concurrently with the code execution. Software bugs were identified and resolved by the researcher.
- v. **Coding** - As the last phase in the v-process development model, the module designs was converted into code by the developer. Unit testing was performed against the written code.

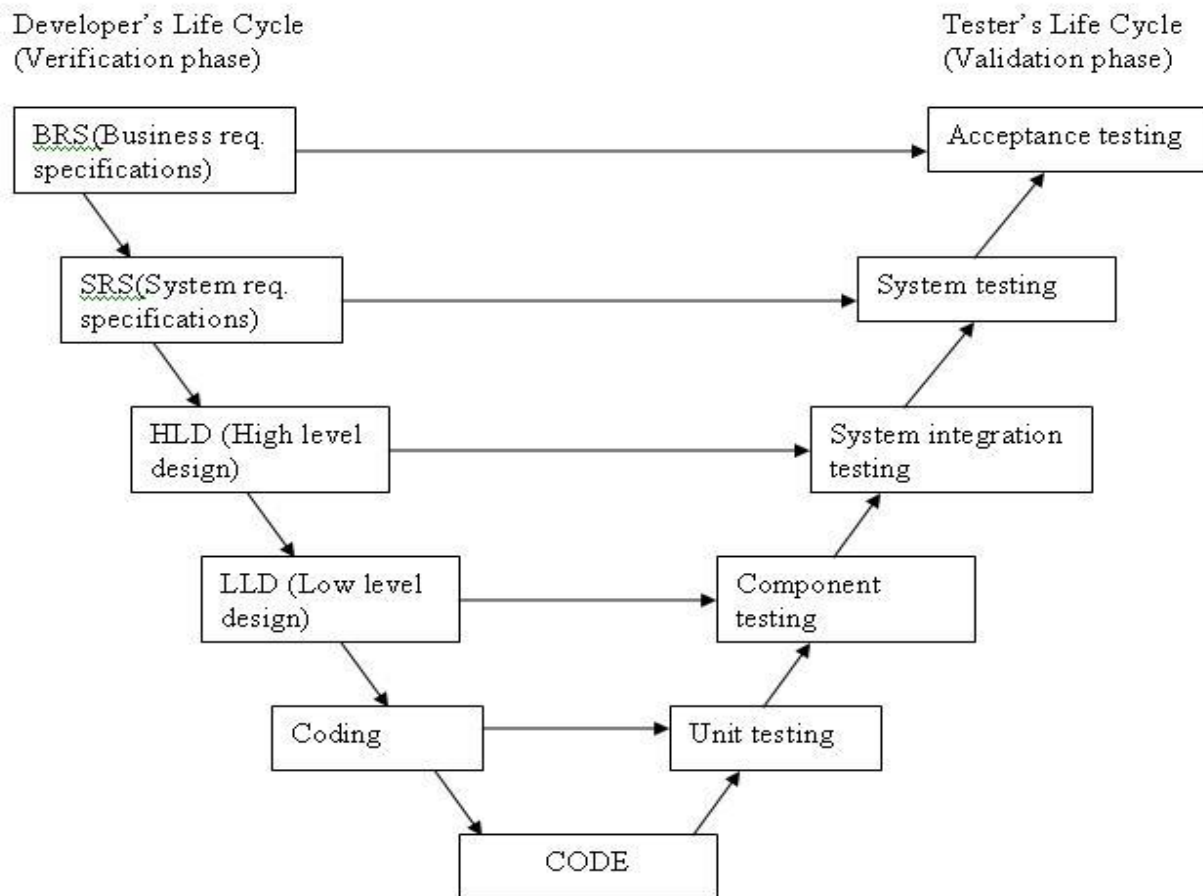


Figure 3.1: The V-process Model, (Nashawaty, 2015)

Since the development required an iterative and rapid development approaches, the RAD and v-process approaches proved to be the most suitable.

3.4 Target Population

A target population is the particular population the researcher has interest in, as intends to extract the research sample from (Kothari, 2004). This target population can be defined as the entire member or the hypothetical sets of people, companies, objects or events that the researcher wishes to extrapolate and generalize the results of the study (Mugenda, 2003). The total population for this research was 50 financial institutions in Kenya with a high level of technology adoption.

3.5 Sampling Procedure

Since the researcher at the time of the study worked in Nairobi, Upper Hill area that hosts various financial institutions in insurance and banking, a convenient sampling approach enabled him to conveniently conduct the study within a busy work and study schedule. The sample selected for this research was seven Kenyan financial institutions that have rolled out IT controls in their environment. According to the Serianu cyber security report (2015), the financial services sector is the most targeted and prone to information security incidents and attacks that can cause the greatest financial implications such as insider fraud, loss of revenue due to service disruptions and hacking.

Three respondents in each organization were selected from the IT operations, IT Risk and IT Audit teams by the researcher. There was total of 21 respondents.

3.6 Data Collection Methods

The study used different approaches to get both primary and secondary data such as questionnaires as the primary data collection method.

- (i) Structured online questionnaires with close-ended questions. These questionnaires were administered to the Information Technology (IT) managers/Chief Information Officers (CIO) and IT Assurance managers depending on the organization and the structure in each. The questionnaires were administered before developing the prototype to understand the user requirements and after development of the prototype to find out the user experience

of using the newly developed prototype. The researcher preferred the online questionnaires due to their convenience.

- (i) Information Desk research was used as a secondary source of information. To deepen understanding of the global best IT control practice, the researcher examined various standards, frameworks and architectures. The researcher also explored the various software development tools and technologies to select the most optimal.
- (ii) Interviews were also used to gather information from the IT respondents under study. An interview is a conversation between people for information gathering purpose in which one person has the role of a researcher (Mugenda, 2003). Interviews were very instrumental since it allowed the researcher to ‘probe’ for more detailed responses where the respondent was asked to clarify what they have said (Kothari,2004; Mugenda;2003). The interviewed offered a better way of understanding the current process of assessing and evaluating the IT controls. The open interviews enabled the researcher get more information and further clarity which helped the researcher deepen the process understanding. In the detailed gathering of the user requirements for the prototype, the interviews served to be very instrumental.

3.7 Data Analysis and Presentation

This entailed organizing the collected data and further breaking them down into smaller, easily understood parts. The Quantitative data collected was analyzed using Microsoft Excel since it allows a useful number of statistical analysis functionalities. The findings/ information of this research is be later on presented using these tools

- i. Tables - Significant variables are summarized by Tables
- ii. Pie Charts – To present the results of the quantitative data in a visual format and facilitate correlations and comparisons within the data.

3.8 Research Quality

3.8.1 Reliability

Reliability was improved by presenting the findings to experts in the field and getting their views on the subject matter. This ensured relevance of the study and its findings. The researcher’s work

was thoroughly reviewed by the researcher's supervisor to ensure that the research objectives were met.

3.8.2 Validity

In order to ensure the validity of this research, respondents reviewed the transcripts of their interviews both for accuracy and to see if there are any comments they would like to add. This way the researcher confirmed that the analysis is based upon evidence and that the findings are accurate.

3.8.3 Objectivity

All data collected from the field is factual and not influenced by personal feelings or opinions in considering and representing facts. The data is not subjective but was ratified by independent observations based on the data collected.

3.8.4 Analysis of the methodologies

In the study, Content analysis was applied to further analyze the IT control assessment methodologies, strengths and weaknesses. This describes making inferences about data (usually text) by systematically and objectively identifying special characteristics (classes or categories) within them. This approach is highly adopted in the study in analyzing the methodologies, frameworks and other approaches addressing the same problem in a research. (Gray, 2009)

3.8.5 Ethical Considerations

In order to uphold high ethical standards in this study, the researcher obtained consent from the participants selected before the survey. Permission was sought from the respondents to participate in the study and the data gathered was treated with a high degree of confidentiality. The received data was used for the sole purpose of this research. The questionnaires to be shared with the respondents have a disclaimer to this effect.

Chapter 4: System Analysis and Design

4.1 Overview

System analysis and design is the process of defining the description (top-down) of the system architecture, design, components, modules and interface in order to match the specific requirements articulated by the user (Faisandier, 2012). System analysis entails the collection and analysis of the user articulated requirements and translating them into logical and conceptual models. System design is defined as the process of defining the architecture, modules, data and interfaces for a system to satisfy specified requirements (Daniel, Barbara & Allen, 2001).

4.2 Data Analysis and Findings

To gather the user requirements extensively, questionnaires were administered to the respondents subject to this research (IT management Line 1 & 2). Interviews were held with the various IT assurance staff in order to understand the current control assessments methodology. The results to the research were collected, analyzed and presented using the pie charts.

4.2.1 Cyber Incidents Caused by IT Control Gaps

As illustrated in Figure 4.1, 41% of the respondents (IT control and process owners) strongly agreed that cyber incidents are caused by gaps in IT controls. 32% agreed to this hypothesis and held it that it was true. 14% of the responded were neutral to where IT control gaps are the causing agents of cyber breaches. 9% of the respondents disagreed to this holding that other factors come in and not gaps in IT controls. 4% of the respondents strongly disagreed that IT controls lapse result to cyber incidents but other factors were the major cause.

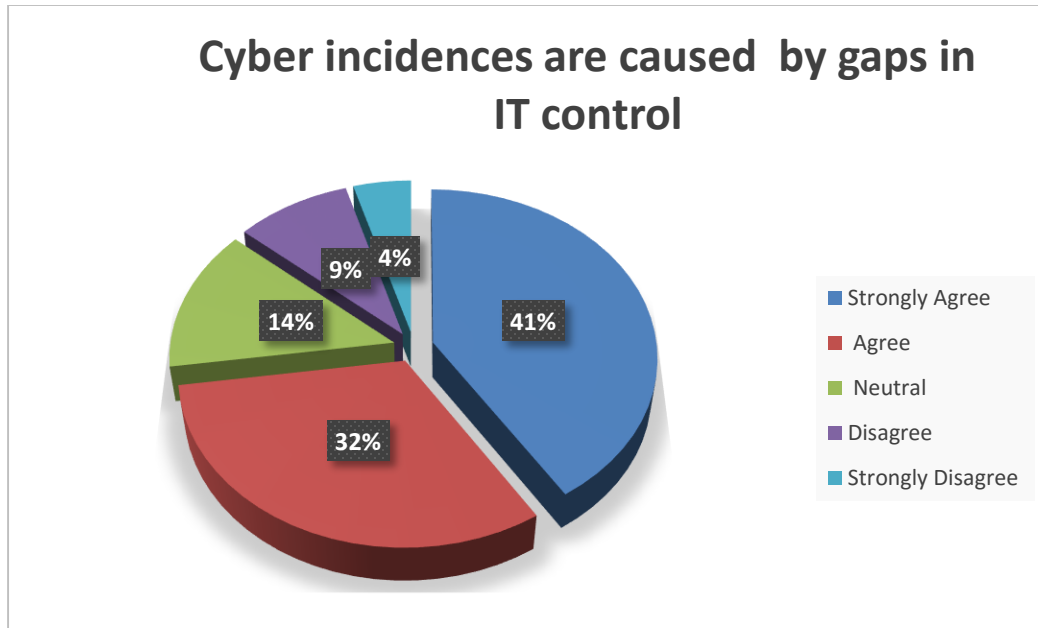


Figure 4.1 : Cyber incidents caused by IT control gaps

4.2.2 Efficiency of The Current IT controls Assessment Methods

43% of the responded strongly disagreed that the current IT controls self-assessment methods are efficient. Another 24% were in agreement that these methods are in-efficient and consume a lot of time and resources. 10% of the sample group respondents were neutral and did not have any opinion on the same. 14% agreed that the current manual methods of assessments were efficient and 9% strongly agreed that their assessment approach is efficient.

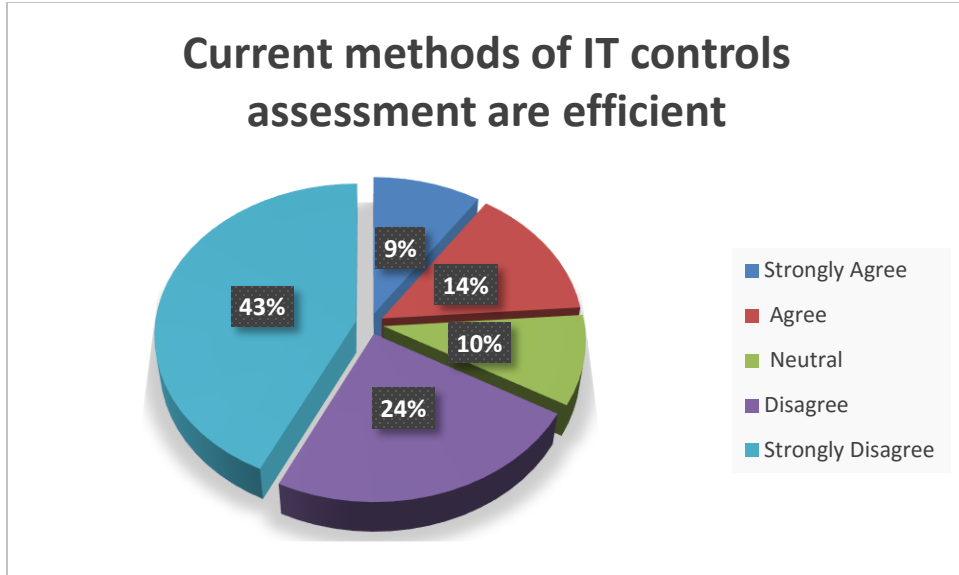


Figure 4.2 : Efficiency of Current Methods of IT Controls Assessments

4.2.3 Visibility of In-effective IT Controls Through Manual Control Assessments

In the current manual controls self-assessments 43% of the respondents strongly disagreed that they obtain visibility of how controls are operating with a focus on control effectiveness. A further 33% disagreed to the capability to oversee their in-effective controls. 5% of the respondents were neutral, 10% agreed and 9% strongly agreed.

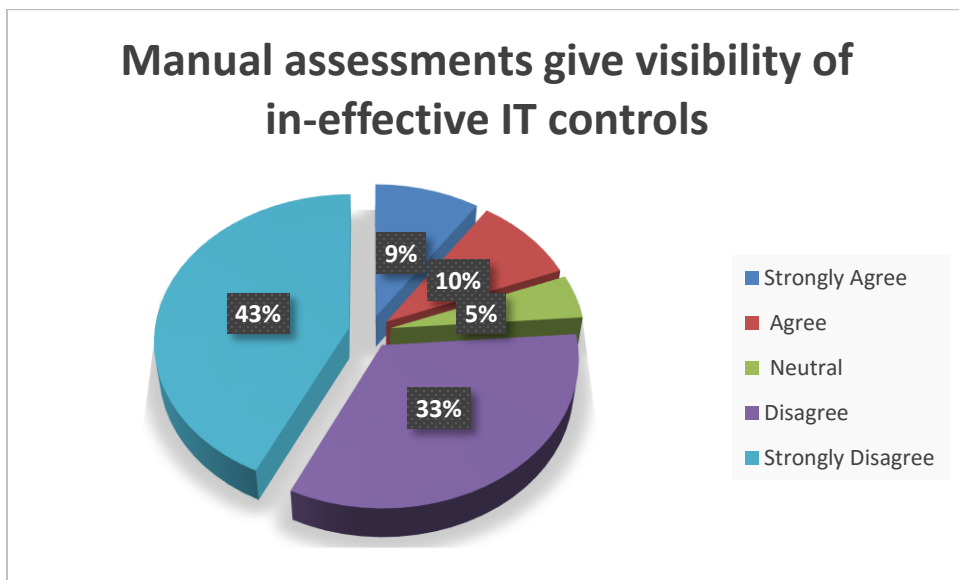


Figure 4.3 : Visibility of In-effective IT Controls Through Manual Assessments

4.2.4 Subjectivity of the Current IT Controls Assessment Methods

To research on the subjectivity of the current IT controls assessment methods, and to establish whether the methods are evidence based and not subjective. 43% strongly agreed to the fact that current control assessment methods are subjective and not evidence based. 33% of the respondents agreed to this claim, 5 % were neutral, 14% disagreed and 5% strongly agreed. This is illustrated in Figure 4.4

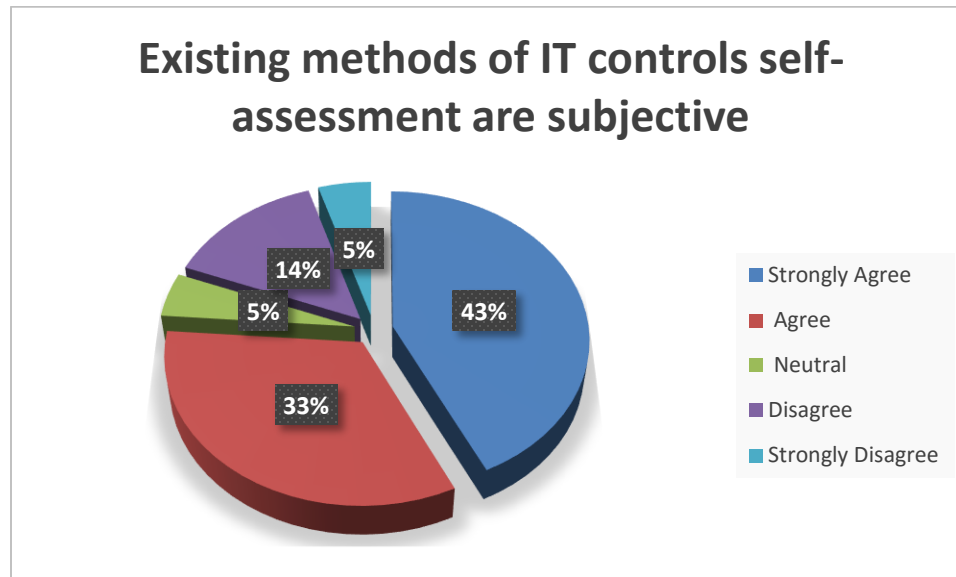


Figure 4.4: Subjectivity of Existing IT Controls Assessment Methods

4.2.5 Effectiveness and Accuracy of System Based Control Self-assessments

48% of the respondents strongly agreed that system based IT controls self-assessment is more effective and accurate. 29% agreed to this, 5% remained neutral, 9% disagreed to the assessment accuracy and effectiveness and 9% strongly disagreed. This is depicted in Figure 4.5.

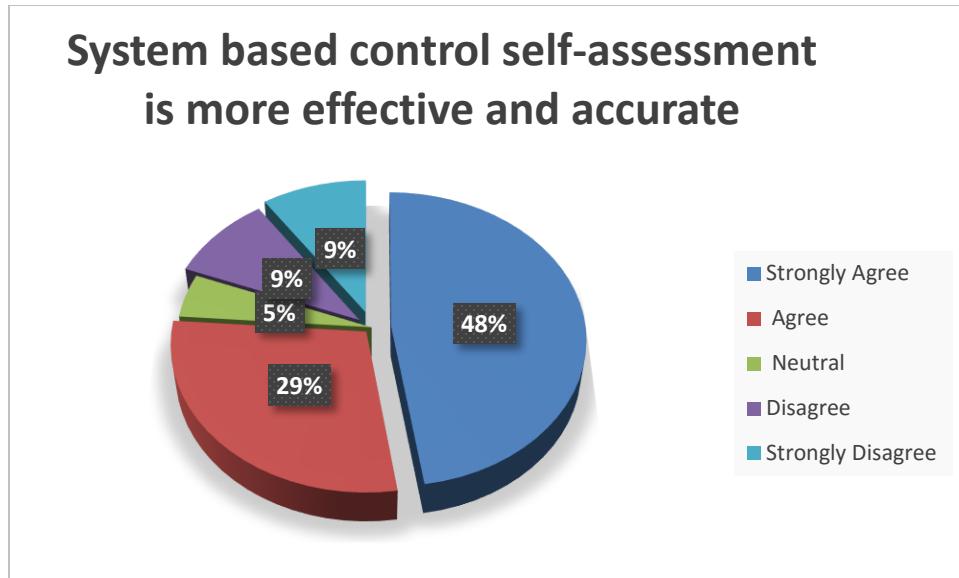


Figure 4.5: Effectiveness and Accuracy of System Based IT Controls Self-assessment

4.2.6 Confidentiality of IT Control Gaps Findings

On the confidentiality of their control gaps findings upon gap assessments performed, 43% strongly agreed that this information is sensitive and highly confidential. 33% agreed to the confidentiality of the gap assessments. 5% were neutral to this, 9% disagreed and 10% strongly disagreed. This is shown in Figure 4.6

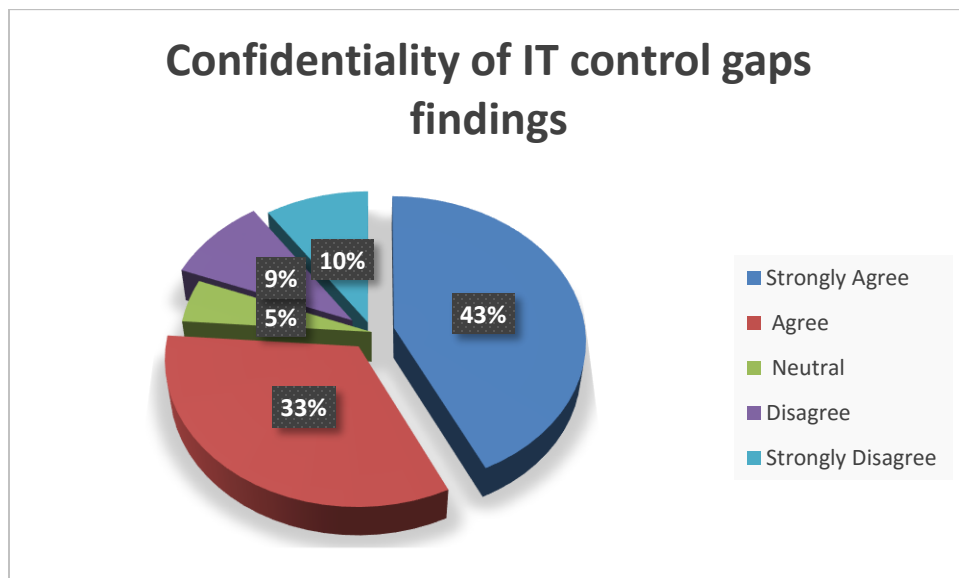


Figure 4.6 : Confidentiality of IT Control Gaps Findings.

4.3 Requirements for the proposed system

4.3.1 End-User Requirements

By administering the questionnaire to the end users of the system, the research established that the users needed a system with the below specific requirements:

- i. A system that would enable IT process owners to evaluate and test their IT controls
- ii. A system that would be able to define the pass criteria of a successful control and a deficiency indicator of an in-effective/ failed control
- iii. A system that would notify management of an ineffective/ deficient control
- iv. A system that would enable management to track remediation efforts on deficient IT controls
- v. An intuitive and user friendly system
- vi. A scalable system that is able to onboard more users incrementally
- vii. A secure system that maintains confidentiality, availability and integrity
- viii. A system that would enable accurate and data driven decision making by embedding intelligent reports.

These user requirements that were gathered from the end-users were further clustered into functional and non-functional requirements. Functional requirements articulate the accrual functioning of the system while non-functional requirements capture the underlying logic and constraints of the system (Daniel, Barbara & Allen, 2001). The system requirements were extracted from the functional and non-functional requirements.

4.3.1 Functional Requirements

- i. The IT control owners and process owners should be created in the system prior to using it
- ii. Authorized users (Control/Process owners) shall be assigned IT controls that fall in their domain and relevant to their duties
- iii. Control owners shall have a view of all their controls, controls objectives and assessment criteria
- iv. The developed system should allow the control owners to assess their controls (Pass or Fail)

- v. The system should give provision for control owners to upload their evidence of control effectiveness (Reports, logs, emails etc.)
- vi. The control should prompt the control owners to track their remediation updates to failed controls
- vii. The system should generate reports as prompted

4.3.2 Non-Functional Requirements

- i. The system should be reliable, secure and efficient
- ii. The system should ensure quality data processing and accurate reports
- iii. The system should be user-friendly and easy to use to novice computer users
- iv. The system should be scalable, agile and extensible to future customizations and change
- v. The system should be resilient and robust
- vi. The system should have interoperability with any operating system and hardware.
- vii. The system should only allow authorized users to have access i.e. strong authentication mechanism

4.3.3 System Requirements

The proposed IT controls assessment system had the following system requirements for its operation

a) Graphical User Interface (GUI)

A graphical user interface shall be developed to enhance usability. The GUI shall be user friendly and intuitive. This shall be used in assessing the controls, giving control evidences and generating reports on assessments.

b) Relational Database Management System (RDMS)

A central database shall be used for easier collection, organization and storage of data. This will facilitate seamless creation, updating, extraction and analysis of data. The system used open source MySQL due to its openness, portability and interoperability

c) System Security

To ensure that the system maintains confidentiality, integrity and availability proper security mechanisms shall be embedded. Proper authentication mechanisms shall be

enforced with strong password controls. To ensure system data availability in the event of a disaster, full data back-ups shall be performed.

4.4 System Process Modelling

A software/system process model is the abstract representation and design of a software process (IEEE, 1995). This is an abstract representation of the software design and function in a standardized format to enable planning, organizing and implementation of a software development project. The software process modelling is composed of software objects, the use case interactions of the system, the sequence activities and events.

4.4.1 Context Level Diagram

There are four users that are engaged and handle this process namely: the control owner, process owner, IT assurance management and the system administrators. The main process is the IT controls assessment by the control owners. The system administrator adds the control owners and process owners in the system as users. Upon successful log-in, the control owners views the controls, assess them and upload all the assessment evidence. The process owners then verify and approve the assessments done by the control owners. If a control has failed, a process for remediation tracking in that case. The IT Assurance management

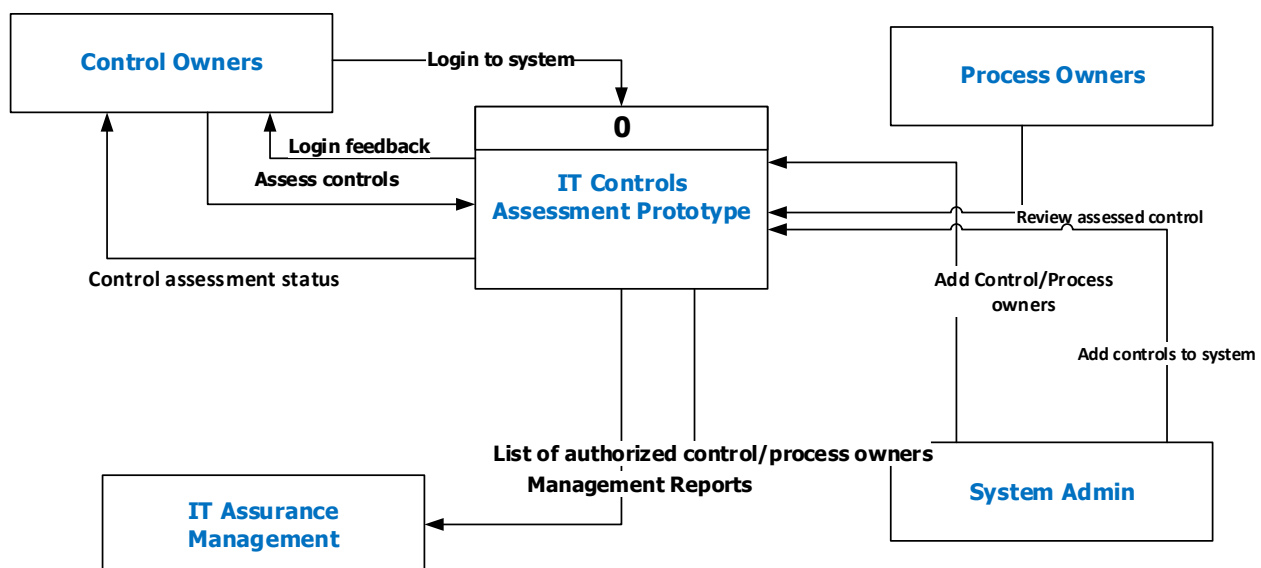


Figure 4.7 : Context Level Diagram

a) Level 0 Diagram

The context diagram (Figure 4.7) illustrated the key processes in assessing the IT controls.

These processes are;

i. Managing users (control and process owners)

The users managed in the system are the control owners, process owners and IT assurance managers that comprise all the authorized users. This process entails the creation of new users in the system, modifying user rights and deleting access of the existing users (access revocation)

ii. Uploading foundational IT controls to system

The system administrator will upload all the IT controls to be assessed in the system with guidance from the assurance management team. These controls will be extrapolated from various IT controls baselines and standards. The control framework used here is NIST SP 800- 53 and COBIT 5.

iii. Assessing of IT controls

This controls assessing process provides an interface to view all the assigned controls to the owners and assess them based on defined benchmarks. Upon assessment control owners will upload evidence to the functional control based on the expected control evidence. The control evidence include but not limited to production reports, screenshots on configurations, email communication, system generated data on control output (Firewall rules, system access matrix etc.)

iv. Review of IT control assessment

Here is a review process of the assessed IT control. The process owners have to log on to the system. The process owners will view the already assessed controls on a dashboard and confirm the assessment on accuracy, relevance and fit to purpose. If a control has passed the assessment, this process will end there subject to independent testing. If the control has failed the assessment, the reviewer will review the deficiency log raised by the control owner as well as the remediation

plan to track all commitments and actions. This step is repeated for all controls assigned to control and process owners.

v. Synchronizing Controls Assessments

This process will happen in the back end and will aim to consolidate all the failed and passed controls. This information will be used to gauge the controls maturity based on a standard maturity spectrum

vi. Reports Preparation

The IT assurance management will enter the desired report fields i.e. Dates, control owner, process owner. This will be selected by distinct categories. The process extract reports for all assessed controls, passed controls and failed controls. All the aforementioned processes have been graphically represented and summarized in Figure 4.8.

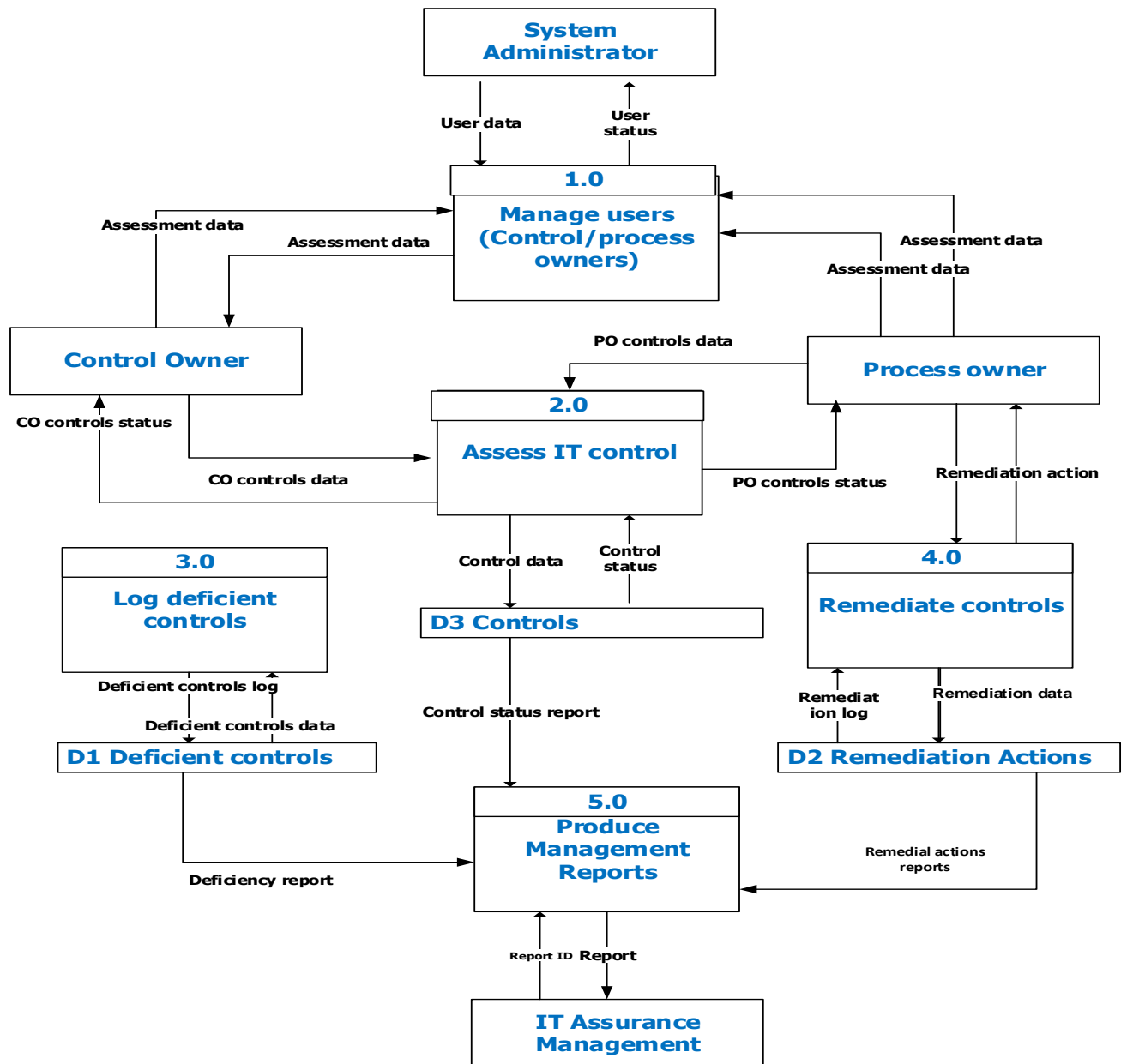


Figure 4.8: Level 0 Diagram

4.4.2 Use case Diagram

In use case modelling, a use case diagram represent a list of well-articulated actions that defines a set of well-defined system interactions that aim to achieve a certain goal. Each use-case interaction is captured as a contract that depicts the system behaviors and represented as a single unit of work

(Gemino & Frasier, 2009). The use case diagram captures most of the system's functional requirements

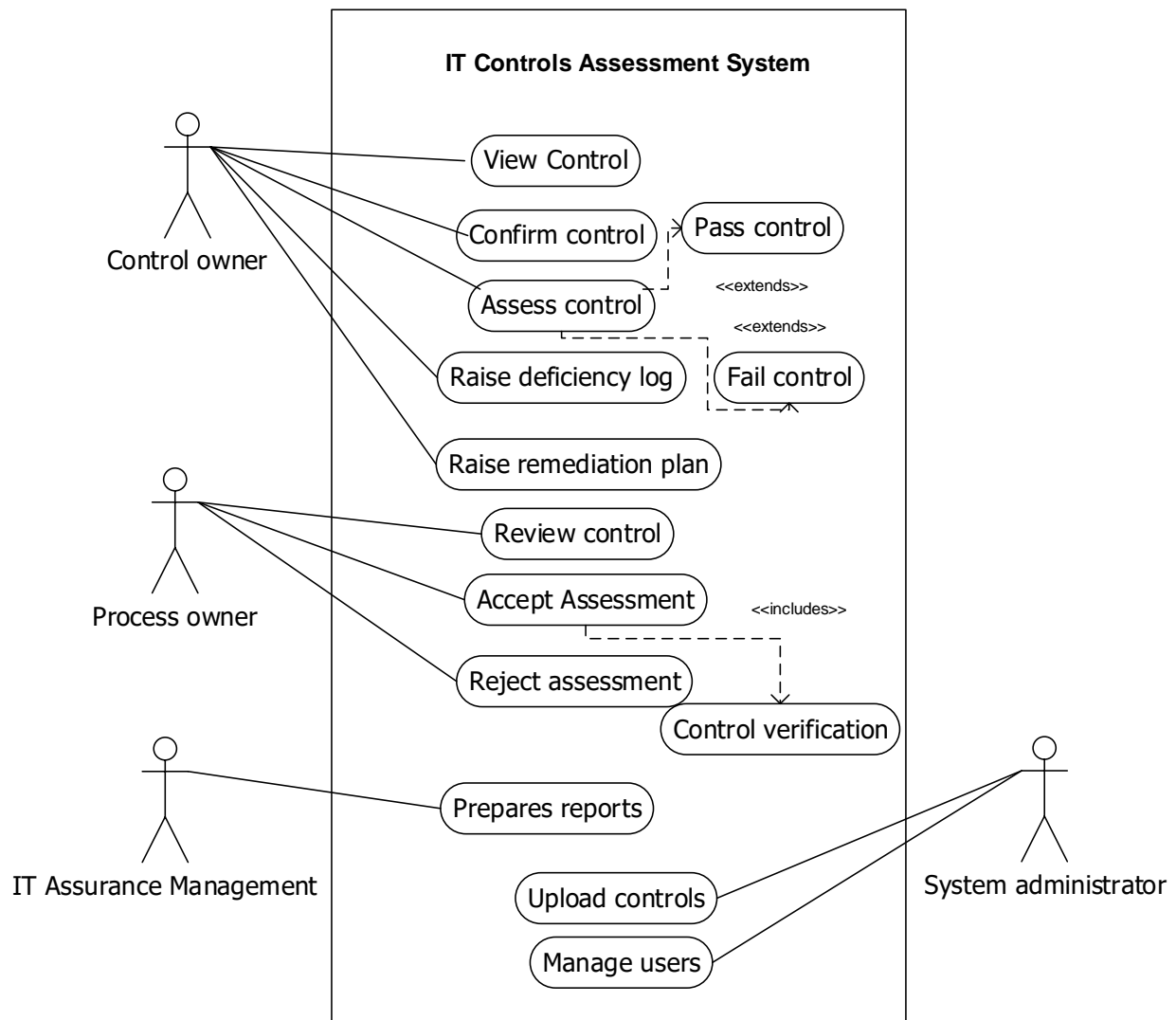


Figure 4.9 : Use Case Diagram

The system use cases can be represented in Table 4.1 that illustrates the major actors and use-cases.

Table 4.1 : IT Controls Assessment System Main Use Cases

Actor	Use Case
System Administrator	Assign controls to owners View reports

Control Owner	Assess controls Raise Deficiency Log Raise Remedial plan
Process Owner	Review control assessment Accept control assessment Reject control assessment Verify control remediation
Assurance Management	View reports

The first use-case entails managing of the control and process owners. As the 1st line IT operations team, they would be responsible for the day to day working of the general computer controls. The system administrator would be responsible for mapping the IT controls to the respective IT personnel across the several control domains such as Networks, Databases, Infrastructure, Project management etc. The control and process owners would provide their details such as email address, full names their roles and area of responsibility to be assigned access rights to the controls assessment system. To update the control user list, it entails highlighting the control-assigned user, clicking on ‘edit’ to supply the update details and clicking the ‘update’ button. Authorization of users to the system are limited to the ones with active accounts. Updating this status gives or denies users access to the system. Table 4.2 represents the control owners’ management use case.

Table 4.2 : Manage Control Owners Use case

ID	Use Case 1
Title	Manage control owners
Description	Assign, update and delete control owners
Actor(s)	System Administrators
Pre-conditions	The system admin has logged in to the system
Post-conditions	Control owners successfully assigned, updated and deleted

Main success scenario	<ul style="list-style-type: none"> i. The admin enters the details of the new control owner (email, full names, Title), selects the control owner and clicks 'save'. ii. For an update of the control owner details, the admin clicks on the edit button, enters the new owner data and clicks 'update'.
-----------------------	--

Table 4.3: Assess Control Use Case

ID	Use Case 2
Title	Assess Controls
Description	Assess control based on performance
Actor(s)	Control Owners
Pre-conditions	The control owner has successfully logged in to the system
Post-conditions	Control owners successfully assigned and updated
Main success scenario	<ul style="list-style-type: none"> i. Select control to assess ii. Pass control iii. Fail control iv. Upload control evidence

Table 4.4 Upload Control Evidence

ID	Use Case 3
Title	Upload Control Evidence
Description	Upload data on control performance
Actor(s)	Control Owners
Pre-conditions	The control has been passed
Post-conditions	Control evidence has been collected
Main success scenario	<ul style="list-style-type: none"> i. Select control evidence to upload ii. Upload control evidence

Table 4.5 : Raise Deficiency Log Use Case

ID	Use Case 4
Title	Raise Deficiency Log
Description	Raise the control deficiency and gaps
Actor(s)	Control owner
Pre-conditions	The control has failed the assessment ('fail' status)
Post-conditions	Control objectives have been defined (Key control indicators)
Main success scenario	Record deficiency log

Table 4.6 : Raise Remediation Plan Use Case

ID	Use Case 5
Title	Raise Remediation Plan
Description	Detail control remedial actions
Actor(s)	Control owner
Pre-conditions	Control has failed and deficiency recorded
Post-conditions	Tracking on remediation is performed
Main success scenario	Remediation plan successfully created

Table 4.7 : Review Control Assessment

ID	Use Case 6
Title	Review control assessment
Description	Review of the performed control assessment
Actor(s)	Process owner
Pre-conditions	Control has already been assessed (Passed or Failed)
Post-conditions	Approval of the control assessment is done
Main success scenario	Control assessment has been agreed

Table 4.8 : Accept Control Assessment

ID	Use Case 7
Title	Accept control assessment
Description	Acceptance of the control assessment
Actor(s)	Process owner
Pre-conditions	The assessment has been reviewed
Post-conditions	Assessment is accepted and status has changed
Main success scenario	Control assessment status has changed

Table 4.9 : Reject Control Assessment

ID	Use Case 8
Title	Reject Control Assessment
Description	Rejection of the control assessment
Actor(s)	Process owner
Pre-conditions	The control has been rated and assessed
Post-conditions	Assessment is rejected
Main success scenario	Control assessment status has changed

Table 4.10 : Verify Control Assessment

ID	Use Case 9
Title	Verify Control Assessment
Description	Verification of the assessed controls
Actor(s)	Review group (Assurance management)
Pre-conditions	The control assessment has been reviewed by the control owner
Post-conditions	Assessment has passed or failed
Main success scenario	Control assessment is independently tested

Table 4.11: View Reports

ID	Use Case 10
Title	View Reports Use case
Description	Reports on : <ol style="list-style-type: none"> i. Controls assessed ii. Controls not assessed iii. Controls passed iv. Controls with deficiency v. Assessment due date
Actor(s)	IT Assurance Management & System Administrator
Pre-conditions	<ol style="list-style-type: none"> i. Users log in successfully ii. Control owners/ process owners updated iii. Control details updated iv. Controls assessed
Post-conditions	Extraction of detailed report
Main success scenario	<ol style="list-style-type: none"> i. User selects category to extract report ii. User selects the sub-category of the report iii. User defines the reporting period iv. User select submit button v. The user extracts the report

4.4.3 Sequence Diagram

The sequence diagram as a software modelling tool provides a visual representation of the interactions between objects in the control assessment process. This details the actors and the object the actors interact with in the execution of the assessment process.

By executing the ‘assess control’ action, the control owner initiates the control assessment process. This is followed by the fail/ pass selection of the control in question where the assessor is prompted to upload control evidence. When controls fail, the process that follow is for a deficiency log to be raised which is mandatory as well as a remedial plan. The control owner then ends the process

once evidence is attached for passed controls and deficiency log and remediation plan recorded for failed controls.

If the control owner has another control that needs to be assessed, they will be prompted on the dashboard where the status will be indicative. This interaction is summarized in Figure

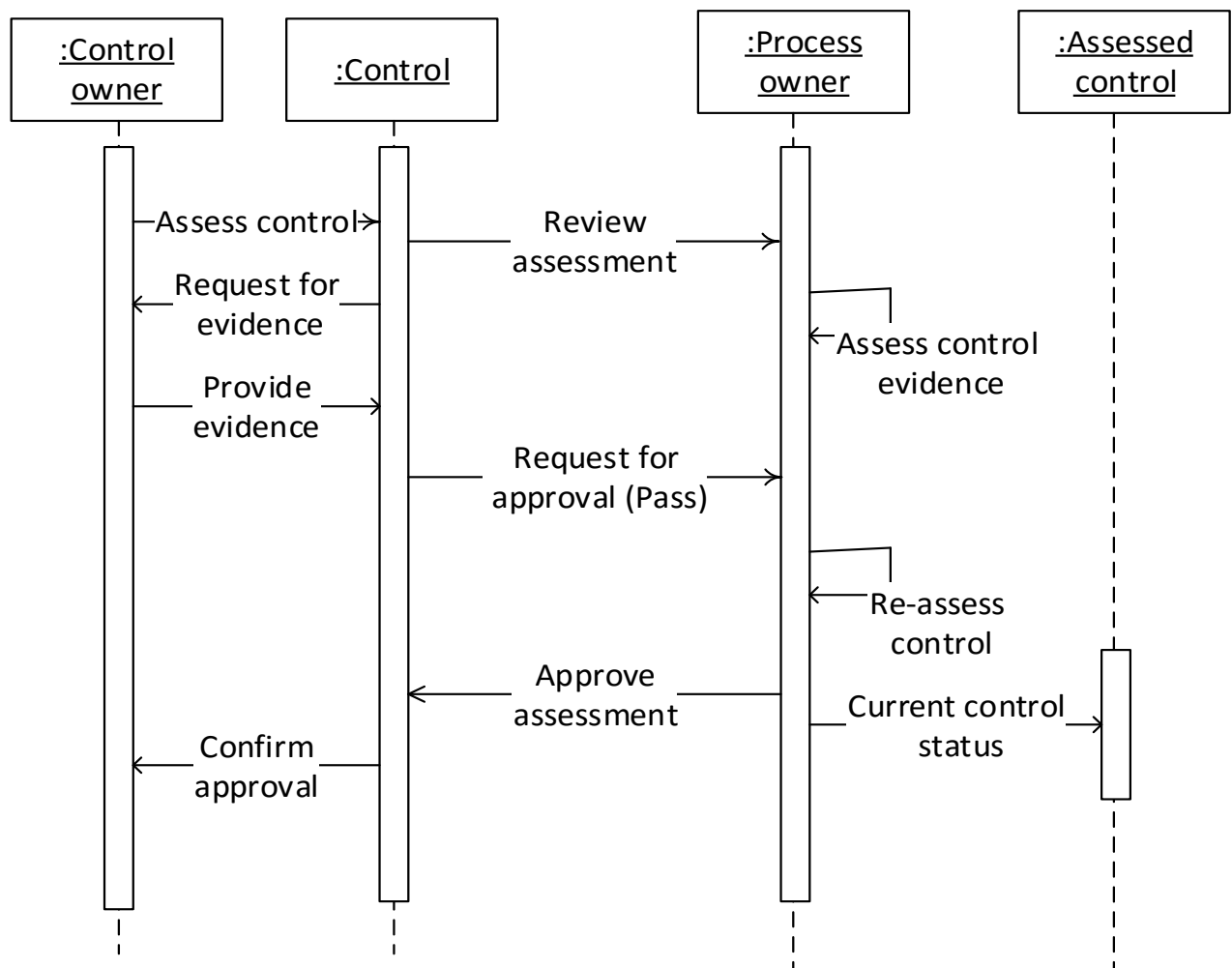


Figure 4.10 : Sequence Diagram

4.4.4 Entity Relationship Diagram

Khaled (2015) defines an entity relationship model as a high level conceptual representation that defines data in terms of the attributes, relationships and their entities. The entity relationship diagram represents how the data is structured and represented in the data base schema. It however does not specify the actual data.

The system administrator manages all the users and assigns controls to the users. The system users are either control owners or process owners. Each user has a distinct user name and profile email address that is linked to their accounts. To log-in, they must provide their log-in credentials. The control owner can perform one or more control assessments which has a unique control ID as the unique identifier. Each control has its control objectives and key control indicators linked to it. Only one process owner can review a control but more than one control can be reviewed by a process owner. The system administrator and assurance managers can generate and view reports.

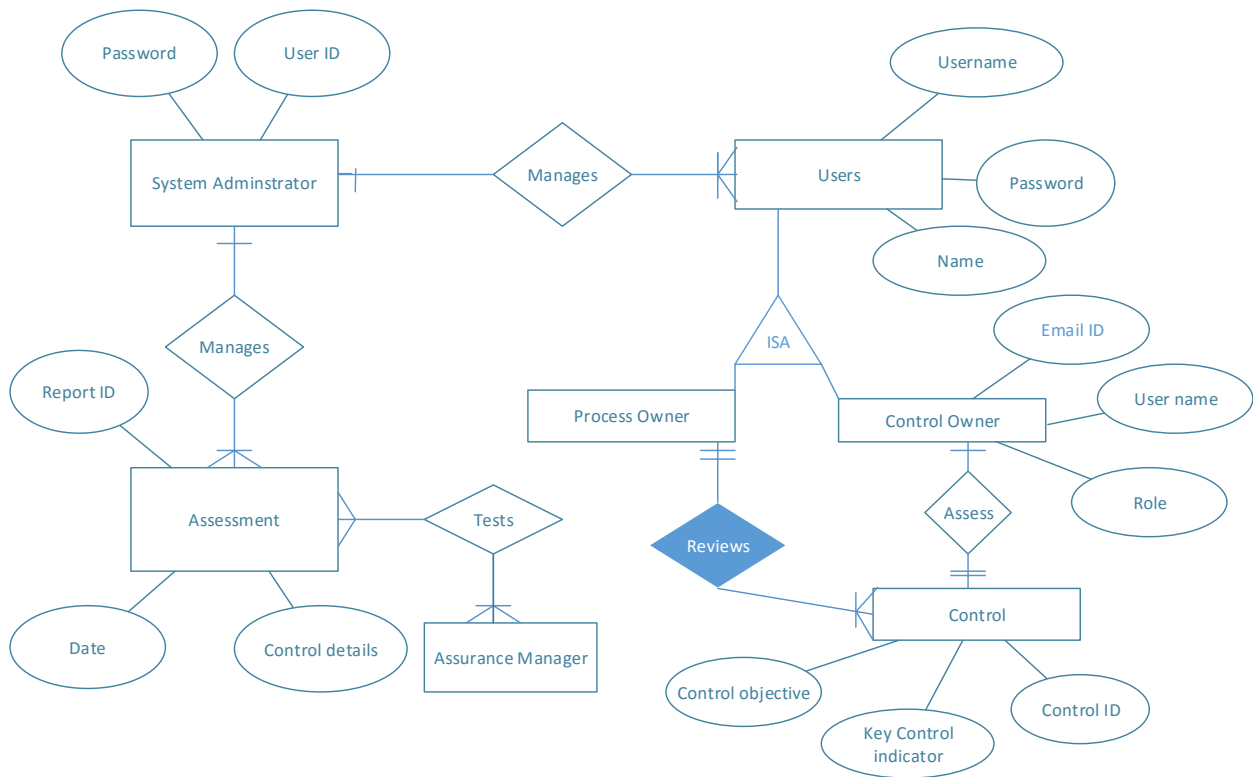


Figure 4.11: Entity Relationship Diagram

4.4.5 Class Diagram

A class diagram is a pictorial model for representing all the classes in an object oriented system; their attributes, connections, methods, inheritances (if any) and methods.

The system administrator can log-in, add controls, add users, manage users and modify the existing controls and users. The administrator can then log-out. The system administrator can view one or many reports and one or many assurance managers can view none to many reports as need be. The inherent attributed 'log-in and 'log-out' are inherited from the superclass Control Owner. Only one control owner can perform an assessment to a single control however a control owner can perform assessments on various controls. Only one process owner can review a single control but one to many controls can be reviewed by a process owner. A process owner can generate zero to many reports for oversight. This is illustrated in figure 4.12

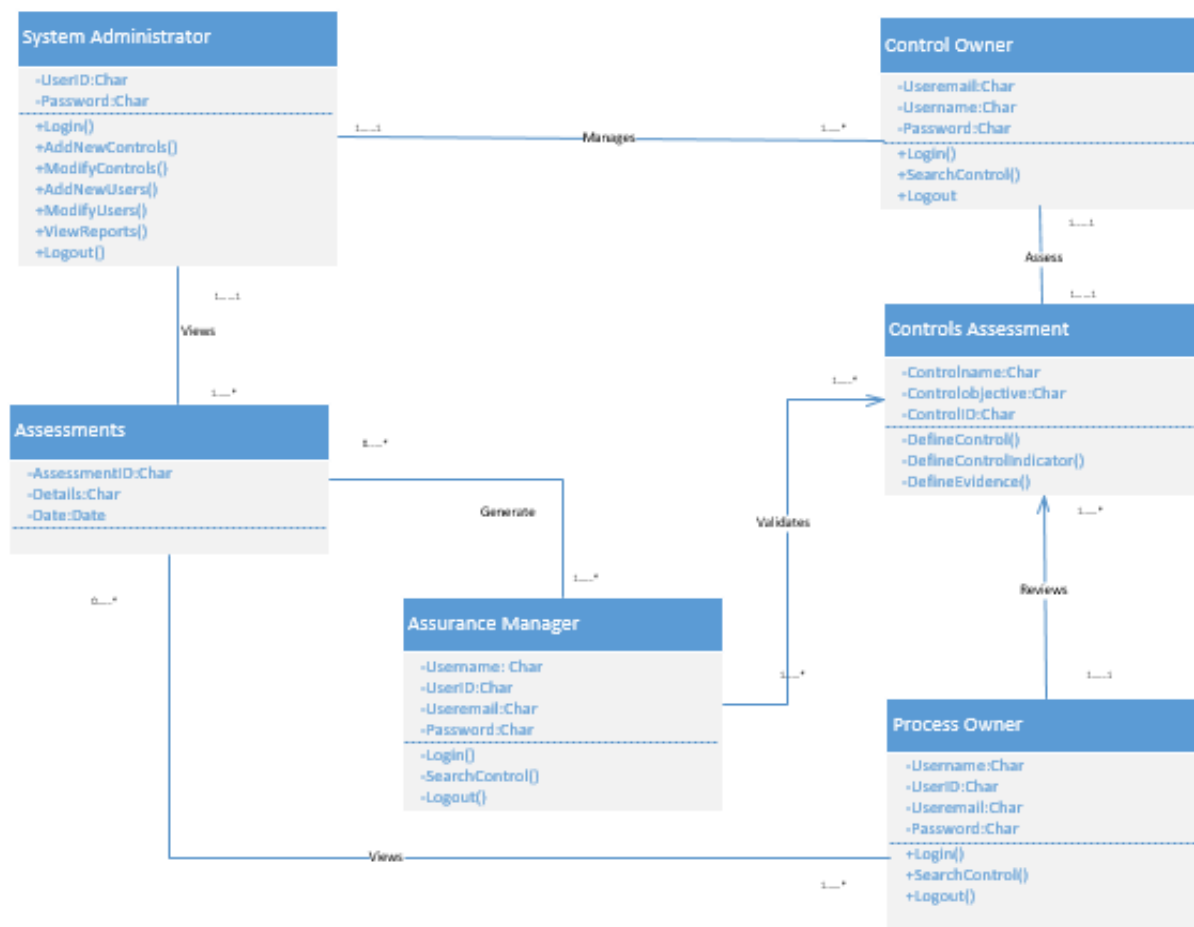


Figure 4.12 : Class Diagram

4.5 Controls Assessment Program Flow

When the control owners successfully log in to the system, they get a view of their assigned controls detailing the control name, objective, key control indicator and expected evidence of control. The assessment process then starts with a either 'Pass' or 'fail' rating to the control. The owner is then probed with performance based question for the control. These are the Key control indicators earlier detailed in the previous chapter that act as guide to assessing the control based on its performance. For a failed control, the system embeds a deficiency log register that seeks details to the control gap. This register assists the control owners in mapping the gaps for further remediation. The system links to the controls knowledge base to give information on all possible control gaps that can be attributed to the highlighted control based on design adequacy and operational effectiveness. If a control gap for failed controls is not indicated, the system cannot go to the next assessment phase. The control owner will the raise a remediation plan that has a tracking percentile to all the actions highlighted to resolve the control gaps. It is mandatory that control evidence is to be uploaded to the system to validate a passed control, but optional for a failed control. This evidence is what the controls assessment and testing hinges on in empirically testing as verifying that the control is truly effective in mitigating IT risks. All the assessments are reviewed and verified by the process owners to ensure supervisory oversight of the control owner assessments. When a control has been rejected by the process owner, the control owner has to re-assess. The deficiency logs and remediation plan are also approved or rejected by the process owners. Once all the controls have been assessed and agreed by the relevant owners, the assessment are subject to an independent review by the IT assurance/ oversight managers. This program flow is summarized in figure 4.13

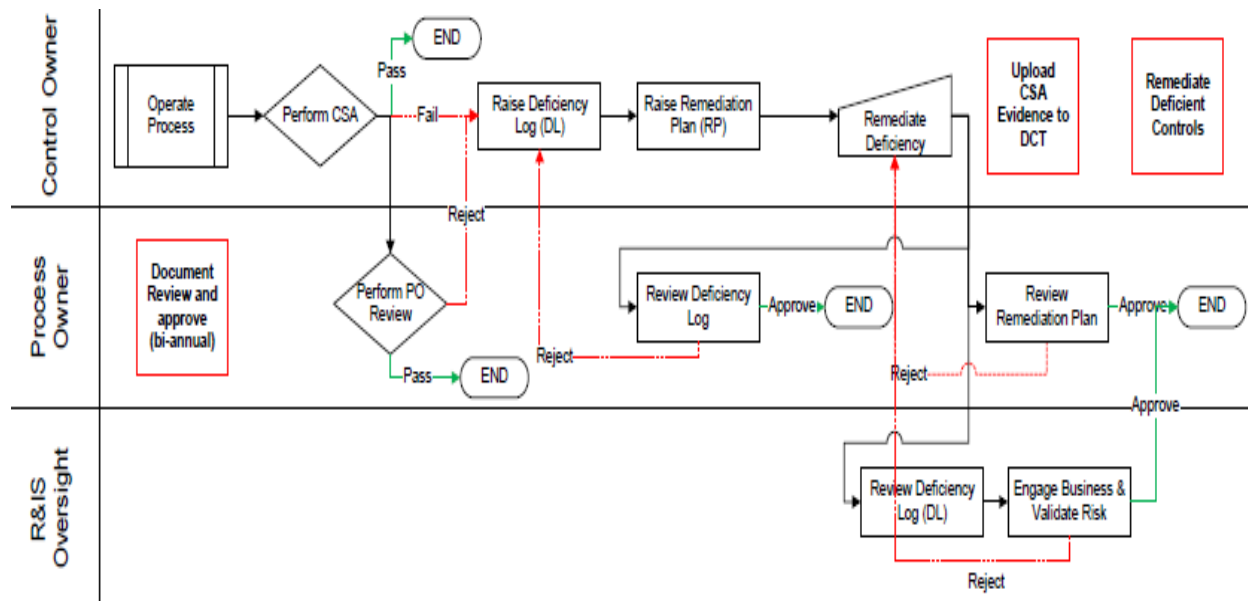


Figure 4.133 IT Controls Assessment Program Flow

4.6 The Prototype Architecture

The architecture of the IT controls assessment prototype is sub-divided into four major distinct components. These components include

- i. The user interface
- ii. The application server
- iii. The internet/ extranet and intranet
- iv. The Database server

As a web based application user interface is accessed through the web browser. These are the Graphical user interfaces that are the first point of contact that the system users use to interact and navigate through the system. The user interfaces can be accessed through standard web browsers such as Internet explorer, Google chrome, Mozilla Firefox, Safari, Microsoft Edge among others.

Having a client-server architecture, the internet relays data from the host server to the client browser. An extranet is set up to allow access to authorized organizations and ensure secure connections are maintained. For organization with a wider regional footprint this would be ideal to allow all users to access this. Standard internet protocols such as TCP/IP will be employed here.

The webserver used for the system is apache 2 and the front end will execute PHP functions. The defined system rules will be implemented to ensure the system login and process flow is maintained. Thus will be translated to the user interface using CSS and HTML. The assessment rules and logic are generated here.

A relational database will support the robust storage capability of the system. The system reports are generated from the different views defined to pull data from the database. This architecture is detailed in Figure 4.13.

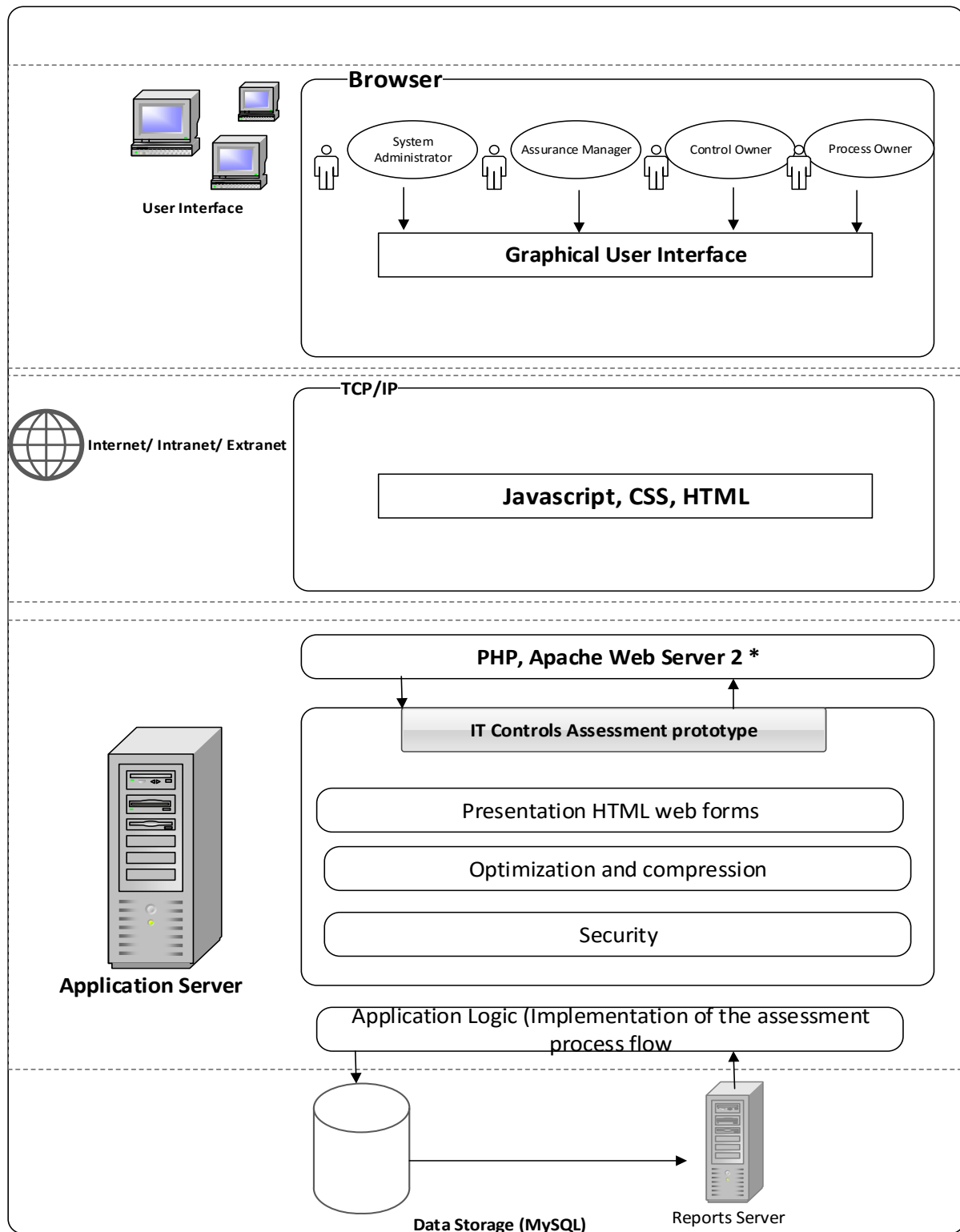


Figure 4.14 : Controls Assessment Prototype Architecture

Chapter 5: System Implementation and Testing

5.2 Introduction

The IT controls self-assessment prototype was designed, developed and implemented using the system design detailed in chapter 4. HTML, PHP, JavaScript, Ajax and MySQL database were used to develop the prototype. PHP was used to execute the application logic which is sequencing the assessment flow and entrenching the rules for effective controls assessments. The presentation of the prototype was enabled through HTML and CSS. For validation and maintaining a dynamic state for the system, Ajax and JavaScript were used. The assessment data from the system is stored in the MySQL database. A thorough testing of the main functionalities was carried out to ensure quality of the system build.

5.3 System Server Requirements

5.3.1 Hardware Requirements

Table 5.1 : Hardware Requirements

Hardware	Minimum Requirements
Processor	Intel Core
Cycle Speed	200MHz
Hard Disk Space	14GB

5.3.2 Server Requirements

Table 5.2 : Application Server Requirements

Software	Minimum Requirements
Operating System	Windows 2008 R2, Linux (Any variant)
Web Server	Apache 2.0 +
Database Management System	MySQL 5.0+

5.3.3 Client Machine Requirements

Table 5.3 : Client Machine Requirements

Software	Minimum Requirements
Web browser	Internet Explorer, Chrome, Mozilla Firefox, Microsoft Edge, Opera
Client Operating System	Windows 7/8/10, Windows XP/Vista, Linux (Any variant)
Processor	Intel Core
Hard Disk Space	15 GB

5.4 System Users, Roles and Access Matrix

The system was designed and developed to have role based access. There is a defined segregation of duty matrix that defines all the users that have access to the system and ensures users have appropriate rights that match their roles. The user roles that have been created are system administrator, control owner, process owner and IT assurance management (Risk & IT oversight). The system is accessed through the internet via a web portal. All user require requisite access and log-in details to the system.

5.4.1 Control Owner Role

The control owners are added to the system and assigned controls by the system administration. Control owners sign-in to the system to view their control specific dashboards. They have to authenticate themselves prior to using the system. The control owners have three major roles; assess the controls, raise deficiency log and raise the remediation plan. This category of users can also receive notifications through emails upon successful assessment and due assessments.

5.4.2 Process Owner Role

The process owner will also need to be authenticated to the system by using his username and password. The authorized process owner reviews all the assessed controls and ensure that quality data (evidence) is uploaded, accuracy is maintained and completeness of control evidence. The process owner would also review the deficiency logs and approve them as well as the remediation

plans to address the control gaps. They also view the reports of all the assessed controls and follow up to ensure all process owner performed their assessments as per the system defined timelines.

5.4.3 Assurance Managers

The IT Assurance managers are responsible for providing oversight in ensuring all IT risks are mitigated, information assets are safeguarded and confidentiality, integrity and availability maintained. They are also authenticated in the system to gain access to the controls assessed, evidence uploaded, deficiency logs created and remediation plans indicated. They perform independent testing of the controls assessment process and the control evidence thereof. The assurance managers provide assurance that there is sufficient information provided and that the remedial actions are suffice in closing out the control gaps and that there is compliance to policy and best practice. They can also update the controls to ensure that emerging risks are also well catered for from a controls relevance perspective. They obtain reports for compliance monitoring, follow up and closure of control gaps in the IT estate. This is done by monthly reporting to the IT managers accountable as per the RACI matrix. The oversight team is also responsible for designing the controls, defining the key control indicators, out lining the expected controls evidence to be uploaded and other control performance metrics.

5.4.4 System Administrator

The system administrator is responsible for the overall maintenance and daily administration of the system. This log-in to the web based system with his privileged administrative rights. The user adds new controls into the system as advised by the IT Assurance managers. These controls are designed by the oversight teams as discussed before. They are responsible for adding control details, adjusting the frequency and mapping all controls to the appropriate users. Since the controls self-assessment is aligned to the individual function of users, controls mapping is specific to each function. The system administrator resets password for user as per requests, he ensured that the segregation of duty matrix is aligned to all user roles. The system administrator also reviews the reports for controls assessed, control owners who have assessed the controls, controls due for assessments and overdue control assessments.

5.5 System Pseudo Code

The controls assessment prototype's major function is the dynamic assessments and controls synchronization to gauge effectiveness. At inception the prototype generates a list of all the defined controls. These included the control objective, description, expected evidence and other control attributes. Mapping of the control assessment against these attributes is performed and stored in the database for reporting. The assessment then correlates against the key control indicators to give it a 'Pass' or 'Fail' rating. The prototype then probes for evidence to validate the assessment. This process is repeated for all the controls per each owner. The prototype then measures the remediation plan to ensure there is constant follow up. This pseudo code is detailed in Figure 5.3

```
control_list= {control_name, other_details};
while assessing {
    select_control (control_list);
    display_control_status_to_the_controlowner();
    get_the_control_evidence_from_the_controlowner(evidence_list);
    assign_the_control_new_status (control_list, assessment_details);

    if (control_pass){
        end assessment ();
        update_assessment_details();
    }
    ELSE
    if (control_fail);
        then raise_deficiency_log (deficiency_details, deficiency_id);
        raise_remediation_plan ();
    END IF
}
}
```

Figure 5.1 The controls Assessment Pseudo code

5.6 Sample Forms Used

Several system interfaces were built to enable the interaction between the end-users and the prototype. Each interface built was specifically for a system task or sub-task which was unique. These user tasks were user management, controls assessment, reviewing controls assessments, reporting on all assessed controls among others.

5.6.1 System User Management

The user management interface provides a use friendly and convenient way of adding users to the system, assigning controls deleting and modifying users. The system administrator uses this interface to enter the details of the users that include, their full names, usernames, role, email address and telephone numbers. These are unique identifier details that are used to link controls to the relevant user with a display of their details. The system administrator add these details to the system and clicks on the save button. To update these details, the system administrator highlights the user details, clicks on edit. After making the changes to the use details, the system administrator clicks on save. The prototype performs a data validation check to ensure that enter data is in the correct data format such like Text, numbers, date etc. before being stored in the database. The system administrator can also delete data by selecting the 'Delete' icon but is prompted to confirm deletion of the data. Upon confirmation, the delete query runs against the user's id stored in the database and subsequently deletes the data.

5.6.2 Performing Controls assessment

Once a control owner has successfully logged in to they access the assessment interface. The controls dashboard gives a listing of all the controls assigned to them. The controls are well detailed to include all the information needed to perform a successful assessment such as control name, objective, description and the evidence to retain. This must be done by the control owner and not the process owner. Control assessments can be done each month, quarter or year depending on the process and frequency of the control. When the user selects the control to assess, the click on the 'assess' button to initiate the process. The user the selects 'Pass' or 'fail' on the drop down based on the status of the control. The control owner then chooses whether the control has passed or failed, then details the reason to the control pass/fail. The process then follows the program flow as detailed earlier.

https://localhost				
free				
-LE/CBP/SP/Control		Jan (2017)	Feb	Mar
		Assess 31-Jan-2017	Assess 28-Feb-2017	Assess 31-Mar-2017
CO.1.01: Firewall configuration and changes 🔑 🖥️ GCC		Assess 31-Jan-2017	Assess 28-Feb-2017	Assess 31-Mar-2017
CO.10.01: Problem management 🔑 🖥️ GCC		Assess 31-Jan-2017	Assess 28-Feb-2017	Assess 31-Mar-2017
CO.11.01: Incident Management 🔑 🖥️ GCC		Assess 31-Jan-2017	Assess 28-Feb-2017	Assess 31-Mar-2017
CO.12.01: Contract Management 🔑 🖥️ GCC				Assess 30-Mar-2017
CO.13.01: Vendor Management 🔑 🖥️ GCC		Assess 31-Jan-2017	Assess 28-Feb-2017	Assess 31-Mar-2017
CO.14.01b: Contracts with Vendors 🔑 🖥️ GCC		Assess 31-Jan-2017	Assess 28-Feb-2017	Assess 31-Mar-2017
CO.15.01a: Asset Management (Network, Storage & Software) 🔑 🖥️ GCC		Assess 31-Jan-2017	Assess 28-Feb-2017	Assess 31-Mar-2017
CO.15.01b: Asset Management (Mobile Apps, POS, Software) 🔑 🖥️ GCC		Assess 31-Jan-2017	Assess 28-Feb-2017	Assess 31-Mar-2017
CO.16.01: Software license management				

Figure 5.2 : Controls Assessment System Dashboard

Control Status: Active

Close

Process Details	Last Assessment (Pass)	Previous Control Test (Pass)
-----------------	------------------------	------------------------------

Assessment: Pass
Nature of Failure:
Comments: Confirmation of exited users have been disabled in the systems. . Pass committed by System.
Attachments:

Aims Exited Users to Disable.msg

FW Exited Users To Disable in AX.msg

Main Details

Ref Number: AP.1.02
GCC Name: Termination of Users
Identified Risk: There is a risk of Financial Reporting misstatement due to Unauthorised access to financial and financial reporting systems that could lead to unauthorised data amendment or destruction.
GCC Owner: [Anthony Muiyuro](#)
Delegate Owner: [Martin Nkonge](#)
Delegate Expiry:
Key GCC: Yes
Test Priority: Low
Compliance: Information Technology
GCC Domain: Access to Programs and Data
Compensating Ctrl:
Compns Not On List:
Attachments:

Findings.docx

RIS ReportAims User Access Review.pptx

RIS ReportDynamics AX User Access Review.pptx

Figure 5.3 Control Assessment Details

To see the control detail, the user clicks on the control highlighted to see a description dialog as detailed in figure 5.5.





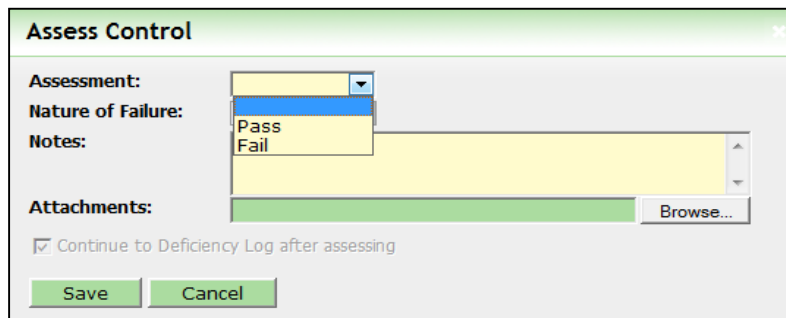
	AP.1.02: Termination of Users	Control: AP.1.02: Termination of Users Control Owner: Anthony Muiyuro Description: On a monthly basis, user lists are extracted from supported systems and validated against the HR system to verify that all users are still employed. All user IDs for users not found in the HR system are disabled or deleted.	Assess n-2017	Assess 31-Jul-
	AP.2.02: Extraction of User ID Revalidation  		Assess n-2017	

Figure 5.4 Assessment Control Details

5.6.3 Uploading Control evidence

A key feature of this control assessment prototype is evidence collection. For each 'pass' assessment, the control owners are required to upload the evidence to justify the control assessment. The control owner selects the 'Upload evidence' button for each passed assessment and attaches the evidence for the control such as Multi-formatted reports, screenshots, email communication etc. The uploaded evidence is reviewed by the process owners and IT assurance team to validate the assignment. All failed controls do not require evidence to be uploaded, but for noting control deficiencies they may be uploaded. Evidence must be uploaded before the control is reviewed again. The system will not allow evidence to be uploaded on a previously reviewed control. The control owner assigns a 'Pass' or 'Fail' assessment of control as per the figure 5.6.



The screenshot shows a window titled "Assess Control". It has several input fields: "Assessment:" with a dropdown arrow, "Nature of Failure:" with a dropdown menu showing "Pass" and "Fail", "Notes:" with a large yellow text area, and "Attachments:" with a green bar and a "Browse..." button. Below these is a checkbox labeled "Continue to Deficiency Log after assessing" which is checked. At the bottom are "Save" and "Cancel" buttons.

Figure 5.5 Assessing a Control

5.6.4 Raise Deficiency log

When a control failure occurs the control owners then explains why control failed and the possible impact of the deficiency. This feature details the control gaps, further noting the possible impact of the Risk should it materialize. The deficiency log will help management accurately address the control gaps based on the specific areas of improvement to ensure relevant measures are taken to efficiently and effectively remediate on control gaps.

Control Details	Assessments (Fail)	Def Log (Awaiting Input)	Rem Plan (Awaiting Input)	Control Test (N/A)
<div> <div>Jan (2016)</div> <div>Feb</div> <div>Mar</div> <div>Apr</div> <div>May</div> <div>Jun</div> <div>Jul</div> <div>Aug</div> <div>Sep</div> <div>Oct</div> <div>Nov</div> <div>Dec</div> </div>	<div> <div></div> <div></div> <div>Fail</div> <div></div> <div></div> <div>Assess</div> <div></div> <div></div> <div>Assess</div> <div></div> <div></div> <div>Assess</div> </div>	<div> <div>29-May-2016</div> <div>30-Jun-2016</div> <div>30-Sep-2016</div> <div>30-Dec-2016</div> </div>		

Deficiency Status: Awaiting Input

Cancel Edit
 Save Changes
 Save and Approve

Control Details

Process Details

Assessment Details (Fail)

Control: PM02.7.01: Procedures have been established by which Service Level Agreements are negotiated and reviewed (with business and vendors). There are defined targets for the availability, reliability and maintainability of IT infrastructure components that are documented

Identified Risk: -

Control Owner: Moses Mareya

Control Test Priority: High

Main Details ▲

Deficiency Name:

Issue Description:

F/R Risk:

Segregatn Of Duties?

Lack of Evidence?

Other:

Created: 29-May-2016 15:18
Created By: Moses Mareya
Modified: 29-May-2016 15:18
Modified By: Moses Mareya

Figure 5.6 : Creating a Deficiency Log

5.6.5 Raise remediation plan

The prototype has been set to have a remediation function to log and track all the remedial actions attributed to closing the control gaps. The control owner explains the actions that will be taken to fix the control and the due date of the actions. The actions that have already been taken are then detailed by the control owner and then they enter the percentile in which the control has been remediated. For a deficient control to be remediated, so that it can return to operating as usual, the remediation plan on the system must be 100% completed and the process owner must have accepted the remediation plan. The process owner approves the remediation when the control owner has completed it. The process owner selects whether they 'approve' or 'reject' the remediation. The process owner then provide a motivation for why they approve or reject the remediation plan. By rejecting the remediation plan will send it back to the control owner to resolve.

Control Details	Assessments (Fail)	Def Log (Awaiting Input)	Rem Plan (Awaiting Input)	Control Test (N/A)								
Jan (2013)	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Fail 12-May-20...

Plan Status: Awaiting Input Close Cancel Edit Save Changes

Control Details	Process Details	Assessment Details (Fail)
Control: KC1: Technical appraisal approval Identified Risk: The technical appraisal is done incorrectly.	Control Owner: Rincon, Alvaro Control Test Priority: High	

Main Details

Name:
Steps Required:
Resource Required:
Due Date: (Awaiting Input)
Complexity:
Estimated Cost:
Attachments:Browse...

Created: 12-May-2015 13:06
Created By: Nagia Fareeaa
Modified: 12-May-2015 13:06
Modified By: Nagia Fareeaa

Remediation


Steps Taken:
% Complete: 0 %
Completion Date:

Figure 5.7 Raising a Remediation Plan


5.7 Prototype Validation

To validate the user data input, the prototype has a data validation check capability to inspect the inputted data. The dynamic data validation check is performed using JavaScript. The prototype gives the user an error message to inform on what has gone wrong and further advice on how to resolve. Various fields were validated against including the username and password on user log-in. Not providing sufficient or accurate log-in information would prompt the user as Figure 5.9.

Sign in to ICT Controls Assessment

Email 

The email field is required.

Password 


The password field is required.

☐ Remember Me [I forgot my password](#)


Figure 5.8 Prototype Validation (Username/ Password required)

All unsuccessful login attempts are captured and recorded in the database. These records serve as audit logs for each user activity. The capture the action and time stamp for review by the system administrator. A failed log-in attempt would display an error prompting the correct log-in details as illustrated in figure 5.10

Sign in to ICT Controls Assessment

admin@ictcontrols.com 

These credentials do not match our records.

..... 

☐ Remember Me [I forgot my password](#)

Figure 5.9 Unsuccessful Log-in

5.8 Testing of Prototype

Testing of a system is the process of evaluating and examining the behavior of a developed system based on the captured requirements specification (Faisandier, 2012).

Several tests were performed to ensure that the system delivers on the specified requirements. Some of these test cases are detailed in Table

Table 5.0.4 System Test Cases

Test ID	Test Case	Expected Outcome	Test Comments
1.0	Log-in		
1.1	No password and username entered	Error dialog box	Pass
1.2	Incorrect password and username entered	Error dialog box	Pass
2.0	Control assessment		
2.1	Leaving out required field	Error dialog box	Pass
3.0	Upload evidence		
3.1	Not uploading evidence	Error dialog box	Pass
4.0	Deficiency log		
4.1	Leaving out required field	Error dialog box	Pass
5.0	Remediation plan		
5.1	Leaving out required field	Error dialog box	Pass
6.0	Role Access		
6.1	Attempting to access an unauthorized page	Session ended User routed to the login page	Pass

5.9 Maintenance of the Prototype

Further development of this prototype to a fully functional system shall be performed. The prototyped will be extended with additional modules and further enhancement will be done to ensure that the final system is robust, agile and scalable. The system will be made more adoptable to enhance interoperability with different software, hardware and platforms. To match the user dynamic needs of the system, frequent system maintenance will be performed.

Chapter 6: Discussions

6.1 Introduction

The research aimed to examine the key IT controls in financial institutions as the first objective. The researcher reviewed the baseline frameworks that articulated the foundational controls that are key to a financial institution. In this comparative study with other methods of IT controls evaluation, the researched was able to baseline these approaches to identify the gaps that would form the base of the prototype. The other objective of the study was to evaluate the different approaches applied to IT controls selection and assessments. The researcher and analyze their strengths and weaknesses and gathered the requirements for an effective IT control assessment framework. The outcome of this study was to develop an IT controls self-assessment prototype that would encompass the proposed IT controls assessment approach. Once the prototype was developed, end user tests were performed to gain an understanding of how the targeted end users experienced and felt about the system. Their perspectives was sought by the researcher based on different elements of system user experience. The researcher maintained the same targeted group of respondents that articulated their user requirements of an ideal IT controls self-assessment system. The respondents were trained on how to use the prototype and a training reference slide shared for reference. Their feedback was then collected by means of a questionnaire and results summarized in pie charts.

6.2 Findings

6.2.1 User Experience Findings

Compared to the other methods of IT controls evaluation a survey of the user experience was performed. Since the other IT controls evaluation approaches are manual and not based on any system implementation, the prototype has a unique automation solution to the problem. From a user experience perspective, 48% of the respondents strongly agreed that the prototype had a very user friendly interface. This makes it easy to use without much strain. 28% of the respondents agreed that the user interface was friendly, while 5% remained neutral in their opinion. The respondents that disagreed and strongly disagreed that the prototype user interface was friendly were 14% and 5% respectively. This is depicted in Figure 6.1.

Very User Friendly System User Interface

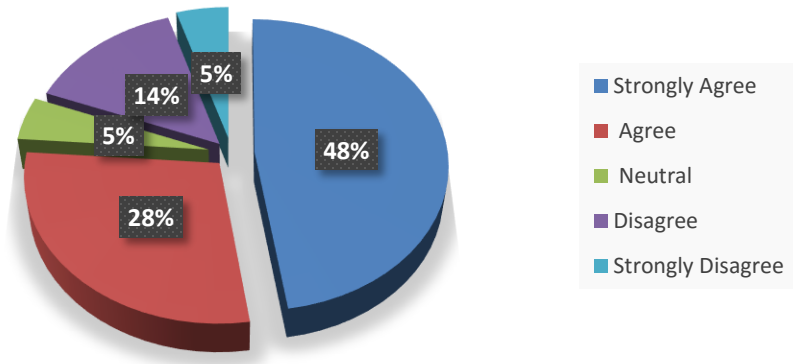


Figure 6.1 : Controls Assessment Prototype User Friendliness

Unlike the other methods of IT controls evaluation, the proposed prototype required users to be trained on usage and be appraised on the controls evaluation flow. 57% of the respondents strongly agreed that they required minimum training in using the prototype is their assessments. 29% agreed to their minimum training needs, 9% remained neutral to the extent of training they would require and 5% disagreed to this. None of the respondents fully disagreed to the hypothesis. This is shown in Figure 6.2.

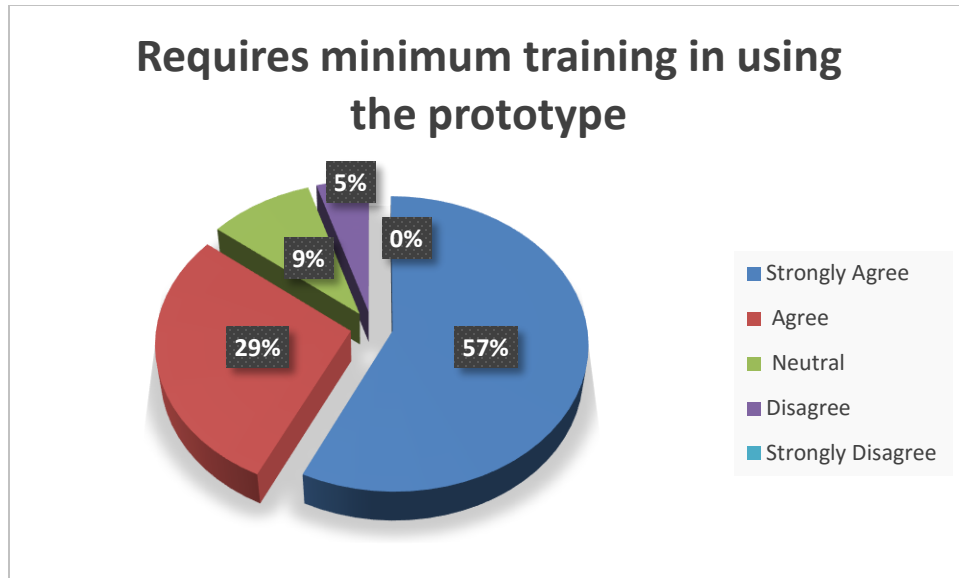


Figure 6.2 : Controls Assessment Prototype User Friendliness

6.2.2 Prototype Accuracy

Each IT respondent that assumed the role of a control owner provide 5 sample IT controls to test using the prototype. Adhering to the control testing guideline, the respondents used the prototype in performing the assessment. They reviewed the system to check if they would get the correct results and visibility of their control gaps based on the evidence provided. The results showed that 97% of the controls assessed gave the correct results and 3% did not give a correct representation of the facts. This was compared to the other methods of IT controls evaluation that comparatively did not give accurate results that could be trusted as a true attestation of the controls. The users viewed that the prototype was able to give results that could be compared with the other methods of evaluation. The notable down-sides to the proposed prototype is that it was less agile and thus would take more time to make a changes as compared to the other methods of assessments. This is shown in Figure 6.3.

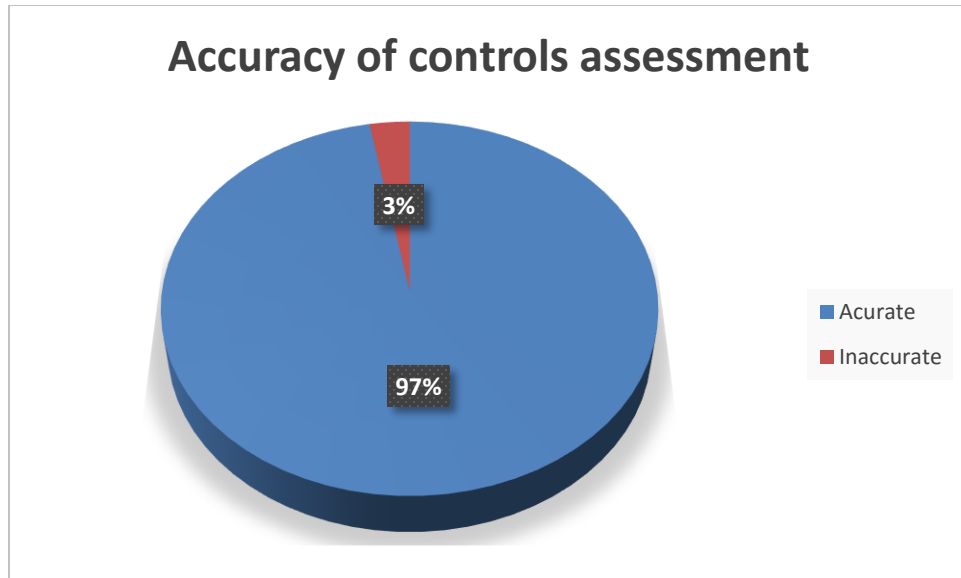


Figure 6.3 : Accuracy of Controls Assessment

6.2.3 Prototype Performance

Though controls self-assessments may tend to be a tedious exercise that entails a lot of data collection and analysis, 62% of the respondents strongly agreed that the prototype made this exercise more efficient, 28% agreed, 5% remained neutral, 5% disagreed with non-strongly disagreeing. Compared to other controls evaluation methods, the prototyped proved to be more efficient since all the control information are provided at a single instance. The other methods entail data collection and compilation which can be prone to errors and may give insufficient results in the controls evaluation. This is summarized by Figure 6.4

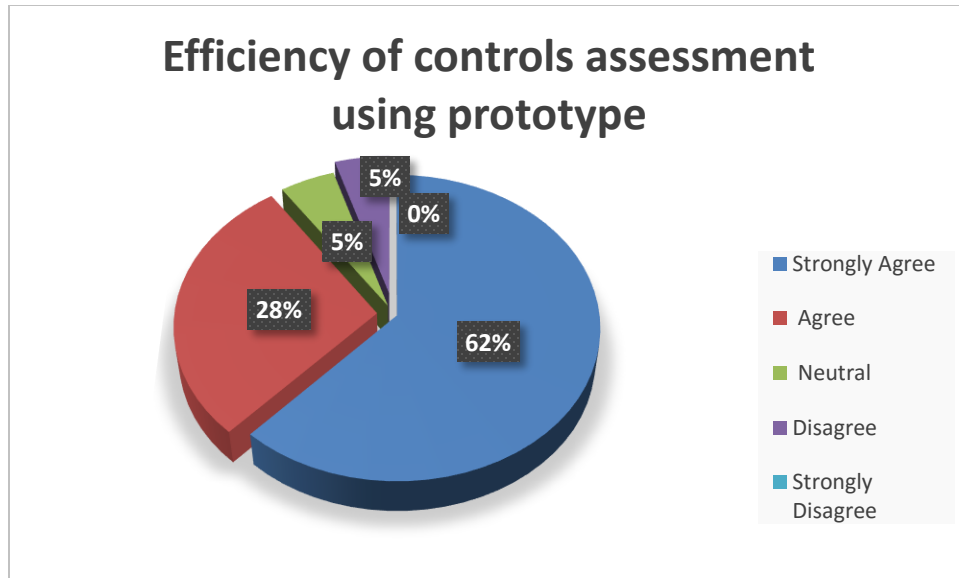


Figure 6.4: Efficiency of Using Prototype in Controls Assessment

6.2.4 Adoption of Controls Assessment Prototype

52% of the respondents expressed their strong interest in adopting the control self-assessment system in their organization. 33% agreed that they would consider adopting the system, 10% remained neutral, and 5% disagreed that they would not adopt it while none totally disagreed. This has been summarized in Figure 6.5. This is indicative of the preference to a system based controls evaluation method by the respondents.

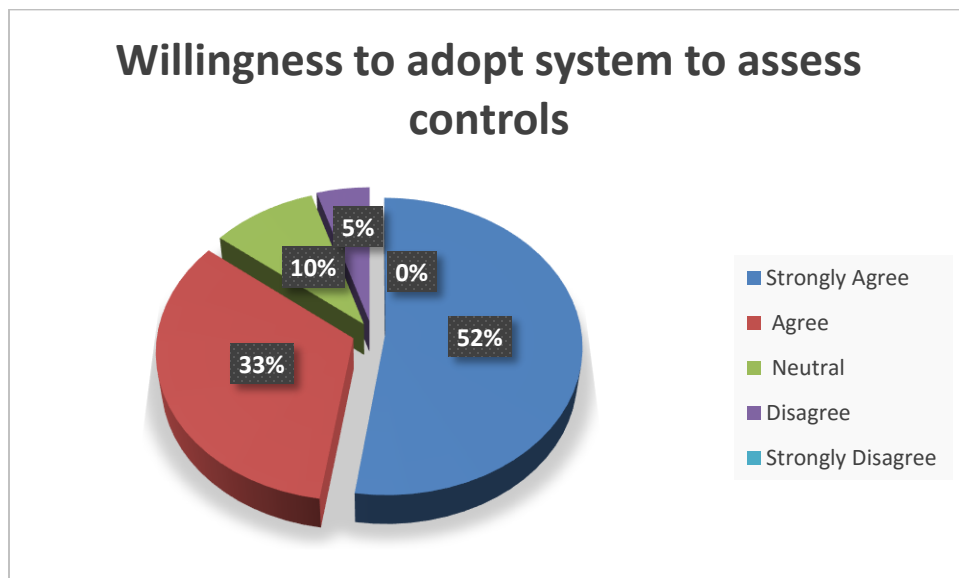


Figure 6.5: Adoption of System Based Control Assessment

6.2.5 Reliability of Controls assessment system

Reliability of the prototype was gauged by the resolve of the respondents to use the system to remediate control gaps. 55% of the respondents strongly agreed that they would use the system to onwardly monitor and remediate all control gaps. 32% agreed that the system was reliable in remediating control gaps, 9% remained neutral while 4% disagreed. None of the responses totally disagreed with the reliability of the system. This is shown in Figure 6.6.

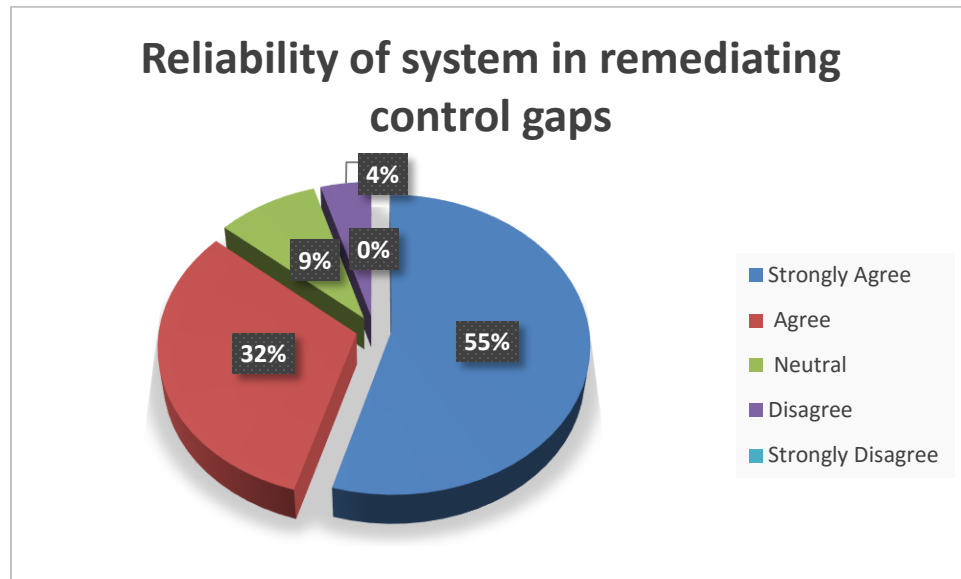


Figure 6.6: Reliability of System in Remediating Control Gaps

6.3 Limitation of this Prototype

Throughout this study, the researcher noted that some organization lacked awareness on the process of controls self-assessments. They do not have a defined approach to assessing their IT controls. This prototype does not address this issue. Among the challenges of assessing IT controls is the lack of a repeatable control assessment process. The lack of a well-defined assessment process does not enable the commitment necessary.

Chapter 7: Conclusions and Recommendations

7.1 Conclusion

Assessing the effectiveness of IT controls has been an uphill task and laden with many manual processes, subjectivity and in-efficient assessment methods. To most organization, control assessment checklists and programs have been the defacto means. The information gathered from these methods lack sufficient data to indicate control effectiveness and cannot empirically gauge the level remediation existing control gaps need to entrench to operate optimally. Lack of a periodic control assessment criteria is the leading cause of information security incidents due to materialized IT risks. Relevant and effective IT controls ensure that all cyber related threats are well protected against, detected, contained and recovered from. The Kenyan financial institutions have be subject to cyber related incidents due to a false sense of control security in some areas in their IT estates. Continuous monitoring of IT controls relevance and effectiveness is an ongoing concern for financial institutions in safeguard against data breaches, service interruption, unauthorized access to their systems and alteration of data. Current approaches to IT controls self-assessments do not have the mechanisms for management to measure the performance levels of already deployed controls, highlight the control gaps based on defined performance indicators and track remediation all the control improvement actions. This calls for a well-integrated system that will have an interactive self-assessment capability for the deployed IT controls.

Most of the respondents as highlighted in the questionnaire found the current manual process of controls self-assessment to be very tedious and in-efficient. They also found it to be subjective and not very effective. When a control gap is detected with the current assement methods, actions to remediate are not highlighted and tracked within a defined timeframe.

This research explores an evidence based IT controls assessment methodology that embeds an iterative process to the identification of controls, controls evidence collection, gap analysis and remediation planning. In addition, the research takes advantage of the RACI model to control ownership to ensure all the relevant stakeholders are involved in assessing the controls with independent oversight. The research build upon standard industry frameworks and best practice and defines the testing criteria for all the IT controls for adoption. These were reviewed in Chapter

2 as the literature review. Management can also have visibility of their controls universe by extracting reports to see control performance.

7.2 Recommendations for Further Research

Each control has a defined performance criteria. For mature organizations that have implemented a SIEM (Security Information and Events Management) solution, the controls assessment system should have a way to integrate to the SIEM solution. This will enable a seamless correlation of all the security incidences and events with the control assessment tool to link the incident to the affected control. This correlation will enrich the control data as evidence collected for any notable gap in the IT control with the protective features. The integration with the SIEM solutions will ensure that there is automatic collection of the security data, linking it to the control and give it all the information required to pinpoint remediation strategies.

The researcher recommends that this integration be made possible by having the solution vendors open up the SIEM to this capability. This can enhance the control data collection that will have the SIEM as the threat intelligence source.

This approach can be the primary control data collection method based on the materialized incidences for immediate action and remediation.

Other recommendations are

- I. Integrating with vulnerability and network scanning tools to detect threats and updating the controls data. This will make the network controls remediation more effective and precise.
- II. Email and text notifications feature to all control owner/process owner when a control gap has been detected based on information received from the SIEM and Vulnerability scanners.

References

- Barnard, L., & Von Solms, R. (2000). *A formalized approach to the effective selection and evaluation of information security controls*. Computers & Security.
- Bedard, J. C., Graham, L., & Jackson, C. (2008). *Archival evidence on detection and severity classification of Sarbanes-Oxley Section 404 internal control deficiencies*. Working paper, Bentley University.
- Chen, Z., & Yoon, J. (2010). *IT auditing to assure a secure cloud computing*. (2010). 6th World Congress on Services.
- Centres for Medicare & Medicaid Services. (2008, March 27). *Selecting a Development Approach*. Office of Information Services, pp. 1-10.
- Da Veiga, A., & Eloff, J. H. P. (2007). *An information security governance framework*. Information Systems Management.
- Daniel, K., Barbara, P., Allen, H.D., & Antje V. K.,(2002). *Functional Requirements, Non-functional Requirements, and Architecture Should Not Be Separated: A Position paper*. Munich: University of Munchen.
- Dhillon, G., & Torkzadeh, G. (2006). *Value-focused assessment of information system security in organizations*. Information Systems Journal.
- Faisandier, A. (2013). *Application System Analysis, Design and Architecture* (Vol. 3). Belberaud, France: Sinergy'Com Publishers.
- Gemino, G., Fraser, S., & Parker, D. (2009). *Use Case Diagrams in Support of Use Case Modelling: Deriving Understanding from the picture*. (ICICT) (pp. 528-534).
- Herath, T., & Rao, H. R. (2009). *Encouraging Information Security Behaviors in Organizations: Role of penalties, pressures, and perceived effectiveness*. Decision Support Systems.

- Institute of Internal Auditors. (2012). *Information Technology Risk and Controls*. Global Technology Audit Guide. Available at, http://www.theiia.org/bookstore/downloads/freetomembers/0_1006.dl_gtag1%202nded.pdf
- ISACA. (2010). CISA® Review Manual 2010. Rolling Meadows, Illinois: ISACA
- ISACA. (2012). CISA® Review Manual 2012. Rolling Meadows, Illinois: ISACA
- ISACA. (2013). CISM® Review Manual 2013. Rolling Meadows, Illinois: ISACA
- ISO/IEC. International Standard: Information Technology. Software Life Cycle Processes, ISO/IEC Standard 12207- 1995.
- IT Governance Institute. (2007). COBIT 4.1. Rolling Meadows, Illinois: ISACA
- IT Governance Institute. (2007). COBIT 4.1. Rolling Meadows, Illinois: ISACA
- Khan, M. A., Parveen, A., & Sadiq, M. (2014). *A Method for the Selection of Software Development Life Cycle Models Using Analytic Hierarchy Process*. International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) (pp. 534-540). New Delhi: IEEE.
- Khan, P. M., & Beg, M. M. (2013). *Extended Decision Support Matrix for Selection of SDLC-Models on Traditional and Agile Software Development Projects*. Third International Conference on Advanced Computing & Communication Technologies (pp. 8-14). New Delhi: IEEE
- Khaled, H.A. (2015). *Extracting Entity Relationship Diagram (ERD) From Relational Database Schema*. New Jersey: International Journal of Database Theory and Application.
- Kothari. (2004). *Research Methodology Methods and Techniques*. New Age International Publishers.


- Lv, J. L., Zhou, Y. S., & Wang, Y. Z. (2011). *A Multi-criteria Evaluation Method of Information Security Controls*. Fourth International Joint Conference on Computational Sciences and Optimization.
- Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. New York, NY: O'Reilly.
- Mugenda, O. M. (2003). *Research Methods: Quantitative and qualitative Approaches*. Nairobi: African Centre for Technology Studies.
- Nashawaty, P. (2015). *Rapid Application Development for Dummies*. Hoboken, New Jersey: John Wiley & Sons, Inc.
- NIST. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 Revision 4: Joint task force transformation initiative. Available at, <http://dx.doi.org/10.6028/NIST.SP.800-53r4>.
- Otero, A. R., Otero, C. E., & Qureshi, A. (2010). *A Multi-criteria Evaluation of Information Security Controls Using Boolean features*. International Journal of Network Security & Its Applications.
- Ou Yang, Y. P., Shieh, H. M., & Tzeng, G. H. (2011). *A VIKOR Technique Based on DEMATEL and ANP For Information Security Risk Control Assessment*.
- Saint-Germain, R. (2005). *Information security management best practice based on ISO/IEC 17799*. The Information Management Journal, August 2005, 60-66.
- Serianu Limited. (2015). *Achieving Enterprise Cyber Resilience Through Situational Awareness*. Kenya cyber security report 2015. Available at, <http://www.serianu.com/downloads/KenyaCyberSecurityReport2015.pdf>
- Serianu Limited. (2016). *Achieving Enterprise Cyber Resilience Through Situational Awareness - "Enhancing visibility and enhancing awareness"*. Kenya cyber security report 2016. Available at, <http://www.serianu.com/downloads/KenyaCyberSecurityReport2016.pdf>

Volonino, L., & Robinson, S. R. (2004). *Principles and Practice of Information Security*. Upper Saddle River, NJ: Pearson Prentice Hall, Inc.

Appendices

Appendix A: Turnitin Originality Report

Turnitin Originality Report

 **Turnitin Originality Report**

Thesis by Antony Mulyuro
From 2016 Plagiarism Check (GS)
(Library Services Plagiarism Checker
(2016+))

Similarity Index	Similarity by Source
11%	Internet Sources: 7% Publications: 4% Student Papers: 0%

Processed on 05-Apr-2017 12:14 PM
EAT
ID: 794672638
Word Count: 16442

sources:

- 2% match (student papers from 07-Feb-2015)
[Submitted to Colorado Technical University Online on 2015-02-07](#)
- 1% match (publications)
[Otero, Angel R., "An information security control assessment methodology for organizations' financial information". International Journal of Accounting Information Systems, 2015.](#)
- < 1% match (Internet from 25-Oct-2010)
<http://www.cihan.org/PDFs/cobit.pdf>
- < 1% match (Internet from 24-Aug-2016)
<https://www.scribd.com/doc/126649453/DISSERTATION-How-to-Motivate-Employees-in-Retail-Supermarket-Industry-in-UK-A-Case-of-M-S>
- < 1% match (Internet from 31-May-2012)
<http://www.itsmfea.co.uk/docs/COBIT-Mapping-ISO-IEC-17799.pdf>
- < 1% match (Internet from 25-Nov-2008)
<http://oasis-open.org/committees/download.php/11414/RunBook%20Session%20with%20Robin%20Basham.htm>
- < 1% match (student papers from 06-Jun-2015)
[Submitted to Study Group Australia on 2015-06-06](#)
- < 1% match (Internet from 05-Oct-2009)
<http://www.unifiedcompliance.com/matrices/live/00574.html>
- < 1% match (publications)
[Otero, Angel R., Gurylrender Telav, Luis Daniel Otero, and Alex J. Ruiz-Torres. "A fuzzy logic-based information security control assessment for organizations". 2012 IEEE Conference on Open Systems, 2012.](#)

Appendix B: User Requirements Questionnaire

User Requirements Questionnaire

Academic Researcher: Anthony Mwangi Muiyuro
MSc. IT, Strathmore University

This research is exclusively for academic purpose only. The main objective of the research is to solicit the user requirements that will be used to develop a prototype for assessing IT controls in financial institutions in Kenya. Kindly provide your honest answers to ensure that the researcher accurately captures the facts. Kindly note that this research will be treated with high confidentiality and your responses will be private and confidential.

1. Cyber security incidents and breaches occur when there is a control gap or existing controls are in-effective
 - ☐ Strongly Agree
 - ☐ Agree
 - ☐ Neutral
 - ☐ Disagree
 - ☐ Strongly Disagree
2. It is easy to establish if IT controls are effective, provided they are in-place (Technology and process controls)
 - ☐ Strongly Agree
 - ☐ Agree
 - ☐ Neutral
 - ☐ Disagree
 - ☐ Strongly Disagree
3. The current process of assessing the effectiveness of IT controls is efficient.
 - ☐ Strongly Agree
 - ☐ Agree
 - ☐ Neutral
 - ☐ Disagree
 - ☐ Strongly Disagree

4. The IT, Risk and Audit teams are prompted immediately once an IT control stops functioning to mitigate risks.
- ☐ Strongly Agree
 - ☐ Agree
 - ☐ Neutral
 - ☐ Disagree
 - ☐ Strongly Disagree
5. The current methodology of assessing effectiveness of IT controls is time saving and user friendly.
- ☐ Strongly Agree
 - ☐ Agree
 - ☐ Neutral
 - ☐ Disagree
 - ☐ Strongly Disagree
6. I believe that the current methodology of assessing IT controls is evidence based and not subjective
- ☐ Strongly Agree
 - ☐ Agree
 - ☐ Neutral
 - ☐ Disagree
 - ☐ Strongly Disagree
7. If a proper system based control assessment is implemented, I believe it would make the self-control assessment process more effective, accurate and efficient.
- ☐ Strongly Agree
 - ☐ Agree
 - ☐ Neutral
 - ☐ Disagree
 - ☐ Strongly Disagree
8. How confidential are the IT control gaps findings in your organization?
- ☐ Very Confidential
 - ☐ Not Very Confidential
 - ☐ Neutral
 - ☐ I do not know

Appendix C: System Usability Questionnaire

User Requirements Questionnaire

Academic Researcher: Anthony Mwangi Muiyuro
MSc. IT, Strathmore University

This research is exclusively for academic purpose only. The main objective of the research is to find out the usability of the prototype for assessing IT controls in organizations in Kenya. Kindly provide your honest answers to ensure that the researcher accurately captures the facts. Kindly note that this research will be treated with high confidentiality and your responses will be private and confidential.

System Usability Rating Scale

Kindly rate the IT controls assessment system with regard to the following criteria:

1. The Graphical user interface is user friendly

- ☐ Strongly Agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree
- ☐ Strongly Disagree

2. I can use this controls assessment prototype with minimum training

- ☐ Strongly Agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree
- ☐ Strongly Disagree

3. Assessing IT controls using this system is more accurate compared to the current controls assessment methods

- ☐ Strongly Agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree
- ☐ Strongly Disagree

4. This is a practical question that aims at testing the accuracy and effectiveness of the prototype. Kindly provide a list of five IT controls that your organization has deployed to the researcher. After the researcher has found them in the system, and run the assessment based questions to input control evidence to the system, try reviewing them and note down your findings based on the control effectiveness and notable indicators (Among those controls, how many were correctly assessed?)

.....

.....

.....

5. The system provides an efficient way of assessing IT controls

- ☐ Strongly Agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree
- ☐ Strongly Disagree

6. I will adopt and use this system in assessing our IT controls.

- ☐ Strongly Agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree
- ☐ Strongly Disagree

7. I will use this system is remediating control gaps.

- ☐ Strongly Agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree

☐ Strongly Disagree

7. Is it likely that you are going to recommend this controls assessment system to other professionals in your field?

☐ Very Likely

☐ Likely

☐ Neutral

☐ Not Likely

☐ Not Likely At All

8. Any Comments

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Appendix D: Interview Questions

Interview Questions

Academic Researcher: Anthony Mwangi Muiyuro
MSc. IT, Strathmore University

This research is exclusively for academic purpose only. Its main objective is to find out the user experience the prototype for assessing IT controls in organizations in Kenya. Kindly provide your honest opinion to ensure that the researcher accurately captures the facts. Kindly note that this research will be treated with high confidentiality and your responses will be private and confidential.

Interviewee: **Organization:**
Interview channel: **Date:**

1. When an IT control is ineffective, what should be the assessment approach to remediate it?

.....
.....
.....
.....
.....
.....
.....
.....

2. What is the current methodology of assessing the effectiveness of an IT control?

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

3. What are the challenges in assessing IT controls?

.....

.....

.....

.....

.....

.....

.....

4. How do you handle controls that have significant gaps and are in-effective?

.....

.....

.....

.....

.....

.....

.....

5. What approach has your organization taken to ensure that implemented controls are monitored to ensure effectiveness?

.....

.....

.....

.....

.....

.....

.....

6. What challenges has your organization faced when determining the cyber risks that need to be mitigated by controls?

.....

.....

.....

.....

.....

.....

.....

7. In your opinion, what needs to be improved in the current IT control monitoring and assessment methodologies?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

b. Remediating an in-effective control?

.....

.....

.....

.....

.....

.....

.....

.....

.....