



UNIVERSITY OF CAPE TOWN
FACULTY OF COMMERCE

Igniting Knowledge and Opportunity



THESIS

Presented for the Degree of
DOCTOR OF PHILOSOPHY

October 2018

Title

*Modeling a Systems-based Framework for Effective IT Auditing and Assurance
for Less Regulatory Environments.*

University of Cape Town; Department of Information Systems



Sampson Anomah

PhD Supervisor

Professor Michael Kyobe

Department of Information Systems

Faculty of Commerce

University of Cape Town, South Africa

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

Declaration:

I submit that this work is my own work. To the best of my knowledge and belief the thesis contains no substantial materials previously written or published by another person without due acknowledgment. Furthermore, I submit also that the research does not contain text which has been submitted and accepted for the award of any other degree or diploma of University of Cape Town or any Institution of Higher Learning.

Signed by candidate

.....

Sampson Anomah

Abstract

Information Technology (IT) has become indispensable in contemporary business processes and in business value creation strategies. Those charged with governance, risk management and compliance are, often, challenged by sophisticated IT oriented decision-making dilemmas due to complex IT use in contemporary business processes. Investors and other stakeholders increasingly expect very rich, reliable and transparent assurance that their interests are safe. Auditors, as a result, are looked upon to expand their role to leverage the functions of those charged with governance and management. IT audit literature, hence, demonstrates existence of several best practices aimed at meeting the increasing demand for more audit and assurance outcomes that bridge the widening audit expectations gaps. In developing countries with less stringent regulatory systems, however, attempts to implement many of these frameworks have proved unsuccessful. Reasons include paucity of guidance in the frameworks and lack of suitable theoretical foundations to resort to for solutions to implementation challenges. Extant literature review reveals scanty research effort by practitioners or academicians in the field in the empirical situation to design a more suitable framework to serve as intervention. In this research an attempt has been made to create an intervention by designing a framework, i.e. an artefact for IT auditing for less regulated business environments. By adductive inference the cybernetics theory of viable systems approach was ingrained as the theoretical foundation from which the variables for the design were extracted. The abduction was based on the diagnostic power and ability to support self-regulation in a less regulatory environment. Action design research (ADR) approach was employed to achieve the research objective. Both qualitative and quantitative techniques were found to be useful for the evaluation and data analysis. At the design phase, a multiple case study method together with workshops were employed to gain insight into the problem and to collect data to support the design process. Four organisations from both public and private sectors in Ghana were selected to participate in the research. At the evaluation stage a survey technique was used to collect data mainly for the validation of construct variables and the refinement of the framework. The questionnaire scale used was 1=Strongly Disagree; 2=Disagree; 3=Somewhat Agree; 4=Agree and 5=Strongly Agree. A total of 136 respondents who included IT audit and Internal audit practitioners, Audit trainees and students, Directors and management staff were involved from four selected organisations. A factor analysis yielded twenty variables extracted from the ingrained theory

for the building of a conceptual model which were grouped into six factors or domains. The entire conceptual model was tested with PLS-SEM technique because of the causal relationships that motivated the development of the conceptual hypotheses. A composite reliability used to assess the internal consistency of the model was overall adequate with values greater than 0.7. Similarly, a convergent validity of the model showed that all the variables were above the threshold value of 0.5. Thus, the model and design theory were found to be reliable and valid. Correlation and regression analysis was applied in testing individual hypotheses and the results helped to reorganise the final framework. The study contributed an artefact in the field of IT audit which represents a comprehensive teachable practitioner's guide for the improvement of the IT audit practice. The framework also serves as guidance to those charged with governance and management in monitoring, self-review and as framework to attain IT audit readiness in less regulatory environments. Implementation challenges are expected to be resolved by reverting to the ingrained theory.

Acknowledgement

My gratitude goes to my supervisor Professor Michael Kyobe for his patience, his smart review skills, immense knowledge in research coaching and continuous support that saw me through my PhD research study. His guidance has been quite important learning experience to me. I cannot imagine a better supervisor for my PhD study.

I would also like to appreciate the University of Cape Town and the Department of Information Systems for hosting me to pursue my PhD studies. Additionally, I thank Professor Irwin Brown for his review of my proposal. I thank also the International Academic Program Office (IAPO) team of the University, particularly, Mr. Leon Petersen for his assistance that made me save cost in diverse ways.

I thank all the individuals that provided support for my research study. I, particularly, acknowledge the institutions that agreed to allow me to use them for my case study, especially, Ghana Audit Service and Kumasi Technical University for the cordial opportunity to interact with their staff during the research process and data collection.

Without my family and friends, I would have burnt out both physically and spiritually during my studies. I would always acknowledge my God for providing me with the strength to persevere in this academic effort.

Table of Content	Page
Declaration:	i
Abstract	ii
Acknowledgement	iv
List of Tables	ix
List of Figures	x
LIST OF APPENDIXES	xi
CHAPTER ONE	1
INTRODUCTION	1
1.0. Introduction	1
1.1. Background to the Study	1
1.2. Research Motivation	2
1.3. Research problem statement	4
1.4. Research Question	5
1.5. Objectives of Research	5
1.6. Research Approach and Instruments	5
1.6.1. Research Instrument Building and Data Collection	7
1.6.2. Relationship Between ADR and the Research Structure	14
1.7. Expected Knowledge Contribution of the Research	15
1.8. Organisation of Research	16
1.9. Conclusion	18
CHAPTER TWO	19
LITERATURE REVIEW	19
2.0. Introduction	19
2.1. Definition of Audit	19
2.2. Theoretical Bases for Auditing.....	21
2.2.1. Agency Theory	21
2.2.2. Stakeholder theory (Inspired Confidence Theory)	22
2.2.3. Lending Credibility Theory.....	23
2.2.4. The Policeman Theory	23
2.2. Objectives of IT Auditing and Assurance	24
2.3. Traditional Scope of IT Audit and Assurance	25
2.3.1. General Control reviews.....	26
2.3.2. Applications Control Reviews.....	27
2.3.3. Contingency Control Reviews.....	27

2.3.4. Compliance Reviews	28
2.3.5. Audit Trail and Evidence Collection Processes in IT Auditing	29
2.5. Practical Approaches to Auditing	31
2.5.1. Continuous Auditing Approach.....	32
2.5.2. Forensic Auditing Approach	32
2.5.3. Risk-based Approach	33
2.5.4. Systems Based Approach	34
2.6. Open Reference Frameworks and Best Practices on IS/IT Auditing	35
2.6.1. Business Oriented Controls Best Practices	36
2.6.2.1. Criticisms of the COSO's Internal Control frameworks	42
2.6.3. IT Service Management Best Practices	43
2.6.4. Business -IT Alignment Best Practices	47
2.6.5. The COBIT Enabling Processes	49
2.6.6. The COBIT Assurance and Assessment Model	52
2.7. IT audit expectations and gaps	57
2.8. Conclusion.....	60
CHAPTER THREE	61
PROBLEM DIAGNOSIS AND CONCEPTUALIZATION	61
3.0. Introduction	61
3.1. Cybernetics	61
3.2. The VSM – The Theory Ingrained Artefact	63
3.3. Functional properties of the VSM	63
3.3.1. Subsystem One (Operations) – S1	65
3.3.2. Subsystem Two (Coordination) – S2	66
3.3.3. Subsystem Three (Control) – S3: Mechanisms for Viability	68
3.3.4. Subsystem Four (Intelligence) – S4	73
3.3.5. Subsystem Five (Policy) – S5	74
3.4. Performance Measurements System of the VSM Operations	81
3.4.1.1. Tactical Planning Level	84
3.4.1.2. Strategic Planning Level	84
3.4.1.3. Normative Planning Level	85
3.5. Criticism of the VSM	86
3.6. Conclusion	86
CHAPTER FOUR	88
BUILDING AN INTERVENTION	88
4.0. Introduction	88

4.1.	Development of the Intervention	88
4.2.	Demonstration of the Artefact	91
4.2.1.	Operations/Process Auditing	91
4.2.2.	The Process Coordination (S2) Audit	92
4.2.3.	The Process Controls (S3) Assessment	97
4.2.3.1.	Investigation (S3*) - (Fraud Risk Assessment For-cause)	100
4.2.3.2.	Demonstration of model	102
4.2.4.	Organisational Process Intelligent (S4) Assessment	111
4.2.5.	Policy (S5) Assessment Process	120
4.3.	Implementation Guideline of the Framework	123
4.3.1.	Creating an IT audit Universe through Audit Process customization	123
4.3.1.1.	Tactical Audit Stage	124
4.3.1.2.	Strategic Audit Stage	124
4.4.	The Metrics for the customisation	125
4.5.	Conceptual Model Development	130
4.6.	Development of Conceptual Hypotheses	146
4.7.	Conclusion	149
CHAPTER FIVE		151
RESEARCH METHODOLOGY		151
5.0.	Introduction	151
5.1.	Philosophical Backgrounds of the Research	151
5.1.1.	The Ontology	152
5.1.1.1.	Constructionism or subjectivism	152
5.1.1.2.	Objectivism	152
5.1.1.3.	The Ontological Position of this Study	152
5.1.2.	The Epistemology	153
5.1.2.1.	Interpretivism	153
5.1.2.2.	Positivism	153
5.1.2.3.	Critical Realism	154
5.1.2.4.	Pragmatism (Mixed method)	154
5.1.2.5.	The Epistemological Research Paradigm of this Study	155
5.2.	Cognitive Processes of Enquiry	156
5.2.1.	Inductive Process	156
5.2.2.	Abductive/retroductive Process	156
5.2.3.	Deductive Approach	157
5.2.4.	The Cognitive Method of Enquiry in this Study	157
5.3.	Research Design	159

5.3.1. Case Study Research Design	160
5.3.1.1. Multiple Case Study	161
5.4. Sample frame, sampling method	161
5.4.1. Data Collection Sites	162
5.5. Construct Measurement and Research Instrument Design	164
5.5.1. Data Collection Techniques	164
5.5.2. Data Analyses process	171
5.6. Consideration of Generalisability of Outcome	176
5.7. Ethical Considerations	177
5.8. Chapter Conclusion	177
CHAPTER SIX	178
DATA ANALYSIS AND REFLECTION ON LEARNING	178
6.0. Introduction	178
6.1. Respondents Characteristics	178
6.2. Reliability Analysis	180
6.3. Factor Analysis	182
6.4. Analysis of Factor Loadings	186
6.5. Conceptual Model Testing and Analysis	189
6.6. Examination of Hypotheses	191
6.6.1. Discussion of Results	192
6.7. Reflection on the Emerging Structure of the Framework	194
6.8. Chapter Conclusion	198
CHAPTER SEVEN	199
FORMALISATION OF LEARNING AND CONCLUSION	199
7.0. Introduction	199
7.1. Overview of Research Process	199
7.3. Summary of Findings and Discussion of Final IT Audit Framework	202
7.4. Generalized outcomes	203
7.4.1. Contribution to Theory Development	204
7.4.2. Contribution to Practice	204
7.5. Limitation and Opportunity for Future Research	207
7.6. Conclusion.	208
8.0. REFERENCES	209

List of Tables

Table 1. Relationship Between ADR and the Research Structure	14
Table 2. The five concepts with its seventeen principles	36
Table 3. The NPLF Score, Maturity Level and Rating	55
Table 4. Governance and management structure of COBIT 2019	56
Table 5. Functions and Processes for the audit of Operations	94
Table 6. Intelligence auditing	114
Table 7. Policy efficiency audit matrix	122
Table 8. Factor Value Checklist	126
Table 9. NPLF Capability Scores	129
Table 10. Description of Concepts in the Construct	134
Table 11. Cases selected	163
Table 12. Measured items of the construct	165
Table 13. Deletions based on missing data	171
Table 14. Method of Construct Reliability Tests	172
Table 15. Models in the hypotheses testing	175
Table 16. Respondents characteristics	180
Table 17. Reliability Statistics of constructs for factor 1	181
Table 18. Reliability Statistics of constructs for factor 2	182
Table 19. Reliability Statistics of constructs for factors 4, 5 and 6	182
Table 20. Total Variance Explained	184
Table 21. KMO and Bartlett's Test	185
Table 22. Rotated Component Matrix	186
Table 23. Relationship among latent variables	191
Table 24: Model validity and reliability	192
Table 25: Summary on Hypotheses testing	193

List of Figures

Figure A. The Stages and Principles of ADR	08
Figure B. The ERM Cube (COSO, 2004)	38
Figure C. Enterprise Risk Management (COSO, 2017)	41
Figure D. The Six Principles of COBIT 2019	48
Figure E. The seven Governance System of COBIT 2019	52
Figure F. COBIT 5 Assessment and Assurance Processes	53
Figure G. The Viable Systems Model	64
Figure H. VSM performance measurement system	83
Figure I. The Alpha Design of IT auditing Framework	89
Figure J: Risk Control Model	99
Figure K. Evidence Collection model and guidance for expert witnessing	102
Figure L. Frequency-Impact Fraud Risk Assessment Matrix	109
Figure M. Conceptual framework for the Development of the Research	131
Figure N. The deductive approach of enquiry in this research	157
Figure O. Cognitive Processes of Enquiry of the Study	158
Figure P. Conceptual Hypotheses	175
Figure Q. Scree Plot	182
Figure R: The Summative Depiction of IS Audit and Assurance Framework	196

LIST OF APPENDIXES

Appendix 1.0.	Survey Instrument	226
Appendix 2.0.	Correspondance	228
2.1.	Ethics Approval Letter	229
2.2.	<i>Ghana Audit Service</i>	230
2.3.	<i>Kumasi Technical University</i>	231
2.4.	<i>Sekyedumase Rural Bank Limited</i>	232
2.5.	<i>Sun Shade Foundation Limited</i>	233

CHAPTER ONE

INTRODUCTION

1.0. Introduction

This chapter discusses the research background and spells out the motivation for the study. It introduces the research question and provides the research objectives together with the relevance of the study to target users. The chapter, furthermore, discusses the approach used to achieve the research objectives and finally, presents the structure of the thesis.

1.1. Background to the Study

Information Technology or Information Systems (IT/IS) audit has been described as the examination and evaluation of systems and processes in place to secure technology infrastructure, the determination of business and compliance risks and inefficiencies associated with policies and operations that affect business goals (Cassidy, 2016). The history of IT audit dates to the late 1960s when the evolution in software development along which business accounting began to change from paper-based to electronic. The earlier form of IT audit began in the 1950s as Electronic Data Processing (EDP). EDP practitioners later formed the Electronic Data Processing Auditors Association (EDPAA) who issued the control objectives best practices for IS/IT auditing. The EDPAA has now changed since 1994, into The Information Systems Audit and Control Association (ISACA) who currently issue Control Objectives for Information and related Technology (COBIT) best practices used for IT auditing (Haislip et al., 2015; Bartens et al., 2015; Zhang & Le, 2013; Rossouw, 2005).

IT auditing has evolved since 1994 and come of age. The high-profile accounting scandals and the sensational corporate failures that rocked big economies around the globe since the beginning of the twenty first century contributed significantly to the rise in prominence of Information Technology (IT) audit (Agrawal & Cooper; 2017; Agrawal & Chadha, 2005). The above development has been responsible for the increase in regulations, legislations and best practices frameworks for governance and IT auditing such as Sarbanes-Oxley Act (SOX), Gramm-Leach Bliley Act (GLBA) and updating of Health Insurance Portability, Accountability Act (HIPAA), Committee Sponsoring Organisations of the Treadway (COSO) and International Organisation for Standards (ISO) standards. Although these are

considered as best practice guidance for auditing, due to their paucity, critics wonder if they constitute complete IT auditing frameworks (Zhang & Le, 2013). The COBIT frameworks for IT auditing by the ISACA has been generally accepted around the world as a defacto IT auditing framework. However, concerns been expressed that, the most current version of the COBIT generation COBIT 2019 and its predecessor COBIT 5 released in 2013, have shifted their paradigm from auditing framework to framework for the governance of enterprise IT (GEIT) (ISACA, 2019; Haislip et al., 2015; Wescott, 2014).

1.2. Research Motivation

Across Africa, Asia, Southern American Countries and the Middle East, abundant natural resources, rising incomes and accelerating investment in infrastructure have attracted multinationals eager to expand their global presence. Government Agencies and Businesses keen on survivability and maintenance of success are investing in solid IT infrastructural strategy to support this. Many of these economies are, however, characterized by opaque regulatory climates, weak regulatory institutions and invisible networks which influence companies and expose them to unacceptable legal and reputational risks (Boateng et al., 2014). Transparency International have always ranked these areas red for weak regulatory systems and high corruption and fraud. They posit that systematic corruption is leaving many of these countries, particularly, sub-Saharan countries struggling to comply with best practices or to uphold the rule of law (Buchanan & Clayton, 2014). Concerns about the role and responsibilities of auditors have become, particularly, crucial.

Increasingly, because of the above, there is high public interest in quality IT audit and information assurance services that go beyond mere IT control reviews or audit of financial statements (Froese, 2010); because successful business organizations now build on a solid IT infrastructural strategy. Users of corporate reports now do not only demand more accountability and transparency with financial statements, they also demand assurance that the organization is aggressively controlling risks contributed by IT use and management's steps to protect strategic business assets (Brazel & Agoglia, 2007). Stakeholders expect an expansion of IT auditors' responsibilities into wider corporate level plans, IT governance assurance and consulting service for chief executives and Boards to keep businesses viable (Zororo, 2014).

Statutory audit and assurance services have proved to be delivering less effective results (Abugu, 2014; Osei-Afoakwa, 2013). Audit and Assurance practitioners often fail to sufficiently address key audit matters with the relevant level of professional and technical expertise due to lack of guidance (Osei-Afoakwa, 2013; Ebimobowei et al. 2011). Audit woefully ignore the comparison of what is practiced with best practices and rarely link them to drivers of business performance, value or change. Audit reports are, therefore, becoming less useful. They are less thorough, superficial rubber-stamp annual exercise which adds little to no value (Omonuk & Oni, 2015).

Generally, however, audit is carried out on basic operational controls touching briefly on tactical and focusing on compliance-oriented issues (Huck, 2016). IT auditors merely concentrate their assessments on IT projects advisory and information security reviews, application control reviews (ACRs) and general control reviews (GCRs) (Svata, 2011). Board of Directors and Senior Managers are, often, not helped by IT audit reports because they don't use tactical information for decision making and they are asking why (Tan, 2015; Underwriters Laboratories Inc., 2006).

Attempts to improve the effectiveness of IT audit outcomes by implementing known best practices have proved challenging in less regulated business environments for several reasons (Kahorongo et al., 2015; Buchanan & Clayton, 2014). Apart from the change in focus (Wescott, 2014) the COBIT 5 framework is criticised for its cumbersome in structure (Moeller et al. 2013). The framework has furthermore been criticised for failure to provide comprehensive customisation guidelines for audit purposes (Zhang & Le Fever, 2013). As mentioned earlier, other known best practices such the COSO integrated internal control framework, SAS, the Statement on Standards for Attestation Engagements (SSAE) No. 16 (formerly SAS 70) the IT Infrastructure Library (ITIL) and ISO standards still suffer from paucity and critics wonder if they constitute complete sets of frameworks for IT auditing (Flood, 2017; McCafferty, 2016). Several of these best practices have often failed to translate well into desired outcomes in areas of less regulatory structures because of lack of sufficient implementation guidance (Kahorongo et al., 2015) and unclear theoretical foundation to leverage the resolution of implementation challenges (Haislip et al. 2015). The motivation for this study is that, with plausible systems theory and on the strengths of existing best

practices a more suitable framework for IT auditing can be modelled for less regulatory environments for desired intervention in the numerous challenges of auditing.

1.3. Research problem statement

The audit service is challenged by expanded assurance demands which require the deployment of integrated, multi-disciplinary framework to achieve the desired effect for stakeholders (Ebimobowei et al., 2011). Attempts to develop a unified structure for auditing dates to Mautz & Sharaf (1961). Persistent deficiencies in the frameworks for internal controls related to IT, however, continue to adversely affect the quality of financial reporting, fraud detection, business performance and other critical success factors affecting the overall business viability (Omonuk & Oni, 2015). Stakeholders firmly believe that a shift in the paradigm of IT audit to match the increasing market demands will be very essential in reviving the confidence in the audit practice before it totally loses its vitality (Appiah et al., 2014). The integration of technology and systems theory into audit solution and even more broadly into the areas of Governance, Risk Management and Compliance have, therefore, been viewed as the most suitable approach to IT auditing in contemporary business environments (Sun et al., 2015; Havelka & Merhout 2013; Iyengar, 2007; Bell et al., 1997). However, the systematic approach to achieve it has been a subject of debate which has challenged practitioners and researchers over the years (Ha, 2005; Kinney, 2003).

A review of extant literature has demonstrated several approaches and best practices recommended for various forms of IT assurance reviews (Buchanan & Clayton, 2014; Zhang & Le, 2013). Systems-based audit framework, notwithstanding, is seen to have the brightest potential to contribute to development of most efficient and effective approach for auditing IT, however, it has received inadequate attention from researchers (Merhout & Havelka. 2008). Available literature demonstrates scanty research effort by practitioners or academicians to explore the subject matter, hence, no such framework exists to provide the needed intervention and guidance for IT auditing in the empirical domain. Omonuk & Oni (2015) believe it is, perhaps, because the discipline is relatively new. The expectation in this study is to contribute to the bridging of this yawning research gap by modelling a framework based on tried systems theory that is fit for arresting contemporary and future IT audit and assurance.

1.4. Research Question

The research is designed to address the following research question:

How efficiently and effectively can systems-based framework for auditing provide solution to IT audit and assurance challenges in less regulatory environments?

1.5. Objectives of Research

The problems of IT auditing in less regulated business environments involve practical challenges in systems development and review. The anticipated causes include theoretical inaptitude, paucity and an unsteady focus of frameworks and best practices for IT auditing. Hence, attempts to known best practices have failed to achieve desired outcomes due to lack of fitting guidance. The goal of the research is to develop a systems-based framework that draws on the strength of an apt systems theory and to apply the rigors of known best practices to demonstrate how to achieve effective and efficient IT auditing and assurance outcomes for less regulatory environments. To achieve this research goal, the following objectives are specified.

1. To explore the evolution and challenges of IS audit in less regulatory environments.
2. To explore the cybernetics theory of viable systems approach (VSA) as a model for analysing and conceptualizing solution design for IS auditing in less regulatory environments.
3. To build a conceptual model (an artefact) that provides the guidance for IT auditing for less regulatory environments.

1.6. Research Approach and Instruments

A research approach defines the plan and procedures for the research that can span the steps from broad philosophical assumptions to detailed methods of data collection, analysis and interpretation of results (Raftery, 1995). Objectivism is the ontological stance throughout the research process in that, it is assumed, knowledge that already exists can be organized and be objectively measured to project more improved and desirable outcomes. The research adopts pragmatism as its epistemological paradigm because the researcher believes, in this study, both qualitative and quantitative paradigms are relevant in pursuance of more desired objectives. This research is aimed at achieving dual goals – to produce academic knowledge and to create an intervention that solves practitioners' problem. The plan of the research is

addressed by, firstly, conceptualising the problems of IS auditing challenges and, secondly, developing a framework (artefact) for a better, sustainable and more improve audit outcome in less regulatory environments. To achieve this goal, the research method has been carefully selected. Action Design Research (ADR) method was identified as the most suitable and logical approach to build the research instrument for a study like this to achieve its desired goal (Sein et al. 2011; Hevner, 2007). ADR is a new method of Design Science Research (DSR) which combines the characteristics of DSR and Action Research (AR) to design very useful and high performing IT artefacts (Masters, 1995). It must be stated for emphasis that the choice of ADR in this study is based on the consideration that it is classified as a typical design research method representing the view of continuous stakeholder participation in the research project (Cronholm et al., 2016). The participation of stakeholders particularly required or, at least, expected in a study like this.

The development of ADR sprang from the need to make designed artefact more relevant for addressing problems in organisational context by involving practitioners and end-users at the outset through to the artefact evaluation stage as opposed to DSR which only involves end-users during evaluation (Hevner et al. 2004). ADR is, therefore, popular for the design of artefacts that are used by practitioners in the field because of their deeper involvement. An artefact in ADR has been defined to reflect the ensembles IT designs or any IT-based system, either hardware or software, model or method that is shaped by the organizational context during its development (Sein et al, 2011). An artefact in design science research has currently established a broad definition that includes models, methods, constructs, instantiations and design theories containing demonstrable or teachable knowledge (Gregor & Hevner 2013; March & Storey, 2008).

ADR methodology involves learning by doing and addresses problems characterised by dependence on human cognitive abilities to produce effective or desirable solutions to complex or ill-defined environmental contexts (Sein et al., 2011; Hevner & Chatterjee, 2010). The purpose of ADR is to generate prescriptive design knowledge through learning from the building, intervention and evaluation of an artefact taking into consideration contextual factors in an organizational setting to address a problem (Peterson & Lundberg, 2016; Sein et al., 2011; Brown, 2009; van Aken, 2004). ADR has attracted importance in IS research because it directly addresses two of the key issues of research in the discipline; firstly, the recognition of the relevance of the central role of the IT artefact in IS research,

although problematic and, secondly, the need to mitigate the perception of lack of professional relevance (Hevner & Chatterjee, 2010; Sein et al. 2011). ADR combines theory generation with the researcher intervention to build a solution for organisational problem. Thus, based on the relevant attributes of a selected theory the researcher can conceptualize an artefact, build and to evaluate its contextual and practical value in business by aligning the needs of people to solve complex problems, to find desirable solutions to change or to improve the existing situations in the natural world (Peterson & Lundberg, 2016; Sein et al. 2011).

1.6.1. Research Instrument Building and Data Collection

Sein et al. (2011) articulates four stages of Action Design Research (ADR), each anchored by principles which form the basis of the design of this research. The purpose for adopting this instrument building approach is the need to link theory with practice and thinking with doing which ADR approach known to encourage. Workshop technique together with questionnaire were used for data collection from the focused research participants for concurrent and subsequent analyses respectively. A workshop is defined in this research as a meeting at which the researcher engages in intensive discussions with target participants at various stages of the research process to debate the underlying theory vis-à-vis emerging research themes, to learn, to collect data to leverage the design with which to plan and focus the research project to validate the final framework (Iversen et al., 2004).

Sein et al. (2011) emphasise four main stages of Action Design Research (ADR). These are: *Stage 1* – Problem Formulation; *Stage 2* – Building Intervention and Evaluation; *Stage 3* – Reflection and Learning and *Stage 4* – Formalising Learning. Each stage in the ADR process is anchored by a set of principles. The ADR process is nested in alpha-beta continuum. The alpha section diagnoses the problem and ends in the development of a prototype solution or artefact. The beta section is responsible for rigorous evaluation of the earlier artefact and builds it up to the abstraction stage. Stages 1 and 2, as shown in the diagram below, are considered as the alpha section and stages 3 and 4 are the beta section. The ADR process is demonstrated in **Figure A** below.

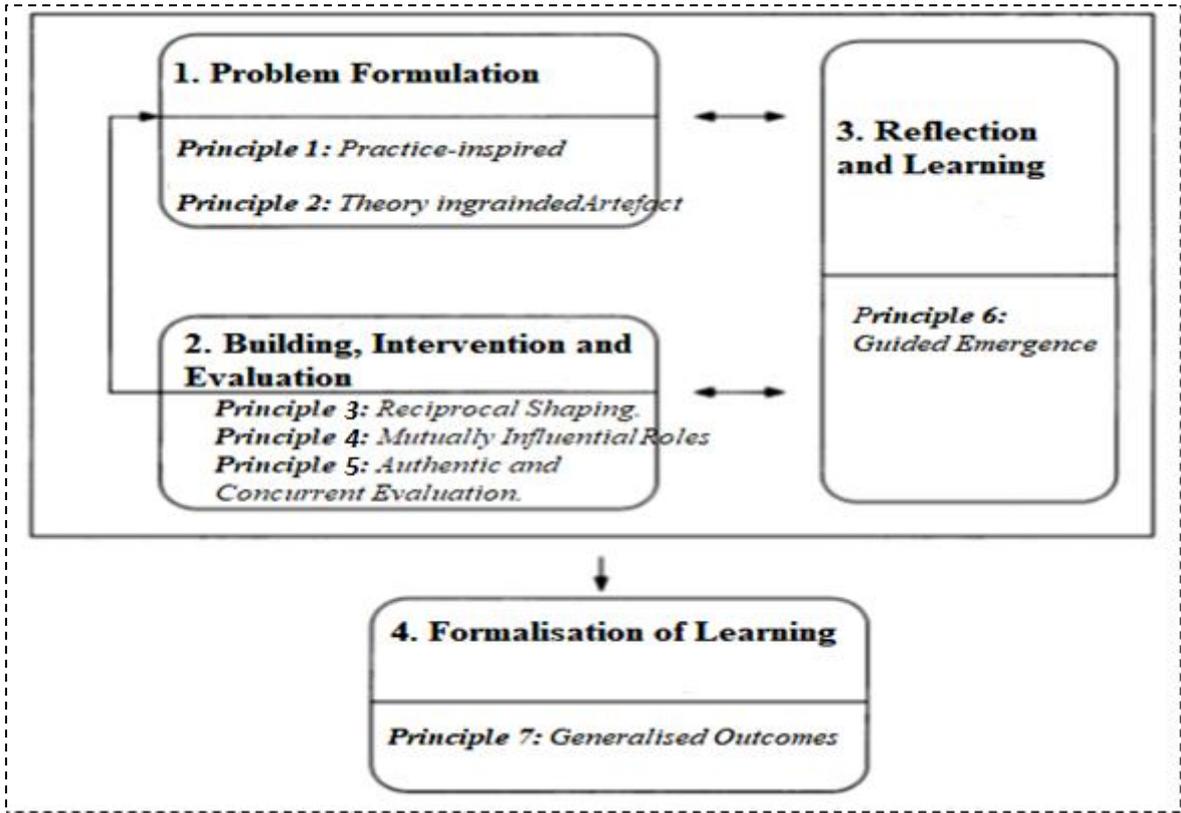


Figure A: *The Stages and Principles of ADR adapted from Sein et al. (2011).*

STAGE 1: The problem Formulation: The research process is initiated by the problem formulation stage. At this stage of the research the problem is perceived in practice as anticipated above by the by researchers. This stage is developed on two principles: Practice-inspired research and Theory-ingrained artefact.

Principle 1 - Practice-inspired research: A practice-inspired or practice led research allows for the incorporation of a conceptual framework together with creative methods and creative output which concern the nature of practice and lead to new knowledge that has practice significance (Mäkelä, 2007). Sein et al. (2011) emphasises on the demonstration of sufficient background knowledge of the problem which should include viewing the problem from the field of practice. The researcher, therefore, plays an active role in the research by collaborating with and sampling the viewpoints, knowledge and the skills of actors and practitioners in the field of the research concerned. This principle involved iterative process designed based on working hypothesis to obtain input from the field. The initial working hypothesis at the problem formulation stage was that the problems of auditing in less regulatory environments are influenced by the theoretical inaptitude. There are, therefore,

practical challenges in the implementation of best practices and frameworks for auditing designed for highly regulated economic environments. The problem formulation stage uses in-depth exploratory literature review to obtain strong technical background knowledge of the problem to demonstrate sufficient background evidence of the challenges. In addition to the review of literature, the research process employs iterative processes to application environment to brainstorm and collect the views of viewpoints of actors and practitioners in the field to validate the working hypothesis.

The iterative processes referred to above involved a series of workshops with different organisations in Ghana to brainstorm with practitioners, expected end-users of the research output including senior managers, the academics and trainees in the field of auditing at different stages in the research process to discuss and obtain their practical views of the problem under investigation. These workshops were crucial to research since it provided the opportunity to secure long-term commitment from the participating organizations beyond this stage. The selection of participating organisations was based on their information-richness. Information-rich sources are those which, by attribute and functions, possess great deal of information relevant for the success of the research (Mills et al., 2010). Four organization in Ghana agreed to participate in the research as sites in a multiple case study design of this study. They were the Ghana Audit Service, Kumasi Technical University, Sun Shade Foundation Limited and Sekyedumase Rural Bank Limited. Formal letters of approval were obtained from the selected organisations who accepted to be used as case sites for data collection in the initial workshops.

The workshops revealed, among several others, that the focus of their reviews has been on operational issues and tend investigate compliance with rules and regulations and, therefore, exception-based reporting exercise. IT audit or internal audit, therefore, persistently amplify faults and constraints and, often, offer little to no countermeasures. Internal auditors are hardly engaged in strategic planning or policy reviews and exert no influence on organisational systems development, thus, limiting their relevance only to tactical and functional management roles. Generally, there is a woeful admission that internal auditors lack the relevant guidance to provide in a value-driven service and this is responsible for the high audit failure exposures that characterise developing countries. This led to the next stage of the problem formulation stage which is guided by the theory-ingrained artefact principle.

Principle 2 - Theory-ingrained artefact: Theory-ingrained artefact articulates the need to conceive a theoretical view of the problem. This involves the selection of what Gregor & Jones (2007) refer to as kernel theory or justificatory theory. The justificatory theory provides sufficient concepts and attributes that guides the solution design of the artefact under construction. It informs the researcher on issues and knowledge requirements including knowledge from the field and the experience of the researcher to be brought under consideration and evaluation to achieve the research objective. Mullarkey and Hevner (2015) stress on seeing the theory-ingrained stage from two phases - Problem Diagnosing phase and a Concept Design phase. The problem diagnosing phase is a rigorous demonstration of research problem informed by the justificatory theory and an expressed need in practice. The Concept Design phase evaluates the design based on attributes and principles of the justificatory theory. In this research, the cybernetic systems theory of Viable Systems approach (VSA) abductively was selected to conduct diagnostics of the problems and to subsequently build the intended interventions. This theory contains concepts and attributes for the performance of diagnosis of complex and irregular problems in a systematic manner and, therefore, found to be very suitable for the diagnosis of IT audit problems, subsequent building of efficient and effective interventions and developing design concepts for the improvement in IT auditing for less regulatory environment.

Justification of the Viable Systems Model as the Ingrained Theory

The VSM has been found to be suitable for this study because it offers a holistic view of the working of the organization as a whole, taking into consideration operational processes, meta-systemic management as well as environment and the interactions amongst them (Leonard, 2009). It has been proposed and reaffirmed the VSM is a powerful tool for diagnosing organizations and identifying the existing strengths and weaknesses prevailing within them. Also, it is used for understanding internal and external organizational structures as well as (re)designing solution on the basis of necessary and sufficient conditions for the viability of any complex system (Leonard, 2009).

The contemporary view of IT audit or assurance, according to ISACA (2013) is that the scope of IT audit functions should reflect all day-to-day functional management processes as well as corporate level functions. This must be based on a framework with the capacity to support the dynamics of the uncertain and complex business ecosystems. By this, auditors

and assurance practitioners can forge a stronger relationship between with those charged with governance and management because both have common goals since they both speak a common language. The suitability of the use of the VSM to pursue the objectives of this study lies in the fact that its structure organizes the five functions of those charged with governance and management which are integral to the organization's viability despite of its size, its business type and environment in which it exists (Espejo, 1995).

Furthermore, the VSM theory, based on complexity sciences, offers more holistic approach to the concept of sustainability. It has been established in the background study that business ecosystems with increasing use of sophisticated technologies are looking for a more resilient and enduring guidance for IT auditing (Flood, 2017; McCafferty, 2016). The increasing use of sophisticated technologies in contemporary business ecosystem has increased risk to Audit and Assurance practitioners. The recognised root causes of these risk issues often cut much deeper to the heart of the audit practice. The sheer complexity gives practitioners audit and assurance practitioners one of their greatest challenges to maintain business viability and survivability of the practice (ACCA, 2016). The VSM has been adopted by several researchers and practitioners for diagnosing organizational structure, performance, and for (re)structuring social and business organizations based on the factors essential and adequate for its long-term viability (Espejo, 2003). This puts the VSM in a suitable position to serve the objective of this project.

STAGE 2 – Building, Intervention and Evaluation (BIE): This stage is often seen in ADR as an iterative process to respond the research question. The second stage of ADR process uses the problem framing and theoretical premises adopted in stage one to build an initial conceptual solution which is subject to further shaping carried out in subsequent iterative process with the participating organisations. Sein et al. (2011) put the BIE activity into IT-dominant and Organisation-dominant continuum. The IT-dominant BIE schema was employed to initialise the BIE activity and to focus on an effort to generate and to manage a more contextually suitable IT artefact. Sein et al. (2011) articulate that the BIE stage is anchored by three principles namely; *reciprocal shaping, mutually influential roles and authentic and concurrent evaluation*. A conceptual framework based on agreed meanings of the ingrained theory was developed at the end of this activity prior to a rigorous evaluation of the IT-dominant BIE schema. At the other end of the continuum of ADR research process

is the organisation-dominant BIE. This focussed on generating design knowledge in business context and ensured that the knowledge generation process was closely reflected the continuous view of practitioners and end-users and connected to organisational context.

Principle 3 - Reciprocal Shaping: This principle bases the shape of the reciprocal solution design concepts of the justificatory theory. The reciprocal shaping principle is often seen as the process to resolve what DeGrace and Stahl (1990) describe as solving "wicked problems" that typifies the 'how' element of a design research question. This brings together the technical and practical knowledge bases to build a rigorous intervention for the further evaluation. It represented the core activities of the research. In this research, technical knowledge bases included best practices and frameworks of IT auditing e.g. COSO guidance, COBIT 5/2019 and ITIL organised to provide the relevant intervention. This was complemented by deep investigation and use of past research work in the subject area as well as the application of the researcher's considerable experience as an accountant, auditor and member of audit committees of the Board of Directors of two financial institutions in Ghana.

Principle 4 - Mutually Influential Roles: This principle emphasises on the importance and impact of the technical knowledge, field experience and mutual learning of the researcher on the subject matter of the study as well as the research team members and practitioners, if any. The dynamics, at this stage and in this principle, are such that it may lead to clashes of perspectives of the practical and theoretical viewpoints of the members on the team and must be well coordinated and synthesised to generate a solution that responds to the research question. In this research, however, there were no research team members as this is an academic exercise in pursuance of a Ph.D. qualification and conflict of research team members' perspectives of the design could be an issue. The researcher was the sole designer and constructed the design based on his practical experience, technical and theoretical knowledge bases and perspectives of practitioners included in the Building of Intervention and Evaluation (BIE) stage as participants whose roles were to shed light on challenges and emerging issues of the field in which the research is based. As stated earlier this state of the BIE is seen to be IT-dominant for the of creating an innovative technological design at the outset (Sein et al. 2011). A conceptual framework was developed at the end of the IT-dominant BIE stage based on the key concepts and relationships identified among those concepts to serve as guide for further development of the study. This led to the formulation

of some practical hypotheses based on the conceptual framework. Participants who included practitioners, expected end users and other interested parties of the field in which the research is based were contacted to express their opinions on validity of the designed intervention for both concurrent and subsequent evaluation and analysis, reflection and learning. This is the organization-dominant BIE process of the ADR efforts aimed at generating a design knowledge which responds to the main research question. Thus, the primary source of innovation of this research is the modelling of an effective intervention for IS auditing for less regulatory environments. More light is shed on the methodology and the use of the participants view on the design in chapters five and six of this research.

Principle 5 - Authentic and Concurrent Evaluation: This stage emphasizes on objective evaluation of the built intervention. Evaluation in a design research is the assemblage of evidence which demonstrates the worth of the conceptual solution to the problem or the artefact. Evaluation also addresses the efficacy, quality, utility, validity assessment. Validity means that the conceptual solution or artefact works and does what it is expected to do, or it provides clear and dependable guidance in operational terms for the achievement of its goals. The utility criterion assesses whether the achievement of goals has value outside the development environment (Peppers et al., 2007; Gregor & Hevner, 2013).

The selected action to achieve this purpose was another series of workshop organized in a formalized organizational setting. Gregor & Hevner (2013) opine that a design science may draw from many potential techniques, such as case studies, experiments and simulations. The objectives of the workshops at this stage were, firstly, to debate the selected variables in the conceptual framework, to identify emerging research themes to, further, aid the principle of reciprocal shaping described earlier and, secondly, to collect data on their view of the themes underlying the construct. The data collection process sampled the views of participants who include audit practitioners and many other expected end users of the framework from selected organizations through structured questionnaire technique carefully designed to measure the extracted variables of the construct. Quantitative data analysis techniques such as factor analysis, structural equation model and correlation and regression analyses were employed for this exercise. The motivation for the use of this technique is in line with the assertion that a quantitative validation of conceptual hypotheses is empirically beneficial in aid of conceptual rigor and design evaluation because it can reduce the risk of non-replicability of results (Schaller, 2016; Chow, 1991).

STAGE 3 – Reflection and Learning: Reflection and Learning is anchored by the principle of *guided emergence*. Stage three ushers in the beta phase of the ADR research process, according to Sein et al. (2011). This is not a complete break from the earlier section as this advances the rigor in the building, intervention and evaluation processes. This phase is characterised by the analysis of field data for the ongoing shaping of the design in practical context through the perspectives of focused groups of participants. Sein et al. (2011) argue that although the term ‘emergence’ which carries a sense of external, intentional intervention may seem antithetical to design which conveys sense of organic evolution, the principle of guided emergence in ADR tolerates and ensures that the designed artefact will reflect the concepts and relationship on the kernel theory as well as the perspectives of focused group and participants. Reflection and learning stage, therefore, advanced the framework conceptually from building a solution for IT audit problems in less regulatory environments to applying that learning to more generalised components and principles of IT auditing for less regulatory environments.

STAGE 4 – Formalisation of Outcomes: This hinges on the principle of *generalised outcomes*. In this research, it formed the conclusion section of study which constitutes a summary of outcomes such as the articulation of the design theory or the abstraction of the design which is considered the meta-artefact in a design research. Generalised outcomes included the communication of the practical value of the designed artefact (Sein et al., 2011).

1.6.2. Relationship Between ADR and the Research Structure

Table 1 below summarises the relationship subsisting between the research design, research objectives, the structure of the research, the and the organisation of the study.

ADR Process Stage	ADR Principles	Research Objectives	Corresponding Chapter
Problem Formulation	1. Practice-Inspired: - Literature Review, - Workshops	<u>Research Objective 1:</u> <i>To explore the evolution and challenges of IT audit environment in less regulatory environments.</i>	Chapter 1 - Introduction, Chapter 2 - Literature review Chapter 3 -

	2. Theory-Ingrained Artefact - Problem Conceptualization	Research Objective 2: <i>To explore the cybernetics theory of viable systems approach (VSA) as a model for analysing and conceptualizing solution design for IT auditing in less regulatory environments.</i>	Problem Diagnosis and Conceptualisation.
Building, Intervention and Evaluation	3. Reciprocal Shaping 4. Mutually Influential Roles 5. Authentic and Concurrent Evaluation	Research Objective 3: <i>To provide the guidance for the creation of informed IT Audit Universe for the delivery of desired audit outcomes.</i> <i>To develop a conceptual solution design to IT auditing problems for less regulatory environments.</i>	Chapter 4 – Conceptual Solution Design, Conceptual framework/Hypotheses & Chapter 5 - Methodology.
Reflection and Learning	6. Guided Emergence	Research Objective 4: <i>To critically ensure that contributions to knowledge are identified and conceptual hypotheses validated.</i>	Chapter 6 – Data Analysis and Results.
Formalisation of Outcomes	7. Generalised Outcomes	Research Objective 5: <i>To contribute to the theoretical and practical knowledge development of IT auditing in less regulatory environments.</i>	Chapter 7 - Conclusion

Table 1 - Relationship Between ADR and the Research Structure.

1.7. Expected Knowledge Contribution of the Research

Clarifying the contribution of a design science research output is very critical to stakeholders in a professional discipline or a field of knowledge (van Aken, 2004). Contribution to knowledge from design thinking perspective has been categorised into two main bases by Gregor and Hevner (2013) - Descriptive knowledge base and Prescriptive knowledge base. Descriptive contribution base is one that expresses knowledge that involves the nature of a natural phenomenon, the laws and regularities of them or the interrelationship among them are. Prescriptive contribution, however, expresses knowledge involving artificial creation or artefacts and how they apply to the improve the environment. The general objective of this research is to make a prescriptive practice-led contribution to knowledge of auditing in the field of IS auditing.

There is a consensus about ADR that it should make a theoretical contribution in the relevant field and provide a solution that is appreciated by target users for being practically useful for the solution of current application challenges or anticipated problems or both (Sein et al., 2011; Gregor & Hevner, 2013; Goldkuhl, 2012). This research aims at modelling a framework for IT auditing for less regulatory environments and expects to contribute to the theoretical development of IT audit field. This is to be achieved by the design of an interventionist guidance through artefact building. The artefact is expected to provide an improvement in the knowledge about IT auditing and practice.

1.8. Organisation of Research

Chapter One – *Introduction*, discusses the research background and spelt out the issues that have necessitated the initiation of the study. It provides the research objectives and provided the opportunity to justify the relevance and importance of finding solution in the empirical situation. The chapter introduced the design science method used and briefly discussed the iterations involved to achieve the research objectives. The Chapter also presented the contribution of the research to knowledge and practice and, finally, the structure of the thesis was outlined.

Chapter Two – *Literature Review* - This chapter discusses literature on the nature, objectives and expectations of IT auditing and assurance. The literature review involves a survey of knowledge that is relevant to the problem at hand. The Literature review section contributes to the problem relevance by supporting the research with the work including the theoretical foundations, open reference frameworks and approaches espoused by various researchers, professional bodies and authors in the problem domain to achieve similar aim in IT auditing discipline (Gregor & Hevner, 2013). This Chapter is also dedicated to identifying the gaps in literature that the research objective is expected to close.

Chapter Three - *Problem Formulation and Conceptualization*

The chapter is an extension of the literature review in the previous chapter. It introduces the kernel theory or justificatory knowledge used to inform the conceptual solution design. Gregor and Hevner (2013) posit that the justificatory knowledge requires some level of judgement of the researcher based on the knowledge obtained from the problem definition

stage of a design science research for which the subsequent effective design provides justification. Ittonen (2010) posits that the main reason for substantial examination of existing theories and ideas is to see if there is any possibility that the existing theory will be able to provide the responses to the problems the researcher seeks to find solutions to. The chapter examines the cybernetics theory of Viable Systems Approach (VSA) for the possibility of providing a conceptual solution for the design of the artefact in this research.

Chapter Four – *Building, Intervention and Evaluation*

Chapter four is dedicated to the presentation of the conceptual solution of the research problem. This includes the conceptualisation of the framework, development of the elements of the construct and the evaluation of the framework. The Chapter outlines the outcome expectations of the developed framework and proceeds to develop some hypotheses on the validity of the framework based upon testing is conducted on target users. The Chapter provides a technique for the customization of the framework to achieve desired outcome. At the end of this chapter a conceptual framework is developed based on the researcher's synthesis of the ingrained theory, literature and the views of practitioners in the field. Consequently, conceptual hypotheses (propositions) are formulated for testing and validation in the application environment.

Chapter Five – *Methodology* – The rigor in the evaluation approach is the driving goal for methods selection (Gregor & Hevner, 2013). The chapter provides details of the philosophical backgrounds of this research subscribes to. It discusses the strategy employed to make knowledge enquiry and to create knowledge including its epistemological paradigm. The methods in this research provide clear rationale for the selections of design and the rigorous evaluation of the artefact in this research. The chapter describes the techniques for data collection, the development of research instruments and methods of data analysis in pursuit of building, evaluating and validating the solution design.

Chapter Six – *Data Analysis Reflection and Learning* - This Chapter provides the statistical analysis of data collected by the questionnaire issued at the end of the second iteration. The purpose of this chapter is to provide validation of the designed framework for

auditing from the application domain. The results of the tested hypotheses are also reported and with the relevant interpretations.

Chapter Seven – *Conclusion (Formalisation of Learning)* - Chapter seven provides the conclusion to the research. In this chapter, the research demonstrates how he has responded to the research question and achieved the research objectives. Furthermore, the chapter summarises the general outcomes of the ADR research and further articulates the practical benefits of the design. The chapter discusses the limitations of the research and provides information on opportunity for future research and development.

1.9. Conclusion

Chapter one introduced the research and contextualised it. It has also shown all the components of the research study. The next Chapter is Chapter two which provides in-depth literature review aimed building the knowledge base of the field of the research. Materials used to develop this chapter include past research outputs in the field, literature from professionals and professional bodies in the field, research articles in databases as well as relevant information available on the internet.

CHAPTER TWO

LITERATURE REVIEW

2.0. Introduction

This chapter discusses literature on the nature, objectives and expectations of IT auditing and assurance. The literature review involves a survey of knowledge that is relevant to the problem at hand. The Literature review section contributes to the problem relevance by supporting the research with the work including the theoretical foundations, open reference frameworks and approaches espoused by various researchers, professional bodies and authors in the problem domain to achieve similar aim (Gregor & Hevner, 2013). This Chapter is also dedicated to identifying the gaps in literature that the research objective is expected to close.

2.1. Definition of Audit

Auditing originates from the Latin word ‘audire’ which literally mean ‘to listen’ (Owolabi et al., 2016). Hence, Romney et al. (2006) define audit as an objective and systematic process of obtaining evidence which include management assertions about economic actions and events and the evaluation of to ascertain the degree of correspondence between those assertions and established criteria and communicating the results to interested users. Flint (1988) describes auditing as a social phenomenon whose usefulness is wholly based in its practical and utilitarian values other than that serves no purpose. An audit can be either an external engagement conducted by certified chartered accounting or auditing firms or an internal engagement performed by an organization’s internal audit function (Merhout & Havelka, 2008). There are three different types of audits according to Romney et al. (2006): *Financial Audit*, *Operational or Performance Value Audit* and *Information Systems audit*. Financial audit refers to an independent examination of the books, accounts, documents and transactional records of an organization to ascertain the extent to which management assertions represents the true and fair view of the financial affairs of that business concern (Power, 1999). *Financial audit* focuses on the financial and, sometimes, operating information for the reliability and integrity of accounting records as well as compliance with specified accounting standards. Practitioners perform their evidence collection and measurements against the specified accounting standards and issue their reports based on whether in their view the financial information represents a ‘true and fair’ view of the state

of affairs of the entity. The details of financial accounting audit are not within the scope of this research.

Operational or Performance Value audit evaluates the economic, efficient and effective use of resources and the accomplishment of established goals and operational objectives. Performance value audit is now highly accepted IT audit concept applicable at the private sector (Sayana, 2002). Performance Value audit integrates value for money into audit and suggests that real value of audit is obtained when an audit approach incorporates the traditional ‘three-E’s’ value-drivers which include *Economy, Efficiency and Effectives* (Grönlund et al., 2011).

Assurance in auditing is generally defined as a type of auditing engagement in which the practitioner communicates or expresses a conclusion designed to provide or enhance the degree of confidence to the intended party who is, often, a party other than the responsible party about the outcome subject matter of the evaluation exercise which often is executed against a certain criterion or criteria. Assurance covers the evaluation of activities not governed by internal and/or external audit standards and thus helps executives to be sure whether the subject matter has or can attain the stated goals. Assurance therefore is a much broader concept in the audit discipline than audit (Svata, 2011). Typically, assurance reports include the results of tests of controls in which the practitioner provides either a reasonable, but *not* absolute assurance that the control objectives in the scope were achieved or, otherwise, assurance cannot be given in the opinion of the practitioner. This contrasts with financial audit whereby practitioners come to the conclusion of whether the financial statements represent true and fair view. The subject matter of assurance engagements can take different forms with different characteristics; however, it is essentially aimed at obtaining a degree of assurance within the context of professional judgment whether or not the subject matter satisfy a suitable benchmark (Christensen et al. 2012).

Information Systems/Technology (IS/IT) audit refers to the whole process for an auditing organization with the help of ICT to assess whether the information technology and other organizational resources are safe, reliable, and effective (Strous, 1998). IT auditing is relatively new compared to financial auditing. The sweeping wave of technologies with increasing complexity in the business has, however, exposed businesses to new risks which include severe extensive competition and sophisticated fraud schemes due vulnerabilities of

IT (Omonuk & Oni, 2015). IT auditing plans and assesses the impacts of information system on financial statement. It organizes and implements auditing projects to produce independent audit reports to identify audit risk, to evaluate enterprise risk controls and information strategies and to optimize a company's operation independently and objectively for the achievement of business objectives (Merhout & Havelka, 2008). One primary purpose of IT auditing is to assess whether or not an information system is meeting stated organizational objectives and to ensure that the system is not creating an unacceptable level of risk for the business. Therefore, although each has a very specific meaning in context, in IT auditing the terms “*audit*”, “*assurance*”, “*attestation*” and “*control*” generally refer to this same general purpose (Svata, 2011).

The issue of risk is becoming more complex and increasingly technical to Audit and Assurance practitioners and the recognised root causes of risk issues often cut much deeper to the heart of the audit practice. The sheer complexity, moreover, gives boards and business executives one of their greatest challenges to maintain business viability and survivability. Independent non-executive directors now face increased expectations of their role. It has, therefore, become very important for auditors to maximize the value of their role by communicating and translating their reports in a timely manner to the understanding of all stakeholders to enhance economic growth. This cannot be achieved without a solid conceptual framework for that purpose (ACCA, 2016).

2.2. Theoretical Bases for Auditing

Hayes et al. (2005) (cited in Ittonen (2010), summarized four main theoretical bases for auditing that requires substantial investigation as follows: Agency Theory, Stakeholder theory (Inspired Confidence Theory), The Police Man Theory and Lending Credibility Theory. Below discussed those theoretical views of demand for audit.

2.2.1. Agency Theory

Agency theory has traditionally been accepted as the dominant theory behind the demand for audit (Adams, 1994). This theory dwells on the knowledge of the agency relationship between those charged with governance and management – as agents of their principal – the shareholders of a company (Ittonen, 2010). Since shareholders do not participate in the functions of those charged with governance and management of the company, it is assumed that the agent has a considerable advantage over their principals in terms of valuable

information for decision making (Mihret, 2014). This situation is referred to as information asymmetry and agency cost (DeFond & Zhang, 2014). This is a reason for the speculation that organizational actions are driven by individual Director's pursuit of self-interest when it comes to governance of contracts bordering on the interests between management or the employee on one side and shareholders on the other side (Mihret, 2014). Thus, differences in risk tolerances can lead to principal and agent being inclined to take different and goal-incongruous actions each (DeFond & Zhang, 2014). Accordingly, the agency theory of auditing argues that audit and the independent review of internal control mechanisms are introduced by management to create a signalling effect to shareholders that management is properly in place and to assure shareholders that those charged with governance and management are discharging their responsibility in good faith for the maximization of their interests (Jensen, 2002).

2.2.2. Stakeholder theory (Inspired Confidence Theory)

Criticisms raised by various corporate governance writers of the agency theory propose stakeholder theory as alternative perspectives of the demand for audit (Mihret, 2014). Proponents of stakeholder theory criticize agency theory on its neglect of the firm's responsibility to a broad range of interested parties or stakeholders other than shareholders of the entity as well as its failure to adequately explain how IT auditing or internal auditing fits into the control framework of capitalist firms. The stakeholder theory suggests that an audit is required based on a tripartite arrangement in stakeholder theory underlying every economic system. The tripartite theory posits that the world of business consists of different groups that are affected by, or participate in, the decisions, behaviour and reporting of a business entity. They include shareholders, managers, creditors, customers, suppliers, employees, government and regulatory agencies (Jensen, 2002). With varying power and interest different stakeholder group can influence decision, behaviour or reporting to the detriment of others (Ramirez, 1999). The stakeholder theory of demand for audit, therefore, says Directors and managers, because of their extensive power to change the behaviour and reporting by their decisions, should consider the interests of all identifiable stakeholders to the firm (Jensen, 2002). Audit and assurance remains the only option for other groups of stakeholders to obtain an independent opinion on the stated plans by those in charged decision making, organisational behaviour and reporting (Nehinbe & Adebayo, 2011; Clas, 2008). Demand for audit in the information age, therefore, is for audit professionals to

evaluate the extent to which management decisions, behaviour and reporting processes deliver value to all groups of interested parties. Internal and IT auditing, for instance, are demanded to provide the assurance that risks of unfairness on unassuming interested party or regulatory compliance failures by those in charge of decision are put in check (Rahman et al., 2014).

2.2.3. Lending Credibility Theory

Lending credibility theory has close relationship with inspired confidence theory. According to the lending credibility theory, investors and lenders face significant risk in doing business in recent years; therefore, auditors are required to primarily function to add appropriate credibility to the financial statements (Ittonen, 2010). Lending and investments involve complex and risky agreements and contracts. According to Baylis et al. (2015) auditors owe an obligation to lenders in terms of predictability associated with evolving market variables that assist contracting parties without regulatory intervention. It is widely acknowledged that high-quality audits directly benefit businesses and indirectly benefit the economy and society in general by assisting in minimizing risk of losses to lenders through ‘due diligence’ assignments. Independent audit is an important service for providing users with assurance on entities historical financial statements and other risks (Mahzan & Hassan, 2015). An Audit report of a company has significant influence on investment decisions since they are integral to investor confidence and are vital to the effective functioning of capital markets. IT audit is a highly valued service since it provides insights into the level of enterprise risks and the extent of ‘due care’ exercised by management to make a real difference to their entity’ operations (Marcello et al, 2017).

2.2.4. The Policeman Theory

The policeman theory says that since those entrusted with governance and control often abuse their privilege. To safeguard assets, therefore, audit is demanded because the expectation is that audit has an enormous role to play in the detection and prevention of fraud (Ittonen, 2010). The policeman theory is one problematic area in auditing where there is existence of an audit expectation gap (Chandler, 2014) because traditional auditing has maintained a passive philosophy towards their responsibility for fraud detection or prevention (Rahaman, 2010). The foundation of this phenomenon is traceable to the famous English case law – re Kingston Cotton Mill Company (1896) in which it was held that an auditor is not bound to be a detective, or ... to approach his work with suspicion, or with a

foregone conclusion that there is something wrong. He, therefore, is a watchdog, not a bloodhound (Chandler, & Edwards. Eds., 2014). According to the Policeman theory attempts to correct this traditional impression. Recent standards on auditing require practitioners to search, discover and prevent fraud in the organization through the investigation of the financial transactions, the financial statement as well as other information (COSO, 2017). The approach to it has, however, continued to attract academic debate among academics and professionals in the field (Omonuk & Oni, 2015; Ebimobowei et al., 2011).

2.2. Objectives of IT Auditing and Assurance

The general objective of Information systems audit is to review and evaluate management's goals and objectives in utilizing technology to support business processes (Radovanović et al., 2010). A primary objective of IT auditing is to provide assurance to relevant stakeholders that an assessed information system is meeting stated organizational objectives and will ensure that the system is not wasting value or creating an unacceptable level of risk primarily from the use of various IT infrastructure, application or service for the business. Several terms have been used to identify the function of IT auditors such as 'assurance,' 'attestation,' 'audit,' and 'control'. Although each can mean differently in specific contexts, however, in IT auditing, they, generally, refer to the delivery of one common purposes (Merhout & Havelka, 2008). generally, IT auditing, assurance or attestation is purported to fulfil the following common criteria.

2.2.1. Confidentiality

This criterion relates to the effectiveness of management's control effort in the protection of sensitive information from unauthorized access and disclosure. In so doing consideration is given to the level of sensitivity of the data as this will determine how stringent the controls over its access is expected to be. Breaches and compromises of confidentiality can lead to significant public reputational harm a business organization, particularly where the information relates to sensitive client data (D'Onza et al., 2015).

2.2.2. Integrity

Integrity criterion concerns the accuracy and completeness of information as well as to its validity in accordance with business values and expectations. Data integrity is an important audit objective in IS/IT audit tests. This is to gain insight into the integrity of controls which

then provides assurance to both management and external report users that the information produced by the organization's information systems can be relied and trusted upon to make business decisions (Radovanović et al., 2010).

2.2.3. Availability

Availability criterion of IT auditing is to ascertain with a certain level of confidence that an information system is the safeguarding of necessary resources and associated capabilities to enable information to be readily accessible when required currently and in the future. Given the high-risk nature of keeping important information stored on computer systems, it is important that organizations gain assurance that the information they need for decision-making is available when required. This implies ensuring that the organization has measures in place to ensure business continuity and ensuring that recovery can be made in a timely manner from disasters so that information is available to users as and when required (Radovanović et al., 2010).

2.2.4. Reliability

This refers to the degree of confidence to which an assessor can determine the consistency of a system or the ability of a system (or component) to perform its required function under stated conditions. The direction of auditor's test to ascertain data integrity in a system in order to be sure that the information is consistent and reliable.

2.2.5. Compliance

Entities risk severe penalties for breaches of rules and regulations and key stakeholders require assurance that necessary compliance procedures put in place by Management have been adequate to avoid potential risk of incurring penalties that may wreck the fortunes of the business (D'Onza et al., 2015).

2.3. Traditional Scope of IT Audit and Assurance

The core of IT auditing is to identify risks and the appropriate controls to mitigate the risk to an acceptable level. Such risks are inherent and pertains closely to IT; without which the risks would not exist at all or would not have the estimated level of likelihood of the risk factor (Sayana, 2002; Rahman, 2014). The risk factors include systems-related issues, such as systems development, change management and vulnerabilities, and other technology-specific factors that can eventually have significant effect on business process,

financial/accounting processing, performance, returns and overall value of the business (Sayana, 2003; Brazel & Agoglia, 2007). IT auditing literature groups controls in socio-technical systems into the categories of general controls, application controls, contingency controls and compliance (Sayana, 2002).

2.3.1. General Control reviews

General Control Reviews in IT auditing involve procedures and working practices with the motives to deter, detect or prevent policy overrides including fraudulent activities by staff or external criminals or both. General control reviews are categorised into – physical controls, administrative controls, technical and logical controls.

- ***Physical and environmental review***– According to Sayana (2002) IT auditing tests should involve the scrutiny of the physical state of security of technological and informational assets. This include source of power supply, air conditioning, heat and humidity and any other environmental factors that require consideration in relation to controls. An important check that the IS auditor is much concerned about is the access rights and permissions.

- ***System administration review*** is mainly people-based and are meant to reduce behavioural risks. Policies that are often adopted under administrative controls are in four forms – separation of duties, rotation of job, ‘need to know’ (least privilege) and mandatory vacation. The purpose of this review is to verify adequacy of controls and impact of weaknesses, to evaluate the security of the operating systems, the scrutiny of live data, database management systems and system administration procedures and compliance. Such substantive testing can be done using generalized audit software (e.g., computer assisted audit techniques - CAATs) (Sayana, 2002).

- ***Technical control reviews*** - Sayana (2002) provides and outline of reviews concerning specific control issues which cover network security and controls reviews including outsourcing policies and Internet security such as ecommerce security and e-Governance controls with its associated risk. Tests include the scrutiny of system’s external and internal connections, perimeter security, firewall and malware protection, control lists for router access, port scanning and intrusion detection methods.

- ***Logical control reviews*** – This mainly relates to end users’ physical access to computing resources including terminal controls and their logical permissions to access resources in terms of regulating and preventing users from performing transactions that are not part of

their normal duties including the creation of detailed reports within the network (Romney et al., 2006).

2.3.2. Applications Control Reviews

Application Controls Review pertain to specific computer applications or automated controls within an end user productivity software. Applications, in this sense, refer to software packages that could be used for purpose ranging from invoicing, payroll, web-based customer order processing system to enterprise resource planning systems (ERPs) that actually used to manage the running of a business (Sayana, 2002). Controls in an application review controls over the input of transactions, controls over data processing, controls over data output, storage and communication. IT audit professional's application control tests include controls that help to ensure the proper access control and authorizations, validations of transactions, error and exception handling and the completeness, accuracy of other types of data. The controls are transaction related which used to manual controls. Typical examples of input control tests include validity control which checks the format of entered data to help prevent possible invalid inputs and reasonableness checks relate to transaction control totals that can be balanced by various units to the source data to ensure all transactions have been posted completely and accurately (Romney et al., 2006).

2.3.3. Contingency Control Reviews

Contingency Control Reviews assurance procedures aimed at evaluating the counter-measures management have put in place to contain the risk that an assessed risk materialises. Businesses face a host of threat of natural and artificial disasters ranging from minor to major such as fire outbreak, flood, earthquake, robbery and failure of external arrangements that the business thrives on. Contingency control reviews examine adequacy management preparedness to face disruptions and still maintain business viability (Kinney, 2003). As a result of recent events, IT audit is fast expanding in nature and scope due to increasing government involvement in the issuance of regulations pertaining to the use of technology (D'Aquila & Houmes, 2014). Contingency Control Reviews involve Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) which include ascertaining, among other things, that management is, for example, maintaining fault tolerant hardware, using appropriate backup and storage procedures, documented and tested to see if they work to avoid unfortunate business process disruption (Sayana, 2002).

2.3.4. Compliance Reviews

Compliance Reviews constitute significant aspects of information systems control and auditing. Recent events have raised attention of governments around the world to what management responsibilities should be to avoid the occurrences economic embarrassment (Ettredge et al. 2011; Schroeder & Shepardson, 2014). Generally, compliance requirements hinge more broadly on corporate governance regulations. Compliance inspection can be major lead to accomplish current governance and internal auditors' responsibility to assess fraud risks and to detect unusual activities (COSO, 2013). The exponential growth in the volume, variety and velocity of data due to the use of Computers in business makes data management ever more complex and challenging. Good governance and best practices support adequate data protection and accurate reporting which require the coordinated interaction of the board/audit committee, management, internal auditors, and external auditors (Ettredge, et al., 2011; Schroeder & Shepardson, 2014). Internal audit has become a best practice requirement that makes sure policies and practices are up to date, enforced and documented and management's role are effectively and efficiently carried out by implementing a comprehensive system of checks and balances that are essential for an effective governance process.

As a result of increased use of technology and the unfortunate recent events, compliance reviews have become critical to assurance providers. As a result, enterprises are faced with several laws, regulations, best practices including contractual agreements and complex service level agreements (SLAs) (Forte & Power, 2005). IT auditing has become integral to ascertaining that client's compliance processes are correct and objectives are being met, i.e., externally imposed business criteria, laws, regulations and contractual obligations to which the business process is subject. Highly regulated environments have almost all IT security standards included requirements to monitor and control system and data access. Notable regulatory requirements in highly regulated environments include - The Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), officially entitled 'The Financial Modernization Act', the 'Sarbanes Oxley Act (SOX) 2002', all in the United States, the Data Protection Act (DPA, 1998) in the United Kingdom (Ettredge et al., 2011) and Article 17 of the European Union's General Data Protection Regulation (GDPR).

Besides the legal regulations other compliance requirements are rather industry-specific. For example, the 'Payment Card Industry Data Security Standard' (PCI DSS) requires the safety and security of Trust Corporation by imposing compliance requirements on most merchants to bring in an external Qualified Security Assessor for a compliance audit. Financial institutions require that any company that stores, processes, or transmits credit card information comply with the PCI DSS because Point-of-Sale (POS) businesses are paranoid, with good reason, about the protection of sensitive customer and company information. Merchants who process credit card transactions are, therefore, responsible for complying with the PCI DSS. IT auditors must have keen understanding and sound interpretation of all compliance rulings/regulations and associated standards/frameworks/methodologies used for auditing and risk assurance (TechTarget.com, 2015). Although IT audit is not Internal Audit, the responsibilities of IT auditing subsumes internal audit. IT audit can, therefore, be either internal or external audit engagement (Kramer, 2003). With the recent technological developments in the business horizon, the IT environment mandates new dimensions that should ensure proper management of change and efficient operations on both existing and new IT assets together with the requirements of flexibility, scalability and elasticity (Brazel & Agoglia, 2007).

2.3.5. Audit Trail and Evidence Collection Processes in IT Auditing

Rapid advancement and widespread use of various forms of Information Technology in business happening globally such as network technology - particularly Internet of Things (IoT), organizational intranets, electronic 'big data' processing, the emergence of the ERP, e-commerce, cloud computing and mobile technologies with its emergent evolution of Bring Your Own Everything (BYOX), have made the management environments of businesses tremendously complex (Brazel & Agoglia, 2007; Froese, 2010). Modern computer systems, network devices and other technological hardware used in enterprise business possesses have the capability to be configured to log various activities on the system for auditing. IT auditing has been seen to be the practice of watching and recording with log files. This constitutes a very important audit trail – a technical system used to detect unauthorized access, to facilitating the reconstruction of events, to promoting personal accountability and to audit a system's general environmental integrity.

Recent developments in software technology has made it possible for some previously time-consuming IT auditing tasks that have been conducted manually for decades to be

automated. In a fraction of the time, Computer-Assisted Audit Techniques (CAATs) can use of audit software to perform huge volumes of analytics and scrutiny of transactions data in which there is audit interest with sharp identification of exceptional or suspicious transactions. It can maintain logs of the tests done for review by peers and seniors. Its advanced features permit the performance of routines and the programming of certain macros that can further enhance audit speeds and efficiency (Sayana & CISA, 2003). This liberates the IT auditor to focus on matters that concern stakeholders such as those charged with governance and management demand, audit quality enhancement and consultancy for business efficacy.

The trend shows there is no turning back to traditional paper-based audit trail and audit evidence. Log files are one of the key tools for discovering and tracking suspicious activities. These activities on a computer system include network traffic, internet access, creating or deleting users, adding users to groups, changing file permissions, transferring files, opening the case and/or changing a hardware component, powering off, deleting system logs, a hardware component fails, breaching system security by a hacker, an inordinate amount of network bandwidth being consumed, or a user attempting to gain unauthorized access to a database and anything else a user, administrator or the system itself might do (Chou, 2015). There are several types of electronic log files on a network system which include operating system log files, internet server logs, and other device logs, third-party logs which must be enabled to archive logged data for a synchronous and asynchronous review. Auditing and Logging Policy provides guidelines for the appropriate use of auditing and logging in computer systems, networks and other devices which store or transport critical and/or security sensitive data (Beland et al., 2014; Sayana, 2002). Related to compliance and governance is access control to the business informational assets and the organisation's Auditing and Logging Policy. Compliance failures are important to IT auditors because an IT auditor considers compliance failure as the symptom or a signal to identify bigger problems related to some risk factor and/or control, such as a defective system or business process that can or does adversely affect the entity. In view of the above, one of the main challenges of traditional auditing in less regulatory and less developed economies is the increasing use of complex computerization in businesses.

Traditional audit problems have not changed much over recent years in less regulatory environments. Audit continues to be people-based and rely heavily on paper-based audit

evidence. Auditors have persistently demonstrated a failure to be a match to the level of complexity and hence often provide superficial reports because they are not adequately equipped with guidance to obtain sufficient appropriate evidence that supports in-depth evaluation or investigations (Tan, 2015; Abugu 2014; Aboa, 2014; Osei-Afoakwa, 2013; Svata, 2011; The Pinnacle Association Ltd., 2007; Underwriters Laboratories Inc., 2006). Omonuk and Oni (2015) found that audit firms in developing countries are not effective in applying Computer-Aided Audit Techniques (CAATs) to audit computerized accounting information systems auditing. The relationship between CAATs use in the empirical situation and their criteria for audit quality was identified to be insignificant and they concluded that local audit firms do not produce quality audit reports. Ebimobowei et al. (2011) empirically found that internal auditors in the public sector in Nigeria have failed to perform their audit responsibility with the relevant level of professional and technical expertise expected by the society.

2.4. Trend and Shortcoming in IT Auditing

Today, systems of internal control address the reliability of financial information, the efficiency and effectiveness of operations, and compliance with laws, regulations, and policies. Those charged with governance as well as management have a responsibility for designing policies and strategies relating to information systems controls and risks minimization (Ratcliffe & Landes, 2009). Svata (2011), however, discovers that IT auditors have excessively focussed their reviews on the reliability of operational controls and failed to make their reviews relevant to those charged with governance since they don't make operational decisions.

2.5. Practical Approaches to Auditing

The quest to close audit expectations gap has led practitioners to develop or advocate for certain approaches to auditing to ensure that desired outcomes are achieved (Kogan et al., 1999; Ha, 2005; Pine, 2008; Chandler, 2014). Efficient audit planning begins with the determination of audit scope, establishment of audit objective, and definition of audit criteria (Rahman et al., 2014). Prominent among them are the continuous audit approach, forensic auditing approach, risk-based approach and systems-based approach.

2.5.1. Continuous Auditing Approach

Continuous auditing emerged and touted for many years as capable of improving audit quality and dealing with audit challenges. Rezaee et al. (2001) explains continuous auditing as a real-time assessment on accounting information. It has the tendency of producing simultaneously audit results within a short period after the occurrence of relevant events (Kogan et al., 1999) and the ability to provide frequent reports to decision makers (Rahman et al., 2014). Research has, however, shown that continuous auditing is more inclined to reactive auditing instead of proactive auditing. Kuhn and Sutton (2010) argue that continuous auditing is currently technologically feasible only in certain industry sectors and for certain limited purposes because it can only be feasibly implemented in a fully automated process where there is instant access to relevant events and their outcomes. Continuous auditing of business information has, therefore, slowly gained momentum because of technological challenges (Byrnes, 2015). The implementation of continuous auditing approach, generally, has proven to be technically and practically challenging in the empirical situation of this study (Omonuk & Oni, 2015; Ebimobowei et al., 2011).

2.5.2. Forensic Auditing Approach

Researchers in the field of audit, fraud investigation and governance in less regulatory economies recommend the development of forensic auditing to ensure optimal use of resources (Dada et al., 2013; Burnaby et al., 2015; Peter et al., 2014; Owojori et al., 2009; Kasum et al., 2005). Crumbley et al. (2009) identify forensic auditing approach as the process of identifying, recording, settling, extracting, sorting, verifying and reporting past financial information as well as supporting evidentiary activities for obtaining successful prosecution for white-collar offences or settling current or prospective legal disputes. Like continuous auditing, forensic auditing is inclined to reactive post-event auditing instead of proactive auditing. Although forensic accounting may have positive potential impact in tackling financial crimes in weak regulatory environments, the public is largely sceptical about its effectiveness due to the presence of some underlying socio-economic order (Anomah et al. 2014). For forensic auditing to produce more useful results, it must involve more predictive investigation analytics and should occupy an aspect of a broader Systems-based framework for audit and assurance (Koskivaara, 2007).

2.5.3. Risk-based Approach

This approach directs audit resources towards areas of the of management assertion such as the statement of the effectiveness of existing internal controls and, therefore, assertion like accounting information may contain misstatements resulting from either error or omission (Karagiorgos et al., 2007). Audit risk-based approach posits that auditors face different forms of risks of issuing inappropriate audit opinion when relying on management assertions and therefore auditors are required to perform procedures to authenticate the assertion (Ha, 2005). Risk is a function of current activity, the changing external environments and management decisions. Audit risks are typically categorized into:

- i. **Control Risks (CR)** – This relates to the likelihood that the entity’s internal control could not timeously prevent or detect and correct an accounting information or disclosure in management assertions such as management assertion regarding the effectiveness of internal controls, a class of transaction or an account balance is material misstated either individually or when aggregated with other misstatements.
- ii. **Detection Risks (DR)** – This is defined as the likelihood that a material misstatement exists in management assertions relating to internal controls or in an accounting information either individually or when aggregated with other misstatements which the procedures performed by the auditor could neither detect nor reduce to an acceptably low level.
- iii. **Inherent Risks (IR)** – The possibility that, before consideration of any related controls, by its nature, a class of accounting information or disclosure in management assertions could be materially misstated either individually or when aggregated with other misstatements (Karagiorgos et al., 2007).

Audit Risk (AR) is, therefore, a function of inherent risk, control risk and detection risk; thus, $AR = IR \times CR \times DR$ (Karagiorgos et al., 2007). The problem with this approach is the narrow view of risk. It deals with risks that inherently internal to the problem with little scope for environmental factors. Risk, however, exhibits itself through both internal and external environmental factors and relationships (Iyengar, 2007). In addition to this, the existing risk-based approach has proved to have a tendency for attitude of continual fault-finding with failure to pay attention to the broader picture. This model, therefore, is only good enough for financial auditing. A holistic systems audit requires a broader approach that

incorporates consideration for environmental and relationship risks (Merhout & Havelka, 2008; Ha, 2005; Bell et al., 1997).

2.5.4. Systems Based Approach

A system is an assemblage of parts organized to interact with each other to function as a single unitary whole. A complete system has a structure, behaviour and pattern, relative strength of the many connections among its parts and the degree to which change affects the interconnections at any given time (Von Bertalanffy, 1971; Bell et al., 1997). Systems approach to auditing originates from the ideas in *systems theory* (Ha, 2005). Systems theory builds on the concept of a living system which is a unified whole made up of integrated parts whose emergent properties constitute irreducible smaller sub-units which interact with environment through structural coupling. By structural coupling, interactions referred to are seen to recur, each triggering changes in the system and resulting in learning, adaptation and development (Bell et al., 1997). Applying this to business organizations, systems approach emphasizes on how parts are interrelated and coordinated to obtain a unified whole, i.e., the organization. The productivity, adaptability, survivability and sustainability of a business organization, therefore, depend on the strength of its intra and inter-organizational interconnections and its response to a variety of environmental changes.

Systems-based auditing approach, in view of the above, can be understood to be a thorough analysis of the conditions of the system that make it succeed as an organization. Ha (2005) posits that systems-based auditing approach belongs to both audit approach and the subject of audit – where systems audit approach is the application of scientific and systematic methods to problem identification and the subject of audit is the going beyond individual audit approach and findings and examining the system in question to identify remedies to identified problems. In recent years, internal auditors are being asked to perform system analytics in order to provide assurance. System-based approach to audit and assurance allows for multiple approaches to be rolled out in one assignment in pursuance to quality and value-added services (Iyengar, 2007; Ha, 2005).

The business environment has been very agile and require multi-disciplinary systems intelligence to run viable entities. The expectation of Directors and Managers of modern entities is for IT auditors to expand their services beyond the traditional scope and to provide further consultancy services to support top executives and managers in their formulation of

short and long-term policies for ensuring viability of their entities. System-based audit analytics is gaining superior significance in auditing to other popular approaches such as continuous auditing because of their limitations described above. Most people agree that for the survival and success of an entity, comprehensive risk assessment is increasingly important yet how to systematically approach risk assessment is still open to debate (Kinney Jr., 2003). In a survey of more than 450 internal audit professionals, it was identified that systems-based auditing approach is the least developed approach to auditing. Information systems to auditing and assurance, therefore, remain the approach that requires improvement to achieve its full potentialities (Jeffrey & Gambier 2016). Researchers, practitioners and existing standards on auditing and best practices have, so far, not given the system-based auditing approach the much-needed attention it deserves to unleash its great potential in the auditing space. Perhaps, it is because accountants and other professional auditing stakeholders are not familiar with complex systems language and analyses (Havelka & Merhout, 2013). Hamdani (2013) posits that many Auditing, GEIT, BPM, SAP, and Balanced Scorecard applications that have been developed on enterprise architecture approach have had experiences of ending some firms up in rather enslaving them in a never-ending expensive implementation process because for lack of a complete cybernetic approach.

2.6. Open Reference Frameworks and Best Practices on IS/IT Auditing

The development of diverse forms of frameworks, legislations and best practices in recent years have proliferated in the information systems management and auditing space. Worth of note is that there is a shift of focus from control to operational controls to a focus on Governance of Enterprise IT (GEIT) (Wescott, 2014). This is not surprising because of the adverse finding relating to IT governance, directions and strategies after several dramatic corporate recent within the first decade of the 21st century that triggered a revolution in the way business is conducted (Agrawal & Cooper, 2017; Zhang and Le Fever, 2013). Open reference frameworks and best practices have been, subsequently, classified into three types (Zhang & Le Fever, 2013). This classification is as follow:

- i. *Business oriented controls*
- ii. *IT Service Management focused controls*
- iii. *Business-IT alignment focused controls standards.*

2.6.1. Business Oriented Controls Best Practices

The most prominent of business-oriented controls best practices are the framework issued by the Committee for Sponsoring Organizations (COSO) and the Statement of Auditing Standards (SAS) frameworks (Flood, 2017).

2.6.2. The Committee for Sponsoring Organizations (COSO)

The COSO was established in 1985. The original objective was to sponsor research into the causes of fraudulent financial reporting. Currently the mission statement of the COSO is to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations (Weller, 2015). The COSO has been instrumental in the issuance of internal control best practices and enterprise risk management best practices.

- Internal Control Best Practice

The COSO released its original Internal Control – Integrated framework since 1992 and has kept being updated. In May 2013, the COSO issued an updated framework. The update had become necessary, perhaps, in respond to certain criticisms of the existing framework. More so because of increasing government oversight expectation, global market and operations, increased complexity of business environments, complex legal and regulatory demands, changes in competencies and accountabilities expectations, indispensable reliance on evolving technologies and expectations relating to preventing and detecting fraud (Murphy, 2015). The new framework, which became effective in December 15, 2014, is purported for the design, implementation and conduct of systems of internal controls and the assessment of their effectiveness. The 2013 integrated framework which retains the five concepts in its original 1992 framework as components of internal control and expands the components into seventeen principles (Martinez, 2014). Table 2 below demonstrates the updates of the five concepts and seventeen principles that are necessary for effective internal control.

Table 2 - The five concepts with its seventeen principles

No.	The five Components	Effective internal control requirements
1.	<i>Control environment</i>	1. Organization demonstrates commitment to integrity and ethical values.

		<p>2. The board demonstrates independence from executive directors and management and exercises oversight of the development and performance of internal control.</p> <p>3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives</p> <p>4. Organization demonstrates commitment to attract, develop, and retain competent workforce.</p> <p>5. Organization upholds and enforces accountability</p>
2.	Risk assessment	<p>6. The organization specifies suitable objectives with sufficient clarity to enable the identification and assessment of risks.</p> <p>7. Through the evaluation of set objectives, the organization should identify and analyse risks analyses risk to determine how they should be managed.</p> <p>8. The organization internal control system assesses fraud risks that can prevent the achievement of objectives.</p> <p>9. The organization identifies and analyses significant change.</p>
3.	Control activities	<p>10. The organization selects and develops control activities.</p> <p>11. The organization selects and develops general controls over technology.</p> <p>12. The organization deploys through policies and procedures</p>
4.	Information and communication	<p>13. Organization uses relevant information necessary to support the functioning of internal control.</p> <p>14. Organization communicates internally to supports the functioning of internal control</p> <p>15. Organization communicates externally with external parties regarding matters affecting the functioning of internal control.</p>
5.	Monitoring activities	<p>16. Organization conducts ongoing and/or separates evaluations.</p> <p>17. Organization evaluates and communicates internal deficiencies timeously for corrective action.</p>

The COSO Internal Control – Integrated Framework, 2013.

A clearly noticeable element in the new internal control framework of the COSO, therefore, is the placing of emphasis on fraud risks and compliance as the new standard for assessing the effectiveness of internal controls. Fraud risk assessments are now to be treated distinct from general risk assessments during an audit to be able to fully comply with the updated

2013 COSO Framework (Ernest & Young LLP, 2014). The COSO 2013 update observes three crucial elements control effective control. These are:

- i. The requirements of the five concepts with its seventeen principles,
- ii. The exercise of professional judgment on the requirements and functioning of internal control.
- iii. The evaluation and testing of internal control to start with strategic and operational objectives and risks (Rittenberg, 2013).

- ***The Enterprise Risk Management Best Practices***

In 2004, the COSO released its Enterprise Risk Management (ERM) framework. COSO provided a depiction of the entirety of an entity’s enterprise risk management by a cube. This represented an organisation as pursuing four categories of objectives, namely; strategic, operations, reporting, and compliance. These were represented at the top of each vertical column in the cube. In addition, the ERM provided eight components by horizontal rows on the cube. The entity’s business units, component or any subset thereof are also represented by the third dimension on the cube. The ERM model has become a widely recommended framework for organizations to tackle. **Figure B** demonstrates the concepts and principles of the ERM.

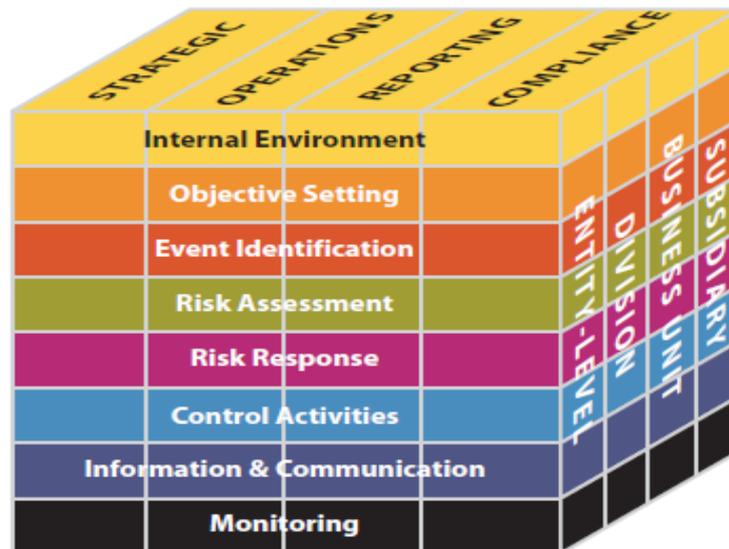


Figure B. The ERM Cube - Source: COSO (2004).

COSO's ERM 2004 considered all activities at Enterprise-level, Division or Subsidiary level and Business unit processes levels of the organization represented cube at the right of the right side. The four objectives at the top of the ERM are:

- **Strategic** – COSO (2004) clarifies this as the entity's mission sets out in broad terms what the entity aspires to achieve. 'Whatever term used, such as "mission," "vision," or "purpose," it is important that management with board oversight – explicitly establish the entity's broad-based reason for being. In it, management sets strategic objectives, formulates strategy, and establishes related operations, compliance, and reporting objectives for the organization. While an entity's mission and strategic objectives are generally stable, its strategy and many related objectives are more dynamic and adjusted for changing internal and external conditions. As they change, strategy and related objectives are realigned with strategic objectives. Strategic objectives are high-level goals, aligned and support the entity's mission/vision. Strategic objectives reflect management's choice as to how the entity will seek to create value for its stakeholders' (COSO, 2004).

- **Reporting** – relevant and reliable reporting provides management accurate and complete information appropriate for its intended purpose and should be upheld. "Accurate reporting supports management's decision making and monitoring of the entity's activities and performance. Examples of such reports include results of marketing programs, daily sales flash reports, production quality, and employee and customer satisfaction results. Reporting also relates to reports prepared for external dissemination, such as financial statements and footnote disclosures, management's discussion and analysis, and reports filed with regulatory agencies" (COSO, 2004, p. 3).

- **Operations** – operations should concern the effectiveness and efficiency of the entity's business processes, including its performance and profitability goals as well as the safeguarding of the entity's resources against loss. Operations may vary in accordance with management's choices about structure and performance. "Operations objectives need to reflect the business, industry, and economic environments in which the entity functions. A clear set of operations objectives, linked to sub-objectives, is fundamental to success. Operations objectives provide a focal point for directing allocated resources, soak competitive pressures for quality and reduce cycle times to bring products to market, or respond appropriately to changes in technology. If an entity's operations objectives are not clear or well-conceived, its resources may be misdirected" (COSO, 2004, p. 3).

- **Compliance** – an entity must conduct their activities, and often must take specific actions, in accordance with relevant laws and regulations. The internal IS auditor’s role is to conduct a comprehensive review of an organization's adherence to regulatory guidelines. As seen above, compliance requirements may relate to laws that establish minimum standards of behaviour, industry-specific rules, markets regulations which the entity integrates into its compliance objectives, pricing, taxes, the environment, employee welfare, contracts and international trade.

The “front of the cube displays the eight components or concepts that audit, and assurance professionals should verify if it is properly in place. These components or concepts are:

- *Internal Environment* – This requires the audit or assurance professional to understand the internal environment that encompasses the tone of the organization, influences on risk appetite, attitudes towards risk management and ethical values.
- *Objective Setting* – The auditor is required to obtain the objectives set by the Board that support the organization’s mission and check their alignment and consistency with the organization’s risk appetite.
- *Event Identification* –The auditor evaluates how the organization identifies internal and external events that affect the achievement of its objectives.
- *Risk Assessment* – This involves the assessment of the likelihood and impact of risks identified, as a basis for determining how to manage them.
- *Risk Response* – Management selection of appropriate actions to align risks with risk tolerance and risk appetite.
- *Control Activities* – Policies and procedures that should operate to ensure that risk responses are effective.
- *Information and Communication* – Information systems that should ensure that data is identified, captured and communicated in a format and time-frame that enables managers and staff to carry out their responsibilities.
- *Monitoring* – How management system is kept track of and modified if necessary” (Weller, 2015, p. 6).

COSO’s enterprise risk management (ERM) model has also attracted some criticisms despite its wide approval. The critics posit that there are missing quintessential elements or aspects about this framework which include questions regarding whether the COSO framework is a

complete framework to achieve a sufficient system of control have been raised. One of “the elements of criticisms of ERM model is that the risk management starts from the wrong place - the internal instead of external” (Weller, 2015 p. 8). Other critical views dilate on the above by averring that the ERM encourages over-simplified approach to risk assessment and views the materialization of risk as a single outcome. This is so because, “the ERM tends to excessively focus on internal risk factors and sudden events with major consequences. The ERM, therefore, insufficiently emphasizes on a range of possible outcomes and slow changes that can give rise to significant risks. Also, it reflects insufficiently the impact of the competitive environment, regulation and external stakeholders’ risk appetite, management and culture” (Weller, 2015, p. 6; Swinkels, 2012).

- *Enterprise Risk Management—Integrating with Strategy and Performance*

In June 2017, the COSO released an updated enterprise risk (ERM) framework which is to replace the 2004 ERM known as Enterprise Risk Management—Integrating with Strategy and Performance. COSO’s main concern for updating the ERM best practices is that it acknowledges that the increasing volatility, complexity and ambiguity of the world has significantly changed the risk landscape. The 2004 ERM is, therefore, no longer sufficient and unadaptable to the changing risk environments admitting that there is still the problems of reliability, relevancy, and trust. The new COSO ERM is represented in Figure C below:



Figure C. Enterprise Risk Management (COSO, 2017).

In the new ERM, it is acknowledged that value is destroyed where there is an embedded possibility of strategy not aligning with the entity’s mission, vision and core values. It calls

for strategy development to be a more structured decision-making that analyses risk and aligns resources with the mission and vision of the organization (COSO, 2017). The new ERM framework provides five (5) principles namely:

- ***Governance and Culture*** – Governance task is to set the organization’s tone for its culture which pertains to ethical values, desired behaviour’s and understanding of risk in the entity. Governance is to establish and reinforce the importance of oversight responsibilities enterprise risk management.
- ***Strategy and Objective Setting*** – Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A ***risk appetite*** is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
- ***Performance*** – Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
- ***Review and Revision*** – By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and considering substantial changes, and what revisions are needed.
- ***Information, Communication and Reporting*** – Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization (COSO, 2017).

2.6.2.1.Criticisms of the COSO’s Internal Control frameworks

The COSO’s updated frameworks, be it a framework for fraud risk assessment or internal controls, now provides a springboard for internal and IS audit to take strategic leadership whether in IT or in related risks, security, training, independent assessments, or consulting activities to help ensure organizations receive optimal value from the framework. This is because research has revealed that organizations with better internal controls perform better, reduce uncertainty about earnings, and enjoy higher stock prices. It is, however, an implicit theme that runs throughout the revised framework that organizations need quality internal and IS audit leadership to leverage COSO 2013’s significant advantages. Internal information systems audit participation is expected to key to successful application of COSO

2013 (Rittenberg, 2013). Yet, a systematic approach to help all areas across the enterprise, realize its many benefits although the most appropriate systematic implementation guidance for risk assessment in audit is still a challenge and has persistently been a subject of debate (Havelka & Merhout, 2013; Iyengar, 2007; Ha, 2005; Kinney, 2003). Moreover, problems expressed by critics of the COSO framework include its high-level generalisation of business problems for all organisations and the paucity in guidance (Balakrishnan et al., 2017). Therefore, the question remains as to whether the COSO's 2013 updated framework which came into force in May 2014 is a complete internal (IS) audit framework or fraud risk assessment guideline (Murphy, 2015; Martinez, 2014). COSO's response to this has been the issuance in September 2016 of Fraud Risk Assessment Guidelines. This guideline, like the previous, applied the five components and seventeen principles as discussed above focusing them on fraud risks.

2.6.3. IT Service Management Best Practices

IT service management best practices comprise the IT Infrastructure Library (ITIL) and ISO/IEC17799: 2005 including related standards in the ISO family of standards.

2.6.3.1. The IT Infrastructure Library (ITIL)

The IT Infrastructure Library (ITIL) is a public framework that describes best practice in IT service management supported by British Standards Institution's standard for IT services management (BS 15000) (Ali, 2014). It provides a framework for the governance of IT, and the management and control of IT services based on the recommendations from experienced IT professionals and academic researchers who are constantly thriving to improve and standardize IT service processes and management. Service management is defined by Cartlidge et al. (2012) as a set of specialized organizational capabilities for providing value to customers in the form of services.

On behalf of the Central Communications and Telecommunications Agency (CCTA), ITIL was founded and published in the UK between 1989 and 1995 by Her Majesty's Stationery Office (HMSO) for use principally in the UK and the Netherlands. ITIL consisted, initially of a library of 31 associated books covering all aspects of IT service provision. ITIL saw revisions between 2000 and 2004 and the initial version was replaced by ITIL V2. ITIL V2 consisted of seven more closely connected and consistent books consolidated within one overall framework. The current version, ITIL V3, consisting of five core publications was

published in 2007 and in 2011, the ITIL 2011 editions were published to address feedback, improve clarity and consistency across the five ITIL core publications with minor additions for better experience to its users (Cartlidge et al., 2012). ITIL provides guidance throughout the service lifecycle to help senior business managers and IT managers achieve the objectives of service management and address the key issues they face in a systematic way. The current ITIL guidance is structured in five lifecycle phases. Each phase is represented in one of *the core ITIL publications* as follows:

1. *“ITIL Service Strategy* – Concerns service transformation management for the achievement of strategic goals or objectives that requires the use of strategic assets.
2. *ITIL Service Design* - Contains guidance on designing IT services, IT governance practices, processes and policies, to realize the strategy and IT environment considerations to ensure quality service delivery, customer satisfaction and cost-effective service provision.
3. *Service Transition* - comprises guidance for the operationalization and management of transition to new and changed services to ensure the requirements are effectively met while controlling the risks of failure and disruption.
4. *ITIL Service Operation* – gives guidance on ensuring value for the customer and the service provider through effective and efficient support and delivery of services.
5. *ITIL Continual Service Improvement* – gives guidance on linking improvement efforts and outcomes with service strategy, service design, service transition and service operation” (Cartlidge et al., 2012, p. 13).

These standards are for demonstrating appropriate IT governance, obtaining maximum return on investment (ROI) in IT and achieving competitive advantage and several outcomes of IT services potentialities (Pollard and Cater-Steel, 2009). Adopting best practice can help a service provider to create an effective service management system. IT auditors, therefore, have derived their IT/IS audit approach by applying ITIL framework to understand how effective and efficient the strategies and if management is simply doing things that have been shown to work effectively and the objectives of IT service delivery have been in accordance with ITIL guidance. The focus of ITIL framework is on the continual measurement and improvement of the quality of IT service delivered, from both a business and a customer perspective. IT audit practitioners deploy the ITIL framework with the aim to provide a reasonable assurance that the organisation is achieving higher user and customer satisfaction

with IT services, improved service availability that is directly leading to increased business profits and revenue, financial savings from reduced rework or lost time and from improved resource management and usage, improved time to market for new products and services as well as improved decision-making and reduced risk (Cartlidge et al., 2012).

The problem with ITIL as an IT audit framework is that it is not designed with all the rigors in a complete IS audit framework. Its focus is IT service management (ITSM) and ignores information security (Ali & Soomro, 2014). ITIL framework is seen as ‘one-size-fit-all’ IT services management practices recommendation since there is no customization guidance available for IT auditing processes. This makes it very difficult for ITIL framework to be implemented as a successful IS audit framework or implemented as a full IT auditing framework. Moreover, for an ITIL project to succeed as an IT auditing framework, a deeper understanding of the business’ customers must be gained for effective implementation in order to produce valuable outcomes. This can render an audit assignment very complex, highly time-consuming and very expensive (Winter, 2012).

2.6.3.2. ISO/IEC 17799: 2005 and related standards in the ISO family of standards

Published by the British Standards Institution (BSI), ISO/IEC 17799:2005 and its related frameworks are to provide information to parties responsible for implementing information security audit within an organization. These are a best practice for developing and maintaining security standards and management practices within an organization to improve reliability of information security in inter and intra-organizational relationships (Zhang & Le Fever 2013). ISO 19011:2011 is a standard that provides guidance on auditing management systems. Auditing management includes auditing principles, practice management in an audit program and conducting management system audits with guidance on the evaluation of competence of engagement team members involved in the audit process, including the person managing the audit program, auditors and audit teams (Mail et al., 2014). ISO/IEC 27002:2013 is the updated version of ISO 27002:2005. This standard gives guidance on organizational information security standards and information security management practices including the selection, implementation and management of controls with considerations of the information security risk environments of the organization. This standard explicitly concerns information security which involves all forms of information security matters such as IT systems security or “cybersecurity”, computer data, documentation, knowledge and intellectual property. The design and intended use of this

guidance is to select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001, to implement commonly accepted information security controls and to develop their own information security management guidelines.

Ye, Lin, Deng and Zhang (2014, p. 12) outline eleven areas of concern of ISO 17799:2005, which audit professionals should be aware of as follows:

- i. “Security Policy - This concerns the assurance that guidance and support for the information security management are in place.
- ii. Organizing Information Security - to ensure that information security in the corporation is managed.
- iii. Asset Management - is to ensure that appropriateness of protection measures to manage the corporate information assets.
- iv. Human Resources Security: to determine that risk human faults, theft, deception or abuse of the information facilities are decreased.
- v. Physical and Environmental Security: to verify if unauthorized access, damage or disturbance to business information is avoided.
- vi. Communications and Operations Management: to obtain satisfaction that information management facilities are securely running.
- vii. Access Control: to manage the access to the informational resources which involves preventive access controls, detective access controls and deterrent access controls.
- viii. Information Systems Acquisition, development and maintenance: to examine the effectiveness of service contracts for ICT.
- ix. Information Security Incident Management: to validate the quality of the risk anticipation policies emergency and recovery measures.
- x. Business Continuity Management: to examine measures for the avoidance of events that can force the termination of the entire business or key business process.
- xi. Compliance: to check if breaches of laws or regulations, contracts or other security requirements are avoided”.

Information security issues have become crucial and strategic issue in organizational management due to the intensive use of information technology. However, standards and guidelines for security information such as ISO/IEC 27001, ISO/IEC 27002, and COBIT still face difficulties in their implementation due to insufficient implementation guidelines

(Sussy et al., 2015). Information security audit alone cannot represent the objectives of IT/IS auditing. It is an aspect of IT auditing and therefore these ISO standards alone cannot represent a complete IS framework for auditing.

2.6.4. Business -IT Alignment Best Practices

Business IT alignment best practices focus on Control Objectives for Information and Related Technology (COBIT). COBIT has been developed since 1996 by Information Systems Audit and Control Association (ISACA), originally for executing IT audit assignments. For the past 15 years, COBIT has gone through different phases of evolution in the hands of international IT, business, security, risk, assurance and consulting professionals whose objective has been to provide their input into what a governance and management framework must provide (Oliver & CISA, 2011). In 1996 COBIT 1 was launched and its focus was on Audit. In 1998 COBIT 2 extended from audit to control. COBIT 3 provided management touch to IT Controls in 2000. COBIT continued building on its success and extended its boundary to touch on key IT governance areas of value delivery and risk management. Between 2005 and 2009 the concentration of the objectives of COBIT 4 and COBIT 4.1 was on business risks, governance and IT value. ISACA developed two additional IT governance frameworks, Val IT™ and Risk IT. The understanding and intelligent deployment of the processes defined by Val IT and Risk IT is expected to significantly help enterprises improve their governance of IT, increase the return on their investments, and efficiently manage IT-related risks. Launched in 2012, COBIT 5 is the latest version of the COBIT generation by ISACA. COBIT 5, combines its earlier models with guidance and resources offered by reputedly known best practice frameworks such as Information Technology Infrastructure Library (ITIL), COSO and related standards from the International Organization for Standardization (ISO) (Oliver & CISA, 2011). COBIT 5, now improved to COBIT 2019, therefore, provides a leading example of reputable ‘best-practice frameworks’ leading in the implementation of holistic enterprise governance of information and technology (EGIT) in organizations.

COBIT 2019 provides six **Principles**, which improves on the five principles in COBIT 5, that enable information and related technology to be governed and managed in a holistic manner for the whole enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders. COBIT 2019 brings together its six key principles that allow enterprises to build an effective

governance and management framework (De Haes & Van Grembergen, 2018) as follows in *figure D*:

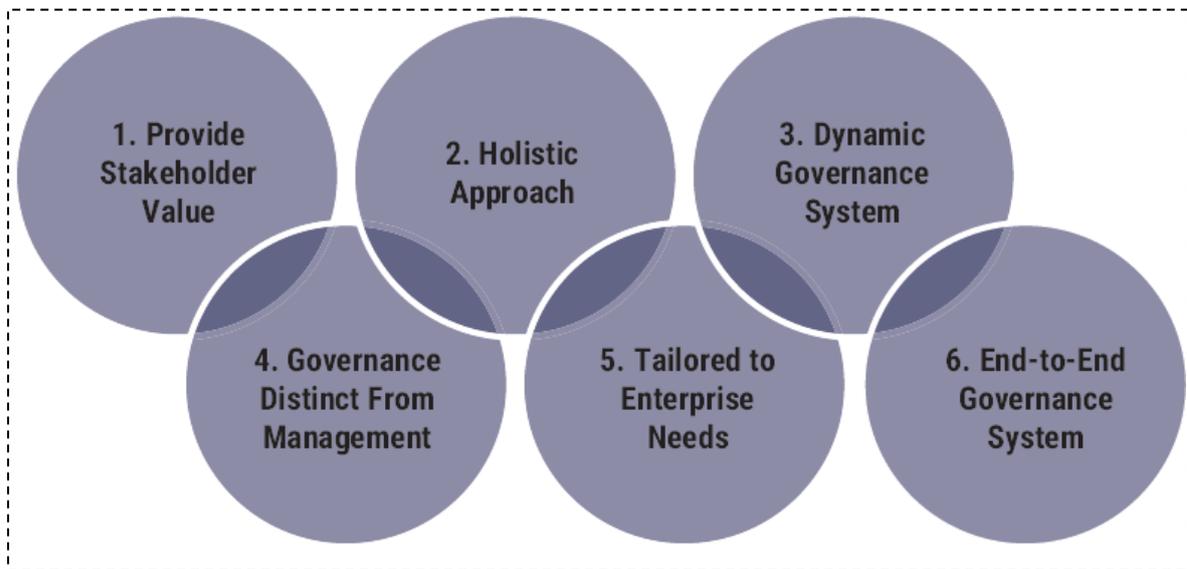


Figure D. The Six Principles of COBIT 2019. Source: ISACA 2019.

The five Principles of COBIT 5 are explained below:

1. Provide Stakeholder needs - As a framework for governance of Enterprise IT, COBIT 2019 meets stakeholder needs by increasing stakeholders' value through the maintenance of balance between the realization of benefits and the optimization of risk in the use of resources. Delivering value requires good governance and management of ICT and information assets of the organization. With its renewed focus on EGIT, COBIT 2019 directs attention on the functions of Executives and Boards and their strategies on IT integration as well as the assurance of greater value in current and future IT investments.

2. Holistic Approach - A governance system for enterprise I&T is built from a number of components that can be of different types and that work together in a holistic way.

3. Dynamic Governance - Each time one or more of the design factors such as strategy or technology are changed, the impact of these changes on the EGIT system must be considered. A dynamic view of EGIT will lead toward a viable and future-proof EGIT system.

4. Governance Distinct from Management - governance is concerned with ensuring that corporate objectives are achieved by evaluating the needs of stakeholders, conditions and options. Governance sets directions through decisions prioritization and monitoring

compliance and performance against the set objectives. Management plans, builds, runs and monitors (PBRM) activities in alignment with goals and directions are set by governance. Governance functions must be distinct and separate from Management functions.

5. Tailored to Enterprise Needs - Depending on the kind of organization and context of operation, COBIT is customizable to serve stakeholder interest by providing a comprehensive framework for achieving the goals of the organization through the translation of strategic goals into specific IT-related objectives and mapping them to specific activities or processes.

6. End-to-End Governance Systems - COBIT 2019 enables information and related technology to be governed and managed in a holistic enterprise-wide manner, taking in the full end-to-end business support activities and functional areas of responsibility and considering the IT-related interests of internal and external stakeholders (ISACA, 2019).

2.6.5. The COBIT Enabling Processes

The enabling processes of COBIT 2019 have been split into two objectives - Governance and Management objectives. The two areas are further split into five (5) domains which in turn comprise a currently total of forty (40) processes. Governance objectives are grouped in the **Evaluate, Direct and Monitor** (EDM) domain in which the governing body evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy. The *Domain - Evaluate, Direct and Monitor (EDM)* of Governance has 5 processes as follows.

- EDM01 Ensured Governance Framework Setting and Maintenance
- EDM02 Ensured Benefits Delivery
- EDM03 Ensured Risk Optimization
- EDM04 Ensured Resource Optimization
- EDM05 Ensured Stakeholder Transparency

Management objectives are grouped in four domains:

Align, Plan and Organize (APO) addresses the overall organization, strategy and supporting activities for information and Technology (I&T). The *Align, Plan and Organize (APO)* has 14 processes as follows:

- APO01 Managed IT and control framework
- APO02 Managed Strategy
- APO03 Managed Enterprise Architecture
- APO04 Managed Innovation
- APO05 Managed Portfolio
- APO06 Managed Budget and Costs
- APO07 Managed Human Relations
- APO08 Managed Relationships
- APO09 Managed Service Agreements
- APO10 Managed Suppliers
- APO11 Managed Quality
- APO12 Managed Risk
- APO13 Managed Security
- APO14 Managed Data

Build, Acquire and Implement (BAI) treats the definition, acquisition and implementation of I&T solutions and their integration in business processes.

The *Build, Acquire and Implement (BAI)* has 11 processes as follows.

- BAI01 Managed Programs and Projects
- BAI02 Managed Requirements Definition
- BAI03 Managed Solutions Identification and Build
- BAI04 Managed Availability and Capacity
- BAI05 Managed organisationnel change enablement
- BAI06 Managed Changes
- BAI07 Managed Changes Acceptance and Transitioning
- BAI08 Managed Knowledge
- BAI09 Managed Assets
- BAI10 Managed Configuration.
- BAI11 Managed Projects

Deliver, Service and Support (DSS) addresses the operational delivery and support of I&T services, including security. This *Deliver, Service and Support* (DSS) has 6 processes as follows.

- DSS01 Managed Operations
- DSS02 Managed Service Requests and Incidents
- DSS03 Managed Problems
- DSS04 Managed Continuity
- DSS05 Managed Security Services
- DSS06 Managed Business Process Controls

Monitor, Evaluate and Assess (MEA) addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements. The *Monitor, Evaluate and Assess* (MEA) domain has 4 processes.

- MEA01 Managed Performance and Conformance Monitoring
- MEA02 Managed System of Internal Control
- MEA03 Managed Compliance with External Requirements.
- MEA04 Managed Assurance.

Besides the six principles above, COBIT 2019 updates the previous COBIT 5 process enablers and replaces them with seven generic Components of Governance System. The Governance System introduced in COBIT 2019 brings on board design factors and methodology which are factors that influence the design of an enterprise's governance system and position it for success in the use of I&T. This culminates in the design of enterprise strategy which is provided by techniques such as the Balanced Scorecard by Norton and Kaplan. The components are explained to be useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector in terms of helping enterprises optimize information and technology use and investment for the benefit of stakeholders (De Haes & Van Grembergen, 2018; ISACA, 2013). The components of a governance system includes all the seven process enablers of COBIT 5 as follows - organizational structures; policies and procedures; information items; culture and behaviour; skills and competencies; and services, infrastructure and applications. Figure E demonstrates the components of governance system provided by COBIT 2019.



Figure E. *The seven Governance System of COBIT 2019.* Source: ISACA (2019)

Although the current objective of COBIT is on governance of enterprise IT and no longer focused on audit. The COBIT 2019 framework builds in the it a flavour of IT project Management and has an inbuilt element that offer customizable platform for the design of a model to carry out IS/IT audit and assurance assignments (ISACA 2019; Zhang & Le Fever, 2013; Oliver & CISA, 2011). The Monitor, Evaluate and Assess (MEA) domain is concerned with the assessment of the needs of the company and whether the current IT system meets the objectives for which it was set up. It is an independent assessment of the effectiveness of IT system and it monitors the controls relevant and necessary to comply with regulatory requirements. Evaluation covers the company’s control processes by internal and external auditors.

2.6.6. The COBIT Assurance and Assessment Model

COBIT identifies the following relationship for IS/IT assurance initiatives and assignments. A stakeholder who is usually the end customer of the evaluation or assurance report and can approve the criteria for the assessment. The stakeholder uses the outcomes of the assurance report of the subject matter for decision making but has delegated operation and custodianship of the subject matter to a responsible party. There is also the responsible party who is the person in charge of the subject matter of the assignment whose responsibilities

are being assessed by the assurance professional. Finally, the assurance professional who uses his professional skills, judgement and some criteria for the assessment and provides an opinion as to whether the subject matter meets the needs of the stakeholder (Svata, 2011). An efficient assessment function will sustain an effective assurance function. Figure F below demonstrates the assurance process and the interested party relationship according COBIT 5:

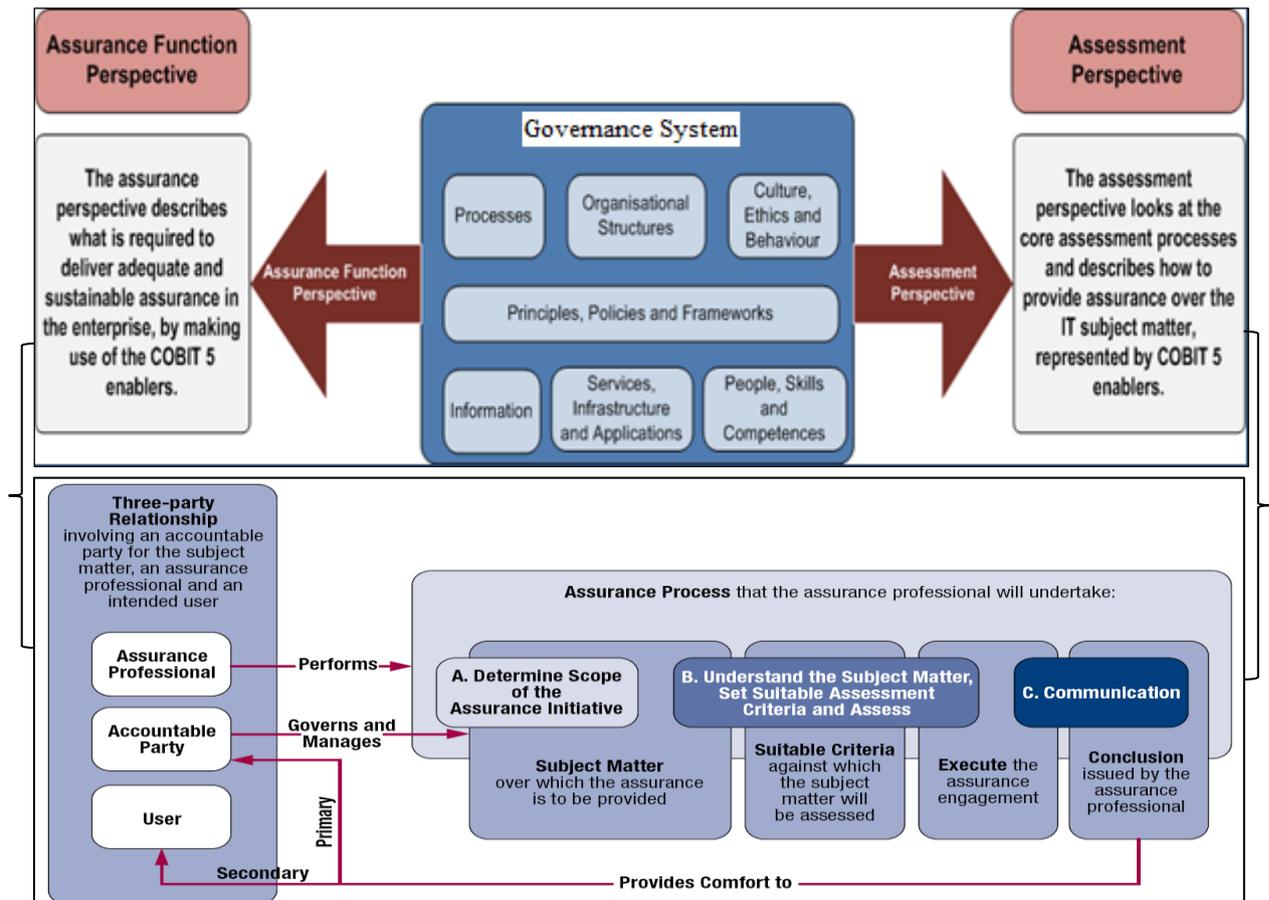


Figure F – COBIT Assessment and Assurance Processes

- i. **Principles, policies and frameworks** – These are the vehicle to translate the desired behavior into practical guidance for day-to-day management. Policies are very relevant to provide leadership and sense of direction as well as corporate culture.
- ii. **Processes** – This describes an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT related goals.
- iii. **Organizational structures** – These are the key decision-making entities in an organization. Understanding the organizational structure assists assurance experts to

appreciate the chain of command in the organization. For efficient audit and assurance service output, the role of Communication with the right persons is very critical. This enables assurance experts to interview the right persons and to communicate relevant reports to the appropriate persons to ensure confidentiality and objectivity. This is to ensure the effectiveness of audit output.

- iv. **Culture, ethics and behavior** – Conduct of individuals and of the organization; very often underestimated as a success factor in governance and management activities. Changes in culture or general behavior can pose a major risk to the survival of an organization over time and the need to monitor changes in culture, ethics and behavior is key to the auditor from the COBIT perspective.
- v. **Information** – This is said to be pervasive throughout any organization dealing with all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself. More objective information also provides comfort to all stakeholders primarily to the accountable party and recognizes the secondary users.
- vi. **Services, infrastructure and applications** – This includes the infrastructure, technology and applications that provide the enterprise with information technology processing and services. The ICT infrastructure, applications, accounting standards and other digital Web services and compliance are included in the investigations to identify IT risks. Here, tests of control involved include general controls, third party solution providers, technical and applications controls.
- vii. **People, skills and competencies** – These concern soft skills or people-related management issues and are required for successful completion of all activities and for making correct decisions and taking corrective actions (ISACA, 2012; Al Omari, Barnes & Pitman, 2012).

2.6.6.1. Capability Measurement

COBIT 2019 updates the COBIT 5 Process Assessment Model (PAM) with the flexibility to use maturity measurements as well as capability measurements. A CMMI-based process capability measurement scheme is introduced. The process within each governance and management objective can operate at various capability levels, ranging from 0 to 5. The

capability level is a measure of how well a process is implemented and performing. The process capability is purported to aid the implementation of COBIT 2019 by enabling an evidence-based, reliable, consistent and repeatable way to analyse IT process capabilities which also enables IS auditors, business executives and boards to analyse and gain insight into change requirements and process improvement initiatives through the deployment of the components of the governance system provided by COBIT 2019 (ISACA, 2019; Varkoi et al., 2016). ISACA maintains the use of the process attributes ratings introduced by International Organization for Standardisation and the International Electrotechnical Commission (ISO/IEC) 15504-3 (now replaced by ISO/IEC TS 33030:2017) to rank business IT processes maturity into six (6) distinct levels and described the scores, referred to as the NPLF scores, for same as follows in **table 3** below:

Score/IT Objective	Range	Maturity Level	Level Rating
<i>N - Not achieved/incomplete</i>	0 – 15% -	Level - 0	<i>Incomplete Process</i>
		Level - 1	<i>Performed Process</i>
<i>P - Partially achieved</i>	15 – 50% -	Level - 2	<i>Managed Process</i>
		Level - 3	<i>Established Process</i>
<i>L - Largely achieved</i>	50 – 85% -	Level - 4	<i>Predictable Process</i>
<i>F - Fully achieved</i>	85 – 100%	Level - 5	<i>Optimized Process</i>

Table 3. *The NPLF Score, Maturity Level and Rating*

The challenge is that ISACA did not provide with the process capability assessment an object metrics for process capability determination. They made referred to process attributes ratings and stressed the importance of recording and maintaining references to evidence of independent expectation to support the assessors' judgement of the attribute of client's IT processes when deploying the Capability Rating Model. This is because, in the view of ISACA process capability as abstract. Hence, they recommend to assessors to use their subjective professional judgement, experience and IT skills, otherwise, use the enterprise's performance in place of Capability (Aliquo & Fu, 2014). Such method for determining an enterprise's capability or performance, however, are not without serious inherent shortcomings leading to high failure exposure in assessments (Percheiro et al., 2017; Linich & Puleo, 2016; Bartens et al., 2015).

In a design of metrics to objectively derive an enterprise’s capability or performance is explored. COBIT 2019 provides four stages of governance design workflow and further provides a number of coded steps to achieve governance objectives. Table 4 below provides details.

Governance System Design Workflow	
1. Understand the enterprise context and strategy.	1.1. Understand enterprise strategy. 1.2. Understand enterprise goals. 1.3. Understand the risk profile. 1.4. Understand current I&T-related issues.
2. Determine the initial scope of the governance system.	2.1. Consider enterprise strategy. 2.2. Consider enterprise goals and apply the COBIT goals cascade. 2.3. Consider the risk profile of the enterprise. 2.4. Consider current I&T-related issues.
3. Refine the scope of the Governance system.	3.1. Consider the threat landscape. 3.2. Consider compliance requirements. 3.3. Consider the role of IT. 3.4. Consider the sourcing model. 3.5. Consider IT implementation methods. 3.6. Consider the IT adoption strategy. 3.7. Consider enterprise size.
4. Conclude the governance system design.	4.1. Resolve inherent priority conflicts. 4.2. Conclude the governance system design

Table 4. Governance Design Workflow.

One of the first steps in ensuring an effective planning process is to create your *IT audit universe* yet it is one audit planning process area where practitioners lack guidance (Balakrishnan et al., 2017). IT audit universe involves the issues and potential procedures the Auditor might perform to obtain audit evidence as it offers the auditor the opportunity for a more effective and robust understanding of the entity, its ICT support processes, its IT strategy, its business model and its legal and regulatory environments to achieve most effective audit outcomes (De Haes & Van Grembergen, 2015). ISACA (2014) stresses the importance of recording and maintaining references to evidence that supports the assessors’ IT skills, audit experience and judgement of process attribute ratings in auditing. There is no objective method yet for performing analytical procedures to obtain evidence that could lead to objective process attribute ratings that would assist the assessor to create IT audit universe that determines desired substantive review procedures for the client. This study explores the possibility of improving the usefulness of the Performance Measurements System provided

by the ingrained theory (VSM) (elucidated in the next chapter) drawing on the strengths of the governance system design workflow, CMMI-based process capability scheme of COBIT 2019 together with maturity standards by ISO/IEC 15504-3.

2.6.6.2. Criticisms of COBIT

COBIT framework has been criticised for being cumbersome in structure with unclear theoretical foundations and, therefore, does not translate effectively in less regulatory environments (Ndlovu & Kyobe, 2016; Kahorongo et al., 2015; Zhang & Le, 2013). Recent studies have revealed that the 40 IT governance processes which is an update of the 37 processes provided by COBIT 5 is often perceived as complex and presented in a less-structured manner without clearly defined organizational structure (Bartens et al., 2015; Zhang & Le, 2013). Perhaps one of the greatest worries of COBIT is its complete change of focus and paradigm in relation to auditing. Like COSO's updated integrated framework, COBIT focuses on governance and management of enterprise IT (GEIT). COBIT no longer emphasizes on auditing and auditor's responsibilities. The designers of the framework recommend auditing and assurance professionals to use their professional discretion and experience to customize and extract their own approach to the planning and performance of audit and assurance assignments (Wescott, 2014). Without customization guidance, however, assurance professionals find the application of COBIT framework as a framework for auditing problematic (DeFond & Zhang, 2014; Devos & Van de Ginste, 2015).

2.7. IT audit expectations and gaps

The literature review has demonstrated the existence of extensive gaps in the expectation persisting between what practitioners are doing and what users of audit outcomes expect in several aspects of audit. Audit expectation gap has various definitions among researchers (Ruhnke & Schmidt, 2014; Koh & Woo, 1998). Liggio was the first to apply the phrase "*expectation gap*" to auditing in 1974 (Ruhnke & Schmidt, 2014). He defined the expectation gap as the difference between the levels of expected performance as scoped by an independent auditor and that imagined by the user of the accounting information audited (Hassink, 2009). Problems of IT audit have, often, been discussed by investigating the concept of expectations and the gaps as critical issues in auditing because of the damage it continues to bring to the essence of the auditing profession especially in less regulatory environments (Omonuk & Oni, 2015; Ebimobowei et al., 2011). Audit expectation gap

phenomenon, therefore, has become a driver of change in recent years because of its impact on the future of the audit profession (Ruhnke & Schmidt, 2014).

Since it got defined, audit expectation gap has been categorised in various concepts of gaps; namely *Reasonableness gap*, *Performance gap* and *Liability gap* (Koh & Woo, 1998). Grönlund et al. (2011) espouse the need for IT auditing framework to address the above gaps from perspective of ‘Three-E’s’ value-drivers namely *Economy*, *Efficiency* and *Effectiveness* respectively.

- ***Reasonableness gap (Economy gap)*** – This concept denotes the difference in viewpoints between what society expects auditors to achieve with the money and time devoted to auditing and what the auditors can reasonably accomplish. The capacity of an auditing approach to reduce time and cost because of its ability to allow repetitive auditing tasks that have been conducted manually for decades, such as counting inventories or processing confirmation responses to be automated. This is expected to afford auditors ample time to focus on quality enhancement activities through advanced analytics evaluation. They can spend more time exercising their professional judgment to gain deeper insights and based on that provide additional value-adding consultancy services without having to charge fees (Merhout & Havelka, 2008). Generally, however, there is lack of an IS audit framework that provide guidance for what is expected to assist stakeholders to assess audit by comparing with the use minimum resources required to achieve its objectives. Recent survey by the ACCA and Grant Thornton International Ltd (GTIL) (2016) reveals that countries without a longstanding tradition of audit have a view that developing audit capacity is essential for enhancing economic growth. However, auditors and managers continue to lack a common understanding and the method to objectively define and evaluate the attributes of audit performance. The survey further reveals that auditors in developing and less regulatory environments do not have enough information to improve audit methodologies. Yet, the future of auditing belongs to those who can adapt, evolve their thinking, innovate and change their approach to auditing.
- ***Performance gap (Efficiency gap)*** – this is viewed as the difference in worldview between what auditors achieve and what society can reasonably expect auditors to accomplish. A well-coordinated activity of evidence collection and evaluation to

determine whether organizational resources are well organized, and ICT has been properly designed to maintain data confidentiality and integrity with appropriate assignment of authority to safeguard assets and to allow organizational goals to be achieved effectively (D'Onza et al., 2015). In countries without long standing tradition of IT auditing, however, IT auditing has persistently remained merely auditing around computers in which practitioners typically focus on hardware, software and basically functional operations (Svata, 2011). There is a definite feeling that the auditing frameworks are, generally, not delivering enough (ACCA, 2016). Audit problems in developing countries with less regulatory environments have not changed over the years due to ill-suited guidance to leverage the demand for change (Tan, 2015; KPMG, 2014; The Pinnacle Association Ltd., 2007; Underwriters Laboratories Inc., 2006). Audit objectives continue to be different from management objectives as audits continue to be fault-finding with people centred approach and relies on paper-based audit trail for audit evidence (Omonuk & Oni, 2015).

- ***Liability gap (Effectiveness gap)*** – this concept has arisen to denote the gap between stakeholders' expectations for auditors to be held liable for audit failure leading to losses to third parties and what liabilities auditors are legally prepared to take for same (DeFond & Zhang, 2014). Complex use of IT in business comes along with sophisticated fraud schemes. The concept of control responsibilities has, unfortunately, often been misunderstood between auditors and those charged with governance and management. This has increased the misconception among users of accounting information about whose responsibility it is to prevent and detect fraud (Murphy, 2015). This misconception has resulted in several litigations in many jurisdictions. Grönlund et al. (2011) argue that, for audit to be value-adding, it is expected that it will take up other non-conventional responsibilities such as timely detection of fraud. Kasum et al. (2005) posit that the demand for auditing services in the future will be much dependent upon the auditors' effectiveness in the detection, deterring or prevention of fraud and corruption timeously in third world countries where the regulatory environments are weak. Recent events show a trend where audit firms are being asked to pay huge compensation with damaging reputational publicity (Abugu, 2014). The viability of modern organizations using IT is getting more and more subtle. Stakeholders' demand for auditors to increase the degree of assurance on the integrity and credibility of

accounting information and other additional information has become phenomenal (Aboa, 2014; Harris 2002). Assurance providers, in this light, are expected to be cocreators of value with those charged with governance and management. However, because the approach to IT auditing has been too prescriptive, overly rule-based or compliance-based (Huck, 2016), audit communications tend to ignore very vital elements that drive performance which must always be evaluated by audit (Osei-Afoakwa, 2013; The Pinnacle Association Ltd., 2007).

2.8. Conclusion

The Chapter made an extensive review of literature. It reviewed the theories on the demand for auditing, explored the nature and scope of IT auditing and discussed the expectations of IT auditors and the gaps in public expectations. The chapter, further, the available open reference frameworks and best practices used for IT auditing also explored the challenges of their implementation in IT auditing in less regulatory environments. The chapter concluded by clarifying the gaps in literature in relation with the development of the desirable framework for IT auditing. The next chapter introduces the abducted ingrained systems theory for development of the conceptual framework. The materials to be used complete this chapter include the information obtained from the researcher's initial workshop with identified participants, literature reviewed in the earlier chapter as well as the researcher's own professional experience for the conceptualisation of the problem. The chapter will make a full description the concepts that were relied on and provide details of the research problem with expected interventions the ingrained can contribute in subsequent the solution design.

CHAPTER THREE

PROBLEM DIAGNOSIS AND CONCEPTUALIZATION

3.0. Introduction

The chapter introduces the ingrained theory. Gregor and Hevner (2013) identify an ingrained theory as the justificatory knowledge which requires some level of judgement of the researcher for its selection. This must be based on the knowledge obtained from the problem definition stage of a design science research for which the subsequent design provides justification. The cybernetics model of viable systems approach (VSA) has, therefore, been selected by abduction for the problem diagnosis and solution conceptualisation. The theory, as explained in chapter one, was found to be apt for this study which seeks an intervention for IT audit challenges for weak regulatory environments because of its attested capacity to aid organisational diagnostics and support self-regulation with effective outcomes without need for reliance on external regulatory authority (Barile et al., 2018; Burgess & Wake, 2012; Polese et al., 2011; Espejo, 2009; Espejo, 2003; Bell et al., 1997). The purpose of an ingrained theory is for diagnosing the problem and for conceptualising a solution design in an action design research (Sein et al. 2013).

3.1. Cybernetics

Burgess and Wake (2012) posit that modern foundations of cybernetics were established on the science of communication and control in animals and machines which can be traced to work of Wiener (1948). The foundations of cybernetics relate to the science of communication and control in animals and machines championed by Wiener (1948). Cybernetics science posits that there are underlying laws which apply to the way the nervous systems and subsystems of an animal maintain control over its actions; or the way in which a species maintains itself within its ecosystem (Hilder, 1995). Stafford Beer originated what is now known as management cybernetics (over the period 1959 - 1985) as a substantial development on the science of cybernetics and called his theory the Viable Systems Model (VSM) (Espejo & Gill, 1997). The VSM employs a multi-disciplinary approach to explore systems structures, constraints, and possibilities relevant to the appreciation of systems deviation-counteracting and feedback events to re-establish regularity (Ashby, 1956; Wiener, 1961; Maruyama, 1963).

Proponents of the science of cybernetics posit that a single system is quite surrounded by a far greater complexity than it can deal with by a simple one-to-one response (Burgess & Wake, 2012). The idea of complexity is, therefore, fundamental to cybernetics thinking. A systematic conceptual framework of auditing would, therefore, provide a means of applying to auditing the well-developed investigation methods and procedures of the sciences for addressing complex systems challenges based on observable, measurable variables derived from the living systems theory (Swanson & Marsh, 1993). A living system is any organism capable of maintaining its identity independently within a shared environment by some necessary, sufficient and interactive mechanisms to maintain survival. A living system is, therefore, an open system that interacts with its environment capable of automatically addressing its internal problems, defects, failures to overcome its 'pathogens', threats and constraints from the environment to re-establish its prior potentialities (Hitchens, 2015). A business organization, like any living system, is a super-organism whose performance and viability depend on efficient coupling and symbiotic alliances of its inter and intra-organizational interconnections as well as external forces (Burgess & Wake, 2012; Bititci et al., 1997).

Business terrains of today is increasingly interconnected. It is an understatement to say that contemporary business entities subsist on the relationship among people, technology, policies and regulations. Modern business environments are enhanced and constrained by technologies of increasing sophistication to fulfil the demands of the market to maintain their existence and identity (Jafarov & Lewis, 2014). Investors and other interested parties attempt to maximise overall satisfaction by drawing value from relationships and complex service systems carried out with the support of technologies. Management and interested parties are concerned with how to strengthen business experiences, competition and control risks in intra-firm and inter-firm relationships for the benefit of competitive advantage and long-term survival. IT spans nearly all organisational activities and because of this IT audit often crosses department boundaries (Kyobe, 2008). A systematic conceptual framework for IT auditing that applies the well-developed investigation methods and procedures of the sciences based on observable, measurable entities developed through living systems theory has a critical essence in contemporary business organisation (Swanson & Marsh, 1993).

3.2. The VSM – The Theory Ingrained Artefact

The VSM was first introduced by Stafford Beer in the 1950s as new management science for the management of dynamic and complex systems (Beer, 1972; 1979; 1981; 1985). Stafford Beer recognized that laws and the science of cybernetics could be applied in a business context to help managers to intervene in complex situations to effectively fulfil their objectives and to create a viable entity. Beer (1985) defined a viable system as an organization that can maintain a separate existence being able to control environmental changes and survive on its own within its environment. A Viable Systems Approach (VSA) is the systems theory behind the VSM. The VSA is defined as a systematic analysis that considers the basic components first before proceeding to more complex higher-level relationships that have impact (Barile et al., 2018; Polese et al., 2011). The VSA is embedded with systems diagnostic tools, concepts and attributes to identify every factor that needs to be involved in the creation of a value stream map for a system. Once the factors have been identified, the selection and implementation of best practical assessment or procedures and processes in repeatable actions should be less challenging. Below analyses the functional components and attributes of the VSM together with the VSA theory and their relevance to systems auditing.

3.3. Functional properties of the VSM

Beer (1985) posits that a viable organization is one that exhibits the functions of management in a set of specifically identified and formalized interrelationships. With the development of technology, particularly, Information Technology (ICT), Beer (1972; 1985) foresaw the traditional bureaucratic philosophy to organizational management to no longer fit as a lens to understanding the structure and process of running an organization in the future. Beer believed that emerging technology provides organizations with a ‘nervous system’ which supports their aims without the burden and drudgery of bureaucracy. Therefore, components of the organizational structure were bound to crumble but the interrelationships between the components which sustain the components would persist (Thomas, 2006). Beer (1985), therefore, based the interrelationships of an organisational structure on five main functions, each of which is a system on its own which interconnect through a series of channels of communication and information flows. These five major functions that must exist in all purposeful organizational systems are: *Operational* sub-system (represented as System one

(S1)), *Coordination* sub-system (represented as System two (S2)), *Control* sub-system (represented as sub-system three (S3)); which contains sub-system (S3*) for monitoring and audits), *Intelligence* sub-system (represented as System four (S4)) and *Policy* sub-system (represented as System five (S5)).

Figure G below is a representation of the above functions and interrelationships of the VSM.

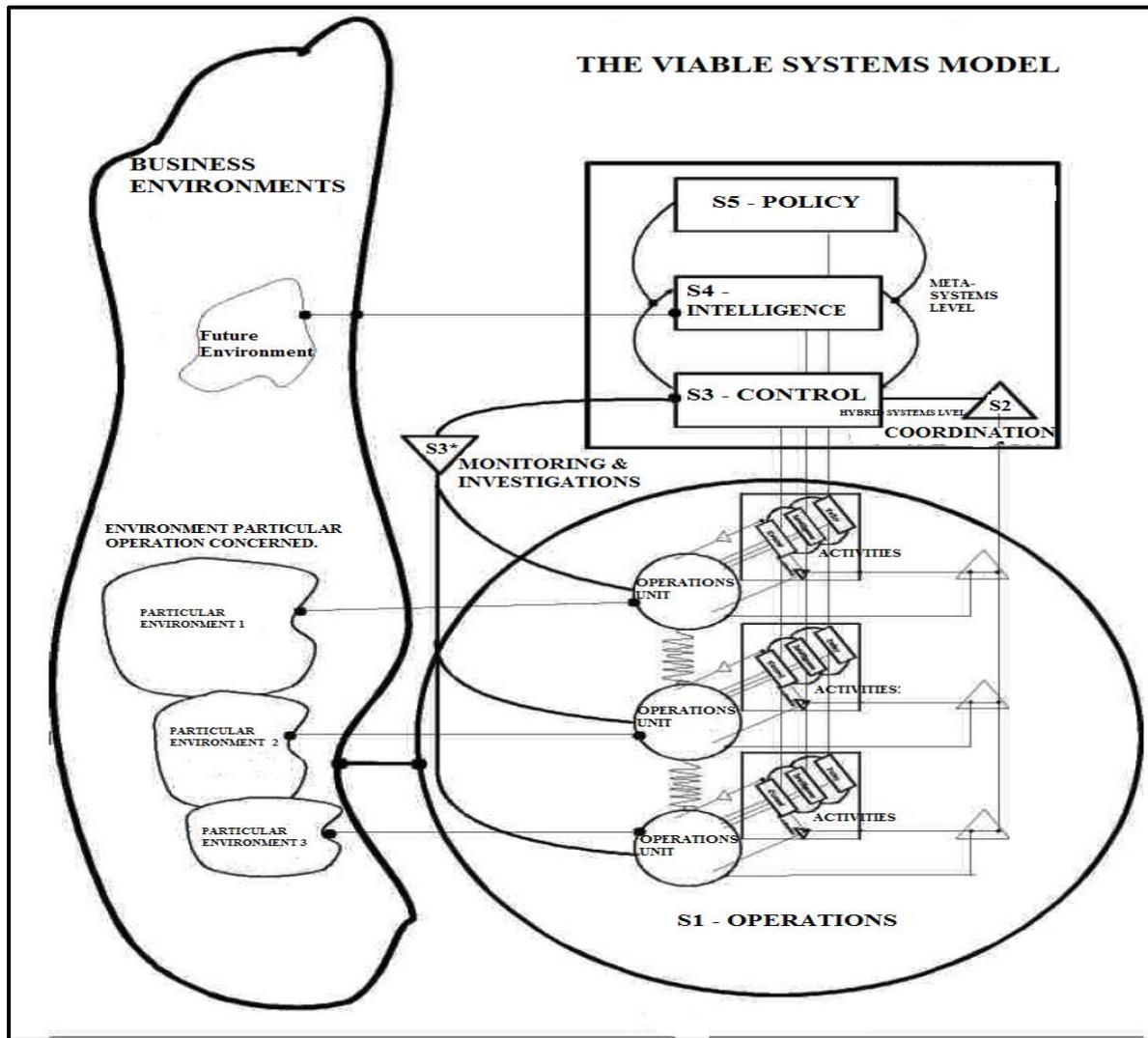


Figure G - The Viable Systems Model – (adapted from Espejo & Gill, 1997).

- **Symbols and interpretation**

Beer used symbols to establish the functions and the mechanisms upon which a viable entity is composed. Beer used the shape of an *amoeba* to symbolize the dynamic and amorphous nature of the business environment within which organizations operate. To symbolize a ‘variety amplifier’ the *triangular shape* is borrowed by Beer from electronics which uses

triangular shapes to symbolize power amplifiers. Amplifiers hone power and work for continuous electronic signals. Likewise, Beer borrowed from electronics the term ‘attenuator’ – an electronic device that reduces power or signal without necessarily distorting its waveform. A variety attenuator is symbolized in the VSM by *a twisted line* or coils. Beer used circles to demonstrate *tasks and activities* in an operation while *rectangles* symbolize *functions* in a process. Lines and arrows are used by Stafford Beer to provide the directions of communications. Straight lines link the functions and symbolize the requirement for an effective top-down communication among functions and vice versa. E.g. to stay viable, policy (S5) must be effectively communicated to each operational management, which then should have the means for translating this into more concrete action plans to be followed by the operation (Hilder, 1995). The *thick curved arrows* between Sub-Systems S3 and S4 and between S4 and S5 are intended to indicate the very rich interaction that needs to exist between these functions. Intelligence (S4) and Operations (S1) require environmental information at varying degrees to function indicated by lines linking them to their respective environments. Operation, for example, needs to have effective communication channels to its environment since a communication breakdown at any point will lead to ineffective action.

This study does not aim to supplant ordinary functions of those charged with governance and management with IT audit functions. It seeks, rather, to develop a framework to carry out IT audit along those functions to align objectives and create an opportunity for management to forge improved and stronger relationship IT auditors for the achievement of common goals (ISACA, 2013). Below elaborate the functions of the components of the VSM, the mechanisms of viability and their relevance to the proposed IS/IT auditing framework.

3.3.1. Subsystem One (Operations) – S1

The operation (S1) is defined as the basic work units or the implemented business processes for which management and IT controls (Espejo & Gill, 1997). It constitutes the core activities of a business process consisting of subtasks each performed typically at defined locations to transform inputs or data into desired goods or services and to deliver then at value to the customers (Beer, 1985 cited in Schwaninger, 2006). Operations is required to ensure organization achieves the objectives for which it exists. Operations is a system of

systems because it invariably contains a number of units of operations involving small teams (cells) of people and varying ICT infrastructure responsible for a variety of complete work or tasks. Therefore, Operations, Sub-system (S1), in the VSM is an autonomous unit which includes localized management centres with their own control environments (Espejo & Gill, 1997).

- **Problem Diagnosis**

One of the challenges of auditing in less technologically developed economies identified during the brainstorming workshop sessions and in the literature review in this research process is that IS auditor are unable to define the relevant scope for the collection of IT audit evidence to guarantee desired assurance outcomes. The scope of an audit specifies the focus, extent and boundary including the environment of a particular audit (Buchanan & Gibb, 2007). Typically, audit is exposed to failure in less regulatory environments either due to a narrow definition of the scope for IT auditing or an overly wide scope definition with elements that do not reflect the essential needs and business objectives of the auditee. These have negative effect on the time and cost of assessments because of the lack of guidance for IT audit practitioners (Ali, 2014).

The implication of the consideration of the function of Operations (S1) in IT auditing process is that it would guide the practitioner to consider all essential IT processes supporting the auditee's primary activities in its value chain considered by management as critical for the achievement of their objectives (Ray, 2009). An auditor's opinion that provides 'reasonable assurance' is based upon evidence. Audit evidence collection process for a viable audit must, first, be related to procedures conducted to understand the entity and its control environments since, in auditing, a robust understanding of the entity and its environment improves the propriety of the auditor's application professional judgment (Bell et al., 1997). A systematic audit of the operations conceived on observable and measurable units of business IT processes of an organisation developed through living systems theory will provide an approach to performing an IS audit that captures relevant audit evidence from sufficient appropriate audit scope for desired IT audit outcomes (Ray, 2009; Bell et al., 1997).

3.3.2. Subsystem Two (Coordination) – S2

Beer (1981) defined coordination function as an anti-oscillatory function borrowing the term, as usual, from electronics glossary. An anti-oscillator in an electronic device is

responsible for regulating a back and forth motion over a central neutral point, usually created by changes in energy. Since IT has taken the centre stage of all the support activities across a contemporary business organization, the role of the IT auditor is to evaluate how IT strategy is improving the core business processes to regulate and serve all relevant interests to reach their goals (Ray, 2009). Regulation of interests does not imply that individuals and stakeholders will have the same interests and purposes but, rather, for results that align the interests however different they are to yield increased efficiency, augmentation of the organization's capabilities, enablement of new processes scanning and detection capacities (Espejo, 2003).

- **Problem Diagnosis**

In every viable organization, there are tangible and intangible independent enablers that support the successful operations and organization of the core business processes which include Information and Communication Technology (ICT), coordinated teams of human resource, procurement and IT firm infrastructure management, information, knowledge, organizational learning, internal and external business relationships, culture and ethics (Shahid, 2014). If, for example, ICT processes and ICT services are implemented, managed and supported in the appropriate way, all aspects of the business will suffer less disruption with legal consequences, productive hours will improve, costs will reduce, revenue will increase, staff motivation will augment, public relations will improve, and the business will be more successful in achieving its objectives (Omonuk & Oni, 2015; Rahman et al., 2014). Co-ordination is viewed as the function responsible for supporting standards of behaviour and knowledge bases for the optimum deployment of those activities and resources across the organisation and for dealing with conflicts to prevent the system from disintegrating (Beer, 1985). COBIT 5/2019 provides seven components of governance system which De Haes and Van Grembergen (2015) posits they represent the 'IT Universe'. These are: 1. **Principles, Policies and Frameworks**, 2. **Process**, 3. **Organisational Structure** 4. **Culture, Ethics and Behaviours**, 5. **Information**, 6. **Service, Infrastructure and Applications**, 7. **People, Skills and Competence**.

Brainstorms with participants together with extant literature confirm that a problem of auditing in countries without longstanding tradition of auditing is that the traditional auditing framework is not delivering enough. A cause of audit and assurance failure is that the

framework used for auditing fails to examine and report on what contributes to value creation in an organizational value chain (ACCA, 2016; Ray, 2009). Practitioners persistently focus merely on paper-based, people-centred reviews and IT audit is almost completely focussed on information security reviews, hardware and application control reviews and woefully ignore organizational ethics, cultural values, structure, reporting lines, authority, rules, human resource policies and practices, competence of personnel and the documentation reviews which are vital intangibles for coordinating and synergising elements that drive business value (Omonuk & Oni, 2015; Svata, 2011; Brazel & Agoglia, 2007).

The implication of considering coordination as an essential IS audit function is that it will provide the IS audit practitioner the guidance to assess the alignment of operational strategy of an organisation to its technology requirements and investigate the skills and experience needed to increase the cohesion and coordination of elements that are vital to business viability which are overlooked in auditing in less regulatory environments (Osei-Afoakwa, 2013; Ebimobowei et al., 2011). Through coordination auditing IT auditors will be expected to bridge the longstanding audit expectation gap of becoming the catalyst for aligning management attention to business process enablers that ensure that conflicts, weak links and insufficient cohesion (Ebimobowei et al., 2011). An inclusion of coordination reviews in an IT audit framework will assist management to amplify their capabilities with the use of vital information on aligning IT resources to business objectives and increase process improvement initiatives in general.

3.3.3. Subsystem Three (Control) – S3: Mechanisms for Viability

Control is defined literally as the process of analysing the actual performance and results of a systems and comparing the result with benchmarks such as target performance standards or best practices to capture, correlate, visualize, and to develop actionable insight to detect and mitigate threats that pose real harm to the organization, and to build a more proactive defence for the future (Hitchens, 2015; Imoniana et al., 2013). Viability of an object, be it a living organism, an artificial system, an idea etc. concerns the ability of the thing to control its variety, i.e. maintain itself within its environment and recover its prior potentialities to remain essentially the same over time. A viable system's control refers to the capacity to prevent, detect, deter, locate, isolate or suppress potential internal problems including vulnerabilities and threats, restore and regulate it to its prior potentiality (Hitchens, 2015).

Control is responsible for the maintenance of cohesion and stability of all parts of the viable system and for adaptation in a living system. Therefore, control plays significant role in the viable systems model (Beer, 1985).

Control is sandwiched between operational processes and strategic designs of a viable system. Thus, at one end of the viable systems continuum is the analysis and the monitoring the '*inside-and-now*' which is the "day-to-day" management responsibility for regulating activities of the organization's internal operations which refer to subsystems 1-2-3. At the other end of the continuum is the analysis of the control environment '*outside-and-then*' which refers to subsystems 4 – 5 that concerns ensuring survivability, i.e. a system's ability to reduce the magnitude of the impact of external threats and pathogens that can cause future disturbances to the achievement of objectives (Álvarez-Molina et al., 2014; Burgess & Wake, 2012). Espejo (2003) concludes that the control mechanisms inside-and-now and that of the outside-and-then constitute the mechanisms for viability. Mechanisms for viability ensure that the system's processes or functions can work together successfully in a properly coordinated fashion and can ensure that the processes are continuously kept under monitoring to support the organisation's co-evolution with agents in its environments. Thus, Control Viability philosophy in the VSM is dually pronged – mechanism for *process cohesion* and mechanism for *process adaption* whereby the later and the former interdepend to determine stability (homeostasis). This philosophy is drawn from electronics and generally accurate in electronic control systems and circuits. Based upon this, control should be a two-way feedback and feedforward control loop systems whereby output of one subsystem is the input of another subsystem and the other control system in-turn responds by sending back error detection and or error correction feedback to the first control subsystem in a systematic concerted continual ongoing effort to achieve an adjusted and unified process (Espejo, 2003).

Control mechanism for process Cohesive Viability – The VSA is designed to conduct observation and diagnosis of complex systems across several disciplines enabled by certain cybernetic concepts. This involves a set of interactive and *systematic* relationship within its own context and suggests a new interpretation of consolidated strategic organisational and managerial practices (Polese, 2011). The control mechanism for process viability entails properties that keep functions of a viable system together as a stable and cohesive whole (Espejo, 2003). These mechanisms for process viability include the concept of *autonomy*.

Autonomy is the freedom of a subsystem to act on its own initiative, within the framework of action determined by the purpose of the total system is understood to create conditions for local viability without disturbing underlying cohesion (Espejo, 2003). For a human activity system to be viable there must be a reasonable level of inbuilt *flexibility* for its units and actors to be functionally viable. Autonomy of a system is linked to the *customizability* of the workings of collectives to achieve viable and desired outcomes (Sagalovsky, 2015). The control mechanisms for cohesion thrive on *voluntary* action involving the identification of desired outcomes together with actions necessary to achieve them which are also modifiable by their consequences (Bititci et al., 1997). The implication of the foregoing for IT auditing is that to uphold viability of IT audit functions the necessary ingredients must include the autonomy, flexibility, customizability, voluntariness and systematization of the framework approach.

Control mechanism for Adaptive Control – The control mechanisms for adaptation contain concepts that ensure that a system has a set of philosophies and methods for co-evolution with its environment (Espejo, 2003). One of the most relevant methods for co-evolution with the environment is the process of *recursion*. The assumption of recursion posits that all living systems are composed of a series of sub-systems, each having capacity to self-organize and self-regulate in all environmental circumstances to sustain survival. By recursion a system works itself out by the processes of continuous self-organisation and self-adjustment among its subsystems or functions (Espejo, 2003). This process is referred to as the process of autopoiesis which is defined as the capacity of a system to evolve through quick inter-relational changes while enabling internal conditions to remain recognizably the same. Autopoiesis is, therefore, synonymous to *agility* which refers to move quickly to adjust to changes (Steinhaeusser et al., 2015). Agility is a rigorous approach recommended for projects in complex and dynamic environments. It leverages continuous learning process for both the audit professional and for management (Hilder, 1995). For a system to be adaptive it must show resilience in its methodology and it is possible where the controls involve *proactivity* and *responsiveness* to the vagaries of the environment (Walker et al., 2002). The implication of these concepts for IT auditing is that to be able to co-evolve in the environmental vagaries concepts of adaptive control are necessary (Schmidt et al., 2014). These concepts are recursion, agility, responsiveness and proactivity. They relate to values

that have received high score in the IT auditing and assurance discipline and research (Deloitte, 2018; Marcello et al., 2017; Deloitte & Touche LLP et al., 2012).

- **Problem Diagnosis**

The problem formulation stage revealed that nagging challenges of auditing in less regulatory environments pertain to the lack of guidance for a systematic approach to review audit risk that is a match the increasing complexity in business processes, people and technology. IT audit projects continue to use the inefficient rigid approach whereby deliverables wait till the end of audit in which value is wasted (Nehinbe & Adebayo, 2011; Osei-Afoakwa, 2013). There is a widening skills gap within audit practitioners approach and the competence required of auditors to meet delivered through the audit approach employed. Risk assessment is reactive and seldom proactive because, typically, audit is a yearly one-off ritual which concentrates on operational and compliance review activities. Audited events including organisation risks assessment hardly take place within the same time frame as the event or risk; hence, huge amounts of funds and resources are lost every year through fraud and corruption before they are found out which prosecutions and punishments alone could not be envisaged to provide material panacea (Petersen, 2015; Sun et al., 2015).

Framework for IT and internal audits is expected to detect problems early and design proactive preventative solutions – the essence of a viable system, yet, practitioners exhibit little or no insight into current IT issues, preventive risk assessment and strategic information systems issues (Svata, 2011). Internal Auditors and Information Systems Auditors woefully ignore effectiveness including comparison of what is practiced with evolving best practices and rarely link them to drivers of business performance or change because of lack of guidance (Egbunike, 2014). The control environment which is defined by IIA (2015) as the totality of attitude of the business executives and management that set the tone of the direction and control of the organization is narrowly scoped to concentrate to functional or tactical managers. Boards and decision makers whose actions are expected to stabilize the business in the long term are ignored in audit reviews. Audit reviews and reports often hardly concern their functions. A framework for IT auditing that recognises complex relationships and agility in control reporting will, therefore, be very expedient for less regulatory environments. Board of Directors and Senior Managers are, therefore, not helped by internal audit and IT audit reports because they don't use functional or tactical information for

decision-making and they are asking why (Tan, 2015). Enterprise Risk assessment is seen as a fault-finding exercise which leads to negative reaction from responsible parties rather than cooperative attitude that conduces to adaptation through the adoptive controls. Adaptive control, therefore, refers to the resilience of a system to maintain its essence in changing contexts (Walker et al., 2002).

The implication of considering Control (S3) function in IS auditing process is that it will provide guidance for efficient and continuous monitoring and auditing of the control environment which is central for the achievement of the primary objectives of the business. It will help to provide reliable reports to internal and external stakeholders, to operate the business efficiently and effectively, to comply with all applicable laws and regulations, and to proactively safeguard business assets. Recent well publicized corporate failures such as the Enron, WorldCom and the 2008 financial crisis across the globe are testimonies of weak monitoring of the control environments (Cassidy, 2016; IIA, 2011). Without a demonstrably effective control environment, no level of operating and coordinating design within a business and IT processes can provide meaningful assurance to stakeholders of the integrity of an organization's internal control structure (The IIA, 2011).

3.3.3.1. Subsystem (S3*)

A major challenge to investors and other stakeholders in less regulated economies is the issue of non-compliance, fraud, corruption and the lack of transparency and probity (Egbunike, 2014; Dada et al., 2013). S3* in the VSM provides for fraud risk assessment which, recently, has become a requirement for every audit that complies with best practices (COSO, 2016; D'Aquila & Houmes, 2015).

- Problem Diagnosis

Several best practices have been put forward by several of these bodies and governments. For example, internal control provision in the Sarbanes Oxley Act 2002 in the United States of America has spawned the development of the policeman theory in auditing. The new COSO best practice guideline displaces the old school attitude of auditing drawn from a seminal English case law of re Kingston Cotton Mill Company (No.2) (1896) which states that 'an auditor is not bound to approach his work with suspicion or with a foregone conclusion that there is something wrong. He is a watch-dog, but not a bloodhound' (Chandler, 2014).

Recent demand for audit in less regulated economies is increasingly for fraud investigation purposes. This is because fraudulent non-compliance with rules and regulation and intentional overrides of ethical behaviours for self-interest concerns have been increasing in less regulatory environments. White colour criminals are taking advantage of the complexity in business environments due resulting from IT to engage in all forms of cybercrimes. In this study, based on the viable systems approach, it is averred that the policeman theory to IT auditing is relevant for less regulatory environments. This should be incorporated with an attitude of continuous monitoring of the control environment. In contrast with the traditional annual fault-finding approach, the proposal in this research is that auditing should be a shared responsibility between auditors and management to achieve better outcomes (Burgess & Wake, 2012).

3.3.4. Subsystem Four (Intelligence) – S4

Intelligence is defined by Hilder (1995) to be a continuous feedback function between the organization and its external environment that is beyond the purview of subsystem S1 that are likely to be relevant for business adaptation and viability. Intelligence is therefore, viewed as the outer eye that is responsible for monitoring and enabling the capacity of management to contemplate the future and to plan accordingly to adapt to shifts in the external environment that may threaten business viability (Espejo & Gill, 1997). The evolution in the technological space and advancing technologies, such as cloud, social media, blockchain technology and mobile devices and the desire towards Internet of Things (IoT), 'Bring Your Own Device' (BYOD) has made business and economic landscape jagged. These technologies come along with new business opportunities as well as risks. The risks include threats and the pressure from severe competition that are already causing the loss of competitive advantages and shrinking revenue margins (Cassidy, 2016). More examples of such risks include complicated agreements and contracts that have expanded operational and strategic risks and hence audit risks (IIA, 2015; Ruhnke & Schmidt 2014). Businesses, therefore, tend to deploy innovative operational strategies such as outsourcing to cut down cost and take advantage of technologies that can improve business processes without necessarily directly developing and managing them. This leads to complicated control environments which involves related dynamics of the risks and threats that border on issues such as business continuity management and information security (Ernst & Young, 2013). This has been the compelling reason for governments, regulatory bodies, industry as

well as investors to begin to scrutinize companies' risk-management strategies, procedures and IT policy of management (Sarbanes Oxley Act, 2002; Kinney, 2003; Brown & CISA, 2014).

- **Problem Diagnosis**

The problem audit and assurance services in developing countries is that technology is far more advanced than the assurance reports of assurance providers. This is because IS auditors still concentrate on application controls, project advisory and compliance-based reviews. They seldom give sufficient attention to the impact of emerging events and innovations in the technological space. Fraudsters are often far ahead in technology than auditors and assurance providers making it challenging for audit to make impact in the development of the auditee. Assurance reports do not deal sufficiently with the effect of the impact of environmental changes on the future opportunities and threats for the auditee (Svata, 2011). As the relevance of IT increases in the measurement of business viability Boards and Management are overwhelmed by the rapidly expanding complexity. Intelligence (S4) auditing, in this study, is developed to ensure assurance service practitioners have a framework that is imbued with the relevant concepts that will bridge gap between the complexity and viability of businesses (Philipson et al. 2016; Singleton, 2014). IT audit functions will be required to apply a broad set of skills and specialisms and a diverse range of resourcing models to ensure a quality audit and insights that management and boards will value (Biske, 2012). In a research conducted by KPMG and IIA (2015) concludes that since intelligence audit seems to be a relatively new subject to most auditors, guidance for performing these audits is desired by practitioners. There is a compelling reason for developing intelligence auditing function that applies the well-developed assessment methods and procedures based on observable and measurable developments through the viable systems approach (Swanson & Marsh, 1993).

3.3.5. Subsystem Five (Policy) – S5

Policy function is defined by Beer as a final sanity check against direction constituting a set of principles, rules, and guidelines formulated or adopted by an organization to reach its long-term goals after extensive debates and decisions have been carried out within and between the Intelligence and Control functions (Espejo & Gill, 1997). Beer links policy to the concept of *homeostasis* in cybernetics and applies *Le Chatelier's* principle which states

that when external constraints are applied to a system in equilibrium then in so far as it is able, it will adjust itself to oppose the constraint and in so doing it will restore its prior potentialities or move to a new point of equilibrium (Hitchens, 2015). The purpose of policy, thus, is to ensure that the entity can adjust itself and adapt to new and appropriate level of equilibrium within the dynamics in the environments. Policies and procedures dictate the manner of occurrence of business processes in each of the operational activities (Espejo, 2003). With recent developments in business environments, the status of IT strategy and risk management are becoming the defining factors of the strategic direction of organizations. ICT is significantly influencing how organizations make current decisions to directly or indirectly adapt to changing business environments that affect future viability. Board members and executives are now expected to get actively involved in providing strategic IT direction and to show active leadership by enabling the achievement of business objectives through IT policy initiatives, ascertaining that IT related risks are appropriately managed and ensuring that enterprise IT resources are utilized responsibly. Stakeholders require that the increased environmental risk assessments be balanced by the assurance that those charged with governance and controls are on top of current and emerging risks and can quickly identify and prioritize the risks that matter (Cassidy, 2016; PwC, 2015). To effectively deliver on this new objective, audit of the future should consider first balancing a deep understanding of the IT environment, applications and computer operations and how both are managed and secondly, the suitability, feasibility and acceptability of the policies and strategies relating them to IT infrastructure and back to organizational goals (Kirk e al., 2008).

- **Problem Diagnosis**

One of the very important weaknesses of audit in less regulatory environments discovered during the workshop session and literature review is that IS auditors and Internal auditors generate reports are not valued by business executives in policy or strategy formulation. This is because internal auditors and IT auditors concern themselves mainly with general information security reviews, application control reviews (ACRs) and general control reviews (GCRs) and provide policy makers mainly with exceptional control reports. As a result, auditors woefully ignore effectiveness or comparison of what is practiced with best practices and rarely link them to the policy drivers of business performance (Tan, 2015). Due to increasing complex business environments, there is the compelling factor for today's

IS/IT auditors to go beyond the traditional IT audit roles of mere tactically based IT projects advisory to include IT governance assurance and policy-making consulting service (Svata, 2011). Policy-making positions are very critical for the viability of organisations as these are expected to provide homeostatic regulation, but it is unfortunate to learn that many policy-making position makers in less regulatory environments are only rubber-stamping what has already been decided within the functional officers because of not having the required in-depth knowledge to pass judgment to scrutinise management briefings (Van Grembergen & De Haes, 2018).

The implication of incorporating policy evaluation as a very essential function of IT auditing in the modelling of a conceptual framework for IT auditing is that practitioners in the field believe that an auditor can learn a great deal about an organization by simply reviewing the strategic plan and examining the company's policies (Cassidy, 2016; Gregg, 2007). If an auditor makes references back to the policy about each finding, the effect is to enable the auditor to establish a cause of problems and, in so far as he's able, specify how to rectify the identified problems in order to restore the entity to its prior potentialities. Thus, if auditors should make policy review a priority in their assignments, then they would be able to create value by generating of high-level information for those charged with governance to improve their control policies and procedures and build confidence in other stakeholders about the performance of the entity (Ebimobowei et al., 2011; and Osei-Afoakwa, 2013; Abugu, 2014). To ensure that IS/IT audit practitioners don't get into the drivers' seat of formulating policies, however, it is essential for guidance to be provided regarding assurance on policy making functions of corporate leadership without compromising their independence and objectivity.

The Environment - Beer adopts an 'open systems' approach in the design of the VSM (Beckford, 1993). Open systems theory refers to the assumption that organizations interact with and are strongly influenced by their environment. A system's environment is scoped by defining its boundary. The environment of business connotes direct and indirect internal or external influences, forces, factors and institutions that have significant impact on the viability of the business. An open system, however, emphasizes on the effects of external influences on the system that cannot be controlled internally. These factors include economic factors e.g. changes in customer demand and disposable incomes; social factors e.g. shift in the population or its composition or cultural changes, modifications in supplier or competitor

strategies; political and legal factors (Hilder, 1995). More so, government regulations and compliance requirements and shifts in demand due to ICT including business arrangement such as outsourcing involve complicated agreements and contracts have expanded operational and strategic risks and, for that matter, audit risks (IIA, 2015; Ruhnke & Schmidt 2014).

- **Problem Diagnosis**

The environment of business in developing nations is characterised by noncompliance and irregularity. Auditors, unfortunately, continue to struggle with effective and efficient approach to execute proportionate risk assessment standards due to lack of adequate guidance. Common deficiencies include the tendency to over-rely on checklists with procedures that have inadequate linkage to the risks they are designed to address. Auditor's risk assessment capacity, therefore, continues to be a mismatch to the challenges posed by components of risks coming from the entity's environments (Flood, 2017; Awuzie & Mcdermott, 2013). Entities' ability to maintain viability in the foreseeable future, as a result, become uncertain due to consequences in mismanagement, fraud and corruption of varying degrees (Philipson et al., 2016). Investors, therefore, expect higher audit quality that can provide early warning of impending failures or threats.

The implication of emphasising on the environment as a concept in the development of the conceptual framework for IS auditing is to engage practitioners with the relevance of the appreciation of the environment to the overall viability of the practice. A robust understanding of the environments within which a business operates will aid audit and assurance reviewers to achieve audit quality (Burgess & Wake 2012). A conceptual framework for IT auditing based on the viable systems approach should support actions in the environment that allow the organisational system to deal with environmental variety that is relevant depending on performance requirements.

Requisite Variety - The term 'variety' is used by Beer (1985) in place of 'complexity' or 'sophistication' which refers to the number of possible states that a system or its 'environment' might exhibit in relation to defined processes and purposes (Thomas, 2006). Variety is defined as a variable of any kind which connotes circumstances, whatever be the kind and nature of the elements, which may be opposed to each other in purpose in such a way that without an underlying mechanism of control, they will show lack of balance,

purpose and relevance (Syntetos & Jackson, 2011). The ‘law of requisite variety’, was propounded by the cybernetics scientist Ashby (1956) and applied as one of the derivative tools of viability states that only variety can destroy variety. Ashby (1956) argues that variety can only be ‘controlled’ if the ‘controller’s variety’ is a match or equal to the variety to be controlled (Brocklesby, 2012). ‘Variety engineering’ is, therefore, defined by Beer (1985) as the process for dealing with probabilistic behaviour whereby a management unit controls element of its internal or external environment by either reducing (attenuating) the variety that are unfavourable to the system objectives (i.e. *variety attenuation*) and increasing (amplifying) the favourable ones (i.e. *variety amplification*) iteratively until a state of an appropriate state of balance or an optimum variety is obtained. To amplify variety, therefore, management may deploy tools directed at supporting organizational cohesion and adaptation such as *structural redesign* - e.g. team work, groups, etc.; *augmentation* - e.g. recruitment/training experts or employing independent experts; *information systems management* - e.g. management or executive information systems etc. Conversely, management may attenuate variety by deploying tools such as information management of systems, delegation, outsourcing, planning, policies, operational budgeting and rules etc. (O’Grady & Lowe, 2016). Variety engineering is, therefore, viewed as a two-way communication loop between variety amplification and variety attenuation (Brockelsby, 2012).

- **Problem Diagnosis**

In business organizations variety exhibit themselves in the sophistication of either internal or external relationships, circumstances and elements such as staff issues, leadership issues, compensation issues, information issues, technology issues, legal and regulatory issues, commercial relationships issues, skills and expertise issues, sales issues, financing issues etc. (O’Grady & Lowe, 2016). As the business horizon keep changing and shareholder needs keep evolving, corporate leadership need for information on value drivers relevant for survival is becoming more important than ever before (Biske, 2012). For example, with increasing globalization and ICT integration in organizational processes, competition has become very severe and survivability has become very critical in current business horizon. With increasing sophistication in people, technology and business process, the issues of audit risks and the IT audit have become very critical in defining the future of the practice

(Knechel & Salterio, 2016; Philipson et al., 2016; Burgess & Wake, 2012; Popa, 2009; Simmons, 1995).

There is a growing belief in countries without longstanding audit and regulatory systems that the audit profession has a significant relevance in providing first-hand consulting service to management to enable economic growth and development according to a survey by the ACCA & Grant Thornton International Ltd. (2016). McCafferty (2016), however, reports that audit has persistently been an annual fault-finding exercise which over-emphasises on compliance in which audit is made to appear intimidating. Auditors end up being stuffed in boxes and nothing is done after all due to framework inadequacies together with logistical problems.

The intervention the concept of variety engineering will bring to IT auditing is to provide the conceptual substrate for attenuating irrelevant non-value adding audit activities and amplifying additional procedures that really tackle client-specific weaknesses and threats. Enterprise risks will properly be matched with its strengths and opportunities to increase alignment with strategies to satisfy the concerns and expectations of many researchers and stakeholders of IT audit framework (Sun et al, 2015; Appiah et al., 2014; Osei-Afoakwa, 2013). Audit findings and reports will be geared towards supporting policies and procedures that really help assure management their directives will address risks and increase opportunities if carried out properly and on timely basis (Aboa, 2014; Svata, 2011; Brazel & Agoglia, 2007). Relevance of IT auditing eventually will be based on the expectation that practitioners will help widen the window for those charged with governance and management to develop confidence and reliance on audit reports to make internal control decisions.

Communication - Stafford Beer saw the need for messages to be transmitted across component boundaries and “translated” into the language of the receiver to ensure understanding and for actions to be taken. He borrows an electronics concept of ‘*transduction*’ to refer to the translation and communication of information across the subsystems and boundaries. The concept of variety engineering, for example, requires skills and critical information and intelligence to take place because, according to Beer *ignorance* is a *lethal variety attenuator* (Hilder, 1995). The term *algedonic signals* was used to refer to

the variety of intra-organizational and inter-organizational reports that support decision making (Khan, Nicho & Cooper, 2015).

- **Problem Diagnosis**

The communication theory states that auditor's function relating to the information communicated provides reasonable comfort level to the target recipient and therefore improvement in the auditor's communication skills is compelling (Endaya & Hanefah, 2013). The stakeholder theory of demand for audit states that various stakeholders create demand for or require relevant and reliable information for decision making within and without the organization. For example, management wants to be informed on its capacity to credibly inform others such as shareholders and regulatory authorities that management is carrying out its fiduciary and legal responsibilities. Workers also wants management to appropriately inform them about risks that they face and, in turn, to inform management about exceptions noted in day-to-day operations. Non-executive directors, regulators and investors demand information relating risk assessments and risk management processes and audit committees who have oversight responsibilities would be comforted by assurance that risks are being managed adequately (Kinney, 2003).

Time is of essence in audit communication. Problems that were presented to the researcher in his interaction with practitioners and other stakeholders include failure to address audit recommendations partly because audit reports are not communicated within the same time frame as the risk or event reported on. Many accounting firms who take up audit assignment in many of these less developed economic environments don't have the techniques to make their assignments deliver value through effective communication (Holmes, 2018). Omonuk and Oni (2015) confirm this by finding that audit firms in developing countries are not delivering effective and audit quality and assurance results because local audit firms lack the guidance to generate quality audit reports and communicate it timeously. Ebimobowei et al. (2011) discovers that internal auditors in the public sector in Nigeria have failed to perform their audit responsibility with the relevant level of professional and technical expertise expected by the society. Osei-Afoakwa (2013) discovers that auditing has become a rubber-stamp exercise, usually lacking value and audit reports are merely requested to satisfy just one of the routine requirements of corporate governance and not for the value it brings to stakeholders.

Implementers of audit recommendations suggest that auditors' communications are bereft of sufficient Key Audit Matters (KAM). KAM is a recent hot audit concept borne out of the investor demand for more detailed contextual information about a business. This is the consequence of increased investor awareness and demand for transparency. It has, therefore, more than ever before brought to the fore the relevance of brisk conversations between the auditor and those charged with governance. Communication rates very critical in an audit assignment. The VSM as a model was found to be relevant for framing a new approach to auditing because of the need to improve IT audit process together with an improved quality of audit communications. When performed with the relevant approach, assurance reports are considered as evidence that those charged with governance and control have carried out their oversight responsibilities (Singleton, 2014). It is, therefore, very important for auditors to maximize the value of their role by communicating and translating their reports in a timely manner to the understanding of all stakeholders. Maximizing the value of IT audit role must, first, be based on the quality of the auditor's approach followed by effective communications. Communication of audit findings must be undertaken in a manner which is suitable for the organization being audited and should contribute to the achievement of its goals (Singleton, 2014). Auditors are expected to include powerful analytical skills that convey deep insights, factual information inspiring trust and credibility as well as demonstrating sound understanding of the business and the impact of the findings. IT auditors' communication must be based on crystal-clear translation of message, signals and incidents in timeous manner to support decision making. Driven by the emergence of social media IT audit practitioners can maintain an ongoing and two-way (i.e., talking and listening) dialogue, both formally and informally, with the rest of the enterprise to ensure their reports are relevant and understood (Chambers & McDonald, 2013).

3.4. Performance Measurements System of the VSM Operations

It is necessary to have a system of analytical procedures for measurement during the planning and the customisation of an assurance assignment that considers the resources and relations that are necessary for an effective organisation and the value chain of activities of operations. This is because the consequences of complexity-based responsibility accounting and assurance systems are significant (Schwaninger, 2006). One such measurement system is the one based on the concepts of *actuality*, *capability* and *potentiality* posited by Beer (1972; 1981) to characterize activity in a System 1 (Operations).

- **Problem Diagnosis**

As stated in chapter two, the challenge with the use of the Capability Measurement is that ISACA did not provide an objective process capability assessment metrics for process capability determination. They made referred to process attributes ratings and stressed the importance of recording and maintaining references to evidence of independent expectation to support the assessors' judgement of the attribute of client's IT processes when deploying the Capability Rating Model. This is because, in the view of ISACA process capability as abstract. Hence, they recommend to assessors to use their subjective professional judgement, experience and IT skills, otherwise, use the enterprise's performance in place of Capability (Aliquo & Fu, 2014). Such method for determining an enterprise's capability or performance, however, are not without serious inherent shortcomings leading to high failure exposure in assessments (Percheiro et al., 2017; Linich & Puleo, 2016; Bartens et al., 2015). Financial auditors have conducted analytical procedures at the planning stage of audit using performance measurements such as accounting and profitability ratios, return of Investments ratios, liquidity, costs and other accounting ratios from financial statements (Pine, 2008; Ha, 2005; Kogan et al., 1999). This helps in discovering and analysing patterns, deviations and inconsistencies as well as the extraction of other useful information related to the subject matter of an audit through analysis, modeling and visualization for planning or performing the audit and directing audit focus on potential areas of risk. Although these elements of financial indicators may be valid and sound, yet the entity may not be viable because of complex interdependencies that comprise viability (Bell et al., 1997). Beer (1981) regards these financial measures as inadequate and insufficient. According to Beer (1972;1981) those financial indicators constitute constraints rather than objective measurement of their going concern (Beckford, 1993). Beer (1981) agrees that the performance analytics of a system needs to be quantifiable and measured on 'pure' numbers which should reflect the survivability of the firm compared to Checkland's qualitative measures of efficiency, effectiveness and efficacy (Espejo, 2009). Beer (1972; 1981) propounded the concepts of *actuality*, *capability* and *potentiality*, known as the 'triple vector indices' or simply the three-factor measurement to characterize the measurement of performance of an autonomous subsystem S1 (Operations). The triple factor indices are a heuristic method that can be applied to performance analytics in nearly all assignments that begin with planning (Espejo, 2009). They are effective measures for its *achievement*, *capability* or *performance* gaps in

a viable system's operational processes. **Figure H** below is diagrammatic representation of the triple vector measurement concepts.

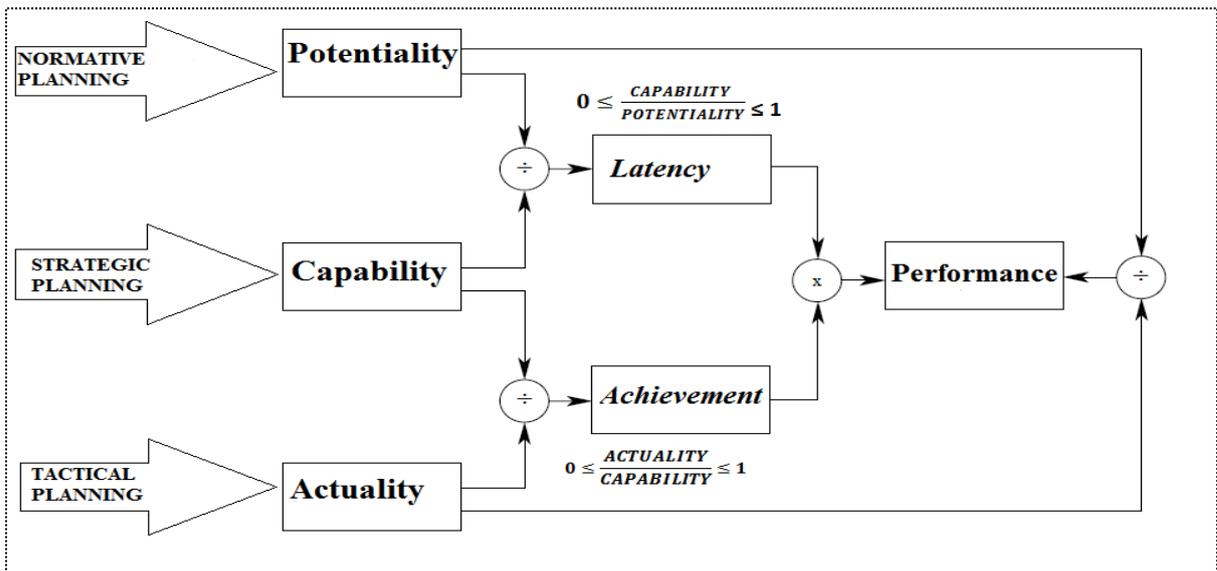


Figure H. VSM performance measurement system.

Beer (1981) defined the three-factor measurement concepts as follows:

- **Actuality:** the measurement of a set of objectives that is achieved today as compared with the set of objectives that could have been done, considering present level of resources and constraints. Evidence of the effectiveness of the implementation management processes or primary functions is obtained in the measurement what it is doing – its actualities. Actualities, therefore, measure the complexity that is matched by the enterprise's operations.
- **Capability:** the measurement of everything that could be done if the organization had been optimally organized given the present level of constraints and resources. Evidence that the organisation is exploiting its resources efficiently to match environmental complexity to achieve optimised outcomes is determined by 'Capabilities'.
- **Potentiality:** the measurement of what the organization could be doing if resources are well defined and developed and constraints are removed. Organisational processes for policy formulation define the enterprise's potentialities. Evidence that intelligence is not being stretched, or cohesion is not well-grounded in the operations of the enterprise or that intelligence-cohesion alignment is inadequate, is addressed by questioning the definition of potentialities (Espejo, 2009).

Beer (1981) proceeds with the elaboration of the measurement concepts by defining three levels of planning relevant to each of the three factor measurement concepts performance namely; tactical level for actualities, strategic level for capabilities and normative level for potentialities.

3.4.1.1. Tactical Planning Level

Tactical planning is defined as, essentially, being a reference projection of efficiency of what the organization currently is doing in terms of the implementation of the primary business processes and the relevant general control functions, compliance with standards and regulations etc. as compared to what it ought to be doing should the present level of achievement of objectives be maintained given the relevant environmental constraints (Paucar-Caceres, 2009). This level determines the organization's actualities. Actualities are deterministic values that are measured as the organization's actual performance. Sources of data includes budgetary performance and projections variances of financial and non-financial objectives. They are deterministic because data can be obtained objectively from managers since each manager knows what his actual degree of productivity is as compared with what he is capable of doing that are capable of moving the organization forward given the current constraints (Espejo, 1979). This process provides can lead to the identification of process improvement opportunities in operations.

3.4.1.2. Strategic Planning Level

Strategic planning is defined as the continuous process of updating capabilities throughout the organisation (Espejo, 1979). Quantitative figures are derived using the indices obtained in *Actuality* and *Capability* at the tactical planning level. *Capability* represents budgetary benchmarks for operational performance. The power of cybernetic planning and analytical review is that it integrates all organizational members and supports the assessment of objectives by defining the gap in achievements for communicating reliable outcomes timeously to management for actions (Bell et al., 1997). The objective of strategic planning is to identify the gaps between current *achievements* and *latency*. Beer (1981) describes the level of achievement of an organization's short to medium term objectives as the ratio of the measure of *actuality* and the measure of *capability*; given in a quantitative relationship as:

$$\text{Achievement} = 0 \leq \frac{\text{ACTUALITY}}{\text{CAPABILITY}} \leq 1.$$

The *latency* of the whole organizational processes can also be determined quantitatively. This refers to an analysis of the *capability* considering constraints of the business unit or the business process compared to the organizational *potentiality* which is the degree of effective allocation of resources that ensures better value than capability when constraints are removed (Espejo, 1979). Latency of the system's process is defined quantitatively by Beer as the ratio of *Capability* and *Potentiality*; given as:

$$\mathbf{Latency = 0 \leq \frac{CAPABILITY}{POTENTIALITY} \leq 1.}$$

Given 'achievement', latency is the measure of capability gap or redundant capacity of the process. The relevance of latency is that highlights the possibility for further organizational development putting into consideration redundant capacity or resources that are present but inactive (Espejo, 2009). The organization's overall '**Performance**' is derived as the product of the latency and achievement or ratio of actuality and potentiality. This is given as: **Performance = (LATENCY × ACHIEVEMENT) or Performance = (Actuality ÷ Potentiality)**. Performance analysis relates to the potentialities and potentialities is the normative measure of policies (Espejo, 2009). These measurements serve as the foundational evidence for further investigations that are geared towards identifying opportunity for assessing risks and recommendable improvements and in so doing the law of requisite variety, feedback and feedforward controls, the concept of recursion and operational processes evaluation, as applied in auditing above, are handy tools.

3.4.1.3. Normative Planning Level

This is defined by Paucar-Caceres (2009) as a process that evaluates the efficiency and effectiveness of the whole organizational policy direction and includes a reflection of the interests, social norms and values of stakeholders. It reflects the performance of those involved with policies and directions with or without constraints on their functions and thus, a measure of the enterprise's potentialities because the potentialities of an organization are defined by its formulated policy (Espejo, 2009). Analysis involved at the normative planning stage is how business strategies can increase alignment with enterprise risk management (ERM) and seek greater collaboration with the other lines of defence. This may lead to the analysis of how to strengthen links and possibilities to forge alliances in the marketplace, looking beyond the organization and drawing on external benchmarks and independent challenge for fresh ideas (PwC, 2016). Normative analysis sees beyond quantitative financial

information often conducted to discover plausible relationships among both financial and nonfinancial data (Kogan et al., 1999; Steward, 2015). Rather, it supports the development of a broader perspective, assists with horizon-scanning and builds out sources of relevant information and insights by venturing its analytical procedures that reflect on the suitability, acceptability and feasibility corporate policies which used to be out of scope of ordinary assignments (PwC, 2016; Byrnes, 2015). A detailed exposition of these concepts and the development of customisation metrics for the proposed framework for IS auditing is submitted at the later part of chapter four to resolve this problem.

3.5. Criticism of the VSM

The VSM has been used successfully within numerous private and public-sector organizations as a conceptual tool for understanding organizations, redesigning and supporting the management of change as discussed above. However, according to Espejo and Gill (1997), critics have two main reasons for their criticism of the model. First, the ideas behind the model are not intuitively easy to grasp e.g. the concept of ‘variety’ is ambiguous and creates implementation challenges (Thomas, 2006) and secondly, in the era of industrial revolution, the philosophy behind the VSM was seen to run counter to the great traditional legacy of organizational thinking - i.e. the traditional hierarchical bureaucratic institutions that operate according to a top-down command structure. Critics further, refutably, argue paradoxically that the VSM is too putative or prescriptive in nature and therefore it is inimical to human freedom (Yolles, 2001). In contemporary era, however, it is, rather, clear that the modus operandi of bureaucracy is characterized by slowness and inflexibility in coping with the increasing rate of change and complexity surrounding most organizations (Beckford, 1993). This is one of the reasons why the attention of systems development professional is now turned towards the VSM for the development of modern flatter technocratic institutions although the VSM is not yet widely known among the general management population.

3.6. Conclusion

The Chapter represented the problem formulation stage of the ADR research. The chapter introduced the ingrained theory and applied its functions and concepts in the diagnosis of IS/IT audit problems in less regulatory environments. The next chapter builds an intervention

to the conceptualised problem in the chapter which the conceptual solution. The materials to be employed for the building of intervention will be based in the strengths of best practice framework such as COBIT, COSO and ISO earlier reviewed as part of the literature above. The development of this chapter will also rely on the researcher's practical experience and will apply the highlighted functions and concepts of the ingrained theory for the development of the conceptual framework culminating in the development of conceptual hypotheses which will be used for further development of the research.

CHAPTER FOUR

BUILDING AN INTERVENTION

4.0. Introduction

This chapter develops solutions that provide the required intervention in the problems discussed in the preceding chapter. The building process of the intervention involves the reliance on the researcher's experience including the knowledge foundation of best practices such as COBIT, Process Capability Assessment Methodology, COSO, ITIL and the viable systems performance indices introduced in chapter two for technical demonstration in the IT-dominant BIE activity in this chapter. The chapter ends in the development of a conceptual framework and the formulation of propositions or hypotheses for further investigation.

4.1. Development of the Intervention

Development breaks problem formulation phase into two namely; the IT audit process design or building phase and the conceptual model development phase. The design or building phase is used to construct a prototype of the prescribed intervention and to provide detailed demonstration of the proposed IT audit processes (Vaishnavi & Kueshler, 2004) which is the essence of this chapter. The building phase concludes with the use of the three-vector performance measurements by Beer (1985) in combination with the governance system design workflow, CMMI-based process capability scheme of COBIT 2019 together with maturity standards by ISO/IEC 15504-3 to design metrics for the creation of IT Audit Universe to customise processes within the framework to achieve desired outcomes at the audit planning stage. The conceptual model development phase concludes in the formulation of conceptual hypotheses for further conceptual development of the framework.

Based on the ingrained systems theory of viable systems approach, therefore, a reciprocal artefact is developed to demonstrate the steps and scope of the proposed viable systems auditing processes. **Figure I**, below, is used to demonstrate the reciprocal artefact built on the ingrained theory to provide guidance for the technical aspects of the prescribed audit processes in the interventionist framework. It must be stated here that this demonstration does not entail all the conceptual principles. All the conceptual principles are entered in the development of the alpha version of the conceptual framework that comes after.

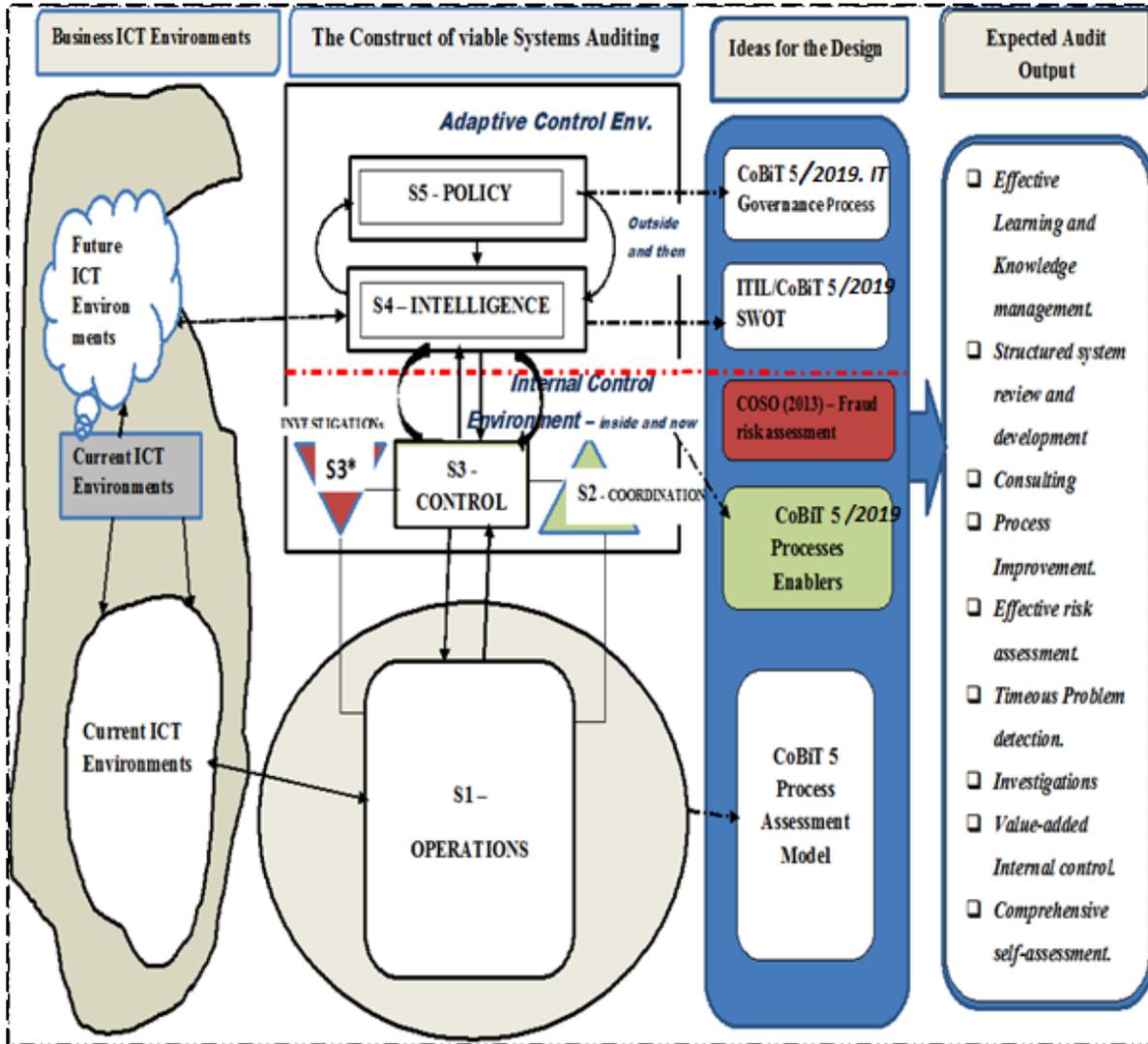


Figure I. Design of IT auditing Framework – Alpha version.

4.1.1. Symbols explanation

The construct and symbols are derived from the viable systems model (VSM) as explained in figure B above in the preceding chapter three. The operational system (S1) is represented here as the basic business processes implemented by the organisation and for which management and IT controls are relevant. Coordination (S2) and Control (S3) represent internal control mechanisms that affect business IT operations. These form the pre-requisites for IT auditing. Subsystems S1-S2-S3, in relation to business IT environments are classified as *current IT Control Environments* and per the viable systems approach, concern assurance ‘inside-and-now’ (IIA, 2015; Lewis & Millar, 2009). Subsystem S4 (intelligence) is represented as the audit and reviews that relate to the management and control both

internal and external environmental information. Subsystem S4 audit and review is therefore seen as the audit of the *total environment* of the organisation (Burgess & Wake, 2012). Subsystems (S3*), with violet color-coded represents the requirement by COSO for auditors to perform fraud risk assessment and investigation. S3* also represent an advocacy for a non-mandatory adoption as well as Compliance with professional guidance, standards, regulations and best practices e.g. SAS Nos. 104 –111 2 in AICPA’s Statements on auditing standards; AS Nos. 8 -15 3 which involves 8 auditing standards addressing the auditor’s assessment of fraud and response to fraud risks during audits issued by the PCAOB; COBIT by ISACA and COSO’s Fraud Risk Assessment (2016) which expanded on Principle 8 of their updated integrated Control framework (2013) (Flood, 2017; Martinez, 2014).

The *thick curved arrow lines* between sub-systems S3 - Control and S4 - Intelligence represents the need for a very rich complementary interaction and communication (i.e. mechanisms for control concepts) that need to be considered by the assessor for the assurance that internal controls are a match to external factors that may have impact on the viability or *control environment* of the *future* of the organisation. To facilitate decision and policy making that support “requisite variety”, the organization’s total control environment (S4) also provides rich interactive feedback to subsystem S5 (Policy). The Policies, Directions and Leadership of Boards and Chief executives constitute a very critical element of an organisational Control Environment (IIA, 2015). The review of these elements is represented as Policy S5. Policy makers rely on the total control environment (S4) to be able to formulate rich and the desirable policies and set the tone for the organisational leadership. Failure is a very lethal variety attenuator according Beer (1972). The interactive concepts with which an assessor is expected to carry out reviews in the viable system auditing approach is represented by another set of thick looping arrow lines with opposite directions linking S4 and S5. In the viable systems auditing approach Subsystem S4 and S5 are classified as an assessment of the organisation ‘*Outside-and-then*’. The single arrow heads show the direction of processes as well as how information flow from one stage of the audit process to another until conclusion of the assignment. The double arrow heads demonstrate the necessity for the auditor to extend the collection and examination of audit evidence from external environment relevant to operational process under of the IT auditor’s evaluation.

4.2. Demonstration of the Artefact

A design science research has been defined as learning through building (Vaishnavi & Kueshler, 2004). The purpose of demonstration is to explain the process of the artefact in solving one or more instances of the problem (Peppers et al, 2007). The demonstration of the IT audit process in this section of the research activity involves applying the strengths of literature of best practices to the functions of the viable systems model together with its relevant relationships drawing on the researcher's professional experience and proofs from practitioners to build a solution design to the problems.

4.2.1. Operations/Process Auditing

ISACA (2013) posits that the contemporary demand for IS audit is principally for the determination of whether the intent of the core processes of a business Operations are being achieved. Operations (S1) audit can, therefore, be defined as a thorough assessment and understanding of the organization's internal operational control processes including its ability to prevent, minimize or reduce the magnitude of finite disturbances to the value chain of a business to provide assurance over the viability of current business processes (Bititci et al., 2000; Ellison et al., 2008). The concepts of autonomy and recursion that underlies operations (S1) ensure that all other sub-functions of a viable system are contained within operations. In the VSM logic, the concept of autonomy and independence is ceded to Subsystem (S1) Operations that calls for systematic examination of functional units of the business processes to achieve effective and rapid outcomes in the changing environment (Khan et al. 2015). Therefore, operations audit is, probably, the most involving of all the functions of IT auditing. The audit process must first identify autonomous units of the business process value chain. Each unit has its own local risks and vulnerabilities which must be assessed systematically for best results.

Structural recursion dictates that the assessment of each autonomous business activity must involve contains all the levels the VSM functions that ensures cohesion or viability *inside-and-now* and adaptation *outside-and-then* (Espejo, 2003). The viable systems approach identified three functions for cohesion inside-and-now in the VSM logic namely operation (S1), Coordination (S2) and Control and investigations (S3/S3*). Two functions were identified as mechanism for adaptation outside-and-then, namely; intelligence (S4) and Policy (S5) (Álvarez-Molina et al., 2014).

Audit from the lens of S1, therefore, encapsulates all five functions of the VSM within each autonomously auditable unit of an organisation (Swanson & Marsh, 1993). The above viable systems approach to auditing operations (S1) is expected to serve as an improvement on the previously ill-defined and poorly approached systems-based auditing.

4.2.2. The Process Coordination (S2) Audit

The essence of a synergistic cohesion of an organisation is coordination. It is, therefore, vital that an assurance framework provides guidance for assessing coordination inside-and-now. It should be re-stated for emphasis that traditional IT auditing has an attitude of glossing over coordination because there is no guidance for its assessment. Coordination Audit (S2) refers to the assessment of process of management activities associated with the how the organization's current IT supports and regulates totality of their attitude that sets the tone of the direction and running of the organization. i.e. the IT Universe. Coordination auditing in the viable systems approach is expected to evaluate the relationship between human beings together with their IT-related resources, documents and procedures that are aimed at positive outcomes. The objective is to identify the weak links among business IT processes that are expected to yield increased efficiency, augmentation effect, enablement of new processes, scanning and detection capacities and aligns their collective interests with the entity's mission, (Nevo & Wade 2010).

The Basel Committee on Banking Supervision (2001) cited in Buffa and Basak (2016) provides a definition of operational risk as the probability that a loss resulting from inadequate or failed internal processes, people, and systems or from external events will occur. Control (S3) relates to the assessment and control of operational risks. Buffa & Basak (2016) distinguish between internal operational risks and external risks depending on whether the institution has control over them. Internal operation risk assessment is categorised into two main categories – routine operational risk assessment (S3) and for-cause operational risk assessment (S3*). COBIT 2019 governance system provides seven (7) independent business process enablers that sum up routine operational risks of an organisation. Enablers are defined by De Haes & Van Grembergen (2015) as the tangible and intangible factors or resources that can individually and collectively influence whether the overall IT management of objectives will work according to plan. These include general control risks, logical control risks, application control risks and contingent control risks. The governance system risk components are inherent in the following: 1. Service, 2.

Infrastructure and Applications, 3. Information, 4. Principles, 5. Policies and Frameworks, 6. Culture, Ethics and Behaviour and 7. People, Skills and Competence (Philipson, Johansson & Scley, 2016).

COBIT guidance for risk are provided with two perspectives: the *risk function* and the *risk management* process. The *risk function* perspective relates to the COBIT governance components that constitute the IT audit universe, as stated above (De Haes & Van Grembergen, 2015). IT audit universe, which constitutes the subject matter of an IT audit, is constructed by the assessor at the planning stage by reviewing the risks and related ICT controls selected and implemented by management. An IT auditor auditing the control environment inside-and-now is, therefore, expected to measure, to evaluate and to assess the operational control environments including the effect of the risk of inefficient coordination and weak links among the elements of the IT audit universe value chain. This will enable auditors to develop insights helpful to provide managers and directors with the assurance that their IT leadership is sufficient for the operational viability of the business and routine operational risks are reduced to an acceptably low level (Bititci et al., 2000; Ellison et al., 2008).

The 'Monitor, Evaluate and Assess', (MEA) program of the COBIT 2019 process directly relate to operational process namely;

- MEA01 Managed Performance and Conformance Monitoring
- MEA02 Managed System of Internal Control
- MEA03 Managed Compliance with External Requirements.
- MEA04 Managed Assurance.

The MEA program measures three COBIT process domains - *BAI (Build, Acquire and Implement)*; *DSS (Deliver Service and Support)* and *APO (Align, Plan and Organize)* with 31 processes. Process audit, process coordination audit and process controls audit are planned around the three domains as a systematic audit process for the operational control environments inside-and-now demonstrated in Table 5 below.

Table 5. *Functions and Processes for the audit of Process (Operations) inside-and-now (S1, S2, S3)*

No.	Routine Control (S3) Elements of risks – IT audit Universe Enablers	Objectives of Coordination (S2) IT Audit Universe	COBIT Program	Subject matter of an Audit of Operations (S1) - Reordered COBIT 2019 Processes - <i>Procedures: Measure, Evaluate and Assess (MEA):</i>
1.	Processes	<i>To understand the business model</i> – The different processes including lines of business an organization has by which it creates value presently and in the future. The degree and method of IT outsourcing in terms of significant cost savings and additional levels of risk that may bring. The objective of coordination audit, here, is to obtain satisfaction that the enterprise processes and related IT services are aligned towards the achievement of the organizational objectives.	<i>Performance and Conformance (MEA01)</i>	<ul style="list-style-type: none"> • DSS01 management of operations. and operational strategy. • DSS06 management of process controls. • BAI01 management of programs and projects. • APO05 management of portfolio. • APO06 management of budget and cost. • BAI06 management of changes.
2.	Organizational structure	<i>To understand the model of the IT function</i> – The organizational structure impacts on the IT use and user analytics models. The degree of centralization or decentralized organizational structure influences decision-making including the allocation of IT resources. Understanding the organizational structure		

		assists assurance experts to appreciate the chain of command in the organization. For efficient audit and assurance service output, the role of communication with the right persons is very critical. This enables assurance experts to interview the right persons and to communicate relevant reports to the appropriate persons to ensure confidentiality and objectivity.		<ul style="list-style-type: none"> • APO008 management of relationships. • APO11 management of Quality
3.	Service, Infrastructure and Applications	<i>To understand the supporting technologies</i> – The types of technologies, installed as well as the diversity in any level of the IT application stack, database, operating system, network infrastructure and specific application’s program code help to make functions faster, smarter and easier. The extent of customization of off-the-shelf software or the capacity to be more reliant on in-house technical support as against the support from the original vendor(s).	<i>System of Internal control, risks and security (MEA02).</i>	<ul style="list-style-type: none"> • BAI09 management of IT assets. • DSS05 management of security services. • DSS02 management of service requests and incidents. • BAI10 management of configuration of technology. • APO10 management of Suppliers.
4.	Information	<i>To understand the use of information to coordinate functions</i> - Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself. More objective and		<ul style="list-style-type: none"> • BAI03 management of IT solution identification. • BAI04 management of IT Availability and Capacity.

		reliable information fosters smooth interoperability and cohesion among functions and functional managers. The degree of <i>IT</i> operational standardization that impacts on the reliability and integrity of the IT infrastructure and related processes rely on and <i>information support</i> .		<ul style="list-style-type: none"> • APO12 management of threat and risk.
5.	Principles, Policies and Frameworks	<p><i>To understand the business model and IT strategy –</i></p> <p>The extent to which the company policies and standards defines formalized IT governance is affected by corporate culture. Operational policies are very relevant to provide functional leadership a sense of direction.</p>		<ul style="list-style-type: none"> • BAI05 management of organizational change enablement. • APO13 management of security. • DSS04 management of disaster recovery plans.
6.	Culture, Ethics and Behaviour	<p><i>To understand the laws and regulations and conduct of individuals and of the organization in relation to them –</i> Culture, ethics and behaviours are very often underestimated but are key success factors in governance and management activities. Changes in culture or general behaviour can pose a major risk to the survival of an organization over time and the need to monitor changes in culture, ethics and behaviour in critical coordination audit function.</p>	<p><i>Compliance with External requirements (MEA03).</i></p>	<ul style="list-style-type: none"> • BAI02 management of requirements definition. • APO09 management of effects of Service Agreements.

7.	People, Skills and Competence	<i>To understand the IT support processes – The extend of the organization’s reliance on the availability and functionality of different technologies in the IT universe and how they assist in creating cohesion of the day-to-day business operations including their related potential risk and impact. Auditor should familiarize and understand the IT skills and competence level of the staff in the organization.</i>		<ul style="list-style-type: none"> • APO02 management of strategy • APO007 management of Human Resource and intellectual capital. • APO04 management of innovations • BAI07 management of change acceptance and transitioning. • BAI08 staff skills and knowledge.
8	Governance System	To understand certain focused governance topics, domain or issues that may be contained in a combination of generic governance components and variants that can be addressed by a collection of governance and management objectives and their components. Examples, small and medium enterprises, cybersecurity, digital transformation, cloud computing, privacy, and DevOps.	Managed Assurance. (MEA04)	<ul style="list-style-type: none"> • DSS06 Management of Business Process Controls, • BAI11 Managed Projects, • APO14 Managed Data.

4.2.3. The Process Controls (S3) Assessment

Controls are instituted by those charged with governance and management to mitigate the effect of risks materialising. S3 deals with operational risks which are defined as a measure of the likelihood and impact of loss resulting from system failure, disruptions of business process, fraud due to failed or inadequate control policies (Buffa & Basak, 2016). Frameworks for operational risk management and theories view risk in two main lenses - Financial/Economic theory and decision theory. Financial risk theory views risk as the probability that an investment's actual returns will be adversely different from expected

returns. Financial risk may be market-dependent, and it is a function of several market factors or may be operational in nature, resulting from fraudulent and corrupt behaviours. Decision theory views risk from behavioural and organisational psychology standpoints. It explains risk in terms of behaviours which explains why some organizations are rational and others not in their risk-based decision making. Regret, therefore, plays significant role in decision theory such that risk management and risk-based decision is a function of the organization's risk attitude, appetite and tolerance (Buffa & Basak, 2016; Bakos,1991).

IT risk may not be clearly isolated from any of the risks above. IT risk can, therefore, manifest from any of the theoretical perspectives. Modern business environments are enhanced and constrained by technologies of increasing sophistication to fulfil the requirements of clients to maintain their existence and identity (Jafarov & Lewis, 2014). IT spans nearly all organisational activities and because of this IT audit often crosses department boundaries. IT use has complicated operational risk and IS auditors require a framework that deals adequately with complexity since complexity destroys complexity (Espejo, 2003). The COBIT processes that deal specifically with control of risks are *APO12, Manage Threat and Risk* for operational risks provided in MEA management processes and *EDM03, Manage Strategic Risk* for strategic risks provided in EDM under the *Ensure Risk Optimization program*. Strategic risk management assessment procedures are evaluated under Intelligence (S4) audit (see below).

Risk assessment inside-and-now under the viable systems approach must involve the inspection and evaluation of the entity's ***Risk Appetite Statement***. COSO (2009) defines ***risk Appetite*** as the degree of risk, on a broad-based level, that a company or any other organization is willing to accept in pursuit of its goals (Delta Risk LLC, 2016). The risk appetite statement describes the organization's *risk attitude* and provides the basis on which Board and Management consider strategic alternatives and the method of setting objectives as well as aligning them with the selected strategy including developing mechanisms to manage the related risks (COSO, 2009). Risk appetite statement should also include the organisation's ***risk tolerance***. Risk Tolerance is defined by COSO (2009) as an organisation's acceptable level of deviation from a set of objectives. The IT auditor has a responsibility to consider the appropriateness of the alignment of the organisation's risk appetite to its risk tolerance and how the risk attitude of management synchronises with the mission, vision and core values of the organisation (COSO, 2017).

Depending on the organization’s risk tolerance and risk appetite, an IT auditor, could proceed to perform impact analysis. *Figure J* below provides the theoretical steps and approach model for routine operational risk control analysis.

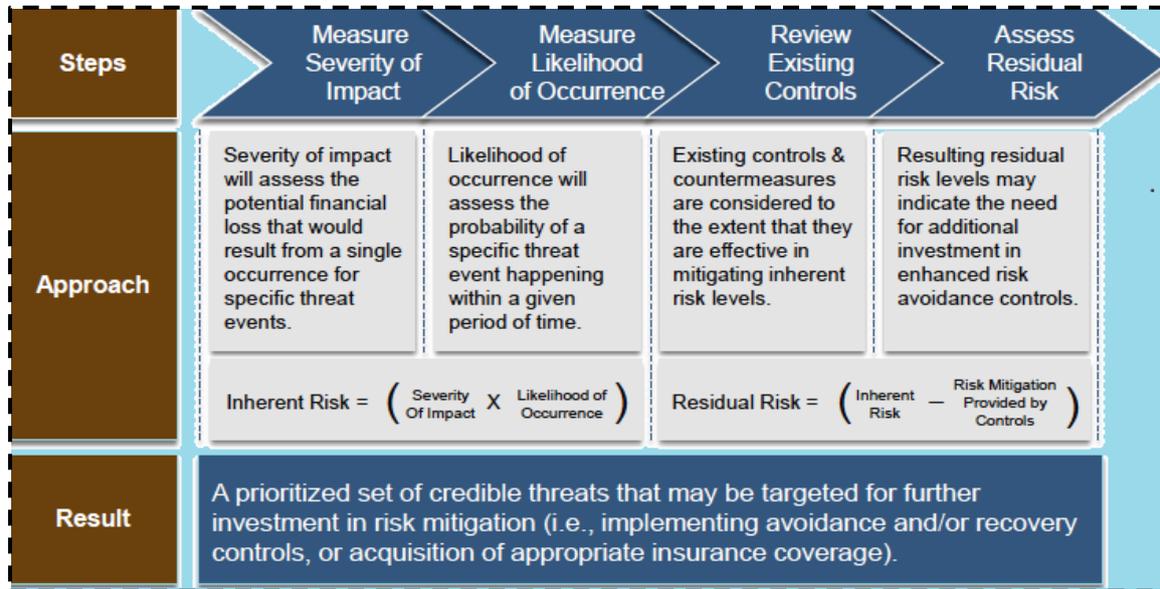


Figure J: Risk Control Model. Adapted from Protiviti Inc. (2014).

Theoretically, there are four potential responses applicable to identified risk depending on the organization’s risk appetite or risk attitude. The model for risk assessment considers the severity of impact and likelihood as the extraneous variety to be matched by the appropriateness of existing managerial controls. Risk control requires the measurement of *residual risk* relative to credible threats by considering *inherent risk*. The result could put the assessor in a more insightful position to provide management with any of the following recommendations or their combination as the organisation’s risk management strategy - ‘*Transference*’ strategy, risk ‘*Avoidance*’ strategy, risk ‘*Reduce/Mitigation*’ strategy and risk ‘*Acceptance*’ strategy, referred to as the TARA model (Kaplan Financial Ltd., 2012).

Transference of risk strategy – A third party is engaged to assume some or all the risk if the adverse event occurs. Steps typically taken to ensure risks are shared include outsourcing or obtaining insurance. Typical transference strategies include outsourcing strategy or insurance strategy. In any case the entity outsourcing or insuring remains ultimately responsible for monitoring e.g. the outsourced activity and ensuring insurance coverage is sufficient.

Avoidance of risk strategy – In an avoidance strategy, an entity refrains from engaging in the activity that has the inherent risk altogether. This strategy has been criticized for being inherently economically unadventurous since risks are unavoidable in business ventures and withdrawing from the business area completely would mean economic assets could be redundancy (Kaplan Financial Ltd., 2012).

Reduction of risk strategy - auditor may recommend for the implementation by management control activities to reduce or mitigate the risk. Because it is very expensive to eliminate risk completely and risk anticipation every possible outcome or circumstance is dodgy, generally, risk reduction strategy is recommended to the decision maker. The auditor, therefore, provides *reasonable assurance* that the chosen strategy can mitigate the risk to a point where the residual risk is acceptable and, thus, meets the entity's goals and objectives.

Acceptance of risk strategy – usually where a risk is assessed to have low likelihood of occurrence and low impact and IT auditor could advise an organization to contain it internally. However, this strategy should be carefully selected by conducting a cost/benefit analysis for either of implementing mitigating strategy or not doing so. It is an IT auditor's responsibility to check documentation to evaluate the rationale for accepting a risk (Sheehan, 2010).

4.2.3.1. Investigation (S3*) - (Fraud Risk Assessment For-cause)

One very devastating operational risk that persists in wrecking business in both the public and private sectors with less regulatory environments is the risk of fraud and corruption. For this reason, global organisations seeking to uphold best practices such as the COSO, have come out with requirements for audit and assurance providers to comply. Auditors responsibility for fraud detection, fraud risk assessment and fraud prevention have been widely debated over the years (Agrawal & Cooper, 2017; Chandler & Edwards, 2014; Knapp, 2001). Recent accounting scandals have, however, contributed to regulatory bodies and frameworks for best practices revising their notes (Agrawal & Cooper, 2017; Abugu, 2014). Fraud risk is a category of operational risk which has very damaging consequences on organizational reputation and the achievement of business objectives. As a result of the effects of fraud on business operational objectives stakeholders have shifted the paradigm of demand for audit to encapsulate fraud risk assessment. Fraud risk assessment involves procedures to obtain sufficient appropriate evidence at the planning stage and during the audit for irregularities and fraud.

The legal definition of the term fraud varies from jurisdiction to jurisdiction. However, essentially the term fraud connotes the use of deception to enrich oneself or to make personal gain dishonestly and all other illegal means of acquiring and possessing an asset to the disadvantages which has the consequence of creating a loss for another person or an entity (Wells, 2017). Common corporate and business fraud that are often encountered by auditors in course of their audit are categorised into three namely; asset misappropriation, fraudulent financial statement and corruption (Hassink, 2009). Misappropriation of funds constitutes the intentional, illegal appropriation of the funds, specifically cash and non-cash resources of another entity for one's own use or other unauthorized purpose. Fraudulent financial reporting is a deliberate misrepresentation of a firm's financial statements and other related non-financial information with the aim of giving investors a false impression about the firm's operating performance and profitability (Wilks & Zimbleman, 2004). Corruption is known in two main circumstances – bribery and extortion and conflict. Extortion belongs to a criminal offense categorized among blackmail and ransom. These offences apply the use of threats, coercion, or intimidation to obtain money, goods, or services that not is characterized by the willingness of the victim to relinquish money, goods, or services because of the threat of possible violence, force, or harm, but not the imminent danger of that harm. Bribery is form of extortion which is an intentional act of offering, giving, receiving, or soliciting things of value with consist of immediate cash, or personal favours, or anything the recipient may view as valuable in exchange for a favour from someone working in an official position such as in politics, business, sports, or public service. A conflict of interest is a quasi-criminal offence where a fiduciary puts his or her self-interest in conflict with that of the principal and obtains personal gains as a result (Hassink, 2009).

The issuance of Internal Control Updated Integrated Framework in 2013 by COSO dawned a separate mandatory requirement to perform fraud risk assessment in all audits. Principle 8 of the updated integrated control framework 2013 makes it mandatory for auditors to perform fraud risk assessment (D'Aquila & Houmes, 2014). The principle emphasizes that evidence of fraud, corruption, misconduct and irregularities can have significant impact on the enterprise's ability to achieve its identified objectives and fraudulent reporting at e.g., subsidiary, division, operating unit and functional levels must be considered to avert possible loss of assets (Martinez, 2014). Since operational risk is a subset of risk management,

auditors often argue that fraud risk is, therefore, the responsibility of those charged with governance and management (Cassidy, 2016).

Petersen (2015) provides fraud risk assessment from two main procedural lenses - *procedures to detect or discover threats and their associated risks* and *procedures to respond to assessed risks*. Demonstration of a mandatory fraud risk assessment as a sub-auditing system which may likely lead to expert witnessing is provided in subsystem S3*. **Figure K** below provides proposed guidance for evidence collection and expert witnessing based on guidance by COSO (2016) for fraud risk assessment.

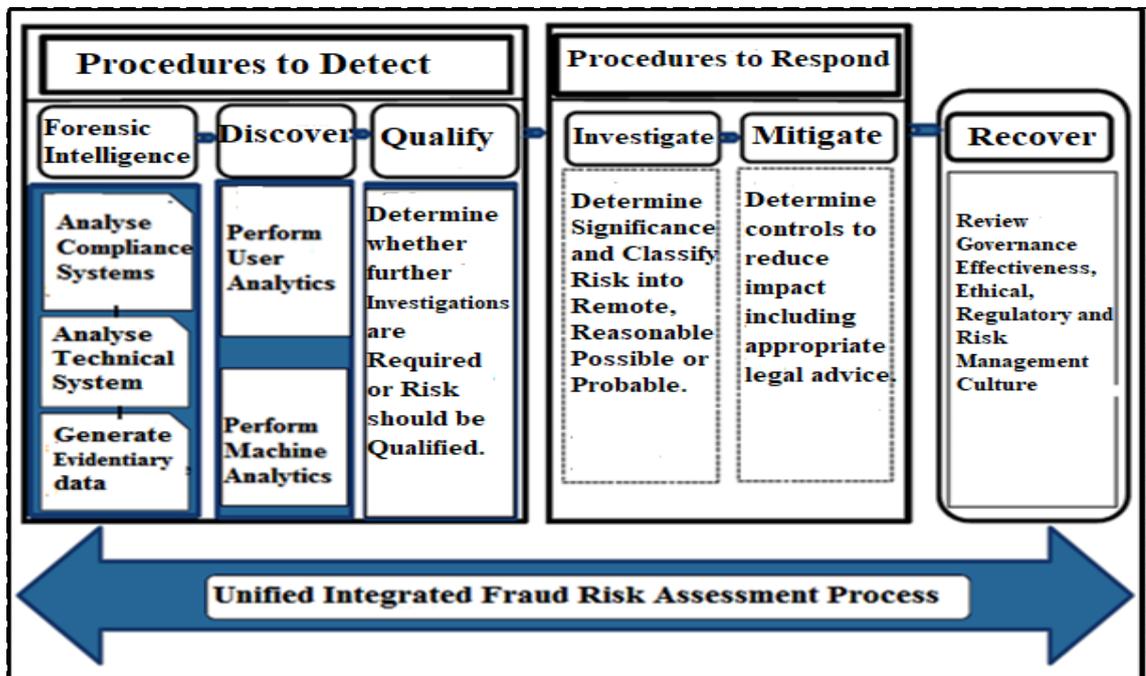


Figure K. Evidence Collection model and guidance for expert witnessing.

4.2.3.2. Demonstration of model

Information Systems auditors are expected to plan their assessments with in-built fraud risk assessment system that provides prompts for additional procedures in fraud risk assessment. This involves 1. Procedures to detect, 2. Procedures to respond and 3. Procedures to recover.

4.2.3.3. Procedures to Detect

The controversy over whether the auditor has a responsibility to detect fraud is now settled with the COSO's Fraud Risk Assessment framework. All audits after 2014 complying with the COSO's best practice have the obligation to perform inherent fraud risk assessment procedures with the aim to detect fraud (D'Aquila & Houmes, 2014). Inherent fraud risk are

risks that material fraud risks are present before management takes action. The assessor should understand the fraud risks a specific client is vulnerable to. This involves fraud risk profiling – the understanding the client’s business processes and the gathering information about the propensity for fraud from internal and external sources (Petersen, 2015). Motivated by the policeman theory, an Information Systems Auditors is expected to keep track of irregularities when planning the collection of audit evidence to detect and prevent fraud timeously. This should be facilitated by a recursive or continuous process and not a one-off yearly event. Continuity denotes continuous monitoring and continuous auditing. Continuous monitoring enables management to review their businesses and processes for the purposes of self-adjustments and self-regulation. Continuous auditing has gain importance within experts for its ability to continually gather data on business processes that support investigations. Monitoring and Auditing should be technology-driven involving automating repetitive tasks e.g. checking errors and verifying violation of controls on real-time basis. This procedure is likely to produce triggers for forensic intelligence profiling of irregularities, procedure to discover and procedure to modify or qualify preliminary evidentiary reports.

ii. Forensic intelligence or events profiling

Forensic data is the mass of information that is generated by an organization for detecting, deterring and preventing fraud, waste and abuse (Chou, 2015). Forensic intelligence profiling involves the review of confidential and the competent handling of the resulting evidentiary data to assess how the organization is effectively managing its fraud risks. COSO (2016) emphasizes on fraud risk intelligence profiling as an act of interviewing, leveraging, brainstorming or resulting from analytical procedures professional scepticism and professional judgment to discern events and issues that constitute triggers for fraud risk investigations. Professional scepticism has been defined by ICAEW (2013) as an attitude that includes a questioning mind, being alert to conditions which may indicate possible misstatement due to error or fraud, and a critical assessment of audit evidence. Professional Judgement is an integral part of professional scepticism which refers to decision on what issues should considered material which require investigation (Rittenberg, 2013). Forensic intelligence is, therefore, purported to *discover* through brainstorming evidentiary materials and incidents that, in the assessor’s opinion constitute material fraud risk issue as a single

event or a series of events in aggregate. Fraud risks typically applicable include: i. incentives, pressures and opportunities to commit fraud ii. risk of management override of controls (or intervention) iii. population of fraud risks iv. risk of regulatory and legal misconduct v. risk to information technology (Kinney, 2003; ISA 240; SAS 99). The above types of fraud risks are categorised into 1. *Compliance based* fraud risk and 2. *Technical* fraud risk (Petersen, 2015; Murphy, 2015).

Compliance base risk - These include policies, rules, regulations, technical security policies, inconsistencies, distortions, inappropriate inclusion or exclusion of information etc. (Kinney (2003). The *Monitoring activities* component of COSO's fraud risk assessment guidelines (2016) provides two principles which states that the assessor should select, develop and perform ongoing evaluations to ascertain whether compliance or technical control measures are present and functioning and to communicate Fraud Risk Management Program deficiencies in a timely manner to responsible parties who include senior management and the board of directors to take corrective action. Forensic intelligence has been defined as a set of information or events that trigger sufficient suspicion for the performance of investigative procedures in pursuance of evidence for further actions which include criminal or civil legal proceeding and other control responses (Ribaux et al., 2006).

Compliance theory developed by Etzioni (1975, 1997) provides a framework by which an IS/IT auditor can determine why organizational actors may fail to comply with regulations and internal controls. Compliance theory states that the failure or achievement of compliance, first, depends on three types of power or degree of influence an actor should induce another to carry out directive or any set of regulations or norms. According to the compliance theory by Etzioni (1997) the form that power takes can be any or combination of: *coercive*, *utilitarian (remunerative)*, or *normative*. Coercive power relates to the application of force and fear to get target participants to comply. Utilitarian/remunerative power uses extrinsic reward systems such as better working conditions, improved salary, merit pay, fringe benefits or job security to entice target participants to comply. Normative power states that target participants do comply because of explicit and instrumental calculations of how the consequences of the behaviours they have available will influence their interests (Mitchell, 2007). Lunenburg (2013) argues, additionally, that any of the above powers will fail to achieve compliance if the target participants are deprived of involvement in the compliance system. Participants involvement is categorized into any of *alienative*,

calculative or *moral* (Etzioni, 1997). ‘Alienative’ involvement negatively orientate participants to the compliance system including the power wielding actor. In ‘Calculative involvement’, participants are either negatively or positively orientated to the compliance system at low intensity. ‘Moral’ involvement highly intensively orientate participants positively to the compliance system (Lunenburg, 2013). Etzioni (1997) applies psychological principles to argue that when an organization employs coercive power with alienative involvement, participants usually react to the organization with hostility e.g., fear and other coercive measures, usually create high-degree of alienation and high compliance failure is the result. Utilitarian/remunerative power typically relates closely to calculative involvement and consideration for compliance with regulations vary with participants’ personal interests. Normative power normally creates moral involvement. It has an embedded participatory management system and therefore invokes intrinsic commitment. The result is high degree of Compliance because participants’ social benefits are featured in the compliance reward system (Etzioni, 1997). In relation to compliance audit, the IS auditor shall consider causes of compliance failure that relate to internal control and coordination failures tracing them to the bigger problem that relates to the appropriateness of the theoretical underpinnings of compliance given the business environment.

Technical based fraud risk – this is the type of inherent risk to information technology processes and instances of or risk of management override of controls or interventions. Typically, evidentiary data are profiled from computer systems itself, such as, logged events in the active directory for analysis for substantiating non-compliance and fraud risk. A primary goal of machine analytics is to proactively obtain insights through the examination of deviations and to detect anomalies from an established point of reference. The technical analysis process requires sampling evidence of threats from computers and digital storage media systems for further analysis. Management overrides of controls may include breaches of access restrictions to hardware and software and suspicious security overrides (Jafari, 2017).

Evidentiary data

Evidence is the conceptual foundation of auditing theory (Toba, 1975). Generation of evidentiary data involves any activity which takes place after the fraud risk assessment process has identified instances and events which serve as triggers to commence investigations (Holmes, 2018). These instances include allegations of fraud, non-compliance

with existing regulations, logical and physical internal controls. The objective is to obtain sufficiently reliable proof to corroborate the assessor's professional scepticism or professional judgement. Sources of evidentiary data include 1. Interviewing neutral third-party witnesses, accessories to the principal suspect and the suspect, 2. Documentary evidence profiling such as personal files, phone and other mobile electronic device records, computer log files, email, financial transactions, security camera video, if any, physical access control bypasses and any other data held by a third party that may be relevant. Since evidence serves as a form of proof of offence, it is subject to various legal tests by attorneys, advocates or lawyers in court. It is very important for auditors assessing fraud risks to consider the value in terms of admissibility and weight of evidence since discovered fraud may end up in court and may be required to provide testimony (Faigman, 2017).

Evidence for fraud is subject to legal admissibility tests in criminal law. Auditors should be meticulous about its quality (Hamer, 2018). The quality of evidence is integral to the admissibility of same in a legal action. The admissibility of electronic evidence depends on the jurisdiction. Electronic evidence such as system log activity files have the same weight as paper-based ones although tweets, text messages and social media chats still struggle to wean itself from the hardly admissible hearsay evidence category (Goode, 2009). Computer animation or simulation, though may be persuasive, has proved to be problematic in its acceptability as it cannot replace the oral tradition in legal practice in many jurisdictions. The admissibility of evidence extracted will depend on the statutory provisions of the jurisdiction concerned. In many jurisdictions, electronic evidence is given the same weight and status as paper-based and others do not. Auditors may seek legal advice to proceed (Hamer, 2018; Faigman, 2017).

iii. Procedures to Discover

Dada et al. (2013) argue that for audit to make any impact in less regulatory environments, the emphasis should be on fraud risk and forensic investigations. Contemporary auditing approach should be such that material fraud risk can be detected, prevented and deterred (Peter et al., 2014; Chandler & Edwards, 2014; Murphy, 2015). Two principal types of analytics may be triggered from the evidentiary data collected to discover the cause of an irregularity which conduces to the prevention of future occurrence. These are **a. user analytics** and **b. machine analytics** (Petersen, 2015).

A. User Analytics

User analytics iterates back to compliance systems analysis. Compliance failures are important to IT auditors since failures lead to staggering costs (Ernst & Young, 2013). Compliance analytics relates to “person-based” or user analysis for causes of irregularity and fraud. Contemporary fraud theory originates from the work by Cressey (1953) known as the Fraud Triangle. The Fraud Triangle has defied criticisms such as dwelling excessively on individual intrinsic factors and placing little emphasis on the social and organizational contribution to fraud to emerge as the framework for spotting fraud (Huber, 2016). According to the Fraud theory by Cressey (1953), there are three factors constituting high fraud risk situations. These are the *Pressure* theory, the *Opportunity* theory and the *Rationalisation* theory. The Pressure theory states that people are inclined to commit fraud where they face debt problems that emanate from circumstances such as overwhelming medical bills, gambling debts or alcohol or drug addiction. Pressure can also emerge from where staff feel undermined, unjustly treated and under job security threat. Craving for ostentatious lifestyle and greed can also constitute pressure, but it usually needs to be associated with injustice. The Opportunity theory argues that there is high propensity to commit fraud where people are given unchecked chances to do so. An example is where people know that due to high level of weak internal controls and vulnerabilities there is little or no chance of being caught and punished. The Rationalisation theory states that where people have the mind-set to justify their unethical and fraudulent behaviours with ignorance of the law, rules and regulations, they are inclined to commit fraud. The Fraud Triangle is particularly important as a model for assessing the risk of fraud and contemporary fraud thinkers such as Dorminey et al. (2012) argue that it is only one component of an overall audit risk assessment plan.

B. Machine analytics

Machine analytics iterates back to technical analysis. Machine analytics are typically “computer-based” which can be used proactively to seek opportunities to prevent and detect fraud, waste and abuse by leveraging information in corporate data assets. This may include the capture of active directory log files *and sensor data* to examine for actionable insights

into potentially damaging threats and their associated risks. The primary function of machine analytics is either first, to detect threats or second to prioritize threats detected. If something irregular is detected in the process, e.g. repeated logon failures, analytics process seeks to discover who did it and why (Beland et al., 2014). A broad range of artificial intelligence and computer technologies are currently being applied by IT auditors in technology-intensive work environments to produce reliable and repeatable results to support continuous fraud risk assessment (Chan & Vasarhelyi, 2011). Massive volumes of data now available inside and outside companies, due to information technology, now makes new data analytics technologies a fundamental trend changing the nature of audit. Recent ‘big data’ technological advancements and analytics are providing an opportunity to rethink the way in which an audit is executed. The problem in less developed regulatory environments for IS audit professionals, however, continues to be with the lack of efficient technology solutions for data capture and concerns for privacy interference (Marques, 2017).

iv. Procedures to Qualify/modify

Procedures to qualify concerns procedures that the auditor shall perform to ascertain whether to pursue a fraud risk issue or an event further or terminate it. COSO’s fraud risk assessment guidelines (2016) – *Information and Communication* component of the COSO’s fraud risk assessment guide, made of three principles provides that an assurance professional is to establish a communication process to obtain information about other potential fraud that may be linked to the discovery and to deploy a coordinated approach to initialize corrective actions (Toba, 1975). This process coincides with procedures to modify or qualify the assessment process which completes the iteration of procedures to detect. Qualification means either the event contains present risk and will require further analysis or threat does not contain present risk, it is a false positive and must be ignored. Since actual threats may be missed or false positives may send Audit teams on wild a chase, qualification or modification must be done with due care and due diligence (Petersen, 2015).

4.2.3.4. Procedure to Respond

An effective fraud risk management assessment should not only obtain prompts of fraud in the system but also it should actively identify where fraud has occurred, may occur, the chances of recurring and who the perpetrators might be in order to find a competent mitigation measures to the problem. Procedure to respond to an assessed fraud risk by an IS

assurance professional are, therefore, in two stage main stages – *procedure to investigate* and *procedure to mitigate*. Procedure to respond to assessed fraud risk is, therefore, purported to determine and formulate propositions to mitigate the effect of the expected adverse outcome (Petersen, 2015).

i. Procedure to Investigate

Procedure to perform full investigation into an assessed fraud risk is occasion by ascertaining that an actual threat of fraud exists after the initial technical and compliance intelligence profiling on fraud risks. To proceed the assessor should be satisfied that there is sufficient proof of any or a combination of motivation, opportunity and rationalisation for fraud (Dorminey et al., 2012). COSO’s fraud risk assessment guideline (2016) - *Risk Assessment* component comprises four principles requiring assurance professionals to perform comprehensive fraud investigation to identify the specific fraud schemes and risks, assess their frequency, future likelihood and significance. The ultimate objective of this exercise is to determine if the fraud risk has crystallised with chances of it recurring or it is one-off. The impact of the assessed event on the organization must be determined (Plan, 2014). The matrix (*Figure L*) below provides heuristic method on the determination of the materiality, impact and future risk of occurrence.

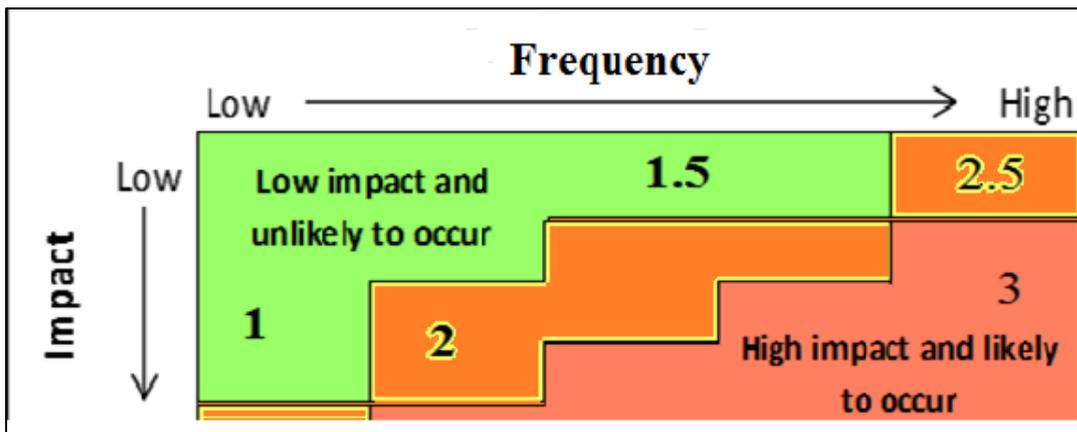


Figure L. – Frequency-Impact Fraud Risk Assessment Matrix - Adapted from Plan (2014).

Materiality of the impact depends on the ranking attributed to the assessed fraud risk. Frequency of occurrence is a function of likelihood and, depending on the organization’s risk tolerance. Risks may be ranked e.g. very High (3) if the impact is high and frequency and likelihood also high (Sheehan, 2010). Where a fraud risk is ranked in the (2) zone, the risk is deemed to be moderate with moderate impact and medium to low frequency. If the

materiality of the impact and frequency are low, fraud risks are ranked in (1) zone although some fraud risks can also be classified with low impact with moderate level of frequency as in (1.5) in the grid. Other risks can also have high likelihood and high frequency but low material impact on the organization and such are ranked in (2.5) zone. Procedure to investigate serves as the lead to an exhaustive evaluation existing fraud control activity and the appropriate actions to be implemented to mitigate residual fraud risks.

ii. Procedure to Mitigate

COSO's fraud risk assessment guidelines (2016) – *Control Activities* component provides a set of mitigation measures that the assessor may recommend for the assessed fraud risk. The assurance provider or IS auditor may select, develops and recommend the deployment of appropriate preventive, deterrent and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner. The guidelines provide five principles that are geared towards enhancing the control environment and these are additional measures that can lead towards ensuring significant change. These involve ensuring that:

1. Staff demonstrate commitment to integrity and ethical values,
2. There is an oversight responsibility which is appropriately exercised,
3. There are well established structure, authority and responsibility,
4. Staff commitment to competence is demonstrated and
5. Appropriate separation of duties implemented, and accountability are enforced.

4.2.3.5. Procedures Recover

Recovery is a post-mitigation procedure aimed at cleaning up 'the mess' and to ensure that management can adopt mechanisms to detect, deter and prevent future occurrence of fraud. The *Control Environment* component of the COSO's fraud risk assessment guidelines (2016) provides five principles to serve as the procedures to recover. Control Environment component of the guidelines requires of assurance professionals to establish and communicate a Fraud Risk Management Programs that demonstrate the expectations of the client's Board of Directors and Senior Management and their commitment to high integrity and ethical values regarding managing fraud risk.

Such procedures include the full eradication of the threat from the operational environment, cleaning up any damage done, performing any required incident/ breach notifications, and

performing root cause analysis to learn from the incident to prevent it from happening again. Options available to the auditor include whistle-blowing to the law enforcement agencies of the State or to demand management action otherwise risk qualified audit opinion based on fraud (Chan & Vasarhelyi, 2011). Additional procedures should involve identifying and analysing residual risks and significant change due to the fraud risk and recommending the setting of the proper tone which the assurance for management action. Other recovery measures include three key areas namely; fraud awareness training to members of staff, organizing workshops on the code of conduct to relevant teams and formulating appropriate anti-fraud policies.

More guidance on auditor's responsibility with regards to fraud and non-compliance prevention, deterring and detection, criminal concerns including management responsibilities and penalization of offenders can be obtained from the Sarbanes Oxley Act 2002 of the USA who have taken steps to legitimize the auditor's responsibility for fraud risk assessment through legislation. IT audit professionals must, however, strictly comply with required ethical standards of *independence, objectivity, integrity, confidentiality, competence and professionalism* espoused in the SOX (2002). Otherwise, the planning and execution of effective fraud risk assessment shall be compromised, and auditors will continue to fail functions to achieve the overall control objectives and outcomes of the menace of fraud in less regulatory environments (Osei-Afoakwa, 2013; Wessels, 2005).

4.2.4. Organisational Process Intelligent (S4) Assessment

Intelligence has been referred to as total risk environment. Total risk environments audit forms the basis of risk assessment 'outside-and-then' (Álvarez-Molina et al., 2014). An Intelligent audit is defined to be an assessment of IT control environments that remain beyond S3-S2-S1. Complexity has become a key issue in contemporary auditing. In the face of an increasing use of IT in business, the traditional centralized approach to risk assessment and control is no longer viable. There are increasing changing interconnections including cause-effect relationships that are defining a new requirement to approach IT auditing. The sources of the complexity can be either technical or environmental or both. The issue of complexity and its effects on audit have become an ongoing debate among stakeholders because of its tendency to increase audit risks and failure exposures. It is these new contextual conditions that triggered the belief, in this research, that both IT audit

practitioners and management in less regulatory environments need a new paradigm of conceptual thinking of auditing. IT presents unique risk factors all areas of business process value chain that are rely on IT support systems to function such as accounting, management systems and, more emphatically, auditing. IT risk factors range from general systems-related issues, for example, systems development, change management and resulting vulnerabilities to other technology-specific factors. The chances are that an audit would lead to the issuance irrelevant or inappropriate reports and opinion because the increased risks. In financial auditing audit risks (AR) arise in the form of inherent risk (IR), control risk (CR) and detection risk (DR). Thus, audit risk (AR) is measured as the product of IR, CR and DR). i.e. $AR = IR \times CR \times DR$ (Karagiorgos et al., 2007). The categorization of the constituents of audit risk, although may be subject to judgement, is aimed at ensuring that requisite controls are put in place. In systems-based auditing, however, Audit risks (AR) arise as a product of Primary Risk (PR), Residual Risks (RR) and Secondary Risk (SR). Primary risk (PR) of IT auditing has been proffered by Singleton (2014) to be predominantly in the form of Inherent Risks. These are risks resulting from circumstances in which transactions and processes are complex due to IT sophistication rather than a control failure which could lead to errors or omissions and exposure to audit failure. Residual risks inherent in systems-based approach to auditing is the product of control and detection risks. Thus, these are the chances that due to the complexity management controls may be flawed or inadequate enough to sufficiently deal with the systemic risks, however, IT auditing is unable to detect it at all or in a timeous manner due to lack of the know-how to identify these issues or communicate it in an exaggeration fashion leading to inappropriate consequences. Secondary risks inherent in IT auditing is the possibility that because of sophisticated business processes and relationships, the consequences of applied controls or solutions in one unit of business processes may have current or future internal or external relationships impact on other units with compromising effect on the viability of organization as a single unified whole. The modified risk assessment model for systems-based auditing, therefore, is $AR = PR \times RR \times SR$; where AR = Audit Risk, PR = Primary Risk, RR = Residual Risk and SR = Secondary Risk. The higher the IT Sophistication the higher the IT audit risks. The IT audit framework qualities that are capable to match the circumstance is the concept of adaptive control.

In a highly uncertain environment, shareholders, regulators, rating agencies and other stakeholders' expectation is that those charged with governance and management will focus

their risk management processes on creating value as well as protecting value (Carvalho & Esteban-Navarro, 2016). Directors and Executives are also realizing the increase in demand for the use of contemporary technologies to improve on performance as well as hone stakeholder transparency in their management processes. It is, however, virtually impossible for an auditor to be knowledgeable in every current or emergent technology. An intelligent IT audit framework is determined by the way it provides guidance for the application of the flux of information and knowledge-bases to manage risks and uncertainties affected by internal and external events or scenarios resulting from the changes (Hitchins, 2015).

The need for intelligence audit has arisen due to the demand for auditors to provide assurance on executive functions including executive decisions and strategic choices necessary for the continuous adaptation of an organization to the environmental changes (DeFond & Zhang, 2014; Svata, 2011). An intelligent IT audit framework is determined by the way it confronts and adapts to the environment or serves as a catalyst for the achievement of competitive advantage by applying the flux of information and knowledge-bases to timeously inform Directors and Managers to deal with environmental risks and uncertainties. Principle 9 of the COSO's Updated Control framework (2013) - *Identifying and analysing significant change* requires of auditors to perform analytics to identify critical environmental changes affecting company's business lines of operations, external operations, new technologies, awareness creation, as well as changes in company philosophy and leadership following a successfully discovery of an irregularity in course of the audit of the internal control environments (S2/S3 and S3*) (COSO, 2013;2017).

A common technique used to evaluate business intelligence is the SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis. COBIT Implementation uses the SWOT analysis to provide a detailed guidance on "recognizing pain points and trigger events" as well as an understanding of the important aspects of formulating the business strategy in the stakeholder involvement section of the program (Shahid, 2014). ITIL V3 also uses the SWOT analysis technique to stimulate the capturing of stakeholder needs, identify *critical success factors* (CSF) and to challenge the applicability of stakeholder needs and to determine the desired service strategies for implementation (Li, 2017). The SWOT technique produces an excellent tool for governance level intelligence variety engineering. Table 6 below demonstrates the proposed approach to auditing an organizational intelligence function.

Table 6. Intelligence auditing

Auditing Intelligence (S4) based on the SWOT matrix					
Significant External Environmental Change Analyses			Critical Strategic Success factors (Governance Variety Amplifiers)		
Digital Transformation	Threats/Opportunities – External IT Operational Risks	Emerging Technologies	Weaknesses/Strengths	Boards and executive IT support adequacy and leadership	Governance and Management (Strategic risks) Assessment
		<ul style="list-style-type: none"> • <i>Social Media</i> • <i>Mobility</i> • <i>Cloud (XaaS)</i> • <i>Internet of Things (IoT)</i> • <i>Cyber-security</i> • <i>Big Data</i> 		Assessment Criteria - Monitor, Evaluate and Communicate: <ul style="list-style-type: none"> i. <i>Governance framework setting and maintenance.</i> ii. <i>Benefit and value delivery.</i> iii. <i>Strategic risk management.</i> iv. <i>Strategic resource management.</i> v. <i>Stakeholder Transparency</i> 	
Business Intelligence Assurance					

Digital Transformation and Intelligence analytics and audit – Emerging technologies enable business innovation and opportunities and they can pose significant threat to the business operational viability. These technologies are increasing at a faster rate and complexity than companies in developing economies can adapt and as a result companies have realized they must be cautious with them in the last few years. Yet, investment portfolios are now being expanded to keep up with emerging technology trends or to master costly legacy issues (Avram, 2014). Agranovich (2017) identifies six key areas driving the digital transformation as the Social Media, Mobile Technologies (Mobility), the Cloud, the Internet of Things (IoT), Cyber-security and the Big Data.

A. Social Media

The social media elements of IT generate business opportunity for companies to extend their brands. It has a great risk to also damage reputation and impair value to the organization.

Therefore, Social Media platforms have become high threat and great opportunity for businesses at the same time. For IT audit to make an impact an Intelligent Assurance must be designed to evaluate policies and procedures in place to manage social media and associated risks within the organization (Ernst & Young, 2013).

B. Mobility

Although mobile operations have gone mainstream, organizations in less developed economies still have outstanding needs. These include untapped opportunities associated with this technology together with its security threats and issues involving outsources and Service Level Agreements since, often, companies lack the in-house resources to exploit the full potential of the technology. With the increase in mobile device capabilities and subsequent consumer adoption, companies are shifting to mobile workforce to adapt to the changes in business environment. These devices and programs such as ‘Bring Your Own Device/Anything’ (BYOD/X) etc. have become an integral part of how people accomplish tasks, both at work and in their personal lives (Tanimoto et al., 2016). Intelligent IT audit concerns include the increasing complexity in assuring business executives of the existence of proper mobile device configuration and reviews, trusted clients, supporting network architecture, sufficient policy implementation, appropriate management of lost or stolen devices, as well as identification of vulnerability through network accessibility and policy configuration.

C. Cloud

To reduce cost and obtain cost advantage as well as to increase operational flexibility and generate a competitive advantage, companies are shifting from maintaining complex internal IT infrastructures and adapting to change to cloud computing initiatives to increase the effectiveness of in-house IT operations. Businesses are earning superior competitive advantages such as rapid deployment, diversification and location, improved security, decreased workload and efficient disaster recovery from cloud technology as service. The cloud, therefore, is very intricate concept covering broad spectrum of online services level agreements (SLAs) which is represented in IT parlance as ‘Anything as a Service’– (XaaS), where ‘X’ is used to stand for ‘Anything’ e.g. Software, Platform, Infrastructure and others (Agranovich, 2017). The complexity of the technology and the legal implications about service agreements create environmental concerns. IT auditors are expected by Boards and

Management to provide them with reports and guidance on the efficiency of SLAs and service availability, problems with control, updates and data ownership, guaranteeing user security passage and auditability and insufficient policy or its enforcement.

D. Big Data, IoT, Cyber-Security

As the volume of structured and unstructured data collected and analysed by organizations increases it is anticipated that IS/IT audit practitioners would apply more analytical skills to complement to amplify their risk perception capacity, professional scepticism and professional judgement and to attenuate audit risks to the practice (Agranovich, 2017). Persico (2016) posits that 'Big data' analysis, data migration, statistical modelling and IT security are all becoming increasingly commonly required skills among auditors. Technologies, moreover, are creating platforms for strategies and tactics that harness emerging and ongoing shifts in what people value and the behaviours they adopt to realize those values. Internet of Things (IoT) technologies, however, poke holes in security and hard fraud perpetrated by organized crime rings is growing globally threatening the realization of value of this value. Indeed, the IT audit of the future will require expertise in risk analysis; qualitative and quantitative skills to challenge predictive models; and understanding of risks beyond the "inside and now" to include business environmental issues such as regulatory, fraud, cybersecurity, industry knowledge and sector specialization (Agranovich, 2017).

IT Audit practitioners should know that under circumstances like this, information, awareness creation, training, education and re-education is the most recommended management variety amplifiers. Here, ignorance is lethal variety attenuator. Amplifying security awareness training programs is pivotal governance variety for an organization's security posture but it is only possible with adequate support and involvement of policy and decision makers (Tanimoto et al., 2016). Significant external environmental scanning and analyses are required as a responsibility of intelligent assurance to identify the risks the expanded use of these technologies pose to the organization's future and to provide confidence to business executives that high-risk areas are under control (Agranovich, 2017).

Compliance - With IT risk profile and threat landscape rapidly changing more than ever before, requirements relating to e.g. complex service agreements, contracts and third-party relation that must do with business change, regulations and information security has become one of the common high-risk areas from the IT environments that those charged with governance want intelligent IT auditing to provide assurance. Compliance risk monitoring

and review has been given full discussion under subsystem S3* - monitoring and investigation. ISO/IEC 27001:2013 provides more guidance on the specific requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization for S3 and S4.

4.2.4.1. Assessment of Strategic Risk and Critical Success Factors

Governance and Management Assessment – Where the entity’ operational IT system controls have been evaluated, one thing that could still inhibit an organization’s ability to implement the requisite change that needs further assessment is adequacy of Boards and Executive involvement support and the manner that they make strategic choices with the goal to create and protect shareholder and stakeholder value. An intelligent assessment monitors, evaluates and communicates to those charged with governance and management all the information relevant relating to the strengths, opportunities, weaknesses and threats in the organization’s *IT universe* that goes beyond sub-system S2 including the environmental risks beyond the scope of subsystem S1 processes.

IT auditors are to evaluate and communicate the adequacy of Boards and executive involvement in IT programs since inadequate or lack of leadership is a signal of the risk that the entity’s IT function is direction-less and, therefore, value and business needs are not being served (Cassidy, 2016). This assessment is in keeping with *Information, Communication and Reporting* principle of COSO’s new Enterprise Risk Management (ERM) – Integrating with Strategy and Performance (COSO, 2016). Although the proper degree of board involvement in e.g. ICT issues depends on many factors, there are four key areas according to Delta Risk LLC (2016) that an IS auditor should ensure that boards show leadership in. First, training; Directors themselves should receive training on ICT issues that are appropriate to their level and role. Secondly, Directors should incorporate ICT issues into their Statement of Risk Appetite for the organization. Thirdly Directors should demonstrate a drive to implement ICT risk management program - vulnerability assessments, predictive threat models, monitoring, detection and reporting that integrate with the institution’s broader enterprise risk management (ERM), e.g. financial risk, market risk, liquidity risk, credit risk, compliance risk and other operational risks (e.g., fraud, litigation, reporting, safety, physical security). Fourthly, Directors should foster an information security culture and increase staff awareness and training throughout the

institution. The COBIT audit program that provides a comprehensive value-driven strategic risk assessment and assurance approach which is the 'Evaluate, Direct and Monitor' (EDM).

The following functions of those charged with Governance and Management are involved:

- i. Governance framework setting and maintenance* - Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. This is to ascertain that governance creates the environment for culture development pertaining to ethical values, desired behaviours, and understanding of risk in the entity. These cultures include IT acquisition, programs change, compliance with legal and regulatory requirements including training and awareness creation of risks of the technological environments such as social media and associated risks as a governance approach (COSO, 2017). 'Intelligent' IT auditing framework must assess and confirm what contingency plans exist, e.g. in case of the Cloud services, any failure, liability agreements, extended support, and the inclusion of other terms and conditions as part of the service contracts (SLAs), as well as availability, incident, and capacity management and scalability (Avram, 2014). The IT auditor should confirm exceptions in governance framework and maintenance assessment and the transparency of their IT-related decisions for discussions with those charged with governance to effectively adapt to the environment.
- ii. Benefit and value delivery* - Assurance provider should determine whether information from the environment enables the creation of reliable and accurate picture of costs and the likely benefits provided so that business needs are supported in a cost-efficient manner to ensure optimal value. This may include the assessment of how management's IT-enabled initiatives, services and assets, e.g. Mobile technologies, are secured and whether the company is creating a vision of a modern company with web technologies such as social media and whether these technologies employed are enhancing business reputation and customer relationships or there is evidence that they are causing damage (Agranovich, 2017).
- iii. Strategic risk assessment* - Assure provider iterates back to procedures at S3 (Control) to leverage this S4 (Intelligence) procedure to determine if stakeholders' IT-related enterprise risk does not exceed their enterprise's risk appetite and risk tolerance (Sheehan, 2010). Its other objective is to provide assurance that the impact of IT risk to enterprise

value is identified and managed and potential compliance failures are minimized (Deloitte & Touche LLP, Curtis & Carey, 2012).

- iv. ***Strategic resource management*** – The assessor should determine if the flux of information (knowledge) available to management is enabling an increased likelihood of benefit realization and readiness for future change. This assessment is for the provision of the assurance that the resource needs of the enterprise are met in the optimal manner, e.g. in case of Big Data, how IT provides sufficient in-house capabilities development, knowledge management or staff/customer development, retention and motivation (Carvalho & Esteban-Navarro, 2016). Additionally, the assessment of an intelligent organization evaluates how IT costs are optimized (Agranovich, 2017). The assessor examines, also, how IT programs promote the identification and efficient management and security of tangible and intangible IT assets, core competencies or product and service differentiation.
- v. ***Stakeholder Transparency*** – The assessors should provide assurance that IT-related objectives and strategies are confirmed to be in line with the enterprise's strategy and it enables effective and timely communication to stakeholders. Intelligent IS auditing (S4) must raise the awareness of businesses to the needs to know how each new technology affects change management and the organization's security defences. Moreover, IT security demands specific tools, training, and variety of administrative and staff controls to keep enterprise and customer data safe. This includes business continuity planning (BCP) and comprehensive contingency planning.

Intelligence (S4) is the staging post to Policy (S5). There is constant loop S4 between S5 to ensure that the output of Intelligent (S4) Audit serves as a solid and logical springboard for Policy (S5) Evaluation input to help the IT auditor to assess the suitability and stability of governance performance (COSO, 2017). Therefore, an Intelligent Audit does not occur in isolation. An intelligence assessment essentially conduces to monitoring and evaluation of actions of those charged with governance that amplify improvement and actions towards stabilisation (*homeostasis*) and attenuate finite disturbances. The assessors should direct assessment to corporate IT policy (S5) governance framework redesign to drive the organization's capacity to shift from current state of organizational equilibrium to a requisite state of equilibrium.

4.2.5. Policy (S5) Assessment Process

Policy is a set of principles, rules, and guidelines constituting directions adopted by an organization management to ensure a smooth process of change by which an organization becomes better suited to its environment (Espejo & Gill 1997). Policy audit is, therefore, directed to evaluating the effectiveness of how Boards and Executives deploy strategic policies to ensure the organization maintains stability especially in the turbulent environments and the future that affect the organization (Cassidy, 2016). Strategy or Policy have become one of slippery and controversial areas of contemporary auditing (Van Grembergen & De Haes, 2018; IIA & KPMG, 2015). A policy-related audit, in comparison with more common audit types such as operational audit and financial audit, is not seen as a distinct type or autonomous unit of IT audit. While some IT auditors consider it as the starting point for each audit, others view policy audit as part of the process of regular operational audits (Gregg, 2007). A third group consider labelling audits by types rather than by topics to provide assurance on all relevant risk does not always seem to do justice to the complexity (IIA & KPMG, 2015).

Boards and executive are responsible for policy direction. ISACA clarifies the objectives of corporate IT policy as a measure aimed at proper governance framework setting and maintenance, risk optimization, resource optimization, benefit and value realization and stakeholder transparency (De Haes & Van Grembergen, 2015). Strategic policy management has three phases, namely; policy formulation, policy implementation and control and policy evaluation (Alkhafaji, 2011). According IIA and KPGM (2015), Policy auditing process can, therefore, relate to the following processes:

- ***Policy formulation process audit*** – Assessing the quality and strategic content of the strategy formulation process.
- ***Policy implementation and control process audit*** – Assessing the degree to which the policy is successfully translated into strategies, goals, objectives and performance targets and implemented at all levels of management hierarchy.
- ***Policy evaluation process audit*** – Assessing the extent to which an organizational management levels have delivered on the desired purpose of the policy to achieve the current performance results.

IIA and KPMG (2015) find that stakeholders have high reservations about policy formulation process audit. The focus of the reservations is based on both practical and

principled arguments. In principle, policy formulation audit attracts the most objections from Board Members since it has the tendency to be critical on their responsibility and can jeopardize the independence of IT audit function. Practically, besides being the most difficult, policy formulation process audit tends to obscure the clear boundary lines between executive function and audit function and, obviously, professional IT auditors would not want to put themselves in the driver's seat. Policy audit is, therefore, open to policy implementation auditing and policy evaluation auditing. This constitutes the audit of police effectiveness (Avram, 2014).

The Balanced Scorecard (BSC) was developed by Kaplan and Norton (1992) as a tool to assist managers to determine whether they have both the right goals and performance measures. According to the BSC policy goals and performance should be measured by four perspectives – *financial performance perspective*, *customer/stakeholder perspective*, *internal process perspective* and *learning, knowledge and development perspective*. The BSC assessment system for strategic management has become a widely implemented and the least criticized top essential framework for analysing, testing and refining business strategy and policy throughout the world (Sheehan, 2010). In spite of its usefulness, what critics say about the BSC include the argument that its usefulness is limited to the completeness and value of information driving the implementation process. Its financial perspective focuses on historical accounting information with all its limitations. Also, the BSC is costly and time consuming to implement since it has been empirically observed that unless someone within the entity has experience with it, external use of consultants and staff training are required, and this can result in staff resistance. The BSC is also, sometimes, criticised that its four perspectives impose a limitation on scope since other e.g. it over-emphasizes on internal issues and fails to evaluate all significant dynamics such as competitor moves which can affect customer satisfaction ruining the balanced scorecard. (Awadallah & Allam, 2015).

ISACA (2012) relied on the strength of the BSC in the design of its COBIT best practice guidelines for evaluating policy effectiveness. COBIT assigns the governance level assurance program of '*Evaluate, Direct and Monitor (EDM)*' as the main procedural goals and aligns enterprise goals cascade with the BSC breaking it down into vision, strategies, tactical activities, and metrics. COBIT aligns its goals cascade with the structure of the four BSC perspectives and comes out with a list of 17 comprehensive approaches to policy

evaluation which, in turn, have three thematic (homeostatic) goals, namely; ***Benefit Realization, Risk Optimization and Resource Optimization*** (Wescott, 2014). **Table 7** below demonstrates the matrix for evaluating policy efficiency based on the BSC and the 17 goals COBIT recommends for IS audit or assurance on policy effectiveness.

Table 7. Policy efficiency audit matrix

Balanced Scorecard Objectives	No	Generic processes for IT Policy Assurance Procedures per COBIT	Governance Assurance Procedural Goals	Policy Goals
		Governance Assurance procedures: <i>Evaluate, Direct and Monitor:</i>		
Financial analysis	1.	Policy for the alignment of technology and strategy with available financial resources and related risks.	[EDM03] Strategic Risk Management	<i>Risk optimization</i>
	2.	Policy on costs for ensuring technology compliance and support for compliance with external laws and regulations.		
	3.	Policy for ensuring financial transparency of technology costs, benefits and risk.		
	4.	Policy on cost for the management of technology-related risk.		
	5.	Policy for ensuring the realization of benefits from technology-enabled and portfolio investments.	[EDM05] Stakeholder transparency	
	6.	Policy for ensuring availability of reliable and useful information for decision making		
Customer analysis	7.	Policy for the delivery of technology in line with business requirements.	[EDM04] Strategic Resource Management	<i>Resource optimization</i>
	8.	Policy for the optimization of technology assets, resources and capabilities.		
Internal analysis	9.	Policy for technology agility	[EDM01] Governance Framework Setting and Maintenance	<i>Benefit realization</i>
	10.	Policy for the Security of information and infrastructure		
	11.	Policy for ensuring adequacy of use of technology solutions.		
	12.	Policy for the enablement and support of business processes by integrating technology into processes.		

	13.	Policy for the delivery of program benefits on time and on budget while meeting requirements and quality standards.		
	14.	Policy for ensuring commitment of executive management for making technology-related decisions.		
	15.	Policy for ensuring technology compliance with internal policies.		
Learning and growth analysis	16.	Policy for ensuring competence and motivation of technology personnel.	[EDM02] Benefit and Value Delivery.	
	17.	Policy for the management of Knowledge, expertise and initiatives for innovation.		

4.3. Implementation Guideline of the Framework

When an IT audit or assurance assignment is not an agreed upon procedures, practitioners are expected to plan and execute the audit based on certain auditor-selected procedures to achieve desired audit outcomes for the client. The practitioner is expected identify the client’s needs based on its level of sophistication, business model and operational risks. Implementation guidelines provide details on how to put the framework into practical use taking into consideration organisational contexts and extent of texts of details necessary (Tay, 2017; Knechel, 2016). The suggested technique for implementation seeks to develop metrics for an objective approach for the creation of IT Audit Universe based on the strengths of viable systems performance measurements for S1 (Operations) and the CMMI-based Capability Assessment Model developed by ISACA for the implementation of COBIT 2019. The performance measurement metrics in the viable systems model, as explain above, provides three levels of planning assessment which serve as the springboard for IT audit planning.

4.3.1. Creating an IT audit Universe through Audit Process customization

Customisation is one of the key IT audit planning processes to assist in the implementation a framework. It involves the selection of substantive procedures from the framework for the creation of client-centric IT audit universe (Tay, 2017). An IT audit framework should provide the metrics to amplify relevant procedures for desired outcomes while attenuating superfluous and less valuable to save cost and time. Based on the triple vector measurement

model, creating an IT audit universe at the audit planning stage can be categorised into three levels, namely: tactical audit stage, strategic audit stage and normative audit stage (Paucar-Caceres, 2009).

4.3.1.1. Tactical Audit Stage

This purely concerns operational IT process assessment and risk control planning which involves test of details for functional vulnerabilities and risk of loss resulting from inadequate or failed internal IT processes, people, and systems controls or from external events (Basak & Buffa, 2016). Tactical audit is, therefore, very relevant in the assessment of the auditee's actuality, thus, subsystems S1 (process), S2 (coordination) and S3 (Control). Initial data source involves a reference projection of what the organization is doing in terms of the general control environments and compliance inside-and-now with standards and regulations etc. compared with what it ought to be doing should the present level of achievement of objectives be maintained given the relevant environmental constraints (Paucar-Caceres, 2009). Investigations include budget objectives, budgetary performance benchmarks and their relevance to current business processes. This process provides leads to the identification of improvement opportunities.

4.3.1.2. Strategic Audit Stage

Strategic audit stage is defined as the process of evaluating continuous capabilities throughout the organization. Strategic audit planning should lead to the creation of awareness of the organization's current achievements as well as its capabilities outside-and-then. Analysis at the strategic audit planning level should involve how business strategies can increase alignment with Enterprise Risk Management (ERM) and seek greater collaboration with the other lines of defence. This may lead to the analysis of how to strengthen links and possibilities to forge alliances in the marketplace, looking beyond the organization and drawing on external benchmarks and independent challenge for fresh ideas (PwC, 2016). The value of Strategic IT audit planning coincides with Intelligence (S4) auditing in the Systems approach. An Intelligent Audit Planning is a total environmental audit planning and, therefore, it integrates all organizational members and supports the assessment of objectives by defining the gap in achievements for the purpose of communicating reliable outcomes timeously to management for actions geared towards the future viability of the organisation (Bell et al., 1997). Quantitative figures are derived using

the indices and are interpreted to identify the gaps between current achievements and budgeted capabilities as discussed below with the triple vector indices.

4.3.1.3. Normative Audit Stage

This is defined by Paucar-Caceres (2009) as a process that evaluates the efficiency and effectiveness of the whole organizational policy direction and includes a reflection of the interests, social norms and values of stakeholders. Normative analysis sees beyond quantitative projections often conducted to discover plausible relationships among both financial and nonfinancial data (Kogan et al., 1999; Steward, 2015). Rather, it supports the development of a broader perspective assists with horizon-scanning and builds out sources of relevant information and insights by reflecting on the suitability, acceptability and feasibility corporate policies (Byrnes, 2015). This coincides with Policy (S5) Audit planning in the viable systems approach.

4.4. The Metrics for the customisation

Chapter two presented a three-vector measurement for operational performance in the viable systems model. It was found that these measurements were very useful for system diagnosis. It was also introduced in chapter two and three that with the aid of the Process Maturity model by ISO/IEC TS 33030:2017, the CMMI-based Maturity Measurement technique of COBIT 2019 together with Governance Design workflow, a quantitative metrics for performing analytical procedures would be designed to provide an aid for the auditor for the creation of an IT audit universe that is contextually suitable for the organisation in the implementation of the framework. In the triple vector business process performance measurement model, '*Actuality*' was defined as what is achieved today based on the entity's IT policies and budget; '*Capability*' was defined as what could be done if the organization had been optimally organized given the present level of constraints and resources and '*Potentiality*' was defined as the measure of the systems performance where resources are well defined and developed and all constraints are removed (Paucar-Caceres, 2009). In chapter two, it was discovered that ISACA failed to provide the steps to objectively determine system capability which is vital in assessing the scope and extent of assessment suitable for the organisation within the period.

COBIT 2019 has provides 17 coded steps contained in four stages as an aid to tailored Design Process Workflow. They are employed and presented in the design of the metrics, here, as

Attribute Code Numbers. These constitute very rich sources of data for consideration for the determination of the value of the capability index factors for IT processes; namely: 1.1. Understand enterprise strategy, 1.2. Understand enterprise goals, 1.3. Understand the risk profile, 1.4. Understand current I&T-related issues, 2.1. Consider enterprise strategy, 2.2. Consider enterprise goals and apply the COBIT goals cascade, 2.3. Consider the risk profile of the enterprise, 2.4. Consider current I&T-related issues, 3.1. Consider the threat landscape, 3.2. Consider compliance requirements, 3.3. Consider the role of IT, 3.4. Consider the sourcing model, 3.5. Consider IT implementation methods, 3.6. Consider the IT adoption strategy, 3.7. Consider enterprise size, 4.1. Resolve inherent priority conflicts and 4.2. Conclude the governance system design. Table 8 below demonstrated evidence collection checklist defined for creation the IT audit universe.

Table 8: Factor Value Checklist.

Factor Index	Attributes Code No.	Factor Rating										Average Factor Rating	
		0	10	20	30	40	50	60	70	80	90		
Actuality	1.1												< 100%
	1.2												
	1.3												
	1.4												
	2.1												
	2.2												
	2.3												
	2.4												
	3.1												
	3.2												
	3.3												
	3.4												
	3.5												
	3.6												
3.7													

	4.1												
	4.2												
Capability		10	20	30	40	50	60	70	80	90	100	≤ 100%	
	1.1												
	1.2												
	1.3												
	1.4												
	2.1												
	2.2												
	2.3												
	2.4												
	3.1												
	3.2												
	3.3												
	3.4												
	3.5												
	3.6												
	3.7												
	4.1												
	4.2												
Potentiality	1.1 – 4.2											= 100%	

To deploy the metrics, preliminary evidence may be obtained for ‘actuality’ through interviews, inspection and observation with the process design workflow as the lens. Since each manager knows what his actual degree of productivity (*actuality*) is, as compared with what he is capable of doing that can move the organization forward (*capability*) given the current constraints, it would not be difficult for the assessor to perform preliminary procedures to obtain fair estimates and attribute applicable value factors for the specific process attribute and strike the average (Espejo, 1979).

Process *Achievement (productivity)* is defined as the ratio of the actuality and capability; given as: $0 \leq \frac{ACTUALITY}{CAPABILITY} \leq 1$.

Process *Latency* is defined as the ratio of the capability and potentiality, given as: $0 \leq \frac{CAPABILITY}{POTENTIALITY} \leq 1$.

Process *Performance* is the product of achievement and latency or the ratio of potentiality and actuality, given as 100% (or 1). It must be noted that actuality can always be less than capability where, the average factor index for actuality is less than 100% and the average factor index for capability is less or equal to 100%.

The process capability model provides a set of scores based on whether the process attributes at that level is 'Not achieved', 'Partially achieved', 'Largely achieved' or 'Fully achieved' referred to as the 'NPLF Scores'. The COBIT 2019 maturity level for focused areas provides a set of maturity levels of a process determined based on the achievement of specific process attributes. This is determined on a scale of zero to five (0-5) levels. This scale demonstrates an increasing maturity or capability of an implemented process. This scale ranges from no achievement level to a level where process purpose is meeting current expected business goals. At level zero (0) - '*incomplete process*', there is no IT process, or the process is not implemented at all, or falls significantly short of any purpose and systematic planning. At level one (1), - '*performed process*', the processes may be a performed process but rather informal and undocumented without data on its associated operational risks. When a process capability is rated at level two (2) - '*managed process*', business processes follow a regular pattern and, at least, the system's inherent risks are managed (i.e. planned, monitored and adjusted). At level three (3) - '*established process*', there is a standardized process which is effectively deployed and documented as a defined process to achieve its process outcomes. At level four (4) - '*predictable process*', there is predictability of process and it operates consistently within defined limits to achieve process outcomes and is supported and driven through quantitative information derived from relevant measurement. Level five (5) - '*optimized process*', depicts a process that achieve the process purposes, with work products or services appropriately established, controlled and beneficial value maintained. Each maturity attribute level falls into a defined score and audit planning as demonstrated in **Table 9** below.

Score	Achievement Range of performance on objectives (thresholds)	Maturity Level	Level Rating	Stage of substantive audit concentration.	
N	0 – 15% - Not achieved/incomplete	Level - 0	<i>Incomplete Process</i>	S1	Tactical
		Level - 1	<i>Performed Process</i>		
P	15 – 50% - Partially achieved	Level - 2	<i>Managed Process</i>	S2	
		Level - 3	<i>Established Process</i>	S3	
L	50 – 85% - Largely achieved	Level - 4	<i>Predictable Process</i>	S4	Strategic
F	85 – 100% Fully achieved	Level - 5	<i>Optimized Process</i>	S5	Normative

Table 9. NPLF Capability Scores.

For example: If *actuality factor* is obtained as = 60% or (0.6) and *capability factor* = 85% (0.85), **Achievement** = (60% ÷ 85%) = 71% (approximately). **Latency** = $0 \leq \frac{CAPABILITY}{POTENTIALITY} \leq 1$; i.e. = (85% ÷ 100%) = 85%; where Potentiality is given as 100%. Performance index of the IT processes for the unit or division or organisation can then be derived as: **Performance** = (LATENCY × ACHIEVEMENT). This is derived as (85% × 71%) = 60%. The result is given in percentages or as decimal number between 0 and 1 or in percentages; thus = 0.6. From the NPLF Table (Table 9) above, the organisation under review has predictable IT process maturity and substantive audit procedures will be Strategic and focused on S4 – Intelligence Auditing for more desired audit outcomes. Of course, the selection of customised audit focus does not exclude the compulsory requirement of conducting fraud risk assessment (S3*).

Generally, therefore, where process performance score below 15% on the NPLF table, IT processes are not even available or too inadequate to achieve significant business objective for the organisation and therefore tactical IT auditing should be focused on. Where the score is between 15% and 50% on the NPLF, IT processes range from performed process to managed process although the IT requirement is at the tactical level with auditing needs based on risk in IT integration, coordination (S2) and control (S3) to achieve operational objectives.

Where the NPLF score is in the range of 50% and 85%, Strategic Audit planning, i.e. Intelligent audit (S4) should be amplified. Tactical or operational audit planning is not required and should be substantive tests should be reduced for tactical level auditing. Finally, where the NPLF score is within the range of 85% and 100%, normative planning should be amplified. At this level, the client requirement is the assurance that Board and Executive are

providing value to the business and optimising the use of IT resources for all stakeholders through efficient and effective IT leadership and policy (S5).

4.5. Conceptual Model Development

A conceptual model for a research study has been defined as the synthetic output of the researcher's understanding of the interconnections among the set of variables identified in his or her literature review which is required to pursue further investigation in the research (Kerin et al., 1992). Chapter three explained concepts or principles from the substrates of the viable systems approach and provided details of dominant variables that contribute to each concept. The exercise identified twenty (20) variables the literature review which are required in the pursuance of further development of the research. The first set of five (5) variables constitutes the IT auditor's role in the proposed IT Audit process above, namely: *operations, coordination, investigations/monitoring, intelligence* and *policy* were extracted from the *Functions* of the systems theory. The second set of nine (9) variables namely; *autonomy, customisability, flexibility, voluntariness, systematisation, responsiveness, proactivity, agility* and *recursion* were discussed under the concepts of coordination *Viability* and *Adaptive Controls*. These principles that underlie the preservation and implementation of the audit processes. The next set of two (2) variables audit *risks* and *relevance* discussed under the concept of *Sophistication* which has bedevilled the functions of the auditor. *Uncertainty* and *Irregularity* were two (2) set of variables that explained the concept of the *Environment*. Finally, *transparency* and *timeliness* were two (2) extracted variables that to be most essential to the concept of *Communication*.

Figure M represents the researcher's conceptual understanding of the hypothetical interconnections among the set of variables identified in his literature review which are required in pursuance of further development of the research.

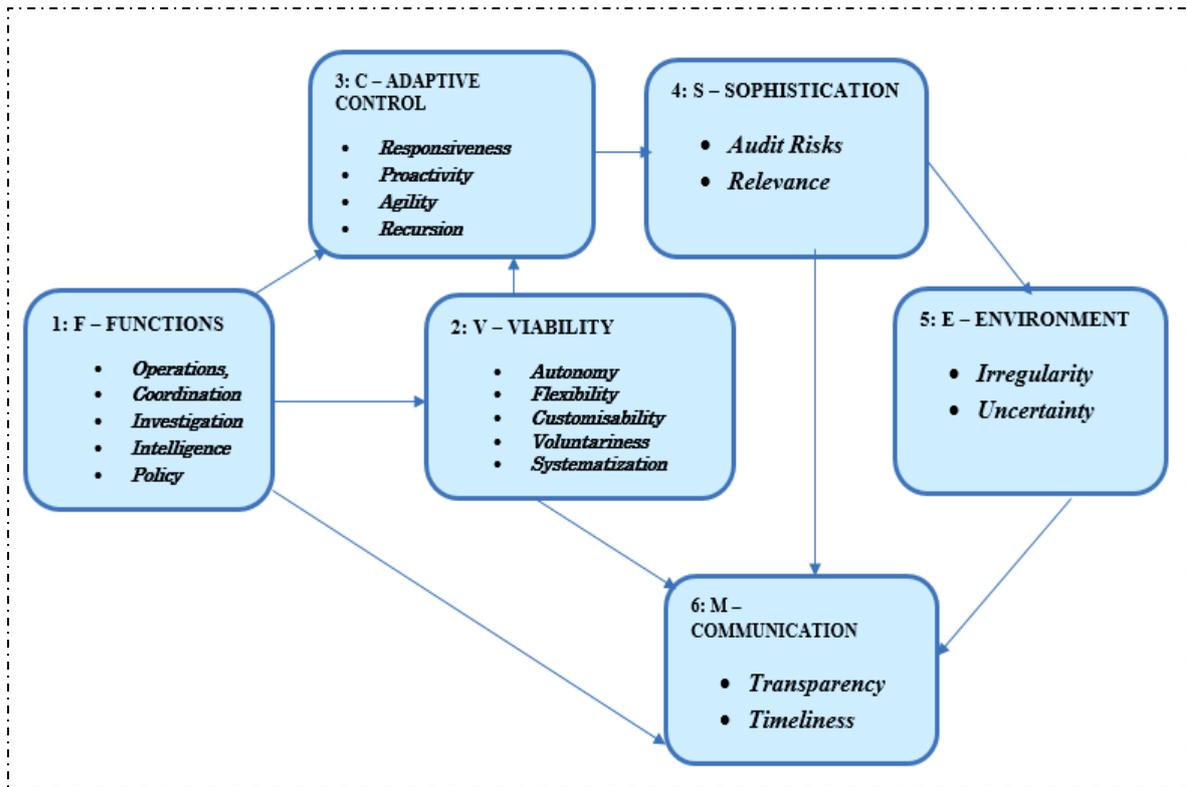


Figure M. *Conceptual model for the Development of the Research*

Following from above, a conceptual model organised into six domains is designed as an alpha version of the framework for IT auditing. These are 1. Functions, 2. Viability, 3. Adaptive controls, 4. Sophistication, 5. Environment and 6. Communication. Each domain constitutes a system each relating to the other to derive a supra systems, i.e. an IT audit framework whose traits are based upon the consonant and resonant relationships of its own subsystems (Barile et al., 2018; Espejo, 2003). The arrow points from predictor variable(s) to a dependent variable.

The ‘*Functions*’ domain is positioned at the starting point for the prediction of various predictor/dependent relationships among the domains of the proposed framework for IT auditing because the ‘functions’ of a system are determined at the start to predict other concepts of viable relationships of a system (Van Grembergen & De Haes, 2018). The ‘*Viability*’ domain is positioned second in the conceptual model because the functions of a viable system are preserved by the mechanisms of viability (Michael & Dunn 2008; Walker, 2002). Furthermore, viability analysis provides the catalyst for the assembling and communicating a broad range of information that has significant influences on an entity’s business processes and further triggers the evaluation of the entity’s business process quality

together with its business process resilience or adaptability (Ellison et al., 2008). This explains the reason for the mediating role of 'viability' domain between process or functions, adaptive control and communication domains. This constitutes Type I audit according to The Statement on Standards for Attestation Engagements (SSAE), (formerly SAS 70) (Nickell & Denyer, 2007; Kramer, 2003).

The over-concentration of risk assessment on operations and failure to analyse strategic dangers by Internal auditing and IT auditing has been criticised as insufficient in addressing total risk environment (Weller, 2015). Barile et al. (2018) posit that the environment is strongly related to sophistication or complexity. Type II audits must focus on the structures in place to match the shifts in the business horizon with business goals and objectives evaluating the appropriateness of technologies and controls to keep the risks and threats within acceptable limits (Kramer, 2003). This means that type II IT audit focuses on adaptive controls to project the quality of resilience and survivability in both the audit practice and in the auditee's system in an increasingly sophisticated and unstable environment (Holmes, 2018; Walker et al., 2002). 'Adaptive controls' domain is, therefore, placed third above the mechanisms for operational viability in the conceptual model. Controls are adaptive if its level of its sophistication is adequate to absorb the evolutionary complexity (Achterbergh & Vriens, 2002). This is because complexity destroys complexity (Hilder, 1995). For the above reason, the 'sophistication' domain is positioned forth and after adaptive controls to ensure that systems audit can absorb the evolutionary volatility (Martin, 2004).

For a system to be able to achieve and sustain desired outcomes in the face of fast environmental changes, therefore, internal audit and IT audit should analyse and determine the appropriateness of management approach in confronting the volatility and sophistication in the light of an increasing sophistication (Sagalovsky, 2015). This explains the rational for the fifth position of the 'environment' domain in the conceptual model after sophistication. Complexity or sophistication and change are pervasive issues in the operational environments of today's business organizations with increasing significance on audit communications. The environment, which constitutes business process, technology, people and relationship, itself constitutes the pre-condition and any condition in-between necessitating efficient communication (Barile & Saviano, 2018) because ignorance lethally impairs a system's survivability (Barile et al., 2018). This explains the mediating role of the environment between sophistication and communication domains. The essence IT audit

quality lies in the value added to decision and policy making through effective communication. Effective communication in IT audit performance is an end-product of the role of the IT auditor (Singleton, 2014). Therefore, the last but not the least domain in the construct is the 'communication' domain. The formative working hypothesis in the conceptual model is, therefore, based on an inside-out formation (Buchanan & Gibb, 1998). **Table 10** below provides an elaborate description of the of the sources of the domains and their relevant principles together with supporting literature to evidence the derivation of the construct.

Conceptual Domains of IS Auditing Framework	Processes and Principles	Description	References
<p>1. FUNCTIONS (IT audit Process factor) – Functions in viable IT auditing is a process. The conceptual foundation of audit evidence is that a viable systems audit process must obtain sufficient appropriate evidence on all autonomously auditable business functions or process for optimal audit output (Toba 1975). To make this possible, it is prescribed IT audit process be effectively aligned with the functions of those charged with governance and management (ISACA, 2013).</p>	<p>Operations – <i>The depth of knowledge of the client’s business greatly facilitates the performance of audit engagement staff. It is, therefore, essential to encourage the gaining of insight of the client’s business operations at the very start of an IT audit engagement (Rezaee et al. 2018). Obtainment of evidence on operations is accordingly placed first in the ordering of IT audit functions.</i></p>	<p>Operations is defined as all components of business processes that together constitute the organization’s chain of value activities. Auditing around various units of business processes within the entity’s value chain together with its information systems constitutes a prescribed new approach to the audit of business operations to tackle audit problems. Operations review is referred to as the ‘actuality’ of autonomous IT audit process because it creates an opportunity for IT audit functions to coincide with the day-to-day functions of management thereby helping to forge stronger relationship between IT auditors and management as they both speak common language. The concept of autonomy links operations reviews to other IT audit functions relating to coordination (S2), monitoring and investigation (S3), intelligence (S4) and policy (S5).</p>	<p>Rezaee et al. (2018); John & Cianfrani (2017); ISACA, (2013) Ray (2009); Simons (1995); Toba (1975)</p>
	<p>Coordination – <i>coordination is placed second because per the VSM, coordination is a control function that</i></p>	<p>Coordination is a control and cohesion function in a complex system which is responsible for ensuring that all the processes or activities in operational value chain work together effectively. Thus, coordination is the corner stone of a viable system. Coordination audit is, therefore, a very</p>	<p>Razak & Muhamad (2017); Ray (2009).</p>

	<p><i>ensures the cohesion of the operational activities (Geerts et al., 2013; Syntetos & Jackson, 2011).</i></p>	<p>important value adding IT audit function responsible for the accurate appreciation of the achievements and capabilities of units of the organizational operations or processes. An IT audit framework design should contain a thorough assessment of the weak links to obtain evidence of the organization's capabilities as compared to its achievements and the role of IT to provide added value solution.</p>	
	<p><i>Monitoring and Investigation</i> – <i>Investigation is a control function sandwiched between coordination and intelligence to keep track of the internal and provides feedforward for external effects that can derail the operational objectives (Espejo, 2009; Hilder, 1995).</i></p>	<p>Monitoring and Investigation is defined as a formal systematic mechanism for examining irregular events with the mind to obtain actual evidence and to discover fraud and other operational risks. The issue of fraud risk and the auditor's responsibility have been debated for decades. As a result of recent development in corporate governance horizon it now no longer tenable for an audit framework to ignore fraud investigation. Fraud risk assessment will contribute effectively in promoting the effectiveness of IT audit functions. The viable systems-based auditing is already endowed with a mechanism for monitoring and investigation (S3/S3*) which involves a proactive philosophy for investigating to discover irregularity timeously and to provide the assurance that management control processes have sufficient policies</p>	<p>Kultanen (2017); Ficco & Rak (2017). COSO (2017); Buffa & Basak (2016); Chandler (2014).</p>

		including internal and external risks vigilance to address every level of operational risk.	
	Intelligence – <i>Intelligence function occurs before Policy function in that to enable Boards and Management to make policy decisions, a total control environment must be explored from the organization’s intelligence systems (Hilder, 1995).</i>	Intelligence is defined as a system is with the capacity to gather and examine external data and communicate with other systems in matters such as adaptability in accordance with current circumstances, security, connectivity and capacity for remote monitoring and management strategies. Intelligence function contributes to the effectiveness of IT audit because it tests for opportunities and anticipates threats coming not only from the organization’s automated systems but also other external sources to examine the organization’s capacity to adapt over time within the changing landscape of business broadening IT audit scope.	THEIIA (2017); Varkoi et al. (2016); Espejo (2009); Bell et al. (1997).
	Policy – <i>Policy is placed last in the IT audit functions ordering because policy is the outcome of the intelligence of the total environment (Khan, Nicho & Cooper, 2015).</i>	<i>Policy</i> refers to a deliberate system of principles to regulate or guide future actions to achieve rational outcomes. Boards, Executives and other decision makers are responsible for policy formulation. Traditional IT audit frameworks do not pay adequate attention to policy makers functions. However, self-regulation on the enterprise governance level occurs when companies conform to the spirit, policies, standards, and substance of good governance. Emphasizing policy-making function audit in a framework for IT auditing will help to increase scope of IT audit. This will ensure	Van Grembergen & De Haes (2018); Gregg (2007); Rossouw (2005).

		auditors examine the likelihood that the vision and values of those charged with governance and management will support the organization's long-term viability which used to be woefully ignored in traditional auditing frameworks.	
<p>2. COHESIVE VIABILITY (IT audit input factor) –</p> <p>Cohesive viability or <i>Viability</i> adopted for short in this study, relates to prescribed concepts critical in IT auditing since they support the creation and use of the organization's and IT audit capabilities (Espejo, 2009). For IT auditing to maintain its essence in an increasingly evolving environment, IT audit's approach to operational control must involve the review of the capacity to allocate resources, to manage the organization's <i>capabilities</i>, and above all, to create the conditions for actors to coordinate their actions (Agrawal & Cooper; 2017).</p>	<p><i>Autonomy – this is a principle underlying operational audit. Autonomy forms the basis for upholding current and future viability of a system's capabilities by enabling a responsible coordination (Espejo, 2009). Autonomy is an input concept. Its position does not make this concept take precedence over other concepts below.</i></p>	<p>Autonomy as applied to auditing is understood as underscoring compliance requirement to determine the substantive procedures that will produce desired outcome based on the context of the total system. Autonomy of IT auditors is enabled by their practical coordination function. Current IT audit systems, and related information review systems, tend to obscure the distribution of autonomy throughout the organization and with this the coordination review requirements of primary activities. Autonomy will contribute to a viability because it draws on the independence of compliance standards values, ethics, knowledge, skills and experience that apply to professionals in the audit of identifiable auditable units of business process value chain of activities.</p>	<p>Rezaee et al. (2018); Marcello et al. (2017); Espejo (2009).</p>
	<p><i>Flexibility - See 'autonomy' above.</i></p>	<p>Flexibility in the VSM connotes the capacity to release the potentials of people, enabling them to handle their problems independently based on</p>	<p>Cassidy (2016);</p>

		<p>their judgement, thus ensuring their ability to survive in complex and rapidly changing environments. By the law of requisite variety, the principle of flexibility states that an actor in a technically complex system with the highest amount of flexibility is likely to have the greatest impact. Flexibility contributes to the viability because it is linked to autonomy and aimed at reducing over-emphasis on rigid rules and checklist auditing. It improves on the auditor's freedom to apply variety of techniques to flex audit approach to make it adaptable to the contextual circumstances.</p>	<p>Rittenberg (2013).</p>
	<p><i>Customizability -</i> <i>See 'autonomy' above.</i></p>	<p>Customization is the process of tailoring a system or process to meet the requirements of a business. This is in keeping with the mechanism for adaptation in the viable systems approach. Customizability contributes to IT audit viability by fostering the drive to meet client's desired audit requirement by focusing on procedures that will yield desired outcomes – a contemporary trend in IT auditing that seeks to achieve viability in the practice. Despite its essence in achieving desired IT audit outcomes, the issue of objective process for the customization of known IT audit frameworks has been elusive.</p>	<p>Tay (2017); Popa (2012).</p>

	<p><i>Voluntariness</i> - See 'autonomy' above.</p>	<p>Voluntariness is defined as the degree to which an innovation is of the use by free will. It serves as an objective-enhancing factor for the adoption of new method or technology. Voluntariness contributes to the viability of IT audit framework because it coincides with principles-based approach to the adoption of best practice guidelines practiced by the United Kingdom in contrast with the mechanistic check listing rules-based approach in the United States of America to audit decision making which leaves legalistic loopholes in the attempt to avert compliance with guidance. Basing voluntariness on the principles-based approach would mean that implementation bottlenecks would be resolved by referring to the principles and concepts of the ingrained theory, i.e. the viable systems approach. This will lead to the focus on the spirit of the guidance which would encourage responsibility and the exercise of professional judgement because it has embedded participatory management system and therefore invokes intrinsic commitment and reliability.</p>	<p>Lunenburg (2013); Wu & Lederer (2009); Bagshaw (2006); Etzioni (1997); Gunningham & Sinclair (1999).</p>
--	--	---	---

	<p>Systematization - See 'autonomy' above.</p>	<p>Systematic approach is a process of assessing units of a systems and the effect on changes of one unit on other units to achieve a holistic result. Systems-based audit approach, although has not received adequate attention, possesses the qualities for more desired audit in contemporary organizations. A systematic framework of auditing contributes to the viability of the profession because it provides a means to apply IT auditing to well-developed investigation methods and procedures of the sciences that are based on observable, measurable entities developed through living systems theory.</p>	<p>Merhout & Havelka (2008); Iyengar, (2007); Ha (2005); Simons (1995). Swanson & Marsh (1993).</p>
<p>3. ADAPTIVE CONTROL – (IT audit input factor). Control is traditionally management function. IT auditors concern about control has been related to its sufficiency or appropriateness in meeting required regulatory standards. IT audits have, therefore, been conducted with compliance-based checklist approach which has proved to be unsustainable (Cassidy, 2016). In today's digital age, where new and higher levels of risk continue to emerge, management are under constant pressure to make faster, more risk-informed business decisions without necessarily changing purpose. IT auditors' consultancy role to management is now highly valued by</p>	<p>Responsiveness - See 'autonomy' above.</p>	<p>Responsiveness is defined as an approach of prompt identification of risk concerns and taking proportionate and timeous action or signaling them to the relevant stakeholders to determine the most proportionate reactions. Responsiveness contributes to adaptive control because it examines the proportionality of the control measure to the control issue identified. As a result, responsive IT auditing will show resilience in its capacity to address a broad range of issues in every organizational context.</p>	<p>Cassidy (2016); Rittenberg (2013); Chambers (2009).</p>
	<p>Proactivity - See 'autonomy' above.</p>	<p>Proactivity in a viable systems approach is defined as a mechanism for adaptation through preventive control approach rather than through reactive approach. Proactivity is a very recent philosophy of control because of the requirement for</p>	<p>Marcello et al. (2017); Schillemans and van Twist (2016); Osei-</p>

<p>Management which calls for IT audit to align their thinking with those charged with governance and management. The resilience of IT audit services is no longer based on strict compliance-based controls, but controls that are adaptive to the strategic objectives, business operations, and IT security (Huck, 2016).</p>		<p>organizations to adapt to the future business environments. Best practices proffer that proactivity which connotes prevention leads to adaptability and it is preferred to the detective philosophy in traditional approach to auditing. Proactivity, thus, contributes to adaptive control by helping auditees to be resilient in meeting future requirements before they are overtaken by the volatile control environment due to the increasing complexity. A survey of audit professionals rated proactivity very high as an approach to achieve desired outcomes of auditing business organizations. To effectively participate in the fight against fraud and corruption IT audit should move away from reactivity to events to proactive approach that underlies adaptive control.</p>	<p>Afoakwa (2013).</p>
	<p>Agility - See 'autonomy' above.</p>	<p>Agility is defined as the ability to flex purpose or direction of control to efficiently address the changes and still maintain reasonable balance in scope, time and cost while improving quality. Agility contributes to adaptive control by its iterative approach to task and the development of risk-driven together with change tolerant approaches to assessments through close collaboration between the assessment team and the responsible party. Agility as an input concept in IT Audit focuses on stakeholder needs, accelerated audit cycles, time-drive insights with short</p>	<p>Deloitte (2018); John & Cianfrani (2017); Schillemans and van Twist (2016); Omonuk & Oni (2015).</p>

		iterations with increased management and executive engagement, reduced wasted effort, and less document generation, thus, making IT audit and control more adaptive.	Chambers (2009).
	<i>Recursion - See 'autonomy' above.</i>	Recursion is defined as the ability of a component of a viable system to continuously produce other viable systems within itself while each component maintains its autonomy at increasing cycle of complexity, thus, ensuring all five functions are repeated at any maturity level of the audit. Recursion contributes to adaptive control by ensuring that an auditable business unit or process is continuously monitored and continuously audited by a complete set of desired audit processes. The effect is a thorough IT audit value co-creating capacity of leveraging self-organization and self-regulation of the auditee.	Rezaee et al. (2018); Deloitte & Touche LLP et al. (2012).
4. SOPHISTICATION (IT audit input factor) – The definition of sophistication is provided as the level or form of complexity a given system can recognize and manage. Technology use in business has complicated people and the business processes. Business risks have, as a result, increased and these have compounded the requirements of the control environments.	<i>Risk-based - See 'autonomy' above.</i>	Audit risk, by definition, is the probability that an auditor would express or communicate inappropriate audit opinion on the of a subject matter of an audit. Fast changing business models brought about by technological developments that is increasing in sophistication has spawned complex operational and business risks. The effect is increased IT audit exposure to failure through the issuance of inappropriate audit report. Inappropriate audit opinion could be an exaggerated report or wrong recommendations	Buffa & Basak (2016); Knechel & Salterio (2016); Egbunike (2014).

<p>Organizational processes, as open systems, are exposed to both local and external impact. Auditors must, therefore, continuously update themselves. The impact of technology, people and process sophistication is an increased exposure to audit failure due to high uncertainty (Barile et al, 2018).</p>		<p>that perpetuate or increase the organization’s vulnerabilities. The concept of requisite variety states that complexity destroys complexity, therefore, IT audit of the future demands an expanded approach to risk assessment based on complexity theory and continuous learning to match up the increasing business sophistication.</p>	
	<p>Relevance - See ‘autonomy’ above.</p>	<p>Relevance is defined as the quality that justifies that an approach is appropriately innovative to the solution of a problem. The existence of relevant and satisfactory internal control systems eliminates the probability of irregularities. Therefore, the relevance of an IT audit framework for less regulatory environments must lie in its ability to support innovative actions in the shared environment that allow the organizational system to control environmental irregularities and sophistication.</p>	<p>Philipson et al. (2016); Burgess & Wake (2012). Popa (2009).</p>
<p>5. ENVIRONMENT (IT audit input factor) – The working definition of ‘environment’ in this research is the observed entities or elements that constitute the fundamental conditions within which a system subsists or operates. The environment contributes to</p>	<p>Irregularity - See ‘autonomy’ above.</p>	<p>Irregularity is defined here as a situation of volatility or mismatch between the challenges posed by complexity from the environment and the internal mechanisms by management to resolve or absorb the challenges in proportionate measures. A viable systems-based auditing approach should recognize the fact that of all the environmental variety, only part of it is relevant to the system;</p>	<p>Knechel & Salterio (2016) ; Ebimobowei et al. (2011).</p>

<p>IT audit effectiveness because it provides the basis to test for opportunities and to anticipate threats. Obtaining understanding the entity and its environment is, therefore, vital in any viable audit because a problematic environment is created over time for business entities by its relations with external agents through the intelligence function at the entity level, the industry level and the economy level (Espejo, 2009). This explains why several standards on auditing such as Public Company Accounting Oversight Board (PCAOB) 12 and International Standards on Auditing (ISA) 315 have dedicated to this concept by various standard setters.</p>		<p>namely that part producing the disturbances that its organization must respond to maintain viability.</p>	
	<p>Uncertainty - See 'autonomy' above.</p>	<p>Uncertainty is defined as a situation being unable to predict or determine relevant course of action with confidence due to jagged environments. The gradual progression of complexity in business processes, technology and people has raised the awareness of the impossibility to realize certainty of performance and, hence, systems audit is increasingly exposed to risk of failure. As open systems, local and external impact characterize uncertainty the environment poses. An efficient system of auditing or system of investigation in less regulatory environments must be one that supports an interdisciplinary approach that draws on diagnostics of systems to develop a set of conceptual and computational tools to make it possible for nonlinear interactions between systems and subsystems.</p>	<p>Barile et al (2018); Everett (2003); Walker et al., (2002).</p>
<p>6. COMMUNICATION (IT audit output factor) –</p> <p>The adopted definition of communication in this study is the act of translating signals and messages and transmitting effectively to target recipient to leverage the process of system change or improvement (Beer, 1972). Communication as an output factor</p>	<p>Transparency - See 'autonomy' above.</p>	<p>Transparency is defined as the succinct, objective and responsible translation including the appropriateness of language used in transmission of messages to make positive impact on target recipients. IT issues have become strategic management issue and IT auditors' role has obtained a place in executives and board rooms. However, since most business executives and directors of organizations are extracted from</p>	<p>Khan et al. (2015); Singleton (2014); Dada et al. (2013).</p>

<p>in IT auditing has the characters of process and concept. Effective communication between the intelligence and policy functions imply that intelligence constitutes a problematic environment that is sensitive to policy directions and that the policy function is sensitive to the opportunities and threats recognized by the intelligence function (Espejo, 2009). Therefore, the communication domain is, perhaps, the most important domain of the IS audit value chain (Singleton, 2014).</p>		<p>perspectives of education or experiences that different from IT, they often lack knowledge, skills and abilities in IT. A transparent communication is not to be exaggerated nor be too complicated to be appreciated by the target recipient. In the design of a viable IS auditing framework the quality of transparency in communication is indispensable since the esoteric nature of the practice can obfuscate reports in audit communications for recipients.</p>	
	<p><i>Timeliness</i> - See 'autonomy' above.</p>	<p>Timeliness is defined as the quality of a feedback being prompt. Communication of IS audit reports should be relevant to policy and decision-making processes and time is of critical essence. An important IT auditor's timely communication quality amplifier is his ability to keep up to date on IT issues. A framework for IT auditing should enable the awareness development in the auditor of emerging technologies and the issues relating to risks, control and value creation capabilities associated with them.</p>	<p>Singleton (2014); Espejo (2003); Beer (1985).</p>

Table 10. Description of the construct of the Conceptual Model

4.6. Development of Conceptual Hypotheses

The relationships identified among the domains of the above conceptual model formed the basis for the conceptual hypotheses formulation. The view of efficient and effective IT auditing based on the conceptual model can be hypothesized from five modular perspectives: 1. Process assessment and alignment model; 2. Adaptive system control model; 3. System co-evolution model; 4. Intelligence assessment model; 5. System value co-creation model. Unless otherwise proven that there is no significant association between the factors stated in the hypotheses below; in which case a null hypothesis H_0 is established, the hypotheses are presumed to be valid. The following are the stated conceptual hypotheses.

4.6.1. Model 1: Process Assessment and Alignment model – Espejo (2009) argues that a viable system depends on the functions governing and controlling it. A viable system's functions, therefore, preserve its viability (Michael & Dunn, 2008). The cause of the sensational corporate failures that rocked more regulated economies around the globe in recent past has been attributed to failure of the functions of those charged with governance, risk management (Agrawal & Cooper; 2017). To make IT audit viable, ISAKA (2013) strongly argue that the effective alignment of IT audit approach with the functions of those charged with management may be a cause for IT audit resilience or viability. The challenge, however, has been the determination of the IT audit workflow processes that effectively align with the dynamics of the functions of those charged with governance and management to cause the viability of the practice (Taylor & Wu, 2014; ISACA, 2013). It is, therefore, hypothesized that;

H1. An effectively aligned IT audit functions with the functions of those charged with governance and management influences the viability of IT auditing.

4.6.2. Model 2: Implementation Control model – Due to recent events user advance the argument in the agency theory that today's audit must be geared towards ensuring that those charged with governance and management are proactive and are exercising controls with the objective to ensuring that the auditee is resilient and adaptive in the wake of the unstable operational environment (Martinez, 2014). Espejo (2009) posits that adaptive control processes involve interactive approach with the functions of those charged with governance and risk management. This is to enable improved tolerance of the system of audit and to reduce audit risks. IT audit adaptability to rapid changes may, therefore, be caused by effective alignment

of IT audit functions with the functions of those charged with management (Michael & Dunn 2008). The challenge for IT auditing, however, is the lack of consensus among researchers and practitioners on the auditing framework that supports effective interaction of IT audit workflow with the functions of those charged with governance and risk management for effective adaptive controls (Huck, 2016; DeFond & Zhang, 2014). Based on this, it is hypothesized that:

H2_A: *An aligned IT audit functions with those of management influences efficient adaptive controls.*

The theory of inspired confidence says that as business technology increases in complexity, the viability of auditing lies in its capacity to influence the resilience of the controls of those charged with risk management (Mihret, 2014). Therefore, the cause of viability of auditing is its capacity to adapt to the changing business environment (Deloitte, 2018; Byrnes et al., 2015). Adaptive learning and stepping out of comfort zone should, therefore, characterised a resilient approach to IT auditing to promote survivability and co-evolution on the complex business horizon (John & Cianfrani, 2017). Yet, IT audit frameworks used by practitioners are characterised by rigid compliance-based approach which, often, is intolerant to changes to changes in the control environments exposing IT audit to failure (Huck, 2016). It is hypothesized, therefore, that;

H2_B. *The viability of an IT audit approach influences its adaptive controls.*

4.6.3. Model 3: Implementation Strategy model – Contemporary processes involve risky arrangements, the causes of increased environmental risks include the fast-changing and sophisticated technologies (John & Cianfrani, 2017). Beer (1985) theorises that complexity destroys complexity. It is, therefore argued, here, that IT audit solutions must possess proportionate technological sophistication to enhance its resilience (Holmes, 2018) The problems of IT audit in developing countries, however, is that although there is an increasing integration of sophisticated IT applications, the level of integration of technology into auditing and control is not sufficient or proportionate enough for IT audit resilience. Auditors continue to employ traditional approach which is an abject mismatch to the sophistication; hence, fraudsters are technologically well ahead of auditors (Omonuk & Oni, 2015; Kultanen, 2017). There is, therefore, increasing need for controls to be adaptive as result of business IT sophistication. It is hypothesized, hereby, that;

H3. *An efficient approach to adaptive controls influences business IT audit sophistication.*

4.7.4. Model 4: Intelligence Assessment Model – The lending credibility or resource-based theory of audit proffers that investment in IT now involves risky, expensive and sophisticated arrangements (Sagalovsky, 2015). The cause of failure of many organisations is their lack of solid advice on their IT resilience vis-à-vis the disruptive digital transformation taking place in the environment (Byrnes et al. 2018; Agrawal & Cooper, 2017). It is argued, therefore, that the cause of the demand for expanded IT audit services is caused by sophisticated technologies and complex contractual arrangements associated with business environments. Complexity destroys complexity (Beer, 1985). IT audit sophistication must proportionately and progressively increase to match the increasing complexity of business environments to avoid the impairment of strategic business assets. Unfortunately, most frameworks for IT auditing over-concentrate guidance on internal operations related compliance and ignore the exploration of strategic environmental issues (Niemi et al., 2018; Huck, 2016). Drawing on this, it is hypothesized that;

H4: The sophistication of IT auditing influences the risks of business environment.

4.6.5. Model 5: System Value Co-creation model - IT Audit may be viewed essentially as information communication service (Walker et al., 2002). Adding value to the role of the IT auditor is based on a quality performance followed by effective communications (Singleton, 2014). The communication theory framework provides perspectives of communication to include psychological, systemic, social, and mechanistic perspectives. There is an ongoing debate within the circles of audit profession that the complexity and volatility of business environment stimulate the expectations of the amount of IT audit communication that is valuable (Sirois et al., 2018; Barile et al., 2018). The psychological view considers communication as not simply the flow of information from the sender to the receiver but, rather, a complete consideration of the complexity of the total circumstances and the environment shared by both the sender and recipient. It hypothesized, therefore, that;

H5_A: The environment of an organization influences IT audit communication.

The Systemic of view of communication considers communication as the transmission of a variety of messages to different interested individuals who interpret it in their own way and draw their own conclusion. Advances in sophisticated business technology has come along with expanded opportunities for communication in a variety of ways such as social media platforms. This phenomenon may be the cause increased demand for IT audit communication

to various stakeholders (Niemi et al., 2018). The increasing sophistication has, however, led to the existence of information asymmetry with different recipients interpreting key audit matters differently (Sagalovsky, 2015; Ittonen, 2010). The challenge is how to overcome the complex relationships, technologies, business process and people that require new and carefully selected methods of communication (Barile et al., 2018). It is hypothesised, therefore, that;

H5_B: Business IT audit sophistication influences audit communication.

The mechanic view considers communication as simply the transmission of information from the originator – first party to the recipient – second party to cause a change. IT audit value lies in the improvement or change in business processes based in the interplay of efficient evidence collection through listening, interrogating, understanding, translating and an effective transmission caused by effective communication of IT audit results to those responsible to stimulate effective change in governance and management processes (Khan et al., 2015; Osei-Afoakwa, 2013). IT audit is still challenged by the amount of audit processes that would proportionately satisfy the increasing demand for IT audit communication that can stimulate valuable change (Singleton, 2014). It is further hypothesized that;

H5_C: The functions of IT audit influence IT audit communication.

The social framework of communication considers the mechanisms for a viable interaction between the sender and the receiver. That is, how the sender communicates forms the basis for the viability of relationships (Sirois et al., 2018). In today's business horizon, therefore, the viability or resilience to maintain strong cohesion by IT audit practice is the cause of timely and transparent communication to various stakeholders. The challenge, however, is how to determine the amount of communication that may stimulate the maintenance of strong cohesion among the variety of interested parties (Singleton, 2014). It is, therefore, hypothesized that;

H5_D: The viability of IT audit influences IT audit communication.

Model 2 and Model 5 are designed to examine instances of multicollinearity whereby a dependent variable could be linearly predicted from at least two predictor variables with considerable degree of accuracy.

4.7. Conclusion

The chapter focused on the presentation and evaluation of the technical elements of the framework for IT auditing. This included a process for the planning and customisation of the

framework for efficient and effective audit outcomes. The Chapter ended with the development of a conceptual framework and some propositions or hypothesis for further development of the research. The chapter concluded with the formulation of propositions or conceptual hypotheses based on the relationships of the relevant concepts of the conceptual framework for the development of the research. The next chapter presents details of the methodology used for data collection and analyses for the completion of the design evaluation and validation of the outcomes. The chapter explains the philosophical background of the research and approach to knowledge creation. It further describes the research design together with the approach of data collection and data analysis and concludes by considering the ethical issues relevant to the research.

CHAPTER FIVE

RESEARCH METHODOLOGY

5.0. Introduction

This chapter develops on the conceptual framework in the preceding chapter and discusses the philosophical reasonings for the choice of methodology. Methodology is part of the research rigor because it demonstrates the selected research instruments and validates the items in the construct. Research rigor is the driving goal for methods selection (Gregor & Hevner, 2013). Methodology, therefore, provides the worth of the design by detailing out the techniques for data collection and evaluation of the artefact in the study. Evaluation addresses the validity and utility of the study. Validity means that the conceptual solution or artefact works and does what it is expected to do, and it provides clear and dependable guidance in operational terms for the achievement of its goals. The utility criterion assesses whether the achievement of goals has value outside the development environment (Peffer et al., 2007; Gregor & Hevner, 2013).

5.1. Philosophical Backgrounds of the Research

An effective research is that which subscribes to a specified philosophical thinking and developed through the research strategy employed as well as the research instruments utilized in the pursuit of a specified research goal or the research objective(s) and in pursuance of the answer(s) or solution of the research question or research problem. Several reasons accounts for the importance of a clear understanding of the philosophical basis of research strategy. The philosophical basis clarifies a research design enabling an early detection of if a strategy will work. Thus, it is useful in the early identification and creation of designs beyond experience. Moreover, the philosophical basis sets the stage to ensure consistency in the application of different methods to a research question. It helps in providing grounding for the research methods within an accepted epistemological paradigm (Lawson, 2010).

It is very important to elucidate the theoretical reasoning behind knowledge generation. Scotland (2012) provides the general philosophical bases of research by explaining a research paradigm as consisting of the following aspects – the Ontology, the Epistemology, Research Approach, Research Strategy and the Research Methods. The ontology and epistemology are philosophical paradigms and theoretical viewpoints that precede the research approach. The research approach determines the choice of methods by providing a better insight into the merits and demerits of the chosen qualitative or quantitative approach to the research (Vedeler, 2000).

5.1.1. The Ontology

The meaning of ontology is traced from the ancient Greek word ‘*ὄν/ον/*’ (*onto-logos*) which translates into English as ‘to exist’ (*the science of being*). Ontology refers to the things that exist or the nature of things ‘knowable’ or the nature of ‘reality’ in the social world (Crotty, 1998). Ontology examines reality in the light of whether it is objective, i.e. it is external to human interpretations or it is created by one’s own subjective consciousness (Dieronitou, 2014). Researchers in every discipline take an ontological position in their expression of their perceptions of how things work within their espoused reality. Two main ontological positions in social science research are identified by Bryman (2004) - ‘constructionism/subjectivism’ and ‘objectivism’.

5.1.1.1. Constructionism or subjectivism

At one extreme end of ontological reasoning is the view of constructivists, known in other term as subjectivists who claim that systems or social entities can and should be considered social constructions built upon the perceptions and actions of social actors. Burrell and Morgan (1979) cited in (Dieronitou, 2014) refer to this set of ontological assumptions is also known as the ‘nominalist-realist’ debate. Constructionists also take the following types of views - ‘relativism’, ‘idealism’ and ‘critical realism’.

5.1.1.2. Objectivism

According to Bryman (2004), objectivism entails the view that a system or a social entity, phenomenon in question, or real value adheres to an external objective reality independent of the researcher’s awareness or knowledge.

5.1.1.3. The Ontological Position of this Study

The view of this research is that there already exists framework and best practices for IT auditing. More so, the problems of auditing in countries without longstanding tradition of auditing and regulatory environments is granted – best practices and standards were not designed with the circumstances of developing countries with less regulatory systems in mind. Several other issues independent of the researcher’s knowledge are responsible for the problems including lack of suitable theoretical foundations, disorganised knowledge bases including paucity of guidance and cumbersomeness in structure, all resulting in implementation challenges. These constitute reality independent of the researcher’s knowledge knowable issues from extant literature and in the application environment. The study aims to model an artefact with independently attestable solutions to IS audit challenges in less regulatory

environments with reduced the risk of non-replicability of the results (Schaller, 2016; Chow, 1991). With a suitable theoretical or conceptual framework, sufficient analysis and synthesis, an objectively verifiable framework that offers more effective and efficient solution to IT audit challenges in less regulatory environments can be conceptualised and developed. In view of this, the research takes the objectivist ontological view.

5.1.2. The Epistemology

The term 'epistemology' has been defined by McCann and Clark (2003) as the sum of the philosophical view of knowledge that presents a theory of knowledge and the justification for what can be regarded as the criteria that knowledge must satisfy to be called knowledge rather than mere beliefs. Cohen et al. (2007) explains epistemology as the nature and form knowledge may take, be created or acquired and communicated to the recipients. It is the reasoning behind knowledge. What is it that is known is the typical epistemological enquiry between the knower and his knowledge (Scotland, 2012). Epistemology can have several theories, which is a set of schools of thought and reasoning processes for performing an empirical and logical work (Mingers & Willcocks, 2004). Epistemological research paradigm has been described by Kuhn (1962) cited in Feilzer (2010) as an epistemological stance that directs research efforts and serves to reassert itself to the exclusion of other paradigms which articulate the theories already established. The epistemological theories of reasoning normally adopted in information systems research are *Interpretivism*, *Positivism*, *Critical Realism*, and *Pragmatism*, each representing a paradigm of research and being an alternative to the others (Yee & Khin, 2015).

5.1.2.1. Interpretivism

Interpretivists concerns a study of phenomena in their natural environment together with the acknowledgement that scientists cannot avoid subjectivity in interpreting a phenomenon (Davidson,1998). Contenders for interpretivist come from the constructivist, specifically, the idealist ontological view since they believe that reality can be fully understood only through the subjective interpretation of and intervention. Boland (1985), therefore, tightly associate interpretive research philosophy to *hermeneutics* - deriving hidden meaning from language, *ethnography* - the study of cultural groups over a prolonged period and *phenomenology* - the study of direct experience without allowing the interference of existing preconceptions.

5.1.2.2. Positivism

Positivist theorists posit that the meaningfulness of reality is independent of existence, in that, the world is external and objective to the research (Yee & Khin, 2015). Positivist theory applies systematic, scientific approach to research, with a worldview that everything that occurs around

us can be explained by knowledge of the underlying universal laws (Fitzgerald & Howcroft, 1998). Positivists are categorised into either quantitative purists or qualitative purists.

5.1.2.3. Critical Realism

Realists proffer that human ideology forms rather an insignificant part of reality. Like positivists, realists think that the external world is a given and that the existence of the external world is independent of thought or experience (Healy & Perry, 2000). Guba (1990) identifies critical realism as extracted from earlier views, particularly of Bhaskar (1975), that humans imperfectly conceive the natural causes of reality. Critical researchers take the critical realist ontological view and are, therefore, closely associated with the new reasoning of *post-positivism*. Habermas (1974), a proponent of critical thinking, summarizes critical theory as, unlike positivism, it is an approach with practical reason, critique, and reflective judgement, incorporated into principles of critical enquiry.

5.1.2.4. Pragmatism (Mixed method)

Pragmatism has emerged as new research paradigm that recognises and accepts variety of ways of interpreting the world if only they support an action, intervention or constructive knowledge (Goldkuhl, 2012; Iivari, 2007). As an alternative epistemological theory, pragmatism contends that are multiple ways to view reality and that empirical enquiry should be open to the researcher apply a mix of methods if found to be relevant in solving practical problems in the real-life situations (Creswell & Plano Clark, 2007; Rorty, 1999; Dewey, 1925) cited in Feilzer (2010). Pragmatists, therefore, do not have to be fastened to one method or technique (Iivari, 2007). The foundation of mixed research methods is on the pragmatist paradigm. Mixed methods research is described by Onwuegbuzie & Leech (2004) as offering great promise for practicing researchers who would like to see methodologists describe and develop techniques that are closer to what researchers use in practice.

Johnson et al. (2007) posit that mixed method can be viewed from the perspectives of qualitative dominance or quantitative dominance. They provide the definitions that distinguish between *qualitative dominant* and *quantitative dominant* mixed methods research. Qualitative dominant mixed methods research has been defined by Johnson et al. (2007) as the type of mixed research in which one relies on a qualitative, constructivist-poststructuralist-critical view of the research process, while concurrently recognizing that the addition of quantitative data and approaches are likely to benefit most research projects. They define quantitative dominant mixed methods research as the type of mixed research in which one relies on a

quantitative, post-positivist view of the research process, while concurrently recognizing that the addition of qualitative data and approaches are likely to benefit most research projects.

5.1.2.5. The Epistemological Research Paradigm of this Study

The question of epistemology is inherent to evaluation rigor in design science research as the issue of how ‘true knowledge’ is achieved in the research process is of concern. As stated above, knowledge objectively achieved is preferred in this research (Niehaves, 2007). Therefore, an objectivist ontology has been preferred for the artefact evaluation. Notwithstanding that, it must be emphasised that, generally, a design research is creative and involves subjectivity (Iivari, 2007). Maccani et al. (2015) refers to Action Design Research (ADR) as a particular case of Design Science Research rather than a methodology and it can assume two different epistemological paradigms. ADR is aimed at contributing to prescriptive knowledge. In this research, the aim is to generate a prescriptive knowledge by which IT audit practitioners can improve their practice. Prescriptive contributions are often associated with “how” research questions (Gregor & Hevner 2013; March & Storey, 2008), just as in this research which asks the question of;

‘How efficiently and effectively can systems-based framework for auditing provide solution to IT audit and assurance challenges in less regulatory environments?’.

To proceed to demonstrate the ‘how’ which DeGrace and Stahl (1990) describe as a ‘wicked question’, a combination of epistemological paradigms was necessary. From the outset, therefore, qualitative methods such as workshop and the application of skills, experience, technical and theoretical knowledge bases were employed to achieve an alpha design of an interventionist artefact. To this end, one would say the research employed qualitative techniques. Peffers et al. (2007) posit that, depending on the nature of the problem venue and the artefact, an evaluation of an artefact could take many forms. A rigorous design evaluation involves the process of observing and measuring how suitably the artefact supports the solution to the problem. In order to maintain objectivity, quantitative data analyses were employed alongside the earlier described qualitative evaluation methods. Thus, a survey technique was used in which a set of questionnaires was designed based on the conceptual framework and administered for data collection and analysis from the field. Therefore, in a research like this, it was impracticable to be either qualitative purist or quantitative purist in epistemological paradigm (Goldkuhl, 2012; Peffers et al., 2007; Hevner, 2007; van Aken, 2004). A typical pragmatic epistemological paradigm is, therefore, adopted for this study since it mixed both paradigms to achieve the desired outcome. Since either qualitative or quantitative analysis can

take objectivist ontological stance (Guba & Lincoln, 1994), it is strongly believed that a mixture of both can take objectivist ontological view and, therefore, the epistemological paradigm of this research is in alignment with its epistemological stance (Chow, 1991).

5.2. Cognitive Processes of Enquiry

A cognitive process of research enquiry and knowledge claim refers to the steps that a research adopts to construct new knowledge (Vaishnavi & Kueshler, 2004). Depending on a researcher's training and interest, scientific process of knowledge inquiry may take one of four possible processes or approaches namely; *inductive*, *abductive*, *retroductive* and *deductive* (Baker, 2000).

5.2.1. Inductive Process

Inductive enquiry process is informally known as bottom-up approach. Inductive reasoning, therefore, starts enquiry from specific observations and measures, begin to detect patterns and regularities through to the formulation of some tentative hypotheses. At the end of the enquiry is the development of broader conclusions helping the researcher to arrive at a theory. It is, therefore, often called theory-building research approach. The goal of a researcher with inductive objective is to infer theoretical concepts and patterns from observed data (Lawson, 2010; Kovács & Spens, 2005).

5.2.2. Abductive/retroductive Process

Kovács and Spens (2005) posit that abduction originates from a mistranslation and should be called retroduction instead. Scientists are finding it difficult in distinguishing between Abductive and Retroductive methods. By the description of Charles Sanders Peirce – an American philosopher (1839 - 1914), abductive and retroductive methods are essentially one and the same (Kovács & Spens, 2005; Eriksson & Lindström, 1997). These approaches involve the use of an analogy, creative or intuitive reasoning to make an inference or knowledge claim to explain an observed distant phenomenon. It involves reasoning used to mentally derive causal claims i.e. theory. If retroduction is to be any one of the forms of knowledge enquiry, then it functions as the initial test for the validity of the inference assigned to the causal explanation issued under abductive enquiry which may lead to the rejection of the original inference or hypothesis (Lawson, 2010).

5.2.3. Deductive Approach

Deductive enquiry is a strategic method in a research study in which the researcher starts the investigation from a more general to a more specific. Informally deductive enquiry has been called a top-down approach as opposed to the bottom-up approach in inductive reasoning. The diagram below (*Figure N*) demonstrates the deductive process of enquiry employed in this research.



Figure N. The deductive approach of enquiry in this research.

At the top or the beginning of the enquiry the researcher thinks up a conceptual solution of the problem through the lens of a *theory that helps in problem solution in the topic of interest* which is then narrowed down to more specific testable *hypotheses or propositions*. At the bottom or end of the enquiry the researcher then engages in *observations* or action to collect data to address the hypotheses to obtain a validation (or rejection) of the conceptual solution through *hypotheses testing* (Bhattacharjee, 2012).

5.2.4. The Cognitive Method of Enquiry in this Study

Design Science Research methodology (DSR) is a unique methodological approach to research that can combine both abductive and deductive methods of knowledge enquiry to achieve the research aim (Vaishnavi & Kueshler, 2004). The cognitive process of enquiry in this study is depicted in *figure O* below.

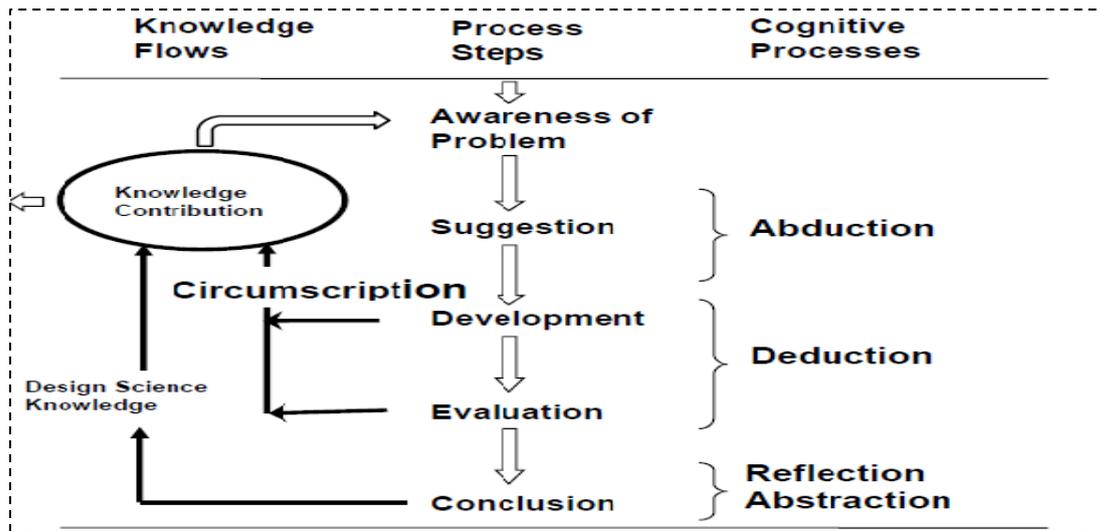


Figure O. *Cognitive Processes of Enquiry of the Study; Adapted from Vaishnavi & Kueshler (2004).*

Chapter one demonstrated the research design and described the workshop technique used to conduct the iterations in this research. The development of the artefact should be a search process that draws from existing theories and knowledge to come up with a solution to a defined problem (Peffer et al., 2007). Therefore, at the top of the enquiry, the viable systems approach was abductively selected to assist the researcher diagnose the research problem, to leverage a conceptual design of an intervention and to aid the development of a conceptual framework to proceed with the research. The iterative approach involved an in-depth literature as well as a discursive enquiry in the contextual practice environment through workshops with practitioners to leverage the literature reviewed. A workshop is defined in this research as a meeting at which the researcher engaged in discussions with focussed group of participants. Other significant purposes of the workshops were to obtain the opportunity of learning to identify emerging research themes, for debating relevant theory. These activities provided insights into the problem and laid the foundation for the inference that the framework used for auditing in less regulatory environment requires theoretical and practical paradigm shifts to efficiently and effectively add value. A creative development of conceptual solution design was subsequently built and demonstrated using knowledge foundation including COBIT framework, COSO guidance and the researcher's professional experience which culminated in the development of a conceptual framework for further development of the research. The iterative exercise involved here included obtaining proofs and inputs of practitioners in the design of interventionist solution and, finally, for collecting data for the rigorous subsequent evaluation of the framework. Respondents included professional auditors and IS audit practitioners,

directors, managers, lecturers and students related to the discipline who were expected to be end-users. This activity is indicated by the circumscription arrows. The end of this activity was characterised by the development of a conceptual model together with the conceptual hypotheses based on the conceptual model (see figure M in Chapter four).

At the bottom of the research value chain, another set of workshops were organised to obtain data on the views of the suitability of the framework in solving the research problem from practitioners and end-users through questionnaire technique. The design of the survey was guided by the construct in the conceptual framework and the aim of the evaluation was to validate the items in the construct and to confirm the propositions or hypotheses thereof based upon which to externalise or legitimise the knowledge contribution made by this research. The conclusion of the research was by reflection on the research problem and knowledge contribution which was towards improvement in the practice of information systems auditing for less regulatory environments. By the description of the knowledge creation process of this study, the researcher submits that the study adopted the deductive approach to scientific enquiry in the end.

5.3. Research Design

The design of a research is defined as the blueprint for conducting a research study that provides the researcher maximum control over factors that may interfere with the validity of the findings (Burns & Grove, 2010). A research design depends on the research question as well as the overarching aim of the research. It accounts for the overall contribution of the research, methods of data collection, and data analysis plan. As mentioned above, the research design of this study is Action Design Research (ADR) conducted in the pragmatist paradigm with aim to develop an IT audit framework - a prescriptive knowledge contribution to knowledge that is appreciated for being useful in action with practical value (Goldkuhl, 2012). ADR is a type of Design Science Research (DSR) has a goal of providing utility in the form of a designed artefact to solve identified business problems (Sein et al. 2011). It constitutes a fledging research methodological paradigm which draws its origin from what Simon (1996) refers to as the sciences of the artificial and engineering. (Hevner et al., 2004).

The alpha version of the framework development focussed on the nature of the framework based on the functional impact of the ingrained theory on the formative framework. Formative style of evaluation was, therefore, employed at this stage which resulted in the development of a framework for auditing that focussed on activities involved in the execution of auditing

process including the procedures for the planning and the customisation of the broad functions of the framework to achieve desired IT auditing or internal auditing outcomes. The beta version of the framework development adopted the summative style of evaluation which incorporates validated preconditions for proposed audit approach including the concepts and principles that make IS audit functions viable within the environment described. A research design is very important in the achievement of the research objective (Yin, 2013). A rigorous data collection and analysis was, therefore, required to achieve the objective of the design of the beta version of the framework as discussed below.

5.3.1. Case Study Research Design

A rigorous design evaluation may draw from many potential techniques, such as case studies, experiments, or simulations (Gregor & Hevner, 2013). In an applied research like this which aims at producing a prescriptive contribution to knowledge of the practice of information systems auditing, a case study and quasi-experimentation methods were found to be imperative to observe and to validate the effectiveness of the designed framework for IS auditing. Yin (2013) defines a case study as is an all-encompassing meticulous method of enquiry to investigate a problem within its real-life context to capture complexities so that the phenomenon and the context can be clearly studied at greater depth. This appropriately offers the researcher a prototype empirical situation to test and validate the new framework (Cooper, 2003) and to make a generalization based on the outcomes.

Yin (2012) describes the advantages of Case Study in various ways including emphasizing on the collection of data for the research study on real-world context in a natural setting, conducting and documenting evaluations as well as being ubiquitously capable of supporting research that address descriptive, prescriptive and exploratory questions. Yin (2013) further notes that a case study research approach is necessary in instances where the researcher intends to learn more about an organization, professional practice group or field of human activity or learning such as accounting or audit which is the focus of this study.

A case study emphasizes on the development of constructs, measures, and testable theoretical propositions or hypotheses (Hyde, 2000). Therefore, a case study is quite frequently used in combination with practice-led research. It is most suitable when applying theory to an already operational organization, with the researcher having the privilege to participate in the daily processes of the organization allowing for better, holistic and meaningful understanding of the characteristics of real-life events, such as the organizational and managerial processes (Berg & Lune, 2004). A Case study was found to be pertinent because the research addresses a

prescriptive question with an aim to evaluate an initiative's effectiveness in producing a particular outcome, i.e. effective solution to IT audit challenges in less regulatory environments.

5.3.1.1. Multiple Case Study

Yin (2012) avers that, in conducting a case study research, one should decide on the suitability of the choice between either of what might be labelled as single or multiple case study. In the discussion of how to keep a case study holistic, a better result is often attributed to a two-by-two matrix which leads to four different case study designs. Unlike a single case study which studies one single large organization or event which may have multiple analysis design, a multiple case design studies two or more different organizations or events for the deliberate purpose of testing the 'conditions under which the same findings might be replicated or deliberate contrasting cases. For this study, multiple case study design was found to be more appropriate. It was necessary to ensure the participation of organisations of variety of sectors of the economy to achieve fair representation in the research outcome and increase confidence in the externalization of the findings. Four organizations in Ghana shown below were, therefore, selected for multiple case study design.

A full experiment, i.e. full IT auditing framework experimentation, would have been useful in a project like this. However, because of some challenges including time constraint and logistical requirements that are typically associated with full experimental designs, a full experiment was not found to be feasible. Again, a full IT auditing framework testing can only be carried out in the natural setting or in real business environment. However, access difficulties and ethical concerns made it very impracticable for a full experiment to be conducted since a full experiment would involve accessing confidential information in the target organizations. A quasi-experimentation was, therefore, adopted to proceed with the testing and the validation processes of the designed framework. Quasi experimental design refers to the application of an experimental mode of analysis and interpretation to bodies of data not meeting the full requirements of experimental control (Cook, 2015; Campbell & Riecken, 1968). Previous research that adopted quasi-experimental approach and or multiple case study include (Spagnoletti, Resca & Lee 2015; Ralph, 2014).

5.4. Sample frame, sampling method

Sampling method in this study was preceded by defining the sample frame. A sample frame refers to a subset of members of a population from which a sample is taken (Wright, 2005). It is an accessible segment of the target population from where a sample can be drawn

(Bhattacharjee, 2012). In this study, as stated above, Ghana was selected as the country for the investigation since it shares the characteristics of less regulatory environments as characterised in chapter one. Another reason for the choice of Ghana is the element of convenience. The researcher Ghanaian National and in case study research like this, the researcher can obtain greater access to information when he or she is familiar with the data collection sites.

The issue of sampling in a case study research is complex because of a variety of ways and flexibility in sampling strategy involved. The aim of a study should, however, be the guidance for the choice of the sampling strategy. Sampling in case study research involves decisions that the research makes in terms of the choice and number of cases to study (Poulis et al., 2013). Selection of cases is an important aspect of hypothesis testing from case studies. Sampling in case study is purposeful and that involves the selection of information-rich cases for in-depth study. The selection of data collection site was by a purposive sampling method. Purpose sampling method was found to be most expedient for the study because of the need to obtain quick access to targeted samples and because there were no concerns for sampling proportionality. Sampling representativeness was ensured by selecting two public sector organisations and two private sector organisations. The data collection sites were, therefore, selected with the purpose of accessing information-rich case sites. Information-rich sites are those that, per the judgement of the research, has great deal of information that will be very crucial to the success of the research and would support confidence in the generalisation process (Mills et al. 2010). Also, the sites were carefully selected to include both public sector and private organisations that had sufficient IT in their business organisation and, therefore from the researcher's judgement, had the people who appreciated the concept of IT auditing including practitioners who could provide the proofs and responses to questions designed to confirm or reject the hypotheses about the conceptual framework of the research. Selected sites included the Ghana Audit Service – a constitutional institution charged with the audit of public service organisations which has experts and practitioners with rich experiences, Kumasi Technical University which has a lot of audit professionals and business IT auditing students, Sekyedumase Rural Bank Limited – a member of Apex Bank of the Bank of Ghana and Sun Shade Foundation, private sector financial NGO (non-governmental organisation) regulated by the Bank of Ghana.

5.4.1. Data Collection Sites

A description of the data collection sites is presented in table below to provide the reader with background to the cases studied.

Table 11. Cases selected

Name of Case	Sector	Industry	Description	Participants in type	No. of responses submitted
Ghana Audit Service	Public	Service (Auditing)	The Ghana Internal Audit Service is made up of professionals and highly educated persons whose function is to conduct audits, evaluation and monitoring of Ministries, Departments and Agencies of the Government of Ghana.	This is the body that undertakes the statutory internal audit service of the public sector. The Kumasi office was the unit used for the study.	36
Sekyedumase Rural Bank Limited	Private	Services (Financial) sector	A registered financial institution that has seven branches across the Ashanti region of Ghana. It is regulated by the Bank of Ghana and member of the ARB Apex group.	Members of staff from the internal audit section, management team and some Directors.	14
Sunshade Foundation Limited	Private	Charitable (NGO)	Very innovative financial NGO with impeccable record from the regulator, Bank of Ghana in Kumasi, Ghana.	Directors, internal auditors and management team	5
Kumasi Technical University	Public	Education	This university has high concentration of professionals in ACCA, ICAG, CISA in the department of Accountancy and Information Systems in Ghana. It was selected to be information rich because of its status of training accounting graduate and professional accountants with students pursuing modules in IT auditing.	Lecturers, Students, Accountants and Audit Practitioners including the internal audit staff of the University.	81
TOTAL PARTICIPANTS					136

5.5. Construct Measurement and Research Instrument Design

Mullarkey and Hevner (2015) demonstrate that a concept design in ADR ensures that an expected design based on the ingrained theory emerges from the iterative interactions of the researcher and the practitioners on the field. It forms part of the rigorous evaluation of design principles and features. This involved the adoption from the ingrained theory the constructs, i.e. qualities, concepts and relationships which informed the building, intervention and evaluation (BIE) of action. Effort was made to ensure that the extraction, adoption and operationalisation of construct variables reflected prior validated studies in extant literature that report high validity score in the measurement of qualities of effective and efficient framework for auditing demonstrated in the conceptual model in Figure M in the previous chapter. Twenty (20) variables were extracted and adopted to constitute the items in the construct in the conceptual model as follows: 1. *Autonomy*; 2. *Flexibility*; 3. *Customizability*; 4. *Voluntariness*; 5. *Systematization*; 6. *Operations*; 7. *Coordination*; 8. *Investigation*; 9. *Intelligence*; 10. *Policy*; 11. *Responsiveness*; 12. *Proactivity*; 13. *Agility*; 14. *Recursion*; 15. *Audit Risks* 16. *Relevance*; 17. *Transparency*; 18. *Timeliness*; 19. *Irregularity*; 20. *Uncertainty*. These items were subsequently grouped into six (6) factors or domain.

5.5.1. Data Collection Techniques

There are several methods for data collection where quantitative data analysis is contemplated but the most traditional and handiest method remains by survey method. Research using questionnaires has been popular in IS compared to other methods of data collection questionnaire technique supports both quantitative data analysis and the epistemological paradigm of this research. Questionnaire provides respondents higher degree of comfort in providing fair and independent opinion and responses than face-to-face interviews. The technique is relatively easy to administer and gathers relatively efficiently large amounts of data at a low cost and time. Structured and predefined response questionnaire permits respondents to provide answers about themselves or some other unit of analysis such as their work group, project, or organization and remain anonymous (Sivo et al. 2006). In the data collection process, each of the 20 variables in the conceptual model was represented by a question/statement which respondents were requested to agree or disagree based on a Likert Scale of 1-5; where 1= Strongly Disagree; 2= Disagree; 3=Somewhat agree; 4=Agree; 5= Strongly agree. Target respondents included practising auditors in the field, IT professionals and other expected end-users of the research outcome such as lecturers, students, directors and senior managers selected from the data various collection sites. To achieve improved clarity of

the structured questionnaire administered to them two professors reviewed them. This resulted in clearer explanation of each question requirement and the reduction of the number of questions. The length of time required to complete the survey was, therefore, estimated to be 10 minutes. Table 11 below represents the key questions used to measure the items together with the relevant references.

Table 12: Measured items of the construct.

Item No.	Key Statements	Item, Code and description	Scale Used	References
1.	Diagnostic IT auditing procedures should start by evaluating the core business processes to understand operational risks and the local control environments.	F1 - Operations – Operations stands for the set of units of business processes within business value chain to which IT processes can be identified and for that matter IT audit can be autonomously conducted to examine the extent of the achievement of operational objectives effectively.	This is measured by Likert scale <i>1= Strongly Disagree; 2= Disagree; 3=Somewhat agree; 4=Agree; 5= Strongly agree.</i>	John & Cianfrani (2017); ISACA, (2013) Ray (2009); Simons (1995); Espejo & Gill, (1995).
2.	There should be a separate IT audit procedure for coordination which identifies weak links within the process control environments with recommended IT responses.	F2 - Coordination – Coordination stands for the purposeful evaluation organisational use of IT to safeguard not only tangible IT assets but also to business intangibles such as capability and the effectiveness of links among subsystems of business process enablers to determine the possibility of process improvement.	This is measured by Likert scale <i>1= Strongly Disagree; 2= Disagree; 3=Somewhat agree; 4=Agree; 5= Strongly agree.</i>	Razak & Muhamad (2017); Ray (2009).
3.	Fraud risk investigation and control in less regulatory environments should involve	F3 - Investigation – Monitoring and Investigation stand for the plausibility of the examination of fraudulent non-	This is measured by Likert scale <i>1= Strongly Disagree;</i>	Kultanen (2017); Ficco & Rak (2017).

	continuous concerted feedforward IT audit process and not a one-off yearly event.	compliance with rules and regulation and intentional overrides of ethical behaviours discover irregularities as a required IT audit function.	2= <i>Disagree</i> ; 3= <i>Somewhat agree</i> ; 4= <i>Agree</i> ; 5= <i>Strongly agree</i> .	Buffa & Basak (2016); Chandler (2014).
4.	There should be a procedure for intelligence auditing which sufficiently addresses internal and external corporate pain points matching them to their associated opportunities from the total environment.	F4 – <i>Intelligence</i> – Intelligences refers to IT audit function of deliberately observing and picking signals from the flux of information from the control environments for the projection of future threats and for the pre-emption of countermeasures.	This is measured by Likert scale <i>1= Strongly Disagree</i> ; <i>2= Disagree</i> ; <i>3=Somewhat agree</i> ; <i>4=Agree</i> ; <i>5= Strongly agree</i> .	THEIIA (2017) ; Varkoi et al. (2016) ; Bell et al. (1997).
5.	An effective framework of IT auditing should have a separate procedural requirement to evaluate IT strategies and executive policy to achieve organizational goals.	F5 - <i>Policy</i> – Policy audit function stands for the need for IT auditors to evaluate governance and corporate level issues to affect the functions of those charged with governance and decision making.	This is measured by Likert scale <i>1= Strongly Disagree</i> ; <i>2= Disagree</i> ; <i>3=Somewhat agree</i> ; <i>4=Agree</i> ; <i>5= Strongly agree</i> .	Gregg (2007); Rossouw (2005).
6.	An effective IT auditing is one that rigidly complies with strict audit standards for auditing business units that act on their own within the organisation to effectively determine their purpose in the total system.	V1 - <i>Autonomy</i> – Autonomy underscores the relevance of obtaining compliance with standards of business processes audit that are IT related for effective diagnostics.	This is measured by Likert scale <i>1= Strongly Disagree</i> ; <i>2= Disagree</i> ; <i>3=Somewhat agree</i> ; <i>4=Agree</i> ; <i>5= Strongly agree</i> .	Marcello et al. (2017); Swanson & Marsh (1993).

7.	An adaptive framework for IT auditing should have a term for a broad class of flexible learning and responses for different organisational contexts.	V2 - Flexibility – Flexibility stands for independent professional judgement which is a prerequisite for a successful IT auditing.	This is measured by Likert scale <i>1= Strongly Disagree;</i> <i>2= Disagree;</i> <i>3=Somewhat agree;</i> <i>4=Agree;</i> <i>5= Strongly agree.</i>	Walker et al. (2002).
8.	A viable framework for IT auditing must espouse identifiable set of recommended procedures while keeping options as open as possible for different organisational contexts.	V3 - Customizability – Customisability refers to the need for functions of an efficient IT auditing to contain the requisite number of focused activities depending on the structural differences of different organisations.	This is measured by Likert scale <i>1= Strongly Disagree;</i> <i>2= Disagree;</i> <i>3=Somewhat agree;</i> <i>4=Agree;</i> <i>5= Strongly agree.</i>	Tay (2017);
9.	A resilient IT audit framework is one with the capacity to support non-mandatory adoption of best practices to maintain its functions and controls.	V4 – Voluntariness - Voluntariness refers to espousing an approach to the adoption of best practice guidelines practices by means of choice to encourage full compliance.	This is measured by Likert scale <i>1= Strongly Disagree;</i> <i>2= Disagree;</i> <i>3=Somewhat agree;</i> <i>4=Agree;</i> <i>5= Strongly agree.</i>	Gunningham & Sinclair (1999).
10.	IT audit planning and execution for less regulatory environments should be couched in systematic procedures that reflect	V5 - Systematization – In an increasingly complex Governance, Risk Management and Compliance regime, systematization in IT auditing implies an approach of recognizing	This is measured by Likert scale <i>1= Strongly Disagree;</i> <i>2= Disagree;</i> <i>3=Somewhat</i>	ISACA (2013); Merhout & Havelka (2008); Iyengar, (2007);

	organizational architecture.	that in fixing one broken thing in one process, other processes may require adjustment to match the change to ensure that the entity works as a unified whole.	<i>agree;</i> <i>4=Agree;</i> <i>5= Strongly agree.</i>	Ha (2005);
11.	A viable systems-based IS audit framework should guide practitioners by providing critical prompts to address a broad range of issues in every organizational context.	C1 – Responsiveness – Responsiveness stands for the ability to address a full range of risk from strategic, operational, compliance, reporting, security, environmental and contingent IT issues in an appropriate and proportionate manner.	This is measured by Likert scale <i>1= Strongly Disagree;</i> <i>2= Disagree;</i> <i>3=Somewhat agree;</i> <i>4=Agree;</i> <i>5= Strongly agree.</i>	Cassidy (2016); Rittenberg (2013); Chambers (2009).
12.	To effectively participate in the fight against fraud and corruption IT audit should move away from reactivity to events to proactive approach.	C2 - Proactivity – Proactivity refers to the need for IT audit to adopt preventative approach to auditing rather than the traditional reactive approach.	This is measured by Likert scale <i>1= Strongly Disagree;</i> <i>2= Disagree;</i> <i>3=Somewhat agree;</i> <i>4=Agree;</i> <i>5= Strongly agree.</i>	Marcello et al. (2017); Schillemans and van Twist (2016); Osei-Afoakwa (2013); Chambers (2009). Ha (2005).
13.	A framework for IT auditing must be embedded with the quality that supports quick changes that allow for capacity building, learning and knowledge management systems.	C3 - Agility – As business progress on the path of increasing technology integration for the improvement of efficiency of their business processes, agile IT audit planning approach is an important principle that must characterise IT audit to match the trend	This is measured by Likert scale <i>1= Strongly Disagree;</i> <i>2= Disagree;</i> <i>3=Somewhat agree;</i> <i>4=Agree;</i> <i>5= Strongly agree.</i>	Deloitte (2018); John & Cianfrani (2017); Schillemans & van Twist (2016); Omonuk & Oni (2015); Chambers (2009).

		and to improve its future relevance.		
14.	An IT audit framework should be driven by value delivered through continuous assessment with short communication cycles.	C4 - Recursion – Recursion refers to continuity which concerns the relevance of continuous monitoring and continuous auditing in which repetitive tasks e.g. checking errors and verifying violation of controls on real-time basis can be automated.	This is measured by Likert scale 1= Strongly Disagree; 2= Disagree; 3=Somewhat agree; 4=Agree; 5= Strongly agree.	Deloitte & Touche LLP et al. (2012); Alles et al. (2005); Espejo (2003).
15.	Since complexity destroys complexity, audit of the future demands expanded scope of risk assessment based on continuous learning to stand up to the increasing sophistication of business.	S1 - Risks – Risk refers to the risk-based approach to auditing and avoidance of the possibility that the IT audit practitioner would issue inappropriate reports due to the inappropriateness of the audit approach due to increasing complexity.	This is measured by Likert scale <i>1= Strongly Disagree;</i> <i>2= Disagree;</i> <i>3=Somewhat agree;</i> <i>4=Agree;</i> <i>5= Strongly agree.</i>	Buffa & Basak (2016); Knechel & Salterio (2016); Egbunike (2014);
16.	Audit of the operational environments is relevant if it involves the assessment and determination of the match between management strengths and capabilities on one side and the environmental forces that pose threat and increase their vulnerabilities on the other.	S2 - Relevance – In a rapidly evolving pace of technology and changes in business models, relevance of IT auditing stands its capacity to fulfil current and future client-centric expectations.	This is measured by Likert scale <i>1= Strongly Disagree;</i> <i>2= Disagree;</i> <i>3=Somewhat agree;</i> <i>4=Agree;</i> <i>5= Strongly agree.</i>	Philipson et al. (2016); Burgess & Wake (2012); Popa (2009).

17.	There is currently weak match between the complexity in the business horizon and Internal and IT auditors' capacity to support innovative actions that allow the organizational system to deal with environmental vagaries.	E1 - Irregularity – Irregularity stands for the endemic behaviours which include poor internal controls and fraud within business organisations in developing countries with weak regulatory systems.	This is measured by Likert scale 1= <i>Strongly Disagree</i> ; 2= <i>Disagree</i> ; 3= <i>Somewhat agree</i> ; 4= <i>Agree</i> ; 5= <i>Strongly agree</i> .	Osei-Afoakwa (2013) ; Ebimobowei et al. (2011) ;
18.	The current approach to IT auditing is saddled with weak capacity to address current internal and external threats and the opportunities of the future environments with reasonable certainty because the framework used does not support it.	E2 - Uncertainty – Uncertainty stands for the current or future inherent IT audit exposure to failure within less regulatory environments due to lack of informed guidance and skills to stand up to the challenge.	This is measured by Likert scale 1= <i>Strongly Disagree</i> ; 2= <i>Disagree</i> ; 3= <i>Somewhat agree</i> ; 4= <i>Agree</i> ; 5= <i>Strongly agree</i> .	Walker et al., (2002).
19.	Brisk communication of audit output enabled by an IT audit framework would greatly minimize transparency challenges and improve stakeholder confidence.	M1 - Transparency - Audit communication is about the inherent conveyance of the integrity, objectivity, independence, professionalism, professional behaviour and confidentiality that are crucial ethical features that must characterise the output of the practice.	This is measured by Likert scale 1= <i>Strongly Disagree</i> ; 2= <i>Disagree</i> ; 3= <i>Somewhat agree</i> ; 4= <i>Agree</i> ; 5= <i>Strongly agree</i> .	Osei-Afoakwa (2013) ; Ebimobowei et al. (2011) ;
20.	Timely audit data translation and communication between audit practitioners and stakeholders of audit output is key to survivability of the auditee and	M2 - Timeliness – This refers to an emerging IT audit philosophy that is about the need to develop spot-on and timeous awareness creation capabilities by the auditor using variety	This is measured by Likert scale 1= <i>Strongly Disagree</i> ; 2= <i>Disagree</i> ; 3= <i>Somewhat agree</i> ; 4= <i>Agree</i> ;	Walker et al., (2002).

	viability of the audit practice.	of emerging technologies.	5= <i>Strongly agree.</i>	
Data Description	This is measured by close ended question – B1 = Qualification, B2 = Discipline, B3 = Profession and B4 = Experience.			

5.5.2. Data Analyses process

The use of a paper-based questionnaire required that the data from the individual questionnaire were inputted into the statistical package for social sciences (SPSS) software for analysis. SPSS is an advanced research software that is widely employed for analysing a range of statistical data. Data analysis was conducted using the SPSS statistics software, version 22. Demographic profiling was used in this study to segment the sample. Each of these variables is tabulated to present descriptive findings. The demographic factors in this study included: level of education, position, status and years of experience in practice.

In dealing with the issue of missing data, Byrne (2001) suggest certain scenarios. These included: (i) investigating the total amount of missing data, (ii) investigating the pattern and impact of missing data, (iii) identifying appropriate techniques, where required, to deal with missing data. In a case study approach, as in the case of this research, sampling was purposeful and as a result data screening was focused on only the screening out of missing data within the questionnaire (Mills et al., 2010). Therefore, the criteria in the table below was used to deal with missing data and to ensure that the data collected for this study were of integrity.

Table 13 - Criteria for deleting missing data

Rule of Thumb
(i) Where less than 15% of variables is missing, data may be deleted but where treated but where 20-30% then data may be treated. To ensure through personal administration of questionnaire that substantial data deletion is avoided.
(ii) In event of variation, an attempt may be made to perform the analysis to include the deleted cases or variables to determine the significance of the variation.

5.5.3. Quality Control of the Research Instrument

Four tests are recommended by Yin (2009) for controlling quality and honing validity and reliability. These are *construct validity*, *internal validity*, *external validity* and *reliability*. Construct validity control in this study was aimed at monitoring the extent to which the operationalisation of the theoretical construct and instruments for the research legitimised inferences made. Internal validity control ensured that the data analysis reflected the objectives set for the research and no other variables apart from those under investigations caused the result. The researcher elected the use of the PLS SEM statistical method of validation (see Table 14 below). This method was found to be expedient due to the dearth of IT audit experts in the field together with other envisaged challenges such as financial impact on the researcher, time and other resources required to deploy the Delphi method. The PLS SEM statistical method of validation is also a valid alternative to achieve the same outcome in an academic research like this study. It has, however, been recommended that future research could use methods such as the Delphi method to validate the model.

External Validity control was purported to ensure that the research output has the quality to fit well in generalization of the results. Reliability control was mainly to make sure that the results are consistent and replicable in similar conditions. The **Table 13** below demonstrates the specific measures quality control activities undertaken.

Table 14. – Method of Construct Reliability Tests

Quality control tests	Research tactic	Research stage	Action taken
<i>Construct Validity</i>	Used of multiple case study including self-administered paper-based questionnaire.	Data collection	Held workshops with focused group participants. Additionally, administered paper-based questionnaire to participants after workshop to respond to prepared questionnaire on Likert Scale basis.
	Experienced professors reviewed questionnaire.	Content review	Two experienced Professors proof-read the questionnaire and commented for amendments were necessary to be made.

Internal Validity	<p>Specified the indicators used to measure each construct in the research model and evaluated the extent to which a set of measures are consistent in representing their target construct.</p> <p>Factor analysis was used to facilitate a search for variables that could be independent of the observed variables believed to be inter-dependent for any possibility to reduce them.</p> <p>Factor analysis is one of the most useful methods for studying and validating the internal structure of instruments.</p>	Data Analysis	<p>Interpretation/implication of statistical test scores.</p> <p>Cronbach Alpha test and factor analysis were used to validate the domain items and to confirm and fine-tuned the variables respectively. Cronbach's alpha test is popular for the testing of the internal consistency of responses to all items measured in a construct and reflects the extent to which independent items of a construct correlate with each other (Nunally, 1978).</p>
		<p><i>Cronbach's Alpha (Internal consistency of construct)</i></p> <p><i>Entire Model Reliability and Validity tests</i></p>	<p>Alpha value (α) of 0.60 is the least reliable value while 0.70 is good in initial phases of theory development or in adaptations of new measurement instruments. Alpha values (α) of 0.80 are deemed as good and represents a strict minimum for advanced stages of instrument development. 0.90 or above is excellent (Gliem & Gliem, 2003; Nunnally & Bernstein, 1994).</p> <p>In a PLS-Algorithm, a composite reliability test was used to assess internal consistency. Values greater than 0.7 are adequate. A convergent validity test to assess variability from the threshold value of 0.5 (McDonald & Ho, 2002).</p>
	<p>Factor Loading provided a means to test for whether items cast under the domains reflected what the respondents actually opined and that responses were consistent.</p>	<p><i>Factor loadings analysis.</i></p>	<p>Factor analysis for identifying underlying factors where eigen values are greater than 1.0. The 'varimax' rotation method seeks to maximize variances of the loadings. This supported the validation and refinement of the data. The correlation of each indicator with its associated construct must be larger than its correlation with any other construct. (Helfrich et al. 2007; Hair et al., 1998; Tabachnick & Fidell, 1996).</p>

	Evaluated all factors together and each factor separately against the hypothesis that there are no factors as well as the appropriateness of factor analysis.	<i>Kaiser-Meyer-Olkin (KMO) and Bartlett's test of Sphericity.</i>	This helped to determine whether factor analysis technique was appropriate for further analysis of the data. If the test value is large and the significance level is small (< 0.05), the hypothesis that the variables are independent can be rejected for further factor analysis.
External Validity	Multiple Case study	Research Design	Applied literal replication logic with same set of questionnaires to all data collection sites.
Reliability	Developed and used in case study protocol and database respectively	Data Collection	Same data collection procedure followed for each case with consistent set of questionnaires for each focused group participants.

5.5.4. Conceptual Model Testing

The partial least square approach in structural equation modeling was used in assessing the interconnectedness among latent variables. The approach combined both factor and multiple regression analyses to measure the structural relationships of the entire conceptual model. This was necessitated for the computation of causal relationships in the literature that motivated the conceptual hypotheses. The PLS-Algorithm of the SMART-PLS was used in analysing the data in the structural equation model framework. The objective was to test the model reliability – composite reliability and convergent reliability by showing the strength, direction and relations using paths analysis among the latent variables. In furtherance to that, the weighting scheme, paths in the PLS-Algorithm was used to estimate the path coefficients and loadings among the latent variables in the entire model (McDonald & Ho, 2002).

5.5.5. Hypotheses testing

Regression and Correlation analysis was performed to estimate the best straight lines to summarise the relationships hypothesized in the conceptual model. An Analysis of Variance (ANOVA) was used for the determination of the statistically significant differences among the means of the independent domains. This approach was necessitated because the focus of the conceptual hypotheses was to confirm or reject the linear and colinear direction of influences between the independent and dependent variables. Hence, the purpose of the hypotheses testing was to confirm or reject the predicted relationship among the variables. The results were used to reflect and emphasize not only on the preliminary design of the conceptual model developed

on the substrates of the viable systems model by the researcher but also on its subsequent refinement through the perspectives of practitioners and end users who participated in the study (Sein et al. 2013). Figure P below is a recast of the conceptual hypotheses based on the conceptual model.

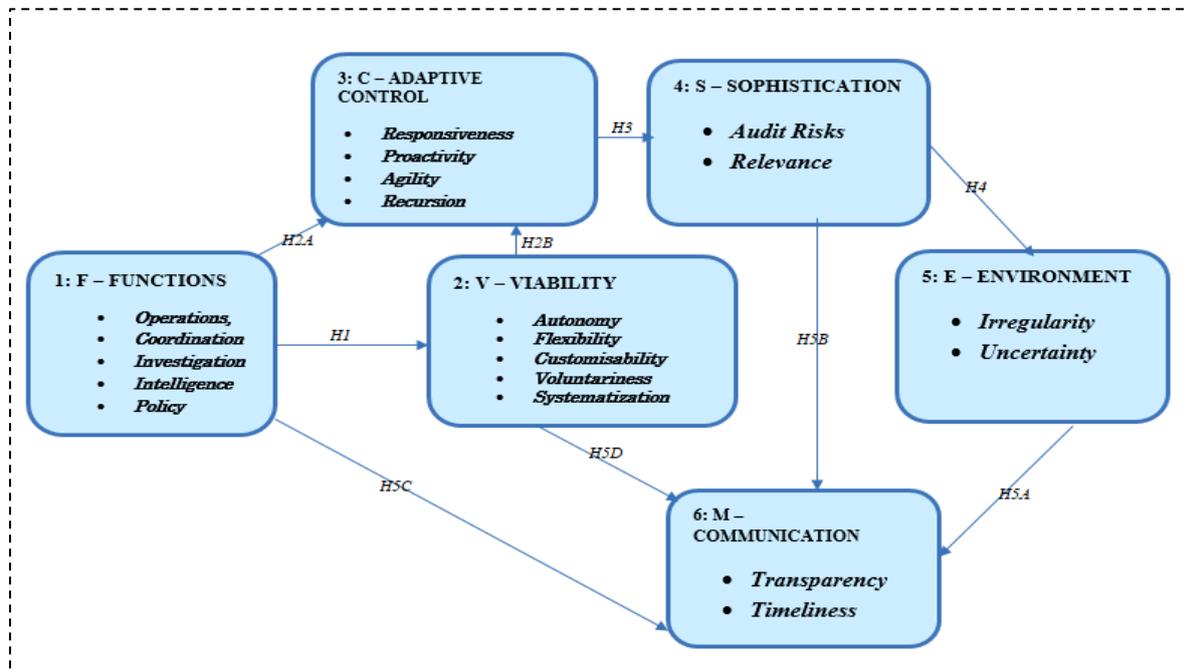


Figure P: Conceptual hypotheses

5.5.5.1. Measurement Models

The techniques in Table 15 below summarises the structural techniques used for the evaluation of the model and the hypotheses testing. The table presents in examining the criteria for the measurements.

Table 15. Evaluation Criteria for Measurement Model.

Appraisal technique	Formulae	Notes
Coefficient of Determination - (R ²): This is the proportion of an endogenous constructs variance that is explained by its predictors.	$r = \frac{“n(\sum xy) - (\sum x)(\sum y)”}{[n(\sum x^2) - (\sum x)^2][n(\sum y^2) - (\sum y)^2]”}$	(i) R ² measured how well the model is predictive of the data. The higher the R ² the greater the predictive or explanatory power (Nils & Ahlemann, 2010). A minimum value of 0.10 of R ² should be significant (Falk & Miller 1992).

<p>Path Coefficients of Determination: (β). This is a measure of the weights used to examine possible causal links in the model.</p>		<p>Path coefficients are evaluated using absolute value, significance and sign. Values close to 1 (or -1) are suggestive of strong causal influence of a latent variable on their linked variable. Values close to 0 suggest weak influence (McDonald & Ho, 2002). Values more than 0.2 (or below -0.2) are regarded as substantial (Chin, 1998).</p>
<p>F-Statistic: This assesses the impact of a given predictor variable on a criterion variable (Chin, 2010).</p>	<p>When probability (p-value) is less than specified significant level to justify the confirmation or rejection of hypotheses.</p>	<p>F-test in Analysis of Variance (ANOVA), was used for the determination of the statistically significant differences among the means of the independent domains (Chin, 2010). Cohen (1998) provides values of 0.10, 0.25 and 0.40 as representing small, medium and large respectively.</p>

5.6. Consideration of Generalisability of Outcome

To increase validity of generalisation in case study research, Yin (2009) encourages the selection of cases using either theoretical replication logic or literal replication logic. Theoretical replication is whereby the researcher applies similar experiments to the selected cases and expects contradictory outcomes. Literal replication refers to whereby a single form of experiment is replicated in all the selected cases. Either way the reliability of the findings is enormously amplified when both types of cases form part of the research design (Markon et al., 2011). Literal replication logic was applied to increase external validity of outcome. Furthermore, as in hypothesis-testing research, the concept of a population is crucial, because the population defines the set of entities from which the research sample is to be drawn. The selection of an appropriate population controls extraneous variation and helps to define the limits for generalizing the findings (Poulis et al., 2013). A sample population refers to all individuals or items possessing characteristics that a researcher seeks to examine (Bhattacharjee, 2012). Ghana, where the study is focused, being within less regulatory environments, constitutes a sample population. On the basis that the external validity analysis and criteria for legitimization of the framework is by inference that concepts already believed to be true beyond all reasonable doubt in the sample population are sufficiently true for all the population that share similar characteristics, it is claimed, therefore, that the external validity

of the research output is applicable in all developing countries with less regulatory environments.

5.7. Ethical Considerations

The application of ethics is very vital in a research in which the researcher requires the collection, analysis and reporting of data obtained from a focused group of participants. The purpose for which ethics is required concerns privacy and confidentiality. Therefore, formal approval was obtained from participating organisations. The approval of the ethics application was subject to the University of Cape Town's designated official's satisfaction as to participant's anonymity, confidentiality of data, and voluntary participation for clearance.

During data collection, that is, at the beginning of every workshop, it was explained to the participants that participation in this study was voluntary and data collection was conducted on anonymous basis. Furthermore, prior to administering the questionnaire to participants, it was made clear to all participants the research significance and the type of information being collected. Also, the participation in the study was based on their interest in the subject. They are under no obligation to participate and that they were strictly to respond to the questions in accordance with the Likert scale provided and not to include personal information about subjects. Furthermore, anonymity and confidentiality of data was ensured by assuring participants that they were not required to provide any identifying information beyond their basic demographic details agreed upon and that only aggregate results would be reported and, therefore, participants are not identified by name in the final report. Data collected from this research is to be kept confidential. No third parties would be permitted to access the raw data.

5.8. Chapter Conclusion

The chapter provided a comprehensive analysis of the philosophical views of this research. The philosophical analyses involved the discussion of the ontology of research in which the stance of this research was identified. In addition to the discussion of the ontology, the chapter gave detailed analyses of the epistemological views of research and situated the view of this this research. The chapter further considered the research strategy and methods of data collection. In it, detailed discussion was provided on the research instruments design and the techniques and processes for data analyses and ethical considerations. The next chapter presents the data analysis and reports. The next chapter will apply the quantitative methods described in chapter five such as factor analysis to evaluate the reliability of the framework and use the PLS SEM to evaluate and validate the entire framework. The research hypotheses will be tested by an analysis of variance (ANOVA) in furtherance of the development of the subject matter of the study.

CHAPTER SIX

DATA ANALYSIS AND REFLECTION ON LEARNING

6.0. Introduction

One usefully unique aspect of ADR as a design science research is the opportunity to, after the authentic and concurrent evaluation, perform internal analysis and reflect on the built artefact based on the contributions and views of practitioners and participants. This was necessitated in the second iteration to the field to solicit the views of practitioners and end-users using structured questionnaire technique. In this chapter statistical tools together with careful observation and professional judgement were employed as guide to the analysis and reflection of the outcomes of respondents' responses to validate the designed model and to either confirm or reject the hypotheses developed from the initial conceptual model. The chapter ends in the design of a meta-artefact, i.e. the framework emerging as the beta version is designed with the relevant knowledge or validated assertions of general learning for efficient and effecting IS auditing in less regulatory environments.

6.1. Respondents Characteristics

This study characterized respondents by their Level of education, Position at their current work place, status and their number of years of working. For the levels of education of respondents, the study's findings demonstrated that 41.2% of the respondents were Higher National Diploma (HND) graduates, with 38.2% being degree holders, 11.0% have some form of Professional certificates, 8.8% with master's degrees and 0.7% PhD holders. Perhaps, because of the fledging nature of IT audit practice in the empirical situation, the number of IT auditors available to provide responses was not as would have been expected. Professionals from the internal audit agency and accounting degree holders responsible for internal auditing were targeted for responses since their duties and experiences were relevant to the research. For the position of respondents, therefore, the study's findings demonstrated that 78.7% of the respondents were accountants and professionals who worked in the internal audit service of Ghana, with 11.8 % being in the IT Auditing practice. 2.2% were in the management class, and 3.7% each were found to belong to the IT and other departments respectively. Table 16 below summarises respondent characteristics.

Table 16. Respondents characteristics

		<i>Frequency</i>	<i>Percent</i>
Level of Education	HND	56	41.2
	1st Degree	52	38.2
	Professional	15	11.0
	Masters	12	8.8
	PhD	1	.7
Position	IT Auditing	16	11.8
	Management	3	2.2
	Internal Auditing	107	78.7
	IT	5	3.7
	Other	5	3.7
Status	Student/trainee	67	49.3
	Auditor	32	23.5
	Manager	5	3.7
	Director	7	5.1
	Other	25	18.4
Years of working	<1 year	27	19.9
	1 - 2 years	43	31.6
	2 - 5 years	18	13.2
	5 years	20	14.7
	Other	28	20.6
	Total	136	100.0

In relation to status of respondents, IT audit students and field trainee staffs of the internal audit service, who are the position to appreciate the research idea and expected to be key end-users of the proposed framework, highly contribute as respondents. They constituted 49.3% of the respondents. Auditors in the category of practitioners in the field provided 23.5% of the total responses due to the dearth of their numbers in the empirical situation. Managers at senior levels in both public and private sector organisations selected for the study provided a total of 3.7% of the responses and members of various of Board of Directors in both public and private organisations that participated in the study constituted 5.1% of the respondents with about 18.4% not unspecifying their status. These provided a wide spectrum of views of practitioners and end-users of the output of the study.

The working experiences of the respondents, likewise, portray a cross section of broad of experiences suitable for a study like this. For the number of years of working, the study's findings reveal that 19.1% of the respondents had worked for less than a year. 31.6% out of the respondents have worked for 1-2 years in their respective roles. 13.2% have working

experience of 2-5 years. 14.7% have working experience more than 5 years and 20.6% chose not to disclose or specify the number of years of experience at their roles.

6.2. Reliability Analysis

The reliability of a **measuring instrument** is defined as its ability to consistently measure the phenomenon it is designed to measure (Ponterotto & Ruckdeschel, 2007; Gliem & Gliem, 2003; Nunnally & Bernstein, 1994). Reliability, therefore, refers to test of **consistency**. The importance of reliability lies in the fact that it is a prerequisite for the validity of a test (Ho, 2006). Simply put, for the validity of a measuring instrument to be supported, it must demonstrably be reliable. Any measuring instrument that does not reflect some elements consistently has little chance of being considered a valid measure of that element (Neumayer & Plümper, 2017). The **Cronbach's Alpha** reliability for the six domains as seen from **tables 17 – table 20** were domain 1 - Functions (F1 - F5) = 0.940, domain 2 – Viability (V1-V5) = 0.827, domain 3 – Adaptive Control (C1-C4) = 0.704, domain 4 – Sophistication (S1-S2) = 0.742, domain 5 – Environment (E1-E2) = 0.752 and domain 6 - Communication = (M1-M2) = 0.623; all of which indicate adequacy in meeting the criterion recommended by Nunnally (1978).

Table 17: Reliability Statistics of constructs for Domain 1 - (F1-F5)

Items (Variables)	Code	Mean	Std. Deviation	Cronbach's Alpha
<i>Operations</i>	F1	3.49	1.082	0.940
<i>Coordination</i>	F2	3.57	1.080	
<i>Investigation</i>	F3	3.65	1.051	
<i>Intelligence</i>	F4	3.69	1.051	
<i>Policy</i>	F5	3.60	1.006	

Table 18: Reliability Statistics of constructs for Domain 2 - (V1-V5)

Items (Variables)	Code	Mean	Std. Deviation	Cronbach's Alpha
<i>Autonomy</i>	V1	2.78	1.052	0.827
<i>Flexibility</i>	V2	2.89	1.059	
<i>Customizability</i>	V3	2.76	1.104	
<i>Voluntariness</i>	V4	2.63	1.108	
<i>Systematization</i>	V5	2.92	1.075	

Table 19: Reliability Statistics of constructs for Domain 3 – (C1-C4)

Items (Variables)	Code	Mean	Std. Deviation	Cronbach's Alpha
<i>Responsiveness</i>	C1	4.13	1.050	0.705
<i>Proactivity</i>	C2	3.98	.873	
<i>Agility</i>	C3	4.06	.814	
<i>Recursion</i>	C4	4.16	.733	

Table 19: Reliability Statistics of constructs for Domains 4 (S1-S2); 5 (D1-D2) and 6 (M1-M2) respectively.

Items (Variables)	Code	Mean	Std. Deviation	Cronbach's Alpha
<i>Risks</i>	S1	3.80	.957	0.742
<i>Relevance</i>	S2	3.79	.853	
<i>Irregularity</i>	E1	3.32	.593	0.752
<i>Uncertainty</i>	E2	3.26	.678	
<i>Transparency</i>	M1	3.64	1.215	0.623
<i>Timeliness</i>	M2	2.99	1.344	

Considering the use of the self-developed scales for the first time to perform the measurement, the cut off value for the alpha coefficient was set up for 0.60 for all the scales (Nunnally & Bernstein, 1994). Based upon this, all the measured items fell within acceptable range.

6.3. Factor Analysis

Factor Analysis was applied for the identification of the core factors. The analysis operates on the notion that large number of observable variables can be grouped and reduced to fewer latent variables that share a common variance. These latent variables or factors, though not directly measured, are essentially hypothetical constructs that are used to represent the variables. The use of factor analysis technique, in this study, was to provide a means to test for whether variables cast under the grouped variables are true reflection of what the respondents opined and that responses were consistent. Factor analysis does not require pre-existing functional relationships to enable the refinement and fine-tuning of variables into manageable groups of variables, which in the case of this study are the predetermined domains of IT auditing exapted from the substrates of the viable system model. Six underlying domains where eigen values were greater than 1.0 using factor analysis were identified and labelled as: **1. Functions**; **2. Viability**; **3. Adaptive Controls**; **4. Sophistication**; **5. Environment** and **6. Communication**.

A principal components method was employed to extract factors or domains constituting the grouping of the identified core items. ‘Varimax’, the rotation method used in this study, sought to maximize variances of the loadings in a certain predetermined fashion. In the scree plot test, the eigen value for the first factor was highest but decreasing for the next four factors which had an eigen value greater than 1.0 as shown in Figure Q below.

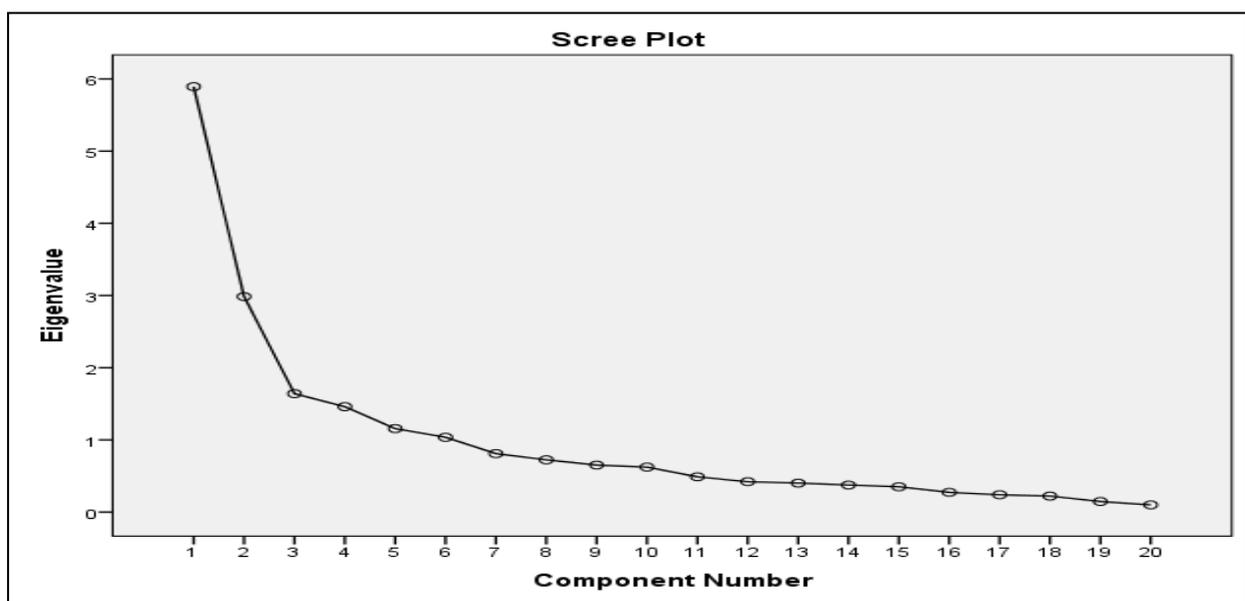


Figure Q: Scree Plot

Table 20: Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.894	29.470	29.470	5.894	29.470	29.470	4.060	20.301	20.301
2	2.985	14.927	44.398	2.985	14.927	44.398	2.976	14.878	35.179
3	1.641	8.203	52.600	1.641	8.203	52.600	2.237	11.187	46.366
4	1.461	7.303	59.903	1.461	7.303	59.903	1.733	8.665	55.031
5	1.157	5.784	65.687	1.157	5.784	65.687	1.612	8.062	63.092
6	1.036	5.179	70.865	1.036	5.179	70.865	1.555	7.773	70.865
7	.810	4.049	74.915						
8	.724	3.620	78.534						
9	.651	3.257	81.791						
10	.623	3.117	84.908						
11	.489	2.443	87.351						
12	.421	2.104	89.455						
13	.402	2.008	91.463						
14	.375	1.875	93.337						
15	.351	1.754	95.092						
16	.273	1.367	96.458						
17	.240	1.201	97.660						
18	.222	1.109	98.769						
19	.146	.731	99.500						
20	.100	.500	100.000						

Extraction Method: Principal Component Analysis.

Table 21, above, reveals that the factor structure accounted for 70.86% of the variance presupposing the existence of a correlational relationship between and among the latent factors.

The Kaiser-Meyer-Olkin (KMO) and Bartlett's test of sphericity tests

The KMO test was employed to measure sampling adequacy for each variable in the model and how suited the data was for factor analysis for the complete model. The measure for sampling adequacy in this test varies between 0 and 1. The rule is that values closer to 1 are better and therefore, a value of 0.6 and above are considered adequate. The KMO measure of sampling adequacy, in this study, was 80.9% (see table 22 below), therefore, the factor analysis was considered a useful validation of the factor analysis model. **Bartlett's test of sphericity** was employed to examine the adequacy of the correlation matrix, that is, the correlation matrix has significant correlations among at least some of the variables. The effect of this test was the

identification of instances of the existence of influences among the variables and the determination of the variables were unrelated or independent and therefore unsuitable for the detection of the emergent structure. Where the variables are independent and of significance level, the observed correlation matrix is expected to have small off-diagonal coefficients of less than 0.05. Bartlett's Test of Sphericity, therefore, tested the hypothesis that the correlation matrix was an identity matrix, that is, all the diagonal terms are 1 and all off-diagonal terms are 0. Furthermore, Bartlett's test of sphericity evaluated all factors together and each factor separately against the hypothesis that there are no factors. If the test value is large and the significance level is small (< 0.05), the hypothesis that the variables are independent can, therefore, be rejected. Table 22 below demonstrates the results of KMO and Bartlett's tests.

Table 21: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.809
Bartlett's Test of Sphericity	Approx. Chi-Square	1337.404
	Df	190
	Sig.	.000

In the instance of the present analysis, as shown in the KMO and Bartlett's test above in table 22, Bartlett's Test of Sphericity yielded a value of 1337.404 and an associated degree of significance smaller than 0.000. Thus, the hypothesis that the correlation matrix is an identity matrix is rejected indicating that one or more factors or domains exist. Factor Analysis is, hence, considered as an appropriate technique for further analysis of the data.

Factor Loading Analysis

Factor loadings measure the degree of interaction of variables or the strength of the agreement of the measured variables and, therefore, are strong enough to remain else to be eliminated. The inclusion or elimination of a variable depends on the cut off threshold used in the analysis. There is an academic debate as to which cut off threshold of rotated factor loadings of variables is appropriate for factor analysis. The size of the cut-off depends on whether the technique is an exploratory factor analysis (EFA) or confirmatory factor analysis (CFA) (Williams et al. 2010). EFA is used where data collected determines the resulting factor without any a priori hypotheses. It is used when the researcher wants to explore the relationships among items to determine if the items can be grouped into a smaller number of underlying factors (Helfrich et

al. 2007). CFA is employed to test factors that have been developed a priori or independent of the researcher's experience. It is used in instances where the researcher wants to establish if items load as predicted on an expected number of factors. Some researchers suggest, for CFA as in this study, stringent threshold as high as 0.7 or higher to confirm that independent variables identified a priori are represented by a factor, on the rationale that the 0.7 level corresponds to about half of the variance in the indicator being explained by the factor (Williams et al. 2010; Herzog & Leker, 2010; Suhr, 2006). Hair et al. (1998) argue, however, that the cut off should depend on the sample size because the 0.7 standard is a high one and real-life data may well not meet this criterion. Tabachnick and Fidell (1996) state that loadings threshold of 0.32 and above can be interpreted where the sample size is large since a large sample size will diminish errors in the data and recommend a large sample size to be 300 participants or more.

Guadagnoli and Velicer (1988) agrees with the above proposal but proposes, however, that if the dataset has several high factors loading scores greater than 0.80, then a size of 150 or more should be sufficient. Comrey and Lee (1992) also agrees with the above but further posit that, depending on the instrument used, loadings more than 0.45, in any circumstances, can be classified as fair or material. Stevens (1992) suggests that irrespective of the sample size and the instrument used, a rotated factor loading cut off rule of thumb of at least 0.4 can apply for interpretation purposes. MacCallum et al. (2001) add that this rule must apply where all items in a factor model have communalities of over 0.60 or an average communality of 0.70. With a total sample size of 136 participants in this study and communalities for each variable in the factor analysis showing a range from 0.77 to 0.88 and factor loadings ranging from 0.50 to 0.899 on all the six domains as shown below in table 23; a cut-off rule for the factor analysis was set at 0.45. It was hoped that this threshold will suppress possibility of errors in the dataset. Loadings of 0.45 and above are, therefore, interpreted and included. Table 23, below, provides the details of the items or components under each of the six component groups of variables or domains showing the value of their observed factors.

Table 22: Rotated Component Matrix^a

Items	Component					
	1.	2.	3.	4.	5.	6.
<i>Autonomy</i>		.517				
<i>Flexibility</i>		.718				
<i>Customizability</i>		.838				
<i>Voluntariness</i>		.827				
<i>Systematic</i>		.682				
<i>Operations</i>	.879					
<i>Coordination</i>	.843					
<i>Investigative</i>	.847					
<i>Intelligence</i>	.789					
<i>Policy</i>	.899					
<i>Responsiveness</i>			.732			
<i>Proactivity</i>			.669			
<i>Agility</i>			.733			
<i>Recursion</i>			.664			
<i>Risks</i>				.848		
<i>Relevance</i>				.846		
<i>Irregularity</i>					.818	
<i>Uncertainty</i>					.860	
<i>Transparency</i>						.860
<i>Timeliness</i>						.805
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.						
a. Rotation converged in 7 iterations.						

6.4. Analysis of Factor Loadings

The above matrix gives the correlation of the variables with each of the six extracted components or factors. A factor loading for a single variable measures the extent to which the variable contributes to the factor. Thus, a very high loading score indicates the dimensions accounted for by the variable within the domain. The values selected for each of the six core factors were extracted for each of the 20 variables of the 6 core factors or domains of the conceptual model. The selection of variables to include in each factor based on variables with

the value maximum in each row. Based upon the rotated matrix analysis in table 23 above, it is confirmed that all the variables had sufficient loading to significantly agree with the related components or domains since all loadings exceeded the set cut off 0.45 for this study. Thus, after rotation, Domain1 (Functions) accounts for 19.22% of the variance; Domain 2 (Viability) accounts for 65.69% of the variance; Domain 3 (Adaptive Control) accounts for 8.43% of the variance; Domain 4 (Sophistication) accounts for 3.12% of the variance; Domain 5 (Environment) accounts for 2.31% of the variance and Domain 6 (Communication) accounts for 1.23% of the variance.

Factor 1 – Functions domain: The factor analysis of the functions domain confirmed all the five variables cast under the domain. All the variables scored very high above 0.800 except for *intelligence* with a score of 0.799. This outcome is very useful in describing the domain as it shows very high correlation among the observed variables within factor 1. Nonetheless, *Policy* audit (S5) emerged as the strongest with loading score of 0.899. IT auditors have been called upon to play key role in the normative function defining ethics, values, professionalism and intentions and the like that make the client’s environments ‘outside and then’ or the ‘inside and now’ meaningful. The objective of policy audit geared towards prevention rather detection. The IT auditor’s role in policy audit is, therefore, critical in fulfilling his value co-creation expectation. This is expected to be achieved through a thorough evaluation of the effectiveness of the whole organizational policy direction by those charged with governance and management including a reflection of the interests, impact of social norms and values of stakeholders. Thorough Operational audit (S1) is confirmed by a very high score of 0.879. This means that the concept of *autonomy*, in domain 2, is required to ensure effective IT auditing, where, autonomy is the process of breaking S1 into auditable units and calling for IT audit to be much more cross functional (Khan et al., 2015). This is leveraged by high score for *recursion* principle of 0.664 in domain 3; where recursion means any level of IT audit customisation or maturity contains all levels of audit functions.

Although fraud detection and prevention have, refutably, said to be not the auditor’s responsibility, a score of 0.847 for investigations shows that stakeholders hold strongly onto their expectation of audit to detect and prevent fraud. The plausible reasons include high operational risks in an amplified sophistication in business processes by ICT. This is evidenced by a high score of 0.848 for risks in factor or domain 4 (sophistication) and underscores the importance for the guidance in (S3* -monitoring and investigation) above. The score for *Coordination* (S2) and *Intelligence* (S4) audit functions were 0.843 and 0.789. This implies

that coordination audit and intelligence audit are highly correlated, and the coordination audit upholds the intelligence audit function.

Factor 2 – Viability domain: The factor analysis of factor 2 confirmed all five variables grouped under the factor. The range of factor scoring ranged between 0.517 to 0.838 presupposing sufficient correlation among the variables within the domain. As mentioned earlier, stakeholders approve with above average scores of 0.517 and 0.682 for *autonomy* and *systematisation* respectively. Stakeholders found these concepts relevant because they are required to preserve the quality of *operations (S1)* audit through identification of auditable units of operations and the importance of cross functional auditing to ensure viability (Khan et al., 2015). This correlated highly with *Customizability* which emerged as the variable with the highest score of 0.838 within the Domain and followed closely by *Voluntariness* and *Flexibility* with a scores of 0.837 and 0.718 respectively. This implies that stakeholders welcome the idea of applying a principles-based approach, independent knowledge, professional experience and objective technique to structure an IT audit process to meet contextual needs of organisations.

Factor 3 - Adaptive Control domain: The analysis for factor 3 extracted four variables with loadings above the cut off score with loading ranging from 0.664 to 0.733. This shows high correlation among the variables within the factor. Participants approved the concept of *recursion* with a score of 0.664 meaning that stakeholders want IT audit implementation process to be very thorough such that any level of customisation shall contains all levels of audit functions below it. This process is successful with *Agility*, hence its high score of 0.733. Agile implementation of IT audit process emerged highest in the scoring in the conceptual contribution to IT audit resilience or adaptive controls in less regulatory environments. Thus, the essence of agile IT *audit control (S3)* is to ensure adaptability to changes. This implies that an IT audit Partner will now be the Scrum Master who, by iterative assessment planning and frequent feedbacks, will continually re-define the auditor's functions to achieve client-centric collaborative and cooperative audit objectives. This correlates highly with the concepts of *proactivity* and *responsiveness* which were scored 0.669 and 0.732 respectively within the domain. To maintain the resilience of IT audit process controls in (S3) in less regulatory environments, preventive controls are very important but equally or more important are detective controls.

Factor 4 – Sophistication domain: Two variables were extracted for factor 4 both of which scored very high of 0.846 and 0.848 for *Relevance* and *Risks* respectively which shows strong

correlation between them and presupposing high contribution to the approach to arrest the issue of increasing sophistication on IT audit effectiveness in less regulatory environments. At a time of rapid change and sophistication, to uphold the essence of control (S3), a forward-looking IT auditing approach to risk assessment is critical for effectiveness audit quality. For IT audit to properly assume its expected role of helping organizations adapt to business change with ease and confidence, while also catalysing audit performance, a self-adjusting theoretical foundation for IT audit is, therefore, apt for the resolution of implementation bottlenecks by referring to the principles and concepts. Risk assessment must, therefore, reflect controls that are adaptive to the changes.

Factor 5 – Environment domain: The factor analysis produced loadings of 0.860 and 0.818 for the variables *Uncertainty* and *Irregularity* respectively implying high correlation between them. It is concluded, therefore, that participants agree both variables contribute immensely to the environment of IT auditing. As rapid environmental change increase uncertainty compounds the problem of irregularity. Participants' consensus, therefore, is that higher uncertainty demands an IT auditing framework to be modelled on a resilient systems theory which does not merely rely on reactive approach but, rather, proactive iterative approach to make all the difference to business success in less regulatory environments. This concession corroborates the conclusions reached in from domains 1, 2, 3, 4 and 5 above.

Factor 6 – Communication domain: The factor analysis for factor 6 included two variables – *transparency* and *timeliness* with scores of 0.860 and 0.805 respectively implying high correlation between the them and high contribution to the effectiveness of IT audit contribution. This presupposes that despite the high requirement for IT audit communication, participants score the need for the communication to be transparent more critical for valuable results. Transparency assurance stands for ensuring a succinct, objective client-centric, collaborative and continual cooperative stakeholder feedback approach.

The extraction Sums of Squared Loadings as well as the Rotation Sums of Squared Loadings all produced a cumulative value of 70.865% representing factor structure which indicates that there is high correlational relationship between and across the factors namely; 1. Functions; 2. Viability; 3. Adaptive Controls; 4. Sophistication; 5. Environment and 6. Communication that constitute the groupings of the measured variables in the conceptual model.

6.5. Conceptual Model Testing and Analysis

The partial least square approach in structural equation modeling was used in assessing the interconnectedness among latent variables. The approach combined both factor and multiple regression analyses to measure the structural relationships of the entire model. As determined above, the latent variables (factors) were function, viability adaptive control, sophistication, environment, and communication. For this analysis, the weighting scheme, paths in the PLS-Algorithm was used to estimate the path coefficients and loadings. This showed the causal relations among the latent variables in the entire model. Subsequently, the bootstrapping was done to test the statistical significance of the path coefficients and loadings. In this regard, the interaction between every two latent variables was estimated using the t-statistics. Thus, t-statistics greater than and or equal to 1.9 was significant at p-value of 0.05 (McDonald & Ho, 2002).

Results

Table 23: Relationship among latent variables

Paths	Original sample	t- statistics	p-values (0.05)
Adaptive control -> Sophistication	0.296	4.606	0.000
Environment -> Communication	-0.113	1.000	0.318
Function -> Adaptive control	-0.139	2.199	0.028
Function -> Communication	-0.015	0.265	0.791
Function -> Sophistication	0.174	1.868	0.062
Function -> Viability	0.542	10.182	0.000
Sophistication -> Communication	0.07	0.596	0.551
Sophistication -> Environment	0.299	2.687	0.007
Viability -> Adaptive control	0.31	4.357	0.000
Viability -> Communication	0.052	0.301	0.763
Viability -> Environment	0.08	0.888	0.375

Five paths in the entire model were significant (Table 23). That is, adaptive control -> sophistication, function -> adaptive control, function -> viability, sophistication -> environment and viability -> adaptive control. These recorded t-statistic values more than the threshold, 1.9 required for a significant p-value at 0.05. The implication is that, in the model,

only the paths that showed significant causal relations are important for consideration in any management decisions.

Table 24: Model validity and reliability

Latent variables	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Adaptive Control	0.64	0.803	0.577
Communication	0.685	0.838	0.722
Environment	0.79	0.89	0.801
Function	0.829	0.891	0.732
Sophistication	0.763	0.886	0.796
Viability	0.941	0.957	0.848

The rho_A (Table 24) measured the extent to which variables were positively related to each other. Mainly, all the variables except adaptive control and communication were below the threshold value of 0.7. The implication is that apart from the two, the remaining variables showed positive relations with other associating variables. On the other hand, composite reliability which assessed the internal consistency of the model was on the whole adequate with values greater 0.7. Similarly, the convergent reliability of the model which was accounted for by the AVE (proportion of variance explained) showed that all the variables were above the threshold value of 0.5. Thus, the model estimates considered point to a model that is valid and reliable.

6.6. Examination of Hypotheses

In furtherance of well-structured conceptual model for IT auditing, regression and correlation analysis was employed to examine the individual hypotheses by measuring the strength of relationship among two or more variables. An analysis of variance (ANOVA) was used for the investigation into whether the survey results were significant, thus, helping to figure out if there is any null hypothesis that should be rejected, or the alternate hypotheses was to be confirmed. The examinations demonstrated how the factors are related and which one of the independent factors influences the related dependent factors the most that confirmed or rejected the hypotheses. In the independent variable selection method, all independent variables were entered. In the case of model 2 and model 5, tolerance and variance inflation factors were used to diagnose whether there were problems of multicollinearity which can occur when independent variables are too highly correlated. Two values for each independent variable were

greater than 7 and lower than 1.0, respectively, indicating that levels of multicollinearity were met within acceptable limits. This indicates that redundant variables in the analysis are not included. The results of the hypotheses testing are represented Table 25 below.

Table 25.

Model	Hypothesis	Model Summary		ANOVA		Estimates			Decision
		R	R ²	F	p-value	Variable	Coefficients	Sig. p-value	
1	H1	0.569	0.324	64.227	0.000	Functions	0.499	0.000	Confirmed
2	H2 _A	0.332	0.11	8.234	0.000	Functions	-0.201	0.010	Confirmed
	H2 _B					Viability	0.271	0.000	Confirmed
3	H3	0.359	0.129	19.832	0.000	Adaptive Control	0.455	0.000	Confirmed
4	H4	0.041	0.002	0.222	0.638	Environment	0.03	0.638	Not Confirmed
5	H5 _A	0.339	0.115	4.26	0.003	Environment	-0.054	0.214	Not Confirmed
	H5 _B					Sophistication	0.209	0.001	Confirmed
	H5 _C					Function	0.063	0.308	Not Confirmed
	H5 _D					Viability	-0.016	0.814	Not Confirmed

6.6.1. Discussion of Results

In model 1, the coefficient of determination test produced an R² value of 0.324, which means that the independent variable explained only 32.4% of the variance of a dependent variable. The ANOVA presented results from the test of the null hypothesis that R² is zero; where R-square of zero indicates no linear relationship between the predictors and dependent variable. The ANOVA table for model 1 shows that the computed F statistic is 64.222, with an observed significance level of less than 0.000, thus the hypothesis that there is no linear relationship between the predictor and dependent variable is rejected. The coefficients section presents the unstandardized beta co-efficient between the predictor variable *Functions*. The beta coefficient is 0.499 (positive) and p-value of 0.000 which is statistically significant. Thus, the higher the alignment of IT audit workflow with the functions of those charged with governance and management, the higher the viability of IT auditing in less regulatory environments. The hypothesis in H1. ‘An effectively aligned IT audit functions with the functions of those charged with governance and management influences the viability of IT auditing.’, is thus, confirmed.

Model 2 was designed to test for collinearity between two independent variables - '*Functions*' and '*Viability*' and their dependent variable *Adaptive Controls*. The R^2 for model 2 was 0.11, which means that the independent variables explained only 11.0% of the variance of a dependent variable. The ANOVA table for model 2 shows that the computed F statistic is 8.234, with an observed significance level of less than 0.000, thus the hypothesis that there is no linear relationship between the predictor and dependent variable is rejected. The coefficients section presents the unstandardized beta co-efficient between the predictor variables '*Functions*' and its dependent variable *Adaptive Controls*. The beta coefficient for '*Functions*' is, however, -0.201 (negative) with p-value of 0.000 which is statistically significant. Thus, the higher the IT audit workflow aligns with functions of those charged with governance and management, the less the adaptive control burden because of the mutually shared control responsibility and technical support through consultancy between the auditor and those charged with governance and management. In other words, the higher the adaptive controls, the lower the substantive audit procedures because auditor, at the planning stage, can customise the audit procedures to focus on most relevant procedures to achieve desired audit outputs. The hypothesis in $H2_A$, that is, '*An aligned IT audit functions with those of management influences efficient adaptive controls.*', is confirmed. The coefficients section presents the unstandardized beta co-efficient between the predictor variables '*Viability*' its dependent variable *Adaptive Controls*. The beta coefficient for '*Viability*' is 0.271 (positive) with p-value of 0.000 which is statistically significant. Thus, the higher the '*Viability*', the higher the *Adaptive Controls*. This also confirms the hypothesis in $H2_B$ that, '*The viability of an IT audit approach influences its adaptive controls.*' The hypothesised multicollinearity in model 2 is, therefore, confirmed.

In **model 3**, R^2 was 0.129; which means that the independent variable explained only 12.9% of the variance of a dependent variable. The ANOVA table for model 3 shows that the computed F statistic is 19.832, with an observed significance level of less than 0.000, thus the hypothesis that there is no linear relationship between the predictor and dependent variable is rejected. The coefficients section presents the unstandardized beta co-efficient between the predictor variable *Adaptive Controls* and the dependent variable *Sophistication*. The beta coefficient is 0.455 (positive) and a statistically significant p-value of 0.000. Thus, the higher the '*Sophistication*' the higher the '*Adaptive Controls*'. This means, therefore, generally the reason why stakeholders are demanding that the control approach in IT auditing should be adaptive is that the business control environment is increasing in sophistication. The hypothesis in $H3$. '*An*

efficient approach to adaptive controls influences business IT audit sophistication.’, is, thus, confirmed.

Model 4: The R^2 for model 4 was 0.002, which means that the independent variable explained less than 1 percent of the variance of a dependent variable. The ANOVA table for model 5 shows that the computed F statistic is 0.222, with an observed significance level of loss than 0.638, thus the hypothesis that there is no linear relationship between the predictor and dependent variable is accepted. The conclusion, therefore, was that there exists no linear relationship between Environment and Sophistication. The hypothesis **H4:** *‘The sophistication of IT auditing influences the risks of business environment’* is rejected.

Model 5: Four hypotheses were formulated to test for multicollinearity between each independent variable - *Environment, Sophistication, Functions, Viability* and their dependent variable *Communication* as follows: **H5_A:** *The environment of an organization influences IT audit communication.*; **H5_B:** *Business IT audit sophistication influences audit communication;* **H5_C:** *The functions of IT audit influence IT audit communication and H5_D:* *The viability of IT audit influences IT audit communication.* The R^2 for model 5 was 0.115, which means that the independent variable explained only 11.5% of the variance of a dependent variable. The ANOVA table for model 5 shows that the computed F statistic is 4.26, with an observed significance level of loss than 0.003, thus the hypothesis that there is no linear relationship between the predictor and dependent variable is rejected. The coefficients section presents the unstandardized beta co-efficient between the predictor variables *Environment, Sophistication, Functions, Viability* and their dependent variable *Communication*. The results reveal that it is only *Sophistication* that significantly influences *Communication*. Therefore, only **H5_B:** *Business IT audit sophistication influences audit communication.* Its beta coefficient is positive and statistically significant (p-value = 0.001). Thus, the higher the *Sophistication*, the higher the *Communication*. The statistical analysis reveals that there is no statistically significant linear relationship between *Viability, Functions, Environment*, and the dependent variable *Communication*.

6.7. Reflection on the Emerging Structure of the Framework

Sein et al. (2013) emphasize that an ensemble artefact in an action design research must reflect not only the preliminary design of the conceptual model created by the researcher for the development of the research but also its subsequent shaping or refinement by either

organizational use of the model or the perspectives of practitioners and end users who have participated in the study. The refinements may range from trivial fixes to substantial changes to the design which constitute the meta-artefact.

The results of the examination of hypotheses reveal that a critical quality of an effective IT auditing for less regulatory environments is a non-linear, multidimensional philosophy. The rejection of the hypothesis in model 4 by respondents implies that the conceptual positioning of the 'Environment' domain at 5th place in the structure of the conceptual framework is rejected. This outcome required significant ramification in the final structure of the conceptual framework for IT auditing for less regulatory environments. This outcome was not unexpected. The standards by the Public Company Accounting Oversight Board (PCAOB) standard 12, The International Standards on Auditing (ISA) 315 and the American Institute of Public Accountants (AICPA) standard AU-C 315 that IT audit provide for the environment to be the main consideration for auditing at the initial planning stage (Flood, 2017). In accordance with the standards on auditing, the auditor's reviews of the environment concern the risks and uncertainties in the maintenance of controls and the irregularities in the implementation of compliance requirements at the planning stage of the assessment are vital to a viable systems audit.

The implication of rejecting the hypothesis in model 4 is that respondents reposition the environment domain at background of the chain of correlated domains of auditing. This is because the environment concerns intelligence that provides a range of factors to guide the assessor the insight to determine the audit process suitable to achieve desired outcomes. Organizations face a wide range of uncertain internal and external factors that may affect achievement of their objectives - whether they are strategic, operational, or financial. The effect of uncertainty on management objectives can be a positive risk (opportunities) or a negative risk (threats) at the entity level, the industry level and the economy level. Background intelligence tests for opportunities and anticipates threats (Espejo, 2009) which is expected by respondents to be a major activity in audit planning that precedes substantive IT audit evidence collection. The effect of irregularities can serve to increase audit risks (Niemi et al., 2018). **Figure R** below is a summative depiction of the emergent structure of the meta artefact design of IT audit framework for less regulatory environments.

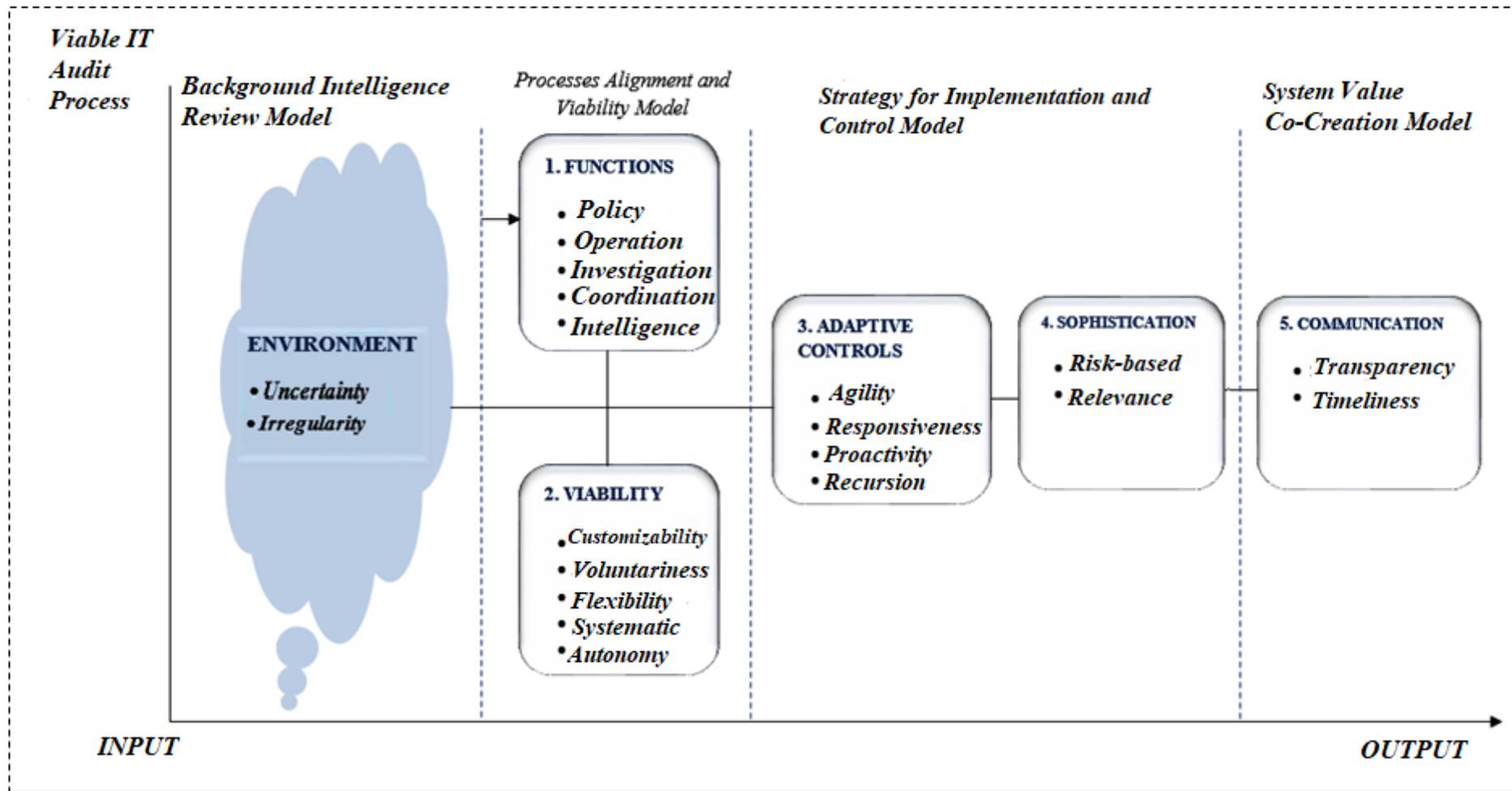


Figure R: The Summative Depiction of IT Audit and Assurance Framework for Less Regulatory Environments

The summative framework for IT audit and assurance refers the outcome of the effort to design a framework for efficient and effective IT auditing for less regulated business environments. The framework, having been built on the substrates of an existing systems theory, is a system on its own. The Viable systems audit process, therefore, has four seamless models. Each of the viable systems audit process models is composed of, at least, one domain to serve as input. The first of the process approach is the background intelligence review model. The input domain for this model is the environment which in turn comprises a set of validated applicable concepts and principles to guide the process which have been elucidated above. The cloud symbol is to represent the environment domain which reflects elements of uncertainty and irregularity.

The second viable systems audit process model is the process alignment and viability model. Two domains provide input for effective deliverables of this process model, namely; the auditor's role or *functions*. The functions are represented by five essential IT audit activities that have been identified to keep the auditor's role effectively aligned with the functions of those charged with governance and management. These functions, by order of importance according to stakeholders' perspective, are policy, operation, investigation, coordination and intelligence. The *viability* domain comprises concepts that preserve the functions. These concepts, by order of importance, are customizability, voluntariness, flexibility, systematization and autonomy. An effective alignment will leverage IT audit practitioners' key role in helping those charged with governance and management for comprehensive approach to risk management and internal control that result in the creation, enhancement and protection of stakeholder value.

The third process domain is the strategy for implementation and control model. Two domains provide input for this process model, i.e. *Adaptive Controls* and *Sophistication*. The *adaptive control* domain constitutes concepts and principles required to implement the viable systems auditing process to achieve its goal of design while ensuring that the audit processes can co-evolve with environment. These, by order of importance, are agility, responsiveness, proactivity and recursion. The *sophistication* domain acknowledges the complexity associated with the IT audit processes, its implications and provides high advocacy for the *risk-based* approach. As a measure to attenuate less cost-effective and superfluous audit efforts, relevance is also scored to be critical input to the risk-based approach. This will require the application of professional judgement and the use of contextual auditing approach explaining why *customizability* was scored very high as an input for IT audit viability.

The fourth and final viable systems process model is the systems value co-creation model. The Communication domain provides the input for the effective achievement of the expected outcomes of the framework use. Communication domain acknowledges the indispensability of continuous collaboration and cooperation and idea sharing between the IT audit practitioner and the relevant stakeholders. This is only possible where IT auditors go about their communication with high degree of transparency. That is, the ability to translate and transmit key audit matters (KAM) to the understanding of the recipients and be timely about it. IT auditors must also show honesty and transparency about the risk that exists or will exist, the remedies being recommended, and what can happen if remedial action is not taken. Singleton (2014) posits that Communication is a critical IT audit success factor that goes beyond IT. Communication maximizes the value of the IT auditor's role as well as actuates the value created by those charged with management. The future of IT audit is, therefore, about adding value to the role of IT audit.

6.8. Chapter Conclusion

Chapter Six concludes the learning and reflection stage of the Action Design Research. The chapter was characterised by quantitative analysis of data collected at the end of the last iteration to the field for practitioners and users' contribution to the design. Factor analysis was used to validate the variables in the conceptual framework. The entire conceptual framework was subjected to validity test using the structural equation model. Regression and correlation analysis together with analysis of variance was used to test the individual hypotheses. This exercise and further reflection culminated in the adjustment of the structure of the conceptual model. A summative design pattern of the framework for IT auditing emerged and explained. The next Chapter concludes the research by summarising and formalising the learning and outcomes of the study. The last chapter is developed using the formalisation of learning approach according to the action design research approach. In pursuance of this, the chapter elucidates the various dimensions of contributions claimed by the researcher. Additionally, the chapter discusses the opportunities of future research as well as the limitations of the research.

CHAPTER SEVEN

FORMALISATION OF LEARNING AND CONCLUSION

7.0. Introduction

Chapter seven provides the conclusion to the research. In this chapter, a summarised overview of the research process is provided. Furthermore, the main research question is revisited and the generalised outcomes that provide the response to the research question are submitted. This chapter discusses the contribution of the research to theory and practice. The chapter concludes by discussing the challenges and limitation of the research and how a study like this provides opportunity for further research in the field.

7.1. Overview of Research Process

The research process was organised in chapters. In chapter one, it was briefly pointed out that although attempts to develop a unified structure for auditing dates to Mautz & Sharaf (1961), however, concerns about the paucity have been raised about various conceptual frameworks developed to achieve a unified structure as the society and investors quest for accountability intensify (Pratt & Peurse, 1993; Swanson & Marsh, 1993; Zhang & Le Fever, 2013). In a fast-changing complex business environment with increasing implementation of sophisticated business technologies, stakeholders of business concerns have come to realize that traditional auditing together with the existing approach to auditing is just unsustainable. As a result of this, the IT audit practice has become the point of reference for the future of auditing in general. Though several frameworks for auditing and governance of enterprise IT have emerged on the market, the challenge for less regulated business environments is that the implementation of these frameworks has not been particularly successful due to implementation challenges caused by certain peculiarities. In spite of this, available literature demonstrates a woefully little research in the field aimed at developing a bridging framework to make those frameworks fit for purpose within less regulated business environments.

The main goal of this research, therefore, as discussed in chapter one, was to fill this research gap by designing framework that would extract a bridging framework out of a suitable systems theory to design an effective and practically resilient approach to IT auditing in less regulated business environments. As a result of weak regulatory systems envisaged by the research for the empirical situation, it was therefore, first of all, necessary to identify a solid systems theory that is suitable to serve as the foundation theory for further development of the study. To

successfully implement the research objectives, action design research (ADR) approach according to Sein et al. (2011) was adopted to develop the study. This approach was found to be the most logical because of the need to consider continuous stakeholder participation in the research project for concurrent and subsequent analysis in the process of building the and evaluating framework.

In Chapter two, a thorough review of theories and other literature on IT auditing used as the knowledge foundation for the demonstration of the proposed framework was conducted. It was noted, as of critical importance in chapters two that due to the issue of globalisation of standards, everchanging nature of frameworks, best practices, standards and the need for IT audit practice to adjust according to the fast changes in the environment which is less regulatory.

At the problem formulation stage, in chapter three, the diagnosis confirmed increasing business risks and expanded stakeholder expectations of audits due to the use of sophisticated information technology. A systems theory that supports self-regulation and capable of responding to changes was identified by abductive inference to be plausible theoretical foundation for effective construction of a framework for IT auditing so that practitioners don't miss the train. The cybernetics theory of viable systems approach, therefore, was selected for investigation and diagnosis of the research problem and further development of a framework for IT auditing for less regulatory environments.

In accordance to the dictates of the ADR approach to the research, chapter four of the study build alpha version framework for IT auditing based on the VSM adopted by abduction for the development of the framework. This stage of the framework combined the substrates of systems theory and the researcher's relevant knowledge bases to build an alpha version of the proposed framework and to elaborate it. The chapter concluded in the extraction and summarization of a conceptual framework based on the features of the underlying systems theory which formed the basis of the conceptual hypotheses for further development of the study.

Chapter five provided philosophical and methodological diagnosis of the approach to a rigorous evaluation of the conceptual model. This culminated in the final lap of the iterations that solicited the views of stakeholders who were selected to participate in the study. A multiple case study approach was employ and a survey technique was used to collect the views of the

participants for subsequent analysis. Qualitative and quantitative techniques were mix for the evaluation and analysis of data collected from the field.

Following from above, chapter six of the research, therefore, focused on the analysis of the views of the selected participants. The data collected were used to validate and to draw conclusions on the conceptual model and, hence, the systems theory used for the development of the conceptual model. The chapter culminated in the examination of the conceptual hypotheses and a reflection of the results. The results necessitated the restructuring of the model and, hence, the outcome was a beta version of the conceptual model for IT auditing for less regulatory environments.

7.2. Research Question Revisited

The research recognized the numerous challenges facing IT auditing practice in less regulated business environments and the expedience for Information Systems experts to contribute in the design and development of a resilient intervention in the face of the fast-changing skills and attitudinal requirements for the delivery of desired improved IT audit outcomes. The study, therefore, adopted the single research question below.

‘How efficiently and effectively can systems-based framework for auditing provide solution to IT audit and assurance challenges in less regulatory environments?’.

To respond to the above research question, the research examined the working hypothesis that cybernetics theory of viable systems approach would produce the expected efficiency and effectiveness of an IT auditing framework for less regulatory environments. This systems theory was selected by abductive inference because the viable systems model is a known powerful systems diagnostic tool for modelling artefacts from its attributes and usage where the regulatory environment is weak. The examination of responses from stakeholders that participated in the research produced results that validated the theory and, hence, the working hypotheses. At the outset of building the proposed intervention, all the concepts and principles relevant to efficient and effective IT audit practice according to professional bodies, practitioners and scholars were elicited from the lens of the underpinning theory. This led to the building of the alpha version of the framework and the researcher was the sole designer.

7.3. Summary of Findings and Discussion of Final IT Audit Framework

Increasing sophistication of business information systems has significant impact on audit of all forms. It was found that corporate governance and management in contemporary business ecosystem has become very complex. Auditors require deeper appreciation and application of complexity theory to make sure that his services are viable and fit for purpose. The study found that a framework designed on the viable systems model and elucidated using available best practices in contemporary IS/IT audit ecosystem would mitigate the problems of IT auditing or assurance in an application domain. In so doing, study confirmed that for IT Auditing to be very effective and efficient the framework used by practitioners and the framework used by management should coincide. By this, the Auditor and those charged with governance and management would be able to agree since they all would speak a common language. Hitherto, objective analytical procedures for preliminary or substantive audit evidence collection was within the confines of financial auditing. This research has found that the viable systems performance evaluation metrics designed by Beer (1972) could be applicable for the design of the metrics for performing objective analytical procedures in IT auditing. This study, therefore, makes available to practitioners an innovative approach to perform quantitative analytical system diagnostics that allow for the identification and design of the audit that is useful for the auditee's circumstances within any given time.

Based upon the ingrained theory it was discovered that an efficiency and effectiveness is an "outside-in-outward" approach as opposed to the existing problematic "inside-out" approach. That is, a thorough operational environment diagnosis should precede the execution of the actual audit process (*inside-and-now*) which should culminate in the diagnosis of the environment once again which includes the strategic environment (*outside-and-then*). This represents much more holistic and improved approach to IT auditing which is the result of this study which, hitherto, was not available to practitioners. **Figure R**, in the preceding chapter provides a summative depiction of the resulting proposed IT Audit and Assurance framework designed on the viable systems model.

The research identified for the design of the framework for IT auditing four models or perspectives for executing any single effective auditing. These models are, *first*, the Background Intelligence model - this represents the investigation of operational environment which is mainly a risk assessment and audit planning model. The *second* model follows the first as an IT Audit Process and Viability Model. This model contains both the IT audit functions or processes as well as the applicable underlying principles that should guide IT audit

processes to preserve viability of the practice. The *third* model – Strategy for Implementation and Control model, presents the Strategy for the execution IT audit processes in order to make IT auditing adaptive to the circumstances of the auditee and its environment. The *fourth* and final model - the Systems Value Co-Creation model, presents the approach to issue IT audit outcomes which is critical for the achievement of the purpose of the practice.

An analysis and evaluation of the final framework showed that all the six domains cast under the four models above showed high correlation among them which represents high level of approval of intended users. The consensus reached from participating stakeholders' perspectives were as follows. IT Audit process must be closely aligned with the functions of those charged with governance and management to optimise IT auditing output. The factor analysis revealed that the most critical IT Audit process is that of policy reviews and assurance. Policy reviews, therefore, must take precedence over operational risk assessment for effective and efficient audit outcomes. To leverage the effective audit process, IT auditors must obtain sufficient intelligence from the operational environment through meticulous coordination. It was further discovered that coordination function correlates highly with viability of the IT Audit processes and that the ability to customize an IT audit framework was highly rated to infer its resilience or adaptability. Effective implementation principles of controls is highly underscored by the concept of agility. Agile implementation correlates highly with concepts such flexibility, voluntary and recursion. These are used to encourage responsible commitment to implementation principles. Moreover, because of increasing sophistication, IT auditing framework is a risk-based and relevant controls approach. Finally, communication comes as value co-creation model and it should not only be timely but more transparent to achieve desired IT Audit outcomes.

7.4. Generalized outcomes

This section sets out the main contributions of the research. At this stage the criteria or explanations of the power to generalise as valid the postulations of knowledge to the field of research are discussed. Furthermore, generalised outcomes concern the extent to which practitioners have approved of the validity or the effectiveness of the design and the reason for which practitioners should adopt the contribution of the research. In spite of the less regulated audit ecosystem within which this research was empirically situated, the contribution of this research is very likely to be also of enormous value to highly regulated audit ecosystems

because of the innovative approach prescribed. The contribution of this research, therefore, can be discussed from two perspectives – contribution to theory and contribution to practice.

7.4.1. Contribution to Theory Development

The research has contributed to the development of the IT audit practice by developing a framework for IT auditing. Gregor and Hevner (2013) refer to this principle as the articulation of a ‘design theory’ and states that this can be treated as a type of artefact. Framework for IT auditing development encapsulates the gravamen of the entire research effort. The research has not just contributed to the development of an artefact, i.e. framework for the conduct of effective and efficient IS auditing in less regulatory environments, but it has been underpinned a solid resilient systems theory. This means that, inherently, implementation bottlenecks would be resolved by referring to the principles and concepts associated with the ingrained theory, i.e. the viable systems approach elicited by the study for guidance. The effect is that users will focus on the spirit of the guidance which would invoke intrinsic commitment and reliability encourage, the exercise of professional judgement and responsible application of the framework because of its embedded participatory management system. The derivation of the design domains and principles was conducted by the process of ‘exaptation’ from the ingrained theory. The process of exaptation in a design research is the act of replacing the concepts, principles and relational traits of theory existing theory propounded and applied successfully in quite a different discipline to that of the researcher’s field to serve another purpose (Gregor & Hevner, 2013). The exapted concepts and principles of the ingrained theory were determined as having reciprocal influence on audit effectiveness with reference to the views of practitioners. On the strength of this alpha version of the framework for IT auditing was built and demonstrated with well-known best practices such as COBIT and COSO frameworks for governance and internal control.

7.4.2. Contribution to Practice

The actual contribution instance of this research to practice is in the category of improvement on IT audit and organisational assurance work practices (Gregor & Hevner, 2013). The IT audit ensemble artefact contribution of this research is the design and demonstration of a comprehensive framework with practical solution to audit or assurance problems that is of the power to provide contextual guidance for IT audit practice. The generalized improvements and utility of the framework for the users include the following.

IT Audit Process Improvement – To maximize their value of their role, it is important that IT auditors are effectual in reporting IT risk and audit results. Agile approach to IT auditing will foster efficiency in coordination and communication between IT auditors and stakeholder thereby minimising systemic challenges of delayed reporting. One significant feature of the proposed framework is either the opportunity to resolve implementation challenges or advancing the processes by referring to the theory that informs the framework.

Effective Learning and Capacity Building – Internal learning and education are key in risk control and it is a significant outcome of the viable systems approach to IS auditing. The viable systems audit approach amplifies policy audit and fosters deeper insight of the client organization. The proposed framework, therefore, will encourage and improve conversations between those charged with governance and the auditor which will contribute to the amplification of effective governance. With enhanced understanding of the business value of internal control and business ethics, IS audit practitioners can provide instructional sessions in Key Audit Matters (KAMs) for staff and other relevant stakeholders. Assurance providers will leverage the knowledge repository of the client and will become the ‘live-blood’ of viable entities.

Support for system development and system review – The problems of most economies in less regulatory environments are systemic. The proposed framework for IT auditing promotes system development and system review through the assurance that the controls are cost effective and operate as intended. Proactivity will encourage early detection of risks and areas of the business processes that require various levels of improvements due to an underpinning agile concept. Hitherto, this form of auditing has not been available in the empirical situation. IT audit practice will no longer be overly operation-oriented but rather an enterprise-wide continuous and rigorous health-check exercise tilted to the review of executive strategies and policies. Thus, IT auditing will shift its paradigm from rigid compliance-based approach to preventative and collaborative approach. The consequence of this is the elimination of the existing of the superficial rubber-stamp audit exercise which adds little to no value (Osei-Afoakwa, 2013; DiGabriele, 2009).

Effective risk assessment - Audit analytics is said to be less costly and less time consuming since the procedures assist the auditor to be able to quickly identify problem areas and to focus attention on critical areas. IT audit practitioners are often challenged by the unfortunate but rampant events of fraud, corrupt practices and breaches of regulations in less regulatory

environments because traditional approach relies on reactive philosophy. Dealing with white-collar crime, conflicts of interest waste, fraud, abuse of assets, infractions of business ethics and serious mismanagement have been, hitherto, a controversial issue in auditing. The framework provides elaborate guidance on their detection, deterring and prevention proffering agility and proactivity in (S3/S3*) as the philosophical bedrock to the management of these phenomena. This is leveraged by the concept of recursion in the audit process gives IT auditing a continuous audit approach flavour which is one of the approaches of risk-based auditing recommended for environments where professionalism, honesty, integrity, political interference, lawlessness and non-compliance with regulations are rampant due to weak regulatory institutions. These qualities have featured highly in contemporary business information systems audit literature on effective risk assessment and management in areas with less strong audit traditions (Rezaee et al. 2018; Marcello et al, 2017Tichaona, 2014; Moeller et al. 2013).

Encouragement of Shared Responsibility – The framework brings improvement to IT audit because it can be used by management in their monitoring and for their ‘IT audit readiness’ self-assessment. By this management should able to resolve issues that would consume IT audit time and increase audit cost prior to the audit itself. With this framework as the enabler IT audit effectiveness is assured because the IT auditor would attenuate the scope of his IT audit universe to amplify procedures on critical areas for more desired audit outcomes. It would be easy for Management and the Auditor to agree because come framework for monitoring and auditing respectively.

IT Audit Practice Management – Objective metrics for customisation of the framework enhances understanding of the business, its legal and technological environments which informs the creation of client-centric IT Audit Universe at the audit planning stage. The effect of this is an improved quality assurance in practice management. IT Audit Partners’ selection of audit team will be based on the skills set and experience required to execute the assignment informed by the created IT audit universe. This can greatly reduce the level of exposure to IT audit failure.

Consultancy – Many an audit assignment in less regulatory environments have yielded no value or have been deemed to be mere formality because auditors have failed to really understand their client’s business. With the framework as the enabler, a broad-based approach and multidisciplinary information systems audit ecosystem is available for Internal auditor and

IT Audit Practitioners to develop more insight into the entity's business than anyone else. Auditors will no longer narrowly concentrate on compliance only but will generate more usefully diverse outcomes and reliable information to enable the effective accomplishment of 'the triad of value that IT audit and internal audit stakeholders want and need in contemporary business environments', namely; 'assure, advise and anticipate' (Deloitte, 2018). Internal IT audit or external auditors basing their internal control reviews on the viable systems framework will, therefore, acquire two hats – one as reviewer of the IT audit space and one as Boards and management consultant or teacher without compromising their independence and objectivity (Tichaona, 2014).

7.5. Limitation and Opportunity for Future Research

This section discusses the challenges that may have implications on the research outcome and the proposal for future research. The issues that might militate against the results of the research border on the Generalisability, Sampling method, and Data collection approach.

Generalisability: The aim of the study was to design an IT Audit Framework that provides improvement to, generally, less regulatory environments. In the process of developing it, the approach was a case study conducted in four organisations in Ghana namely; Ghana Audit Service, Sekyedumase Rural Bank Limited, Sun Shade Foundation and Kumasi Technical University in Ghana. In a study like this, it would be expected that only IT audit practitioners and academicians in the field would participate, however, the challenge of the dearth of IT audit practitioners made it necessary to include non-practitioners. These included Internal Audit practitioner, Students of IT auditing, Accountants, Managers and Directors. Furthermore, this study was based in Ghana. The basic assumption for generalisation is that matters held to be true in an empirical situation, hold true for all other situations that are known to share common characteristics. Although Ghana is deemed to have less regulatory environmental tendencies, it is important to acknowledge regional differences which may affect the generalisability of the results. More so, as stated above, in spite of the differences in the regulatory environments, highly regulated business ecosystems can still find this framework very useful due to the approach prescribed.

Sample Size: The number of people that participated in the study was 136 who were limited to four selected cases for the study. As a result, paper-based survey instrument administered directly to respondents could be relied upon. Although the cases were carefully selected to capture significant number of stakeholders, the resulting limitation emanated was the dearth of

practitioners in the empirical domain. Where the sample size is small compared to the population to which the results is extended, reliability of the outcomes may be impaired.

Data Collection approach and analysis: The study adopted survey technique to solicit the views of the respondents on the concepts and processes of an IT audit framework elicited from the underlying theory. The purpose was to evaluate the effectiveness of the designed model. A quasi-experimentation technique was adopted for the evaluation of the framework in which professional judgement and quantitative techniques were employed during the evaluation. Likert scales were used as the main data collection technique in the survey instrument to collect data for the subsequent quantitative analysis. The technique is, however, measures self-reported variables and responses are subject to variations in the attitudes and beliefs shaped by respondents' IT audit experiences. In the case of this study, however, a good number of respondents was not practitioners.

Directions for Future Studies

Future research could address the limitations of this research by extending the empirical model to include more than one jurisdiction and include more cases to evaluate the framework for its reliability. To increase the sample size of experts, future researchers could involve online administration of survey instrument to obtain wider reach to professionals and academicians in the field across the population to improve reliability of results.

Again, future research could adopt the Delphi Method where enough experts could be engaged for the validation of the model as an alternative to the PLS-SEM technique employed in this study for the validation of the framework together with full experimentation in the application domain.

7.6. Conclusion.

The research made prescriptive contributions to the response to the research question in two phases. Firstly, it contributed to theory development, i.e. framework for auditing, through the abstraction based on the concepts and attributes of the viable systems approach. This represents the artefact of this action design research. Secondly, the research made contribution to practice in terms of providing an elaborate guidance and procedures that are expected to achieve outcomes that appropriately proportionate intervention to the challenges of IT auditing and practitioners are willing to adopt. Practitioners, managers and future researchers are called upon to implement the solution design and to augment its further development. Academic

institutions can design their training based on this the design since it provides a coherent and teachable set of ideas and solutions to IT auditing in contemporary business ecosystems.

8.0. REFERENCES

- Aboa**, Y. P. J. D. (2014). Continuous Auditing: Technology Involved.
- Abugu**, J. E. (2014). Re-examining the basis of auditors' liability in Nigeria and the United Kingdom. *International Journal of Disclosure and Governance*, 11(3), 231-254.
- ACCA**, (2016). Audit Needs to Respond More Quickly to Change, Evolve or Die, New Report Finds, <http://www.accaglobal.com/uk/en/discover/news/2016/march/future-of-audit.html> (accessed on 28th March 2016).
- Achterbergh**, J., & Vriens, D. (2002). Managing viable knowledge. *Systems Research and Behavioral Science*, 19(3), 223-241.
- Ackerman**, M., Rucker, B., Wells, A., Wilson, J., & Wittmann, R. (2009). IT Strategic Audit Plan. *Journal of Technology Research*, 1, 1.
- Adams**, M. B. (1994). Agency Theory and the Internal Audit, *Managerial Auditing Journal*, Vol. 9 Issue: 8, pp.8-12.
- Agranovich**, B. (2017). Technology Innovation: Enabling Risk Management Through Utilization of New Digital Technology, <https://fievy.com/browse/document/digital-transformation-strategy-2249>, (accessed on 18th January 2017).
- Agrawal**, A., & Cooper, T. (2017). Corporate governance consequences of accounting scandals: Evidence from top management, CFO and auditor turnover. *Quarterly Journal of Finance*, 7(01), 1650014.
- Agrawal**, A., & Chadha, S. (2005). Corporate governance and accounting scandals. *The Journal of Law and Economics*, 48(2), 371-406.
- Ali**, S. M. and Soomro T. R (2014). Integration of Information Security Essential Controls into Information Technology Infrastructure Library—A Proposed Framework. *International Journal of Applied*, 4(1).
- Aliquo Jr**, J. F., CISA, C., & Fu, Z. (2014). DuPont Drives Continuous Improvement with COBIT 5 Process Assessment Model.
- Alkhafaji**, A. F. (2011). Strategic management: formulation, implementation, and control in a dynamic environment. *Development and Learning in Organizations: An International Journal*, 25(2).
- Alvarez-Molina**, E. R., Martinez, L. G., Castanon-Puga, M., & Rodriguez-Diaz, A. (2014, November). A Neuro-Fuzzy System as a complex system of emergent behavior in organizations. In *Complex Systems (WCCS), 2014 Second World Conference on* (pp. 463-468). IEEE.
- Anomah**, S., Ayebofo, B., & Agyabeng, O. (2014). Forensic Accounting—A Multifaceted Standard for Cleaner Stewardship in Weak Regulatory Environments. *Research Journal of Finance and Accounting*, 5(2), 32-41.

- Appiah, S. C. Y., Ametepe, K., & Dapaah, J. M.** (2014). Systemic barriers to the fight against corruption by anti-corruptions institutions in Ghana. *Journal of Emerging Trends in Economics and Management Sciences*, 5(5), 465-473.
- Ashby, W.R.** (1956). *An Introduction to Cybernetics*, Methuen, London.
- Avram, M. G.** (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*, 12, 529-534.
- Awadallah, E. A., & Allam A.** (2015). A Critique of the Balanced Scorecard as a Performance Measurement Tool, *International Journal of Business and Social Science Vol. 6, No. 7*.
- Awuzie, B.O. & Mcdermott, P.** (2013), Understanding complexity within energy infrastructure delivery systems in developing countries: adopting a viable systems approach, *Journal of Construction Project Management and Innovation Vol. 3 (1): 543-559*, 2013 ISSN 2223-7852.
- Bagshaw, K.** (2006). Principles v Rules. <https://www.icaew.com/-/media/corporate/files/technical/ethics/principles-vs-rules.ashx?la=en> (accessed on 07 February 2018).
- Baker, M. J.** (2000). Selecting a research methodology. *The Marketing Review*, 1(3), 373-397.
- Bakos, J. Y.** (1991). A strategic analysis of electronic marketplaces. *MIS quarterly*, 295-310.
- Balakrishnan, R., Matsumura, E. M., & Ramamoorti, S.** (2017). Finding Common Ground: COSO's Control Frameworks and the Levers of Control. *Journal of Management Accounting Research*.
- Barile, S., Polese, F., Pels, J., & Sarno, D.** (2018). *Complexity and Governance*. Springer International Publishing.
- Barile, S., & Saviano, M.** (2018). Complexity and Sustainability in Management: Insights from a Systems Perspective. In *Social Dynamics in a Systems Perspective* (pp. 39-63). Springer, Cham.
- Bartens, Y., De Haes, S., Lamoen, Y., Schulte, F., & Voss, S.** (2015). On the Way to a Minimum Baseline in IT Governance: Using Expert Views for Selective Implementation of COBIT 5. In *System Sciences (HICSS), 2015 48th Hawaii International Conference on* (pp. 4554-4563). IEEE.
- Baylis, R., Burnap, P., Clatworthy, M., Gad, M., & Pong, C. K.** (2015). Private Lenders' demand for Audit. Available at SSRN 2557618.
- Beckford, J.L.W.** (1993). *The viable system model: a more adequate tool for practising management?* (Doctoral dissertation, University of Hull).
- Beer, S.** (1985). *Towards the Cybernetic Factory* (originally published in 1962). In: Harnden R, Leonard A. (eds.) 1994. *How Many Grapes Went into the Wine. Stafford Beer on the Art and Science of Holistic Management*. Wiley: Chichester pp. 163–228.
- Beer, S.** (1981), *Brain of the Firm*, 2nd ed., Wiley, New York, NY, (with history of CyberSyn project).
- Beer, S.** (1972). *Brain of the firm: A development in cybernetics*. New York: Herder & Herder.
- Beland, K., Larson, K., Rowley, T., Mueller, M., Smith, C., Rizzo, A., & Rendell, M.** (2014). Security and Audit Trail Capabilities of a Facilitated Interface Used to Populate a Database System with Text and Graphical Data Using Widely Available Software. *Journal of Software Engineering and Applications*, 2014.
- Bell, T. B., Marrs, F. O., & Solomon, I.** (1997). *Auditing organizations through a strategic-systems lens: The KPMG business measurement process*. KPMG Peat Marwick LLP.

- Bhattacharjee, A.** (2012). *Social Science Research: Principles, Methods, and Practices*, ISBN-13: 978-1475146127.
- Biske, S.** (2012). Risk intelligence and emerging role of internal audit, <http://www.m.businessfinancemag.com/risk-management/risk-intelligence-and-emerging-role-internal-audit> (accessed on 07 October 2015).
- Boateng, A. A., Boateng, G. O., & Acquah, H.** (2014). A Literature Review of Fraud Risk Management in Micro Finance Institutions in Ghana. *Research Journal of Finance and Accounting*, 5(11).
- Brazel, J. F., & Agoglia, C. P.** (2007). An Examination of Auditor Planning Judgments in a Complex Accounting Information System Environment*. *Contemporary Accounting Research*, 24(4), 1059-1083.
- Brocklesby, J.** (2012). Using the viable systems model to examine multi-agency arrangements, *Journal of the Operational Research Society*, 63, 418–430.
- Brown, T.** (2009). Change by design.
- Bryman, A.** (2004) (2nd ed). *Social Research Methods*. Oxford: Oxford University Press.
- Buchanan, I. & Clayton E.** (2014). Doing Business Where Governance Is Weak - Eight principles for succeeding in markets prone to ethical and legal risks, <http://www.strategy-business.com/article/00265?gko=4bad3> (accessed on 03 December 2015).
- Buchanan, S., & Gibb, F.** (1998). The information audit: an integrated strategic approach. *International journal of information management*, 18(1), 29-47.
- Buffa, A. M., & Basak, S.** (2016). A Theory of Operational Risk. In *2016 Meeting Papers* (No. 352). Society for Economic Dynamics.
- Byrnes, P. E., Al-Awadhi, A., Gullvist, B., Brown-Liburd, H., Teeter, R., Warren Jr, J. D., & Vasarhelyi, M.** (2018). Evolution of Auditing: From the Traditional Approach to the Future Audit 1. In *Continuous Auditing: Theory and Application* (pp. 285-297). Emerald Publishing Limited.
- Byrnes, P. E., Al-Awadhi, C. A., Gullvist, B., Brown-Liburd, H., Teeter, C. R., Warren Jr, J. D., & Vasarhelyi, M.** (2015). Evolution of Auditing: From the Traditional Approach to the Future Audit. *AUDIT ANALYTICS*, 71.
- Cartlidge, A., Rudd, C., Smith, M., Wigzel, P., Rance, S., Shaw, S., & Wright, T.** (2012). An Introductory Overview of ITIL® 2011. *Berkshire, United Kingdom*.
- Carvalho, A. V., & Esteban-Navarro, M.** (2016). Intelligence audit: Planning and assessment of organizational intelligence systems. *Journal of Librarianship and Information Science*, 48(1), 47-59.
- Cassidy, A.** (2016). *A practical guide to information systems strategic planning*. CRC press.
- Chambers, R. & McDonald, P.** (2013). Succeeding as a 21st Century Internal Auditor:7 Attributes of Highly Effective Internal Auditors, *The Institute of Internal Auditors and Robert Half International Inc*.
- Chambers, R.** (2009). Internal Auditing Is Once Again Demonstrating Its Agility and Versatility. <https://iaonline.theiia.org/internal-auditing-is-once-again-demonstrating-its-agility-and-versatility> (accessed on 1st March 2018).
- Chandler, R. A., & Edwards, J. R.** (Eds.). (2014). *Recurring Issues in Auditing: Professional Debate, 1875-1900: Professional Debate 1875-1900*. Routledge.
- Chandler, R. A.** (2014). The watchdogs who failed to bark: the auditors of the Kingston Cotton Mill. *Accounting Auditing and Accountability Journal*.

- Chin, W. W.** (2010). How to write up and report PLS analyses. In *Handbook of partial least squares* (pp. 655-690). Springer, Berlin, Heidelberg.
- Chin, W. W.** (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research*, 295(2), 295-336.
- Chou, D. C.** (2015). Cloud computing risk and audit issues. *Computer Standards & Interfaces*, 42, 137-142.
- Chow, S. L.** (1991). Conceptual rigor versus practical impact. *Theory & Psychology*, 1(3), 337-360.
- Koh C. H., & Woo, E. S.** (1998). The expectation gap in auditing. *Managerial Auditing Journal*, 13(3), 147-154.
- Clas, E.** (2008). Business continuity plans. *Professional Safety*, 53(9), 45.
- Cohen, L., Manion, L., & Morrison, K.** (2007). *Research methods in education* (6th Edition). London: Routledge.
- Cohen, J.** (1988). Set correlation and contingency tables. *Applied Psychological Measurement*, 12(4), 425-434.
- Comrey, A. L., & Lee, H. B.** (1992). Interpretation and application of factor analytic results. *Comrey AL, Lee HB. A first course in factor analysis*, 2.
- COSO** (2017). Enterprise Risk Management Integrating with Strategy and Performance. <https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf> (accessed on 05 November 2017).
- COSO**, (2004). Enterprise Risk Management — Integrated Framework, http://www.coso.org/documents/coso_erm_executivesummary.pdf (accessed on 12 August 2015)
- Cressey, D. R.** (1953). Other people's money; a study of the social psychology of embezzlement.
- Cronholm, S., Göbel H., & Hjalmarsson, A.** (2016). Empirical Evaluation of Action Design Research. Australasian Conference on Information Systems, 2016, Wollongong.
- Crotty, M.** (1998). *The foundations of social research*. London: Sage.
- Crumbly, D.L., Heitger, L. E. and Smith, G. S.** (2009). Forensic and investigative accounting. CCH Group: 3-5.
- Dada, S. O.; Owolabi S, A; Okwu, A. T** (2013). Forensic Accounting a Panacea to Alleviation of Fraudulent Practices in Nigeria. *International Journal of Business Management & Economic Research*, Vol. 4 Issue 5, p787-792. 6p.
- D'Aquila, J. M. & Houmes R.** (2014). COSO's Updated Internal Control and Enterprise Risk Management Frameworks, THE CPA JOURNAL/MAY 2014.
- DeFond, M. L., & Lennox, C. S.** (2015). Do PCAOB Inspections Improve the Quality of Internal Control Audits. *Available at SSRN 2574506*.
- DeFond M. & Zhang, J.** (2014). A review of archival auditing research, *Journal of Accounting and Economics*, 275–326.
- DeGrace, P., & Stahl, L. H.** (1990). *Wicked problems, righteous solutions*. Yourdon Press.
- De Haes, S., & Van Grembergen, W.** (2015). *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5*. Springer.
- De Haes, S., Van Grembergen, W., & Debreceny, R. S.** (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, 27(1), 307-324.

- Deloitte**, (2018). Agile Internal Audit Planning Performance Value, <https://www2.deloitte.com/global/en/pages/finance/articles/gx-agile-internal-audit-planning-performance-value.html#> (accessed on 1st March, 2018).
- Deloitte & Touche LLP**, Curtis, P. & Carey, M. (2012). Risk Assessment in Practice. http://www.coso.org/documents/COSOAnnncsOnlineSurvy2GainInpt4Updt2IntnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20October%202012.pdf. (accessed on 20 September 2016).
- Delta Risk LLC**, (2016). Cybersecurity and the Board of Directors, <http://www.delta-risk.net/>, (accessed on 30 January 2017).
- Devos, J.**, & Van de Ginste, K. (2015). Towards a Theoretical Foundation of IT Governance—The COBIT 5 case. *Electronic Journal Information Systems Evaluation Volume*, 18(2).
- Dieronitou, I** (2014). The Ontological and Epistemological Foundations of Qualitative and Quantitative Approaches to Research, *International Journal of Economics, Commerce and Management*, Vol. II, Issue 10, ISSN 2348 0386. United Kingdom.
- DiGabriele, J. A.** (2009). Implications of regulatory prescriptions and audit standards on the evolution of forensic accounting in the audit process. *Journal of Applied Accounting Research*, 10(2), 109-121.
- D'Onza G.**, Lamboglia R. and Verona R, (2015). "Do IT audits satisfy senior manager expectations? A qualitative study based on Italian banks", *Managerial Auditing Journal*, Vol. 30 Iss 4/5 pp.
- Dorminey, J.**, Fleming, A. S., Kranacher, M. J., & Riley Jr, R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 27(2), 555-579.
- Ebimobowei, A.**, Kereotu, O. J., & Brass Island, P. M. B. (2011). Role theory and the concept of audit expectation gap in South-South, Nigeria. *Current Research Journal of Social Sciences*, 3(6), 445-452.
- Egbunike, A. P.** (2014). Transition to 21st Century Audit: An Imperative for Fraud Detection in Nigeria. *Research in Applied Economics*, 6(1), p202-p215.
- Ellison R. J.**, Goodenough J., Weinstock C, and Woody C, (2008). Survivability Assurance for System of Systems, TECHNICAL REPORT, CMU/SEI-2008-TR-008, ESC-TR-2008-008.
- Endaya, K. A.**, & Hanefah, M.M. (2013). Internal Audit Effectiveness: An Approach Proposition to Develop the Theoretical Framework”, *Research Journal of Finance and Accounting*, Vol. 4 No. 10, pp. 92-103.
- Eriksson, K.**, & Lindström, U. A. (1997). Abduction—a way to deeper understanding of the world of caring. *Scandinavian journal of caring sciences*, 11(4), 195-198.
- Ernst & Young** (2013). Ten key IT considerations for internal audit Effective IT risk assessment and audit planning; [http://www.ey.com/Publication/vwLUAssets/Ten_key_IT_considerations_for_internal_audit/\\$FILE/Ten_key_IT_considerations_for_internal_audit.pdf](http://www.ey.com/Publication/vwLUAssets/Ten_key_IT_considerations_for_internal_audit/$FILE/Ten_key_IT_considerations_for_internal_audit.pdf) (accessed on 14 November 2016).
- Espejo, R.** (2009). Performance management, the nature of regulation and the CyberSyn project, *Kybernetes*, Vol. 38 Iss 1/2 pp. 65 – 82.
- Espejo, R.** (1979). Information and Management: The Cybernetics of a Small Company, *Management Research News*, Vol. 2 Iss 4 pp. 2 – 15.

- Espejo, R.** (2003). The Viable System Model - A Briefing About Organizational Structure, SYNCHO Limited.
- Espejo, R., & Gill, A.** (1997). The viable system model as a framework for understanding organizations. Phrontis Limited & SYNCHO Limited.
- Ettredge, M., Heintz, J., Li, C., & Scholz, S.** (2011). Auditor realignments accompanying implementation of SOX 404 ICFR reporting requirements. *Accounting Horizons*, 25(1), 17-39.
- Etzioni, A.** (1997). *Modern organizations*. Englewood Cliffs, NJ: Prentice Hall.
- Etzioni, A.** (1975). *Comparative Analysis of Complex Organizations*, Rev. Simon and Schuster.
- Everett, J.** (2003). The politics of comprehensive auditing in fields of high outcome and cause uncertainty. *Critical Perspectives on Accounting*, 14(1-2), 77-104.
- Faigman, D.** (2017). Evidence: Admissibility vs. Weight in Scientific Testimony. *The Judges' Book*, 1(1), 11.
- Falk, R. F., & Miller, N. B.** (1992). *A primer for soft modeling*. University of Akron Press.
- Feilzer, Y. M.** (2010). Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm. *Journal of mixed methods research*, 4(1), 6-16.
- Ficco, M., & Rak, M.** (2017). Security SLAs for Cloud Services: Hadoop Case Study. In *Reshaping Accounting and Management Control Systems* (pp. 103-114). Springer, Cham.
- Fitzgerald, B., & Howcroft, D.** (1998). Towards dissolution of the IS research debate: from polarization to polarity. *Journal of Information technology*, 13(4), 313-326.
- Flint, D.** (1988). *Philosophy and principles of auditing*. Hampshire: Macmillan Education Ltd.
- Flood, J. M.** (2016). AU-C 315 Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement. Wiley Practitioner's Guide to GAAS [2015](#): Covering all SASs, SSAEs, SSARSs, PCAOB Auditing Standards, and Interpretations, [91-117](#).
- Forte, D. & Power, R.** (2005), Sarbanes Oxley: maybe a blessing, maybe a curse, Computer Fraud and security – War & Peace in Cyberspace.
- Froese, T. M.** (2010). The impact of emerging information technology on project management for construction. *Automation in construction*, 19(5), 531-538.
- Geerts, G. L., Graham L. E, Mauldin E. G, McCarthy W. E and Richardson V. J.** (2013). Integrating Information Technology into Accounting Research and Practice. *Accounting Horizons* 27:4, 815-840.
- Gliem, J. A., & Gliem, R. R.** (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.
- Goldkuhl, G.** (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, 21(2), 135-146.
- Goldmann, P. and Kaufman H.** (2009). *Anti-Fraud Risk and Control Workbook*, John Wiley & Sons Inc., USA.
- Goode, S.** (2009). The admissibility of electronic evidence. *Rev. Litig.*, 29, 1.
- Gregg, M.** (2007). Certified Information Systems Auditor Exam Prep: Understanding the Role of IT Governance. <http://www.pearsonitcertification.com/articles/article.aspx?p=728428&seqNum=3> (accessed on 23rd December 2016).

- Gregor, S., & Hevner, A. R.** (2013). Positioning and presenting design science research for maximum impact. *MIS quarterly*, 37(2).
- Gregor, S., & Jones, D.** (2007). The Anatomy of a Design Theory, *Journal of the Association of Information Systems* (8:5), pp. 312-335.
- Grönlund, A., Svärdsten F. and Öhman P.,** (2011). Value for money and the rule of law: the (new) performance audit in Sweden, *International Journal of Public Sector Management*, Vol. 24 Iss 2 pp. 107 – 121
- Guadagnoli, E. & Velicer, W.** (1988). Relation of sample size to the stability of component patterns. *Psychological Bulletin*, 103 265-275.
- Guba, E. G., & Lincoln, Y. S.** (1994). Competing paradigms in qualitative research. *Handbook of qualitative research*, 2(163-194), 105.
- Guizzardi, G.** (2007). On ontology, ontologies, conceptualizations, modelling languages, and (meta) models. *Frontiers in artificial intelligence and applications*, 155, 18.
- Gunningham, N., & Sinclair, D.** (1999). Integrative regulation: a principle-based approach to environmental policy. *Law & Social Inquiry*, 24(4), 853-896
- Ha, B.** (2005). System-based auditing and monitoring of government programs and projects. *International Journal of Government Auditing*, 32(4), 11.
- Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L.** (1998). *Multivariate data analysis* (Vol. 5, No. 3, pp. 207-219). Upper Saddle River, NJ: Prentice hall.
- Haislip, J. Z., Masli, A., Richardson, V. J., & Watson, M. W.** (2015). External reputational penalties for CEOs and CFOs following information technology material weaknesses. *International Journal of Accounting Information Systems*, 17, 1-15.
- Hamdani, K.** (2013). Viable System Model - Management Cybernetics: science of effective organization, https://www.youtube.com/watch?v=c-1ZnqXSt_k, (accessed on 12 July 2015).
- Hamer, D. A.** (2018). The Unstable Province of Jury Fact-Finding: Evidence Exclusion, Probative Value and Judicial Restraint after IMM V the Queen.
- Hassink, H.F.D. et al.** (2009). Corporate fraud and the audit expectations gap: A study among business managers; *Journal of International Accounting, Auditing and Taxation* 18 (2009) 85–100.
- Havelka, D., & Merhout, J. W.** (2013). Internal information technology audit process quality: Theory development using structured group processes. *International Journal of Accounting Information Systems*, 14(3), 165-192.
- Healy, M., & Perry, C.** (2000). Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm. *Qualitative market research: An international journal*, 3(3), 118-126.
- Helfrich, C. D., Li, Y. F., Mohr, D. C., Meterko, M., & Sales, A. E.** (2007). Assessing an organizational culture instrument based on the Competing Values Framework: Exploratory and confirmatory factor analyses. *Implementation Science*, 2(1), 13.
- Herzog, P., & Leker, J.** (2010). Open and closed innovation—different innovation cultures for different strategies. *International Journal of Technology Management*, 52(3/4), 322-343.
- Hevner, A., Chatterjee, S.** (2010). Design Research in Information Systems, in *Design Science Research in Information Systems* (pp 9-22). Springer.
- Hevner, A.R.** (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, 19, 2, 87-92.
- Hevner, A.R., March, S.T., Park, J. & Ram, S.** (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28, 1, 75-105.

- Hilder, T.** (1995). The Viable System Model. Retrieved June 28, 2005.
- Hildbrand, S., & Bodhanya, S.** (2015). Guidance on applying the viable system model. *Kybernetes*, 44(2).
- Hitchins, D.** (2015). Systems & Systems Engineering - Viable Systems Model; https://www.youtube.com/watch?v=-dwzb_NN4II (accessed on 7 August 2015).
- Ho, R.** (2006). *Handbook of univariate and multivariate data analysis and interpretation with SPSS*. Chapman and Hall/CRC.
- Holmes, A. M.** (2018). Automated Investigations: The Role of the Request Filter in Communications Data Analysis. *Journal of Information Rights, Policy and Practice*, 2(2).
- Huber, W.** (2016). Forensic Accounting, Fraud Theory and the end of the fraud triangle.
- Huck, V.** (2016). King IV report on corporate governance released; <http://www.theaccountant-online.com/news/king-iv-report-on-corporate-governance-released-5654840/>, (accessed on the 3rd November, 2016).
- Hyde, K. F.** (2000). Recognizing deductive processes in qualitative research. *Qualitative market research: An international journal*, 3(2), 82-90
- IIA, (2015).** Definition of Internal Auditing. <http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/?search%C2%BCdefinition> (accessed on 08 December 2015).
- IIA, (2011).** Auditing the Control Environment, www.theiia.org/guidance, April 2011 (accessed on 02 January 2017).
- IIA & KPMG, (2015).** Strategy-related Auditing - Exploratory research on the consideration of strategic risk and organizational strategy in internal audits. A Discussion Paper.
- Iivari, J.** (2007). A paradigmatic analysis of information systems as a design science. *Scandinavian journal of information systems*, 19(2), 5.
- Irwin, A. S., & Slay, J.** (2010). Detecting money laundering and terrorism financing activity in Second Life and World of Warcraft.
- ISACA (2013).** Why, When and How to Migrate to COBIT 5, <http://www.isaca.org/Knowledge-Center/COBIT/COBIT-focus/Documents/COBIT-Focus-Vol-3-2013.pdf> (accessed on 25 March, 2015)
- Ittonen, K.** (2010). A theoretical examination of the role of auditing and the relevance of audit reports. *University of Vaasa, Finland*.
- Iversen, J. H., Mathiassen, L., & Nielsen, P. A.** (2004). Managing risk in software process improvement: an action research approach. *Mis Quarterly*, 395-433.
- Iyengar, V., Boier, I., Kelley, K., & Curatolo, R.** (2007). Analytics for audit and business controls in corporate travel & entertainment. In *Proceedings of the sixth Australasian conference on Data mining and Analytics-Volume 70* (pp. 3-12). Australian Computer Society, Inc.
- Jafarov, N. and Lewis, E.** (2014). Mapping the Cybernetic Principles of Viable System Model to Enterprise Service Bus. *IT in Industry*, vol. 2, no. 3.
- Jeffrey, N. & Gambier, A.** (2016). **The Future of Audit** http://www.accaglobal.com/content/dam/ACCA_Global/Technical/audit/ea-future-of-audit.pdf (accessed on 16 December 2016).
- Jensen, M.C.** (2002), Value maximization, stakeholder theory and corporate objective function, *Business Ethics Quarterly*, Vol. 12, No. 2 (Apr., 2002), pp. 235-256.
- John, E., & Cianfrani, C. A.** (2017). Beyond the Requirements. *Quality Progress*, 50(4), 46.

- Kahorongo, T. C., Reddy, N., & Karodia, A. M. (2015).** The Adoption of Information Technology in the Governance System of the Bank of Namibia. *Business and Management Studies*, 1(2), 77-96.
- Karagiorgos, T., Drogalas, G., Pazarskis, M., & Christodoulou, P. (2007).** Internal Auditing as a Main Tool for Efficient Risk Assessment. In *2007 Management of International Business & Economic Systems (MIBES) Conference*.
- Kasum, A. S., Adefila, J. J., and. Olaniyi T. A. (2005).** 'The Global Endemic Nature of Financial Malpractices: An Analytical Appraisal.' *African Journal of Management*, 1(1), pp11-20.
- Kerin, R. A., Varadarajan, P. R., & Peterson, R. A. (1992).** First-mover advantage: A synthesis, conceptual framework, and research propositions. *The Journal of Marketing*, 33-52.
- Khan, S., Nicho, M., & Cooper, G. (2015).** A Role Allocation Model for IT Controls in a Cloud Environment. *Review of Business Information Systems (RBIS)*, 19(1), 5-14.
- Kinney, Jr. W. R. (2003).** Auditing Risk Assessment and Risk Management Processes, The Institute of Internal Auditors Research Foundation, ISBN 0-89413-498-1.
- Kirk, R., Hunt S. & Nikitin F. (2008).** Developing the IT Audit Plan. The Institute of Internal Auditors (IIA). Fla.32701-4201.
- Knapp, C. A., & Knapp, M. C. (2001).** The effects of experience and explicit fraud risk assessment in detecting fraud with analytical procedures. *Accounting, Organizations and Society*, 26(1), 25-37.
- Knechel, W. R., & Salterio, S. E. (2016).** Auditing: Assurance and risk. Taylor & Francis
- Kogan, A., Sudit, E. F., & Vasarhelyi, M. A. (1999).** Continuous online auditing: an evolution. *Journal of Information Systems*, 13(2).
- Koskivaara, E (2007).** Integrating Analytical Procedures into the Continuous Audit Environment, *Journal of Information Systems and Technology Management*. Vol. 3, No. 3, 2007, p. 331-346, ISSN online: 1807-1775.
- Kovács, G., & Spens, K. M. (2005).** Abductive reasoning in logistics research. *International Journal of Physical Distribution & Logistics Management*, 35(2), 132-144.
- KPMG & IIA (2015).** Strategy-related auditing - Exploratory research on the consideration of strategic risk and organizational strategy in internal audits, Discussion paper, June. 2015.
- Kramer, J. B. (2003).** *The CISA prep guide: mastering the certified information systems auditor exam*. John Wiley & Sons.
- Kroeze, J. H (2012).** Interpretivism in IS – a Postmodernist (or Post-positivist?) Knowledge Theory, *AMCIS 2012 Proceedings*. Paper 7.
<http://aisel.aisnet.org/amcis2012/proceedings/PerspectivesIS/7> (accessed on 31 August 2015).
- Kuhn, J.R & Sutton G.S (2010).** Continuous Auditing in ERP System Environments: The Current State and Future Directions, *Journal of Information Systems*. Vol. 24, No. 1. pp. 91–112.
- Kultanen, E. (2017).** Prevention and detection of fraud in a Ugandan university organization.
- Kyobe, M., (2008).** The influence of strategy-making types on IT alignment in SMEs, *Journal of Systems and Information Technology*. Vol. 10 Issue: 1, pp.22-38.
- Lane, M. (2014).** Enterprise Architecture and COBIT 5, <http://blog.orbusoftware.com/enterprise-architecture-COBIT-5/> (accessed on 12 July 2015).
- Lawson, A. E. (2010).** Basic inferences of scientific reasoning, argumentation, and discovery. *Science Education*, 94(2), 336-364.

- Lewis, E. & Millar G.** (2009). The Viable Governance Model - A Theoretical Model for the Governance of IT, Proceedings of the 42nd Hawaii International Conference on System Sciences 2009.
- Li, H. J., Chang, S. I., & Yen, D. C.** (2017). Investigating CSFs for the life cycle of ERP system from the perspective of IT governance. *Computer Standards & Interfaces*, 50, 269-279.
- Li Y., Yu, J. J., Zhang, Z., & Zheng, S. X.** (2014). The Effect of Internal Control Weakness on Firm Valuation: Evidence from SOX Section 404 Disclosures. Available at SSRN 2529273.
- Linich, D. & Puleo, M.** (2016). Taming complexity with Analytics. CIO Journal, Deloitte Consulting LLP, <http://deloitte.wsj.com/cio/2015/12/21/taming-complexity-with-analytics/> (accessed on 04 October 2017)
- Lunenburg, F. C.** (2013). Compliance theory and organizational effectiveness. *International journal of scholarly academic intellectual diversity*, 13(1), 1-4.
- MacCallum, R. C., Widaman, K. F., Preacher, K. J., & Hong, S.** (2001). Sample size in factor analysis: The role of model error. *Multivariate Behavioral Research*, 36(4), 611-637.
- Maccani, G., Donnellan, B., & Helfert, M.** (2015). Action design research: a comparison with canonical action research and design science. In *At the Vanguard of Design Science: First Impressions and Early Findings from Ongoing Research Research-in-Progress Papers and Poster Presentations from the 10th International Conference, DESRIST 2015. Dublin, Ireland, 20-22 May*. DESRIST 2015.
- Mahzan, N., & Hassan, N. A. B.** (2015). Internal Audit of Quality in 5s Environment: Perception on Critical Factors, Effectiveness and Impact on Organizational Performance. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 5(1), 92-102.
- Mail, A., Pratikto, P., Suparman, S., Purnomo, P., & Santoso, B.** (2014). Relationship between Internal Quality Audit and Quality Culture toward Implementation Consistency of ISO 9000 in Private College of Sulawesi Province, Indonesia. *International Education Studies*, 7(9), p175.
- Mäkelä, M.** (2007). Knowing through making: The role of the artefact in practice-led research. *Knowledge, Technology & Policy*, 20(3), 157-163.
- Marcello, S., Ray, T., Carmichael, D., Peterson, J., Ramamoorti, S., Collelli, S., & Nearon, B.** (2017). The Future of Auditing: A Roundtable Discussion. *The CPA Journal*, 39.
- March, S. T., & Storey, V. C.** (2008). Design science in the information systems discipline: an introduction to the special issue on design science research. *MIS quarterly*, 725-730.
- Markon, K. E., Chmielewski, M., & Miller, C. J.** (2011). The reliability and validity of discrete and continuous measures of psychopathology: a quantitative review. *Psychological bulletin*, 137(5), 856.
- Marques, R. P.** (2017). Continuous Assurance and Business Compliance in enterprise information systems. In *enterprise information systems and digitalization of business functions* (pp. 99-199). IGI Global.
- Martin, S.** (2004). The cost of restoration as a way of defining resilience: a viability approach applied to a model of lake eutrophication. *Ecology and Society*, 9(2).
- Martinez, R. A.** (2014). 2013 COSO Framework Overview. <https://chapters.theiia.org/los-angeles/Events/Documents/COSO%20Risk%20Assessments%20by%20Roger%20Martinez%20and%20Vasquez%20Co.pdf> (accessed on 09 December 2015).

- Maruyama, M.** (1963). The second cybernetics: Deviation-amplifying mutual causal processes. *American scientist*, 164-179.
- Masters, J.** (1995). The history of action research. *Action research electronic reader*, 22, 2005.
- Mautz, R. K., & Sharaf, H. A.** (1961). The Philosophy of Auditing, American Accounting Association. *Monograph No. 6. Sarasota, FL: American Accounting Association.*
- McCafferty, J.** (2016). Audit leaders in Africa voice frustration at the difficulty of bringing corruption to light, <http://misti.com/audit-news-trends/big-challenges-for-public-auditors-in-africa>. (accessed on 30 -12 – 16).
- McCann, T. V., & Clark, E.** (2003). Grounded theory in nursing research: Part 1- Methodology. *Nurse Researcher (through 2013)*, 11(2), 7.
- McDonald, R. P., & Ho, M. H. R.** (2002). Principles and practice in reporting structural equation analyses. *Psychological methods*, 7(1), 64.
- Merhout, J. W., & Havelka, D.** (2008). Information technology auditing: A value-added IT governance partnership between IT management and audit. *Communications of the Association for Information Systems*, 23(1), 26.
- Michael, K., & Dunn, L.** (2008). The use of information and communication technology for the preservation of aboriginal culture: The Badimaya people of Western Australia. In *Information Communication Technologies: Concepts, Methodologies, Tools, and Applications* (pp. 2652-2655). IGI Global.
- Mihret, D. G.** (2014). How can we explain internal auditing? The inadequacy of agency theory and a labor process alternative, *Critical Perspectives on Accounting* 25 (2014) 771–782.
- Mills, J., Bonner, A., & Francis, K.** (2008). The development of constructivist grounded theory. *International journal of qualitative methods*, 5(1), 25-35.
- Mingers, J. & Willcocks L.** (2004). *Social Theory and Philosophy for Information Systems*, John Wiley & Sons Ltd.
- Mitchell, R. B.** (2007). Compliance theory: compliance, effectiveness, and behaviour change in international environmental law. *The Oxford Handbook of International Environmental Law*, 893, 900-910.
- Moeller, B., Ere, K., Loeser, F., & Zarnekow, R.** (2013). How Sustainable is COBIT 5? Insights from Theoretical Analysis and Empirical Survey Data.
- Mullarkey, M. T., & Hevner, A. R.** (2015). Entering action design research. In *International Conference on Design Science Research in Information Systems* (pp. 121-134). Springer, Cham.
- Murphy, M. L.** (2015). Preventing and detecting fraud at not-for-profits. <http://spr.ly/nfpfraud2015> (accessed on 19 December 2015).
- Ndlovu, S. L., & Kyobe, M. E.** (2016). Challenges of COBIT 5 IT Governance Framework Migration. In *CONF-IRM* (p. 58).
- Nehinbe, J. O., & Adebayo, F.** (2011, September). Audit and research challenges in digital forensics. In *Cybernetic Intelligent Systems (CIS), 2011 IEEE 10th International Conference on* (pp. 86-91). IEEE.
- Neumayer, E., & Plümper, T.** (2017). *Robustness Tests for Quantitative Research*. Cambridge University Press.
- Nevo, S., & Wade, M. R.** (2010). The formation and value of IT-enabled resources: antecedents and consequences of synergistic relationships. *MIS Quarterly*, 163-183.
- Neyland, D.** (2007). Achieving transparency: The visible, invisible and divisible in academic accountability networks. *Organization*, 14(4), 499-516.

- Ngwenyama, O. K.** (1991). The critical social theory approach to information systems: problems and challenges. *Information systems research: Contemporary approaches and emergent traditions*, 267-280.
- Nickell, C. G., & Denyer, C.** (2007). An introduction to SAS 70 audits. *Benefits Law Journal*, 20(1), 58-68.
- Niehaves, B.** (2007). On Epistemological Pluralism in Design Science. *Scandinavian Journal of Information Systems*: Vol. 19: Iss. 2, Article 7.
- Niemi, L., Knechel, W. R., Ojala, H., & Collis, J.** (2018). Responsiveness of auditors to the audit risk standards: Unique evidence from Big 4 audit firms. *Accounting in Europe*, 15(1), 33-54.
- Nils, U. & Ahlemann, F.** (2010). Structural equation modeling in information systems research using partial least squares. *JITTA: Journal of Information Technology Theory and Application* 11.2: 5.
- Nunnally, J. C., & Bernstein, I. H.** (1994) *Psychometric theory*. (3rd ed.) New York: McGraw-Hill.
- Nunnally, J.** (1978). *Psychometric methods*.
- O'Grady, W., & Lowe, A.** (2016). Management Control: The Influence of Cybernetics and the Science of the Unknowable. In *Pioneers of Critical Accounting* (pp. 31-51). Palgrave Macmillan UK.
- Oliver, D., & CISA, C.** (2011). Delivering business benefits with COBIT: An introduction to COBIT 5. *COBIT Focus*, 3, 1-3.
- Omonuk, J. B., & Oni, A. A.** (2015). Computer Assisted Audit Techniques and Audit Quality in Developing Countries: Evidence from Nigeria. *J Internet Bank Commer*, 20 (127), 2.
- Orlikowski, W. J., & Baroudi, J. J.** (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research*, 2(1), 1-28.
- Osei-Afoakwa, K.** (2013). The Games Ghanaian Auditors Play with Their Reports. *International Journal of Business and Management Tomorrow*, 3(1).
- Owojori A. A. and Asaolu T.O** (2009). The Role of Forensic Accounting in Solving the Vexed Problem of Corporate World, EuroJournals Publishing, Inc. ISSN 1450-216X Vol.29 No.2 (2009), pp.183-187.
- Owolabi A. S., Olamide, J. O., & AyodejiTemitope, A.** (2016). Evolution and development of auditing. *Unique Journal of Business Management Research* Vol. 3(1), pp. 032-040.
- Paucar-Caceres, A.** (2009). Measuring the performance of a research strategic plan system using the soft systems methodology's three 'Es' and the viable system model's indices of achievement. *Systemic Practice and Action Research*, 22(6), 445-462.
- PCAOB** (2013). Considerations for Audits of Internal Control over Financial Reporting. Staff Practice Alert No. 11. October 24. Washington D.C.
- Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S.** (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3), 45-77.
- Persico, F.** (2016). How Technology is Transforming Audit, <http://www.accountingtoday.com/accounting-technology/> (accessed on 13 December 2016).
- Peter, M., Aliyu Dadi, E., Ebong Inyang, G., & Abba Ogere, Z.** (2014). Application of Forensic Auditing in Reducing Fraud Cases in Nigeria Money Deposit Banks. *Global Journal of Management and Business Research*, 14(3).

- Petersen C.** (2015). Surfacing Critical Cyber Threats Through Security Intelligence - A Reference Model for IT Security Practitioners, www.logrhythm.com/SIMM-CEO (assessed on 01 October 2015).
- Peterson, A. M. & Lundberg, J.** (2016). Applying action design research (ADR) to develop concept generation and selection methods, *Procedia CIRP* 50 (2016) 222 – 227.
- Philipson, S., Johansson, J., & Scley, D.** (2016). Global Corporate Governance-The Maelstrom of Increased Complexity: Is it Possible to Learn to Ride the Dragon?. *Journal of Business and Economics*, (3).
- Pine B.** (2008). A risk-based approach to auditing financial statements, http://www.accaglobal.com/content/dam/acca/global/PDF-students/2012s/sa_feb08_pine.pdf (accessed on 15 January 2016).
- Polese, F., Carrubbo, L., & Russo, G.** (2011). Managing Business Relationships: between service culture and a Viable Systems Approach. *Esperienze d'Impresa: Dipartimento di Studi e Ricerche Aziendali, Università di Salerno*, (2).
- Pollard, C., & Cater-Steel, A.** (2009). Justifications, strategies, and critical success factors in successful ITIL implementations in US and Australian companies: an exploratory study. *Information systems management*, 26(2), 164-175.
- Ponterotto, J. G., & Ruckdeschel, D. E.** (2007). An overview of coefficient alpha and a reliability matrix for estimating adequacy of internal consistency coefficients with psychological research measures. *Perceptual and motor skills*, 105(3), 997-1014.
- Popa, M.** (2012). Methods and techniques of quality management for ICT audit processes. *arXiv preprint arXiv:1201.0395*.
- Poulis, K., Poulis, E., & Plakoyiannaki, E.** (2013). The role of context in case study selection: An international business perspective. *International Business Review*, 22(1), 304-314.
- Power, M.** (1999). *The Audit Society: Rituals of Verification*. Oxford: Oxford University Press.
- Pratt, M. J., & Peursem, K. V.** (1993). Towards a conceptual framework for auditing. *Accounting Education*, 2(1), 11-32.
- PwC,** (2016). Key Challenges, <http://www.pwc.co.uk/services/audit-assurance/internal-audit/key-challenges.html> (accessed on the 26th December 2016).
- Radovanović, D., Radojević, T., Lučić, D., & Šarac, M.** (2010). IT audit in accordance with COBIT standard. In *MIPRO, 2010 Proceedings of the 33rd International Convention* (pp. 1137-1141). IEEE.
- Raftery, A. E.** (1995). Bayesian model selection in social research. *Sociological methodology*, 111-163.
- Rahaman, A. S.** (2010). Critical accounting research in Africa: Whence and whither. *Critical Perspectives on Accounting*, 21(5), 420-427.
- Rahman, A. A. B. L. A., Al-Nemrat, A., & Preston, D. S.** (2014). Sustainability in Information Systems Auditing. *European Scientific Journal*, 10(10).
- Ralph, P.** (2014). Lab-based action design research, Companion Proceedings of the 36th International Conference on Software; Hyderabad, India.
- Ramirez, R.** (1999). Stakeholder analysis and conflict management. *Cultivating peace: conflict and collaboration in natural resource management*, 101-126.
- Ratcliffe, T. A & Landes C. E.** (2009), *Understanding Internal Control and Internal Control Services*, American Institute of Certified Public Accountants Inc., (AICPA), New York, NY, 10036-8775.

- Ray, E.** (2009). Adding value: How modern internal auditing assists organizations in achieving strategic objectives, The Institute of Internal Auditors Research Foundation.
- Razak, N., & Muhamad, R.** (2017). Using Audit Committee and Internal Audit Function Inter-Relationships to Drive Up Effectiveness. *Asian Journal of Accounting Perspectives*, 8(1).
- Rezaee, Z., Sharbatoghlie, A., Elam, R., & McMickle, P. L.** (2018). Continuous auditing: Building automated auditing capability. In *Continuous Auditing: Theory and Application* (pp. 169-190). Emerald Publishing Limited.
- Rittenberg, L. E.** (2013). COSO 2013 a reflection of the times: the long-awaited Internal Control-Integrated Framework update aims to help organizations better design and implement controls, with an eye toward today's business challenges. *Internal Auditor*, 70(4), 60-66.
- Romney, M. B., Steinbart, P. J., Zhang, R., & Xu, G.** (2006). Accounting information systems (Vol. 7). Englewood Cliffs, NJ: Prentice Hall.
- Rossouw, G. J.** (2005). Business ethics and corporate governance in Africa. *Business & Society*, 44(1), 94-106.
- Ruhnke, K., & Schmidt, M.** (2014). The audit expectation gap: existence, causes, and the impact of changes. *Accounting and Business Research*, 44(5), 572-601.
- Sagalovsky, B.** (2015). Organizing for Lean: autonomy, recursion and cohesion, *Kybernetes*, Vol. 44. Issue: 6/7, pp.970-983.
- Sayana, S. A., & CISA, C.** (2003). Using CAATs to support IS audit. *Information systems control journal*, 1, 21-23.
- Sayana, S. A.** (2002). The IS Audit Process. *Information Systems Control Journal*, 1, 20-22.
- Schaller, M.** (2016). The empirical benefits of conceptual rigor: Systematic articulation of conceptual hypotheses can reduce the risk of non-replicable results (and facilitate novel discoveries too). *Journal of Experimental Social Psychology*, 66, 107-115.
- Schillemans, T., & van Twist, M.** (2016). Coping with Complexity: Internal Audit and Complex Governance. *Public Performance & Management Review*, 40(2), 257-280.
- Schmidt, et al.** (2014). Towards Recursive Plan-Do-Check-Act Cycles for Continuous Improvement, *Proceedings of the 2014 IEEE IEEM*.
- Schwanninger, M.** (2006). The Evolution of Organizational Cybernetics. *Scientiae Mathematicae Japonicae*. 64. No 2. 405-420.
- Scotland, J.** (2012). Exploring the philosophical underpinnings of research: relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms. *English Language Teaching*, 5(9), p9.
- Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R.** (2011). Action design research. *MIS quarterly*, 37-56.
- Shahid, A.** (2014). Strategic Planning Using COBIT 5, Volume 2, April 2014, http://www.isaca.org/knowledge-center/COBIT/documents/cf-vol-2-2014-strategic-planning-using-COBIT-5_nlt_eng_0414.pdf (accessed on 14 September 2015).
- Sharbatoghlie, A., & Sepehri, M.** (2015). An Integrated Continuous Auditing Project Management Model (CAPM). In *4th International Project Management Conference*.
- Sheehan, N. T.** (2010). A risk-based approach to strategy execution. *Journal of business strategy*, 31(5), 25-37.
- Simmons, R.** (1995). *Levers of Control – How Managers use innovative control systems to drive Strategic Renewal*, Business School Press, Boston, Massachusetts.
- Simon, H.A.** (1996). *The Sciences of the Artificial* (3rd ed.). Cambridge: The MIT Press.

- Singleton, T.** (2014). IS Audit Basics: Beyond the IT in IT Audit (Part 2), ISACA Journal. Vol. 4.
- Sirois, L. P., Bédard, J., & Bera, P.** (2018). The informational value of key audit matters in the auditor's report: evidence from an Eye-tracking study. *Accounting Horizons*.
- Sivo, S. A., Saunders, C., Chang, Q., & Jiang, J. J.** (2006). How low should you go? Low response rates and the validity of inference in IS questionnaire research. *Journal of the Association for Information Systems*, 7(6), 17.
- Soileau, J., Soileau, L., & Summers, G.** (2015). The Evolution of Analytics and Internal Audit. *EDPACS*, 51(2), 10-17.
- Spagnoletti, P., Resca, A., & Lee, G.** (2015). A design theory for digital platforms supporting online communities: a multiple case study. *Journal of Information Technology*, 30(4), 364-380.
- Strous, L.** (1998, January). Audit of information systems: The need for cooperation. In *SOFSEM'98: Theory and Practice of Informatics* (pp. 264-274). Springer Berlin Heidelberg.
- Steinhaeuser, T., Elezi, F., Tommelein, I. D., & Lindemann, U.** (2015). Management Cybernetics as a Theoretical Basis for Lean Construction Thinking. *Lean Construction Journal*, 01-14.
- Stevens, J. P.** (2012). *Applied multivariate statistics for the social sciences*. (5th edition). Routledge.
- Steward, T. R.** (2015). Data Analytics for financial statement audits. *Audit Analytics*. 105.
- Suhr, D. D.** (2006). *Exploratory or confirmatory factor analysis?* (pp. 1-17). Cary: SAS Institute.
- Sun, T., Alles, M., & Vasarhelyi, M. A.** (2015). Adopting continuous auditing: A cross-sectional comparison between China and the United States. *Managerial Auditing Journal*, 30(2), 176-204.
- Sussy, B., Wilber, C., Milagros, L., & Carlos, M.** (2015). ISO/IEC 27001 implementation in public organizations: A case study. In *Information Systems and Technologies (CISTI), 2015 10th Iberian Conference on* (pp. 1-6). IEEE.
- Svata, V.** (2011). IS Audit Considerations in Respect of Current Economic Environment? *Journal of Systems Integration*, 2(1), 12-20.
- Swanson, G. A., & Marsh, H. L.** (1993). A systems-based conceptual framework for auditing. *Systems Research and Behavioral Science*, 10(1), 29-40.
- Swinkels, W. H. A.** (2012). Exploration of a theory of internal audit. Eburon Uitgeverij BV.
- Tabachnick, B. G., & Fidell, L. S.** (1996). Analysis of covariance. *Using multivariate statistics*, 8(1), 321-374.
- Tanimoto, S., Yamada, S., Iwashita, M., Kobayashi, T., Sato, H., & Kanai, A.** (2016). Risk assessment of BYOD: Bring your own device. In *Consumer Electronics, IEEE 5th Global Conference on* (pp. 1-4). IEEE.
- Tay, S.** (2017). Risk Management in Internal Audit Planning. In *Theory and Practice of Quality and Reliability Engineering in Asia Industry* (pp. 69-73). Springer, Singapore.
- THEIIA** (2017). Global Perspectives: Internal Audit in the Age of Disruption <https://na.theiia.org/periodicals/Public%20Documents/GPI-Internal-Audit-in-the-Age-of-Disruption.pdf> (accessed 01 March 2018).
- The Pinnacle Associates Ltd** (2007), The Behavioral-based online auditing-revolutionary change, [http://www.pinnacleassoc.com/documents/125d2cd78f8b558b4fb8a92133d30d37 The Auditing Revolution.pdf](http://www.pinnacleassoc.com/documents/125d2cd78f8b558b4fb8a92133d30d37%20The%20Auditing%20Revolution.pdf) (assessed on 27 April, 2015).

- Thomas, R.** (2006). Is the Viable System Model of organization inimical to the concept of human freedom? *Journal of Organizational Transformation and Social Change*, 3(1), 69.
- Tichaona, Z.** (2014). IT Governance Assurance and Consulting: A Compelling Need for Today's IT Auditors, *EDPACS: The EDP Audit, Control, and Security Newsletter*, 49:6, 1-9.
- Toba, Y.** (1975). A general theory of evidence as the conceptual foundation in auditing theory. *The Accounting Review*, 50(1), 7-24.
- Underwriters Laboratories Inc.**, (2006), The Auditing Revolution is already happening, are you part? <http://www.the-hpo.com/downloads/Auditing%20Revolution.pdf> (assessed on 27 April 2015).
- Vaishnavi, V.**, & Kuechler, W. (2004). Design research in information systems.
- Van Aken, J. E.** (2007). Design science and organization development interventions: Aligning business and humanistic values. *The Journal of Applied Behavioral Science*, 43(1), 67-88
- Van Aken, J. E.** (2004). Management research based on the paradigm of the design sciences: the quest for field-tested and grounded technological rules. *Journal of management studies*, 41(2), 219-246.
- Van Grembergen, W.**, & De Haes, S. (2018, January). Introduction to the Minitrack on IT Governance and its Mechanisms. In *Proceedings of the 51st Hawaii International Conference on System Sciences*.
- Varkoi, T.**, Nevalainen, R., & Mäkinen, T. (2016). Process Assessment in a Safety Domain-Assessment Method and Results as Evidence in an Assurance Case. In *Quality of Information and Communications Technology (QUATIC), 2016 10th International Conference on the* (pp. 52-58). IEEE.
- Vedeler, L.** (2000). Observation research in pedagogical fields. [*Observasjonsforskning I pedagogiske fag*; in Norwegian]. Gyldendal Akademisk. Norway.
- Von Bertalanffy, L.** (1971). The History and Status of General Systems Theory.
- Walker, B.**, Carpenter, S., Anderies, J., Abel, N., Cumming, G., Janssen, M., ... & Pritchard, R. (2002). Resilience management in social-ecological systems: a working hypothesis for a participatory approach. *Conservation ecology*, 6(1).
- Weller, N.** (2015). COSO Enterprise Risk Management Framework, <http://www.accaglobal.com/zm/en/student/exam-support-resources/professional-exams-study-resources/p1/technical-articles/coso-enterprise-risk-management-framework-part-1.html> (accessed on 11 August 2015).
- Wescott, R. E.** (2014), Using COBIT 5 as an Audit tool, <http://www.isaca.org/Knowledge-Center> (accessed on 26 July 2015).
- Wessels, P. L.** (2005). Critical information and communication technology (ICT) skills for professional accountants, *Meditari Accountancy Research Vol. 13 No. 1 2005* 87-103.
- Wiener, N.** (1948), *Cybernetics: Or the Control and Communication in the Animal and the Machine*, MIT Press, Cambridge, MA.
- Wilks, J.T.**, and Zimbleman, M.F. (2004). Using Game Theory and Strategic Reasoning Concepts to Prevent and Detect Fraud. *Accounting Horizons*, 18, 3, 173-184.
- Williams, B.**, Onsmann, A., & Brown, T. (2010). Exploratory factor analysis: A five-step guide for novices. *Australasian Journal of Paramedicine*, 8(3).

- Winter, K.** (2012), *ITIL Adoption – the Challenges*, APMG-International is a global examination institute. Head Office, Sword House, Totteridge Road, High Wycombe, Buckinghamshire UK HP13 6DG
- Woods, M.** (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research*, 20(1), 69-81.
- Wu, J., & Lederer, A.** (2009). A meta-analysis of the role of environment-based voluntariness in information technology acceptance. *Mis Quarterly*, 419-432..
- Yee, C. M., & Khin, E. W. S.** (2015). Positivist Research and its Influence in Management Accounting Research. *Journal of Accounting Perspectives*, 3(1).
- Yin, R. K.** (2012). A (very) brief refresher on the case study method. *Applications of case study research*, 3-20.
- Yin, R. K.** (2013). *Case study research: Design and methods*. Sage publications.
- Yin, R. K.** (2003). *Case study research: Design and methods*, 3 edn. Applied Social Research method series, vol. 5.
- Yolles, M.** (2001). Viable boundary critique. *Journal of the Operational Research Society*, 35-47.
- Zhang, S., & Le F. H.** (2013). An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model. *Journal of Economics*, 1, 5.
- Zororo T.** (2014). IT Governance Assurance and Consulting: A Compelling Need for Today's IT Auditors, the EDP Audit, Control, And Security (EDPACS) Newsletter, VOL. 49, No. 6.

APPENDIX A – Survey Instrument



DEPARTMENT OF INFORMATION SYSTEMS

INTRODUCTION

This research has been approved by the Commerce Faculty Ethics in Research Committee of the University of Cape Town, South Africa. The goal of this questionnaire is to solicit your opinion on how you perceive the efficacy of the underlying concepts and relationships of an innovative framework for Information Systems (IS) auditing based on the viable systems model in less regulatory environments. Your responses are deemed to be your fair assessment of the framework. The aim of the responses in this questionnaire is to assist the researcher confirm or reject certain hypotheses.

This questionnaire will take at about 10 minutes to complete and to return to the administrator directly. Since this questionnaire requests your perception based on your professional experience and assessment of the viable systems framework for auditing which has been introduced to you through our interaction in a workshop, there is no true or false answer. You are also assured that questionnaire seeks to obtain your private organizational or personal data, and neither will your responses be shared. Thus, confidentiality of your responses is guaranteed. Your participation in this research is, however, voluntary and you may choose to withdraw.

<p><i>Please indicate your level of agreement or disagreement with each of the following statements regarding the viable systems framework for IT auditing and assurance by circling your choice in the scale. Only one choice required in each question.</i></p>		<p>Questionnaire Scale: 1=Strongly Disagree; 2=Disagree; 3=Somewhat Agree 4=Agree 5=Strongly Agree</p>				
Questions						
Code No.	Section A – Collects data on efficiency of the prescribed framework					
F1	Diagnostic IT auditing procedures should start by evaluating the core business processes to understand operational risks and the local control environments.	1	2	3	4	5
F2	There should be a separate IT audit procedure for coordination which identifies weak links within the process control environments with recommended IT responses.	1	2	3	4	5
F3	Fraud risk investigation and control in less regulatory environments should involve continuous concerted feedforward IT audit process and not a one-off yearly event.	1	2	3	4	5
F4	There should be a procedure for intelligence auditing which sufficiently addresses internal and external corporate pain points matching them to their associated opportunities from the total environment.	1	2	3	4	5

F5	An effective framework of IT auditing should have a separate procedural requirement to evaluate IT strategies and executive policy to achieve organizational goals.	1	2	3	4	5
V1	An effective IT auditing is one that rigidly complies with strict audit standards for auditing business units that act on their own within the organization to effectively determine their purpose in the total system.	1	2	3	4	5
V2	An adaptive framework for IT auditing should have a term for a broad class of flexible learning and responses for different organizational contexts.	1	2	3	4	5
V3	A viable framework for IT auditing must espouse identifiable set of recommended procedures while keeping options as open as possible for different organizational contexts.	1	2	3	4	5
V4	A resilient IT audit framework is one with the capacity to support non-mandatory adoption of best practices to maintain its functions and controls.	1	2	3	4	5
V5	IT audit planning and execution for less regulatory environments should be couched in systematic procedures that reflect organizational architecture.	1	2	3	4	5
C1	A viable systems-based IS audit framework should guide practitioners by providing critical prompts to address a broad range of issues in every organizational context.	1	2	3	4	5
C2	To effectively participate in the fight against fraud and corruption IT audit should move away from reactivity to events to proactive approach.	1	2	3	4	5
C3	A framework for IT auditing must be embedded with the quality that supports quick changes that allow for capacity building, learning and knowledge management systems.	1	2	3	4	5
C4	An IT audit framework should be driven by value delivered through continuous assessment with short communication cycles.	1	2	3	4	5
S1	Since complexity destroys complexity, audit of the future demands expanded scope of risk assessment based on continuous learning to stand up to the increasing sophistication of business.	1	2	3	4	5
S2	Audit of the operational environments is relevant if it involves the assessment and determination of the match between management strengths and capabilities on one side and the environmental forces that pose threat and increase their vulnerabilities on the other.	1	2	3	4	5
E1	There is currently weak match between the complexity in the business horizon and Internal and IT auditors' capacity to support innovative actions that allow the organizational system to deal with environmental vagaries.	1	2	3	4	5

E2	The current approach to IT auditing is saddled with weak capacity to address current internal and external threats and the opportunities of the future environments with reasonable certainty because the framework used does not support it.	1	2	3	4	5
M1	Brisk communication of audit output enabled by an IT audit framework would greatly minimize transparency challenges and improve stakeholder confidence.	1	2	3	4	5
M2	Timely audit data translation and communication between audit practitioners and stakeholders of audit output is key to survivability of the auditee and viability of the audit practice.	1	2	3	4	5
Section B - Demographic Profile - Optional						
B1	What is your current highest level of Education?	HND	1 st Degree	Professional	Masters	PhD
B2	What is your field of education/professional background?	Auditing	Management	Accounting	IT	Other
B3	What is your role in your organization?	Student/trainee	Auditor	Manager	Director	Other
B4	How long is your experience in the above role?	≤1 yr.	≤2 yrs.	≤ 5 yrs.	≥ 5 yrs.	Other

Thank you for participating in this research.

APPENDIX – B

2.1 Ethics Approval Letter



Faculty of Commerce

Private Bag X3, Rondebosch, 7701
2.26 Leslie Commerce Building, Upper Campus
Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369
E-mail: com-faculty@uct.ac.za
Internet: www.uct.ac.za

 @Commerce_UCT  UCT Commerce Faculty Office

25 August 2017

Mr Sampson Anomah
Department of Information Systems
University of Cape Town

REF: REC2017/08/010

Dear Mr Anomah

Project: Modeling a Systems-Based Framework for IS Auditing and Assurance for Less Regulatory Environments.

Thank you for submitting your study to the Faculty of Commerce Ethics in Research Committee.

It is a pleasure to inform you that the EIRC has **formally approved** the above-mentioned study.

Approval is granted for the period of 12 months. Should you require an extension or make any substantial changes to the research methodology which could affect the experiences of participants, you must submit a revised protocol to the Committee for approval.

Please note that the ongoing ethical conduct of the study remains the responsibility of the principal investigator.

Your sincerely

SAMANTHA ALEXANDER
Administrative Assistant
University of Cape Town
Commerce Faculty Office
Room 2.24 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695
Office Fax: +27 (0)21 650 4369
E-mail: samantha.alexander@uct.ac.za
Website: www.commerce.uct.ac.za

“Our Mission is to be an outstanding teaching and research university, educating for life and addressing the challenges facing our society.”

2.2 Ghana Audit Service

AUDIT SERVICE

In case of reply the
number and date of the
letter should be quoted

My Ref. No: AR/ADM.40^A/139

Your Ref. No:

Tel: 233 (0) 302 664920/28/29

Fax: 233 (0) 302 6751495

Website: www.ghaudit.org



P. O. Box 407
Kumasi
25 April 20 17

Mr. Sampson Anomah
Dept of AAIS
Kumasi Technical University
Kumasi

PERMISSION TO CONDUCT DATA COLLECTION

I refer to your letter on the above subject and write permitting you to use the Audit Service, Kumasi for the test data collection.

Thank you.

SULLEY SAAKA
ASSISTANT AUDITOR-GENERAL
REGIONAL AUDITOR, ASHANTI REGION

2.3 Kumasi Technical University

KUMASI TECHNICAL UNIVERSITY

Vice Chancellor:

Telephone No.: 0322022387/0322022388

Fax: 0322022387

Residence: 0322028068

Our Ref: KsTU/ADM/PS.509

Your Ref:.....



P. O. Box 854
Kumasi, Ashanti
Ghana Africa

20th April, 2017

**MR. SAMPSON ANOMAH
AAIS
KUMASI TECHNICAL UNIVERSITY
KUMASI**

Dear Sir

RE: APPLICATION FOR PERMISSION TO CONDUCT DATA COLLECTION

We write to acknowledge receipt of your letter dated 13th April, 2017 regarding your request to conduct data collection from the University.

Approval has been given to enable you collect the data for your research work.

Thank you.

Yours faithfully

**FLORENCE E. AFLAKPUI (MRS.)
SNR. ASSISTANT REGISTRAR - HRD
FOR: AG. REGISTRAR**

2.4 Sekyedumase Rural Bank Limited



SEKYEDUMASE RURAL BANK LIMITED

Head Office: P. O. Box 21, Sekyedumasi - Ashanti, Ghana. Tel: 0501286178

Our Ref:.....

13 April 2017

Your Ref:.....

.....20.....

TO WHOM IT MAY CONCERN

I can confirm that Mr. Sampson Anomah, a Ph.D. candidate of the University of Cape Town, South Africa, has contacted our Bank to engage in data collection exercise for his research programme in Information Systems Auditing and Assurance.

We have no problem in assisting him obtain the data in the method he has already outlined to us for the collection of his data any time he is prepared to commence it.

Thank you.

Faithfully yours,

SEKYEDUMASE RURAL BANK LTD

Emmanuel D. Kuffour
EMMANUEL D. KUFFOUR

(GENERAL MANAGER)

AGENCIES: Ejura - 0501286162 Aboabo Ksi - 0501286163 Anloga Ksi - 0501286164 Anyano - 0501286165
Seko - 0501286161 Tafo Ksi - 0501286166 Kenyase - 0501286167

2.5. Sunshade Foundation



Sun Shade Foundation-FNGO

(A Non-Governmental Organisation)

Bankers:
Prudential Bank, Cocobod
Fidelity Bank, Stadium
The Royal Bank, Ash Town
National Investment Bank, Adum

P. O. Box AN 23160,
Ash Town-Kumasi
Tel.: 03320 26397 / 020 2028875 / 020 4212823
e-mail: info@mysunshade.org

To whom it may concern,

University of Cape Town,
South Africa.

13 April 2017

Dear Sir /Madam,

LETTER OF INTRODUCTION

(RE: SAMSON ANOMAH)

The above-mentioned Ph.D. candidate of the University of Cape Town has approached our institution to conduct his data collection in his research in Information Systems Auditing and Assurance.

He has indicated he will have a workshop with our internal audit staff and management team in which he intends to introduce his viable systems auditing framework after which he will administer questionnaire to solicit our views on the framework.

We would like to assure you that we are in the position to assist Mr Sampson Anomah whenever our co-operation is needed to ensure a successful research programme.

Thank you.

Yours faithfully,

Isaac K. Akohene -Asiedu,
(Executive Director),
Sun Shade Foundation -FNGO
Tel: +233 03220 26397;
Mobile: 026 347 3170 / 020 440 6148
Alternative Email: ikeasiedu@yahoo.com;
Website: www.mysunshadef.org

EXECUTIVE DIRECTOR
SUN SHADE FOUNDATION
P. O. BOX AN 23160
ASH-TOWN, KUMASI

Providing Financial Support and Business Advisory/Consultancy Services to Women Groups and Small Business Owners
Sun Shade Foundation (SSF).....Place of Possibilities