

THE USAGE OF INFORMATION SYSTEMS, FACTORS AFFECTING THE USAGE AND ITS IMPACT ON FINANCIAL AUDIT PROCESS AND ON E-FRAUD DETECTION

THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

By

Asha Baleche Katamba

OCTOBER 2018

DECLARATION OF ORIGINAL AUTHORSHIP

I declare that the work contained in this thesis has not been previously submitted for any degree or diploma at the University of Nottingham Malaysia Campus or any other higher education institution within or outside Malaysia. To the best of my knowledge and belief, the thesis contains no material previously published or written by another scholar except where due reference is made.

Signed:……..…

Name: Asha Baleche Katamba

Student No.016463

School: University of Nottingham Business School

Date:……

ABSTRACT

This study is driven by the motive to understand the usage of IS by external auditors amid their clients' move into e-business platforms in processing and storing information. It is reported that the e-business models have improved business availability, accessibility, cost and time, but have also increased complexities, chances for fraud, errors, theft, damages and other irregularities. Specifically, electronic-based transaction fraud can easily be committed by internal or external system experts and might stay for a long time undetected, hence increasing the chances for audit risk. On the contrary, there are IS tools that can help auditors to examine clients' financial information where it is difficult to do so manually and also to detect fraud. It will therefore be critical and essential to understand the extent of use of IS by external auditors when auditing their computerised clients. Most studies in this area have either focused on internal auditors or in developed countries making external auditors and emerging markets especially those in Africa to be unrepresented. Yet, advances in technology are spreading across the African countries; and audit firms in these countries are anticipated to utilise technology for various productivities. For Tanzania, this will be the first study to investigate the extent of use of IS among external auditors as e-business is gaining momentum in the country and also electronic-based fraud were reported on the rise. With that, the study explored the extent of IS usage among external auditors, factors influencing the usage of IS and the impact of IS usage on the audit process and on e-fraud detection. A concurrent mixed method approach was espoused where interview was the main enquiry tool and surveys a secondary enquiry. The unified theory of acceptance and use of technology (UTAUT) was adopted and modified with inclusion of external factors to understand the factors for IS usage among external auditors. Data were collected in two phases. In the first phase, the study interviewed 13 external auditors at management level from audit firms that were allowed to audit banks and financial institutions. In the second phase, questionnaires were sent out with an intention to obtain a larger sample in understanding the motivation for IS usage and to complement the interview findings. SPSS and NVIVO were used to analyse the data from surveys and interviews respectively. The interview data were analysed in themes while the survey data were analysed in demographics, percentages, frequencies, means, standard deviations and inferential statistics such as EFA and regression. The findings revealed that external auditors in Tanzania make use of office automation technologies (Word Processing, Excel; Electronic working papers), audit automation technologies (ACL, IDEA, GAM-X, PCAS, Auto-Audit, SASoft, AS2; Excel), Networking and data transfer (Teammate, EMS, E-mails; work related-messengers) and Ecommerce technologies/Intruders detection technologies (Ethical hacking

tools). On the factors for IS usage, the interview findings showed that external factors were the strongest drivers that inspired auditors to increase the use of IS namely; clients' related factors and the audit oversight body. Meanwhile, the survey results also showed that clients' factor was the most significant predictor that influenced auditors to increase the use of IS and efforts expectancy. Furthermore, the findings revealed that IS had improved the audit process from documentation, audit testing and reporting as it enhanced auditors to adhere to audit standards and in assessing risks better than manual processes. Lastly, IS tools enabled auditors to detect e-fraud that occurred electronically. The use of ethical hacking tools through penetration testing was one of the techniques that auditors employed by detecting unauthorised access to the entity's system. As a result, it increased detection rate, deterred new fraud from occurring and reduced financial statement frauds. The types of e-fraud that were discovered using IS tools include IT related faults, illegal access to the entity's system by a terminated senior employee, stealing passwords, opening fake accounts and transferring cash therein, transferring cash in small denominations from multiple customers, mobile banking sim-swap fraud and fake hotel bookings among others. The findings of the study open an understanding on the impact of IS usage among external auditors in Tanzania, which has useful insights for developing countries, accounting professionals, software developers, investors, accounting oversight bodies and scholars. The study is expected to foster IS usage in auditing so as to increase the level of audit assurance in computing-business-platforms.

PUBLICATIONS

1. Asha Baleche Katamba, Angelina Yee Seow Voon, How Shi Min, Hsin Vonn Seow, (2017) Information Systems Utilisation by External Auditors in Tanzania; *Review of Integrative Business and Economics Research*, Vol. 6 (4) pp.377-388. ISSN: 2304-1013

2. Asha Baleche Katamba, Angelina Yee Seow Voon, How Shi Min, Hsin Vonn Seow, (2017) The Impact of Information Systems on Financial Audit: An over View of External Auditors' Preparedness to Tackle Clients Automated Environment, *Advanced science letters;* Vol. 23 (11), pp. 10692-10695. DOI: /10.1166/asl.2017.10132

CONFERENCE PROCEEDINGS

1. Asha Baleche Katamba, Angelina Yee Seow Voon, How Shi Min, Hsin Vonn Seow, (2017) Information Systems Utilisation by External Auditors in Tanzania, 2nd Iternational conference on information in business and technology management (I2BM), Georgetown, Penang, Malaysia. 18th - 20th April 2017.

2. Asha Baleche Katamba, Angelina Yee Seow Voon, How Shi Min, Hsin Vonn Seow, (2017) The Impact of Information Systems on Financial Audit: An Over View of External Auditors' Preparedness to Tackle Clients Automated Environment,in International conference on social and inter-disciplinary business research (SIBR) Bangkok, Thailand. 25th -26th May 2017.

ACKNOWLEDGEMENT

I express my sincere gratitude to my supervisor Dr. Angelina Yee Seow Voon, who introduced me to see a new perspective of auditing and guided me through my PhD process. Her constructive comments, encouragement and great support are thoroughly appreciated; including tutorial guidance on how to use NVivo software which simplified a lot the analysis of qualitative data. I am also grateful to my co-supervisors, Dr. How Shi Min and Hsin-Vonn Seow for their tireless guidance, reading my work and providing comments during the supervision period. Their invaluable help and suggestions are paramount in this thesis.

I am truly thankful to the internal assessment committee at Nottingham University Business School (NUBS) especially Dr. Lau Chee Kwong for his hard comments, criticisms and feedbacks on my annual progress reports that helped immensely to improve my thesis. I am also thankful to Mama Laurencia Ndali of National Board of Accountants and Auditors (NBAA), Mr. Focus Lutinhwa, Mrs. Safina Ulotu and Catherine Uliwa for their time and efforts to introduce me to different respondents during data collection; without their help, the process of data collection would be impossible. I am also grateful to my PhD colleagues especially Dr. Eliasu Mumuni, Dr. Fadila Puteh, Aloyce Kundy, Chin Chin, Dilnaz Bibi and Nguyen Tan for sharing knowledge, discussions and many supports whenever I needed them.

I would like also to extend my appreciation to all my respondents anonymously for accepting to be interviewed and to fill in the survey questions. This thesis would not be completed without their inputs and participation. Without forgetting Ms Indrani Pillay who edited my thesis, her comments on my work helped greatly to improve on grammatical errors and flow of sentences.

Lastly, I thank my husband Adam Katamba and daughters Sukaina and Shihaam for their love, support, understanding and patience during the long period of my absence. Allah the Almighty may bless you all.

TABLE OF CONTENTS

DECLARATION OF ORIGINAL AUTHORSHIP ..... **I**
ABSTRACT ..... **II**
PUBLICATIONS ..... **IV**
CONFERENCE PROCEEDINGS ..... **V**
ACKNOWLEDGEMENT ..... **VI**
TABLE OF CONTENTS ..... **VII**
LIST OF TABLES ..... **XII**
LIST OF FIGURES ..... **XIV**
LIST OF APPENDICES ..... **XV**
LIST OF ABBREVIATIONS ..... **XVI**
CHAPTER 1 ..... **1**
INTRODUCTION **1**
1.1 Background of the Study 1
1.2 Research Gap and Justification of the Study 7
1.3 Main Aim of the Study 10
1.3.1 Specific Research Objectives 10
1.3.2 Specific Research Questions 10
1.4 The Conceptual Framework of the Study and the UTAUT 11
1.5 The Adopted Research Methodology 11
1.6 Significance of the Study 12
1.7 Organisation of Thesis 13
1.8 Definition of the Main Terms 15
1.8.1 Information Systems (IS) 15
1.8.2 External Auditor 15
1.8.3 Electronic Based Fraud (E-fraud) 15
1.8.4 E-fraud Detection 16
CHAPTER 2 ..... **17**
LITERATURE REVIEW **17**
2.1 Introduction 17
2.2 Financial Audit in Perspectives 17
2.3 The Evolving Audit Objectives: From Ticking to Clicking 18
2.3.1 Auditing of Bookkeeping 19
2.3.2 Audit Evidence and Internal Controls 19
2.3.3 Computerised Auditing 20
2.4 Information Systems in Perspective 22
2.5 Impact of Information Systems on Financial Audit 24
2.6 Relevant Technologies for Audit Purposes 26
2.7 Factors Influencing the Usage of IS in Auditing 28

2.8 Utilisation of IS and its Impact on the Audit Process....32
2.9 E-fraud and the Use of IS Tools for Fraud Detection....35
2.9.1 Fraud Classification....37
2.9.2 E-fraud....39
2.9.3 Modes of Committing E-Fraud....43
2.9.4 The Role of Auditors in Relation to Fraud Detection....47
2.9.5 Is Identifying E-fraud the Role of Auditors?....50
2.10 Various Techniques and their Impact on E-fraud Detection....53
2.10.1 The Fraud Triangle....54
2.10.2 Chances, Tips and Internal Control Mechanisms....55
2.10.3 Continuous Auditing (CA)....57
2.10.4 Data Mining Techniques....58
2.10.5 Forensic Audit....62
2.11 The Adoption of IS tools in Auditing in Developing Countries....64
2.12 Summary of the Chapter....71

CHAPTER 3....72

THEORETICAL FRAMEWORKS UNDERPINNING THE STUDY....72

3.1 Introduction....72
3.2 Theory of Reasoned Action (TRA)....72
3.3 Diffusion of Innovation (DOI)....73
3.4 Technology-Organisation- Environment (TOE) Model....75
3.5 Technology Acceptance Model (TAM)....76
3.6 Information Technology Audit Quality (ITAQ) Model....79
3.7 Towards a Proposed Theoretical Framework for the Study....80
3.8 Unified Theory of Acceptance and Use of technology (UTAUT)....82
3.9 Hypothesis Development and Proposed Theoretical Model....87
3.9.1 Performance Expectancy....88
3.9.2 Efforts Expectancy....89
3.9.3 Social and Organisational Influence....90
3.9.4 Facilitating Condition....91
3.9.5 Clients' Factor....93
3.9.6 Audit Professional Factor....94
3.9.7 Moderator: Voluntariness....95
3.9.8 Other Moderating Variables (Age, Gender and Experience)....95
3.10 Linking the Conceptual Framework with the Research Problem....97
3.11 Summary of the Chapter....100

CHAPTER 4....101

A CASE STUDY OF TANZANIA....101

4.1 Introduction....101
4.2 Demographic Features of Tanzania....101
4.3 Economic Reforms in Tanzania....102
4.4 The State of ICT in Tanzania....103
4.4.1 E-government....105
4.4.2 E-Learning....105
4.4.3 E-Business....106

4.5 The Tanzanian Financial Sector..... 106
4.6 Mobile Banking Risks in Tanzania..... 108
4.7 Regulatory Authorities in the Financial Sector in Tanzania..... 110
4.8 The Accounting Regulation and External Audit Environment in Tanzania..... 111
4.8.1 Audit Firms in Tanzania..... 112
4.9 Summary of the Chapter..... 114
CHAPTER 5..... 115
RESEARCH METHODOLOGY..... 115
5.1 Introduction..... 115
5.2 Research Design: The Mixed method Approach..... 115
5.3 Research Scope..... 119
5.4 Population and Sample..... 120
5.5 Sampling Procedures..... 122
5.6 Data Collection..... 127
5.7 Qualitative Data Collection..... 128
5.7.1 Interview Protocol..... 130
5.7.2 Piloting the Interview Questions..... 133
5.7.3 Practising Brackets..... 135
5.8 Qualitative Data Triangulation..... 136
5.9 Transferability, Validity and Reliability..... 137
5.10 Quantitative Data Collection..... 139
5.10.1 Piloting the Questionnaire..... 141
5.10.2 Research Variables..... 143
5.10.3 Data Measurements..... 145
5.11 Data Analysis..... 146
5.11.1 Qualitative Data Analysis-Thematic Analysis..... 147
5.11.2 Quantitative Data Analysis..... 150
5.12 Should Hypotheses/Propositions be Used to Predict the Outcome?..... 153
5.13 Questionnaire Development..... 154
5.13.1 Organisational Profile..... 154
5.13.2 Date of Establishment..... 154
5.13.3 Demographic characteristics of Auditor..... 156
5.13.4 Response Rate of the Questionnaire..... 158
5.14 The Value of Mixed method Research: a Message for Future Researchers..... 160
5.15 Summary of the Chapter..... 162
CHAPTER 6..... 163
QUALITATIVE FINDINGS..... 163
6.1 Introduction..... 163
6.2 What is the Extent of IS Usage by External Auditors in Tanzania?..... 163
6.2.1 The Choice of Audit Software..... 168
6.2.2 Ethical Hacking..... 170
6.2.3 Discussion on the IS Usage..... 171
6.3 What Factors influence the Usage of IS by External Auditors in Tanzania?..... 175
6.3.1 External Factors..... 176
6.3.2 Internal Factors..... 188

6.3.3 Discussion on the Factors for IS Usage 194
6.4 What is the Impact of IS on Financial Audit Process? 195
6.4.1 Planning and Audit Team Composition 196
6.4.2 Documentation of Audit Work 196
6.4.3 Audit Testing 197
6.4.4 Execution of the Audit 198
6.4.5 Communication and Information Sharing 199
6.4.6 Report Writing 200
6.4.7 IT Consulting Services 200
6.4.8 Discussion on Impact of IS on Audit Process 200
6.5 How do Auditors Detect E-fraud? 201
6.5.1 Understanding the Client's Business/IT Environment 202
6.5.2 Risk-Based Audit and Professional Scepticism 202
6.5.3 Adjusting Audit Methodology 205
6.5.4 The Use of Forensic Expert 205
6.5.5 The Use of Penetration Testing 206
6.5.6 Discussion on E-fraud Detection Procedures 206
6.6 What is the Impact of IS on E-fraud Detection? 207
6.6.1 Increased Fraud Detection 207
6.6.2 Reduction in Financial Statements Fraud (FSF) 208
6.6.3 Types of E-fraud Detected 209
6.6.4 Discussion on Impact of IS on E-fraud Detection 214
6.7 Summary of the Chapter 217

CHAPTER 7 219

QUANTITATIVE FINDINGS 219

7.1 Introduction 219
7.2 Demographic Features of Participated Firms and Respondents 219
7.3 The Usage of IS 222
7.4 Factors Influencing the Usage of IS 225
7.4.1 Data Screening 225
7.4.2 Checking for Parametric Assumptions 226
7.4.3 Exploratory Factor Analysis (EFA) 229
7.4.4 Reliability of Measured Scales 232
7.4.5 Multi-Collinearity Test 233
7.4.6 Multiple Regression 234
7.5 Results and Interpretation 238
7.5.1 The Co-efficient of Determination (R^2) and F- Statistics 238
7.5.2 Performance Expectancy (PE) 238
7.5.3 Efforts Expectancy (EE) 239
7.5.4 Social and Organisational Influence (SOI) 239
7.5.5 Facilitating Condition 240
7.5.6 Clients' Factor (CF) 241
7.5.7 Audit Professional Factor (APF) 241
7.5.8 Hierarchical Regression on Demographic Factors 242
7.5.9 Moderating Variable: Voluntariness 242
7.6 Summary of the Chapter 243

CHAPTER 8..... 244

DISCUSSION, RECOMMENDATION AND CONCLUSION..... 244

8.1 Introduction..... 244
8.2 Summary of the Key Findings..... 245
8.3 Discussion of the Findings..... 249
8.3.1 The extent of IS Usage by External Auditors in Tanzania..... 250
8.3.2 Factors Influencing the Use of IS by External Auditors in Tanzania..... 252
8.3.3 The Impact of IS on Financial Audit Process..... 257
8.3.4 The Impact of IS on E-fraud Detection..... 258
8.4 Limitations of the Study..... 260
8.5 Recommendations for Future Research..... 261
8.6 Conclusion..... 262
8.7 Contribution of the Study..... 265

REFERENCES..... 268

LIST OF TABLES

Table 2.1 IS Tools That Aid Auditors in Performing Audit Tasks....27
Table 2.2 Frauds statistics in the UK for a period of 20 years from 1987- 2007.... 41
Table 2.3 Fraud in Computing Environment....44
Table 2.4 E-fraud that were Reported in Kenya....46
Table 2.5 Software that Can Assist Auditors to Perform Different Functions.... 64
Table 3.1 Number of Citations in the Use of Models of Technology Adoption in Business and Management.... 78
Table 3.2 A summary of technology theories used in auditing....80
Table 3.3 UTAUT Elements.... 82
Table 4.1 Penetration of ICT in Tanzania....104
Table 4.2 Bands in Promotion for Auditors.... 112
Table 5.1 Summarised Concurrent Mixed method Strategies.... 117
Table 5.2 Scope, Population and Sample of the Study....122
Table 5.3 Active Professional Memberships Registered by NBAA....126
Table 5.4 Defining Sample Size and Population....127
Table 5.5 Reliability Tests for the Pilot Study.... 142
Table 5.6 Profiles of Interviewed Respondents....149
Table 5.7 Summary of Research Objectives, Variables, Data Measurement and Data Analysis of the Study.... 152
Table 5.8 Table 5.8 Structure of the Questionnaire.... 156
Table 5.9 Breakdown of Survey Response Rate.... 158
Table 5.10 Missing Data in the Questionnaire.... 159
Table 5.11 Response According to Seniority.... 159
Table 6.1 Types of IS Tools Used by External Auditors in Tanzania....164
Table 6.2 Factors of using IS by external auditors in Tanzania....176
Table 7.1 Profile of the Participated Audit Firms....219
Table 7.2 Summary of the Respondents' Profile....221
Table 7.3 IS Usage and Voluntariness....223
Table 7.4 Number of Years since Adoption of IS Tool....223

Table 7.5 Types of Software Used by External Auditors.....224
Table 7.6 Benefits of IS Usage.....225
Table 7.7 Residue Statistics.....228
Table 7.8 Normality Tests.....229
Table 7.9 Exploratory Factor Analysis.....230
Table 7.10 Regrouped-Exploratory Factor Analysis.....231
Table 7.11 KMO and Bartlett's Test.....232
Table 7.12 Reliability Test.....233
Table 7.13 Correlations (r).....234
Table 7.14 Model Summary[b].....235
Table 7.15 ANOVA[a].....236
Table 7.16 Coefficients[a].....237
Table 8.1 Summary of the Key Findings.....248

LIST OF FIGURES

Figure 2.1 Fraud Classification..... 38
Figure 3.1 Technology Adoption Stages.....74
Figure 3.2 The Original TAM Model.....77
Figure 3.3 The Original UTAUT Model.....83
Figure 3.4 Modified UTAUT- A..... 84
Figure 3.5 Modified UTAUT-B.....85
Figure 3.6 Modified UTAUT -C..... 86
Figure 3.7 Proposed Conceptual Framework of the Study..... 97
Figure 4.1 Mobile Banking Frauds in Tanzania.....109
Figure 5.1 Concurrent Embedded Mixed Method Design..... 118
Figure 5.2 Schematic Relationship between IV and DV..... 144
Figure 5.3 A Schematic Relationship between IV, MV and DV..... 145
Figure 6.1 Thematic Coding on Types of IS Tools.....175
Figure 6.2 Thematic Coding on Factors Influencing IS Usage by External Auditors..... 195
Figure 6.3 Thematic Coding on Impact of IS on Financial Audit Process..... 201
Figure 6.4: Thematic coding on how auditors detected e-fraud.....207
Figure 6.5: Thematic Coding on Impact of IS on E-fraud Detection.....217

LIST OF APPENDICES

Appendix I: Summary of Theoretical Review of the Literature..... 292

Appendix II: Relevant Technology in Auditing.....296

Appendix III: Various E-fraud Detected through Data Mining Techniques..... 298

Appendix IV Questionnaire..... 299

Appendix V: Interview Guide..... 304

Appendix VI: Normality Tests..... 305

Appendix VII: Total Variance Explained.....306

Appendix VIII KMO, Bartletts Test and Total Variance Explained for Individual Variables..... 307

Appendix IX Hierarchical Regression..... 310

Appendix X A Summary of Nodes Generated by Nvivo Software (Thematic Coding).....313

Appendix XI Research Ethics Approval Issued by REC at NUBS, the University of Nottingham Malaysia Campus.....315

Appendix XII: An Approval Letter to Conduct the Research Issued by NUBS, the University of Nottingham Malaysia Campus..... 316

LIST OF ABBREVIATIONS

AAT	Audit Automation Technologies
ACCA	Association of Certified Chartered Accountants
ACL	Audit Command Language
AICPA	American Institute of Chartered Accountants
AMF	Assets Misappropriation Fraud
APB	Auditing Practices Board
APF	Audit Profession Factor
ATEC	Accounting Technician Certificate
ATM	Automatic Teller Machine
BBA	Bachelor of Business Administration
BBN	Bayesian Belief Network
BCom	Bachelor of Commerce
BFIA	Banking Financial Institution Act
BI	Behavioural Intention
BOT	Bank of Tanzania
BSc	Bachelor of Science
CA	Continuous Auditing
CAATTs	Computer Assisted Audit Tools and Techniques
CF	Clients' Factor
CFE	Certified Fraud Examiner
CISA	Certified Information Systems Auditor
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPA	Certified Public Accountants
CPA (K)	Certified Public Accountants from Kenyan accounting professional board
CPA (T)	Certified Public Accountants from Tanzanian accounting professional board
CPBC	Commercial and Private banking certificate
CPM	Certificate in Procurement Management
CPSP	Certified Procurement and Supply Professional of Kenya (CPSP-K)
DCG	Directed Compounded Graph
DSE	Dar es Salaam Stock Exchange
DV	Dependent Variable
EAC	East African Community
ECT	E-commerce Technologies
EE	Efforts Expectancy
EFD	Electronic Fiscal Device
ESS	Estimated Sum of Square
FC	Facilitating Condition
FSF	Financial Statements Fraud
FSs	Financial Statements
GAS	Generalised Audit Software
GASI	Generalised Audit Software over the Internet
GDP	Gross Domestic Products
GDT	General Deterrence Theory
IAA	Institute of Internal Auditors
ICT	Information Communication and Technology
IDEA	Interactive Data Extraction and Analysis
IDT	Intruders Detection Technologies
IES	International Education Standard
IFAC	International Federation for Accountants

IMF	International Monetary Fund
IFRS	International Financial Reporting Standards
IS	Information Systems
ISA	International Standards on Auditing
ISACA	Information Systems Audit and Control Association
IT	Information technology
IT & T	Information Technology and Telecommunications
ITAQ	Information Technology Audit Quality
IV	Independent Variable
MBA	Master of Business Administration
MPRS	Multistage-Purposive Random Sampling
NADTT	Networking and Data Transfer Technologies
NBAA	National Board of Accountants Auditors
NN	Neural Network
NUBS	Nottingham University Business School
OAT	Office Automated Technologies
OLS	Ordinary Least Square
PAS	Proprietary Audit Software
PGDA	Postgraduate Diploma in Accounting
PE	Performance Expectancy
PEOU	Perceived Ease of Use
PwC	PricewaterhouseCoopers
RO	Research Objective
ROSC	Report on Standards and Codes
RQ	Research Question
SADC	South African Development Community
SAS	Statement of Auditing Standards
SASoft	Specialised Audit Software
SEC	Security and Exchange Commissions
SEE	Standardised Error of Estimates
SME	Small and Medium Enterprises
SOI	Social and Organisational Influence
TAM	Technology Acceptance Model
TCRA	Tanzania Communication and Regulatory Authority
TOE	Technology, Organisation and Environment
TPB	Theory of Planned Behaviour
TPSF	Tanzania Private Sector Foundation
TRA	Theory of Reasoned Action
UK	United Kingdom
UNMC	University of Nottingham Malaysia Campus
US	United States
UTAUT	Unified Theory of Acceptance and Use of Technology

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

The world has increasingly embraced technological innovations that have led into society's migration from manual practices to digital-based products and services. Governments are moving into e-governments, institutions into e-learning and traditional business practices into e-business, e-procurement and e-banking platforms. Specifically, in the area of business, technology has changed the way of effecting transactions, making payments, recording and storing information, which is reflected in the evolving e-business models. Business to business, business to consumers, business to business to consumers and consumers to consumers are some of the pure dot com models adopted by businesses (Kotb and Roberts, 2011). Even more, these models are opted to occur in cloud where an entity's data are stored in a shared pool managed by a third party in form of infrastructure, software or platform as a service (Lal and Bharadwaj, 2016).

These technological advancements and sophistication have improved business availability, accessibility, cost and time, at the same time have increased complexities, chances for fraud, errors, theft, damages and other irregularities (Simkin et al., 2015; Paula et al., 2016). It is reported that 75% of large corporations surveyed in 2013 by KPMG had experienced at least one fraud incidence in that year, a 13% upsurge compared to five years back when the same survey was done in 2008 (Sacks, 2014). Similarly, the average cost of cyberattacks per organisation in the US was estimated to be $11.6 million for 2013, 26% higher than in 2012 (Ponemon Institute, 2013). In the UK, cybercrime has become the most dominant fraud where half of the surveyed companies reported to have been victims of fraud. As a result, 24% of the victims lost more than $1 million (£720,000) in a period of two years (Brian, 2018). Meanwhile, a report by PwC (2014) found that electronic banking fraud globally was 57% while other sectors combined was only 16%. The report cited the intense fraud

targeting the financial sector where attackers reached the extent of installing computer chips into the systems of several retail banks and managing to commit frauds via mobile networks. Indeed, technology has widened the scope of risk particularly fraud to become complex and borderless (Simkin et al., 2015). It is posing a challenge to financial auditors as their clients are exposed to a variety of risks that keep on expanding from audit risk to business risk (Hunton et al., 2004; Simkin, 2015). Electronic fund transfers fraud, hacking, credit card fraud, insurance fraud, identity theft and accounting fraud are just a few reported risks in the computing business environment (Braun and Davis, 2003; Newman and Clarke, 2003; Alanezi and Brooks, 2014; Boyle et al., 2015).

In the Eastern part of the African continent where the Internet is a barrier, digital mobile devices are used extensively to effect financial transactions through mobile banking services (Rumanyika, 2015). Indeed, mobile banking has revolutionised the economies of the nations but it has also witnessed the mounting of mobile banking fraud in the region with millions of cash lost to digital fraudsters (Kigen et al., 2014, Masamila, 2014; Rumanyika, 2015; Paula et al., 2016). In Kenya for instance, where mobile banking is a dependable means of payments for more than 80% of the population, it has now turned into a conduit for fraudsters. Mobile banking fraud in Kenya increased by 25% in 2013 where attackers use loopholes in the IT systems to commit fraud (Kigen et al., 2014). In Uganda, the leading mobile money provider (MTN), lost an approximately US$3.4 million in cash through internal fraud organised by its staff (Morawczynski, 2015), while a related fraud incident cost TIGO in Rwanda about US$700,000 (Mugisha, 2014).

In Tanzania, which is the focus of this study, digital fraud in the mobile banking ecosystem was reported to be on the rise. Mobile banking fraud incidences increased from 265 cases in 2008 to 673 cases in 2013, a 39% upsurge compared to five years back (Lubua, 2014), with some single incident costing several million dollars in cash terms (Rumanyika, 2015). For instance, a report found that a total of 7 billion Tanzanian shillings (approximately $4.4 million) was tapped from numerous customers of Exim Bank due to collusions between employees and external IT hackers, making it one

of the largest ever cyber-bank robberies in Tanzania (Ihucha, 2014). As a result, banks must refund their customers, creating loses to investors and the economy. Furthermore, the government could be losing millions of tax revenue due to cash leakages under such complex digital-crimes if proper detection and deterrent mechanisms are not put in place (Alanezi et al., 2014; Paula et al., 2016). Hence, there is a need for intervention between various stakeholders in the issue of mobile banking fraud occurrences in Tanzania and specifically *"independent auditors are the first line of defence in the fight against fraud"* (Walker, 1999; in Porter et al., 2008; pp.143). Therefore, this study explored the extent of IS usage among external auditors in Tanzania and the techniques used to detect fraud in the digital business environment.

It is important to highlight that Tanzania stopped setting its own accounting/auditing standards fourteen (14) years ago. In 2004, the National Board of Accountants and Auditors (NBAA) which is the regulatory body for the accounting profession in Tanzania, in collaboration with the Ministry of Finance, Tanzania Chamber of Commerce Industry and Agriculture and World Bank representatives reached a decision to harmonise Tanzanian accounting/auditing standards to those of international (NBAA, 2006). A full convergence of standards was completed in 2006 where Tanzania adopted all the 41 International Accounting Standards (IASs), the newly-amended International Financial Reporting Standards (IFRSs), and International Standards of Auditing (ISAs) without amendments (World Bank, 2005; NBAA, 2006). Today, the NBAA depends totally on the International Federation for Accountants (IFAC) which is responsible for setting IASs, IFRSs and ISAs. Subsequently, all the listed companies on Dar es Salaam stock exchange (DSE) including small and medium enterprises (SMEs) are required to report their financial performance according to IFRSs. Therefore, the usage of IS by external auditors in Tanzania will be discussed with respect to IFAC standards and other major players in international accounting harmonisation especially the American Institute of Certified Public Accountants (AICPA) of the United States of America (US).

Even though the International Education Standard No.8 (IFAC, 2006) requires accounting professionals to be equipped with "IT systems for financial accounting and reporting", it does not make it mandatory for auditors or audit firms to adopt specific types of technology. This allowable voluntariness in technology usage raises questions as to what motivates external auditors to increase the use of IS (Curtis and Payne, 2014). This question has also been addressed in one of the research objectives.

Meanwhile, as the cost of fraud to businesses is growing hastily, the audit profession is getting concerned on the issue. In the recent amended ISAs, the role of the auditor has been widened by emphasising on assessment of risk of material misstatements due to fraud and included as one of the auditor's important responsibilities (Porter et al., 2008; Simkin et al., 2015). ISA 240.3 (IFAC, 2009a), considers two types of fraud that can result into material misstatements, namely (1) financial statements fraud (FSF) and (2) transactions fraud or assets misappropriation fraud (AMF). AMF which involves a misuse or stealing of the entity's assets for personal gain, characterises most electronic-based frauds as the culprits always target cash and cash equivalents which can easily be manipulated through digital technologies (Jans et al., 2009). Meanwhile, FSF which is a deliberate concealing of evidence in financial statements (FSs), can occur for various reasons such as management pressure to inflate earnings, portraying liquidity condition of an entity, raising equity capital (Lau and Ooi, 2016) or for personal motives (Jans et al., 2009). However, AMF might also result into FSF where the culprits are part of the management who prepared the reports and they want to conceal their acts within the FSs (ACFE, 2006). Hence, ISA 240 requires auditors to critically assess the possibilities for opportunities, incentives and rationalisation for individuals to commit fraud and other irregularities (IFAC, 2009a). The standard stands as a guide to both financial auditors and the company's management to take correct measures. However, the duty of fraud assessment and reporting to shareholder rests on the external auditors (Dyck and Zingales, 2010).

Similarly, the Public Company Accounting Oversight Board (PCAOB, 2007), issued Auditing Standard No. 5, the American Institute of Certified Public Accountant (AICPA) amended Statement of Auditing Standards (SAS) No.82 and issued SAS No.99; both emphasising on fraud during FSs audit (Senft and Gallegos, 2008). For example, in identifying risk and fraud in the computing platforms, SAS 316.52 indicates that the auditor needs *"to employ technological tools to gather more extensive evidence about data contained in significant accounts or electronic transaction files"* (AICPA, 2006). Likewise, ISA 300 (Ref: Para. 7–8, A8–A11), encourages the use of IS tools in a situation where audit judgement cannot be sufficient to guarantee assurance when testing controls and evidence in electronic business platforms (IFAC, 2009d). The efforts and concerns in these standards are consistent to prior scholars who contended that audit quality cannot be merely interpreted as compliance with the audit standards, but also compels the use of advanced audit technology for effective audit (Willborn, 1989; No and Vasarhelyi, 2017). However, there is scanty of research that investigated the extent of use of IS by external auditors and the techniques they use to detect fraud in computing business platforms.

In an effort to simplify audit procedures in the digital environment, system vendors have invented several IS mechanisms that align with the changing environment. These mechanisms are known as Computer-Assisted Audit Tools and Techniques (CAATTs). CAATTs were established to have various ability including simplifying audit procedures (Biestaker et al., 2001, Banker et al., 2002; Greenstein-Prosch et al., 2008), fraud detection and identifying unusual transactions (Janvrin et al., 2009; Ahmi and Kent 2013, Curtis and Payne, 2014). Concurrent Audit Tools, Integrated Test Facility and Embedded Audit Modules can assist auditors to control the entity's systems and transactions on real-time (Kotb and Roberts, 2011). The tools are meant to be used by both internal and external auditors (Kotb and Roberts, 2011; Ahmi and Kent, 2013). However, not enough of research has been done to examine the use of these tools by external auditors in developing countries while e-business is gaining its momentum.

It is imperative therefore, to discuss the concept of external auditors in much detail by highlighting their position as risk assurance providers in the digital age. External auditors are overseers of the activities of the company in all material matters including statutory and compliance of an entity's financial reporting (Porter et al., 2008). In ISA 315.60, '*Identifying and Assessing Risks of Material Misstatement through Understanding the Entity and its environment'* requires external auditors to understand the business environment of their clients in all aspects including the major line of their clients' business; their customers, suppliers, finances and most importantly the entity's IT environment (IFAC, 2009b). Similarly, ISA 200.7 requires auditors to "*practice professional scepticism*". Scepticism is an attitude that includes a questioning mind when auditing a client. The standard urges auditors to become more alert on possibilities of material misstatements in the FSs due to fraud, error and other irregularities (IFAC, 2009c). ISA 200.5 further requires auditors to have a critical assessment of audit evidence to assess any possibility of fraud or otherwise. The evidence surrounding computerised business environment needs the understanding of electronic-based controls and the use of IS tools and techniques to ensure effective risk assessment (Janvrin et al., 2009; No and Vasarhelyi, 2017).

To sum up, external auditors have a substantial part to play in the events of identifying fraud (whether online or offline) and reporting to the management and shareholders (Dyck and Zingales, 2010). The fact that they have access to internal and external information makes them proficient monitors better than the management and internal auditors. Therefore, the increasing fraud in computing business segments brings to mind the question of competence, skills, due care, independence and resources capabilities; and external auditors are superior in exercising these attributes (Alleyne and Howard, 2005). In fact, each stakeholder in business relies on the external auditor; and so, do the oversight bodies. This asserts the important position of external auditors in relation to their overall strategic duty of care bestowed on them as noted by Farrell and Franco (1999,

pp. 4) "*When fraud occurs within the company, the first question external stakeholders would ask will be where were the auditors?"*

1.2 Research Gap and Justification of the Study

As audit clients continue to integrate technology in processing and storing of information, auditing is expected to change from manual periodic detection to technology based, real time prevention (Alles et al., 2008, Janvrin et al., 2009; Ahmi and Kent, 2013). In other words, auditors must also adopt or intend to adopt new IS tools and techniques to ensure effectiveness in auditing. There is a significant contribution by researchers in this area of audit technology. Researchers have examined how auditors are making a move to embrace technology in other parts of the world. However, there are still a few gaps that this study has identified and intends to make contribution to the literature.

First, in studying the impact of IS (auditor's systems) in financial audit, it is important to understand whether auditors use any technology and what motivated them to use or limit the use of IS. Many studies that explored the usage of IS in auditing have focused on determinants that affect internal auditors' utilisation of IS (see Appendix I). Internal auditors being employees of the organisation that have already adopted technology (i.e. e-commerce), limits the understanding on the pace and perception of IS use in audit profession which is of interest to several stakeholders (Kotb et al., 2012). Omoteso et al. (2010) and Ahmi and Kent (2013) and contended that IS tools in auditing are meant to be used by both internal and external auditors for varied efficiency. However, the purpose of utilising IS among external auditors may be different from that of internal auditors. Internal audit is mostly focusing on operational activities within the organisation, while external audit focuses on compliance audit (Porters et al., 2008). Hence, different factors may influence them to adopt technology which subsequently affects the extent of their usage. Furthermore, external audit involves both an independent person as well as a firm that need to appreciate technology usage through internal and

external assessment (Bagranoff and Vendrzyk, 2000; Kotb et al., 2012; Ahmi and Kent, 2013). Hence, this study has based the enquiry on the experiences related to external auditors' utilisation of IS.

Second, prior scholars have focused their studies on understanding auditors' use of specific, unique or advanced categories of IS such as GAS or continuous auditing (CA) methodology (see Appendix-I). Such an investigation could be relevant to developed economies because they have reached a higher level in technology diffusion. However, for numerous other countries where little is known on whether auditors are using any technology, it needs a different approach to restructure the definition of IS (Melville et al., 2004). Hence, it may be reasonable to define IS as any computer application or software so as to allow investigation of all levels of IS usage (perhaps with GAS or CA) rather than focusing on a particular category of software. Therefore, this study has investigated all levels of IS from simple to high end technology application in order to understand a holistic nature of tools used and how it helps auditors to achieve audit objectives.

Third, the extent of usage of IS among external auditors in developing countries is still unclear. A few studies that explored IS usage in the external audit environment have focused on the developed world, for instance Portugal (Pedrosa et al., 2015), US (Janvrin et al., 2009; Curtis and Payne 2014), UK (Ahmi and Kent, 2013), Germany (Greenstein-Prosch et al., 2008) and Singapore (Debreceny et al., 2005). Henceforth, emerging markets particularly those in Africa are under researched in this area. Yet, the advances in technology is fast spreading across the African countries (Miah and Omar, 2012); and audit firms in these countries are anticipated to utilise technology for varied productivities; and for Tanzania this will be the first study to investigate the extent of usage of IS among external auditors.

Fourth, prior studies in audit technology have examined the level of IS adoption and factors of IS usage in developed countries. Even though these studies reported inconclusive findings, none explored the post-adoption impact of IS on the audit process and on e-fraud detection. In other words,

studies did not explore how auditors used technological tools to identify e-fraud which can be a cause of material misstatements. E-fraud may stay for a long term undetected, hence increasing the chances of audit risk (Cosserat, 2004). As a result, auditors may issue a clean report when in fact one or two items of fraud or error that are material to FSs were undetected. Since e-fraud occurs through interlinked digital devices, it is anticipated to be detected through the use of IS tools and techniques such as Interactive Data Extraction and Analysis (IDEA), Audit Command Language (ACL), WIZ Rule or other advanced web-based technologies (Mooney et al., 2000; Kotb and Roberts, 2011). Similarly, specific advanced applications and techniques such as data mining, CA or forensic audit can help auditors to identify fraudulent transactions in highly-digitalised environments (Kirkos et al., 2007; Jans et al., 2009; Omoteso et al., 2010; Ngai et al., 2011). Unfortunately, there are limited studies that examined the impact of IS usage in e-fraud detection and how auditors detect fraud in computing platforms. Therefore, this study explored how external auditors use IS tools and techniques to spot frauds in electronic business platforms and the impact of IS usage on e-fraud detection. Furthermore, available studies did not explore how the use of IS tools has improved the audit process which is the core business of the audit firm. This study identified this gap and incorporated the post-adoption impact of IS usage on the audit process and e-fraud detection in one concept of IS usage in the external audit environment.

Additionally, the method of enquiry for all the 18 summarised relevant literature (see Appendix 1) except Curtis and Payne (2014), have used survey method to collect data. Survey is a powerful tool for collecting large amount of data but it tends to largely test a theory on already identified factors from the prior literature (Creswell, 2009). Due to differences in culture and the extent of need of technology of different countries, there is a possibility that some identified factors may not necessarily be applicable to a particular setting due to differences in the level of technology and the environment where the audit operates (Goodhue and Thompson, 1995). Hence, this study adopted a simple mixed method approach by using interview as the main enquiry tool supported by a survey to

confirm and triangulate the findings. Therefore, this investigation could be deeper as compared to other previous studies and is anticipated to bring a fresh insight on technology acceptance and usage in a developing country perspective.

1.3 Main Aim of the Study

The main aim of this study is to explore the extent of usage of IS by external auditors in Tanzania by understanding the factors that influence the usage and the impact of IS usage on financial audit process and on e-fraud detection.

1.3.1 Specific Research Objectives

The study advanced the following research objectives (RO):

RO1. To explore the extent of IS usage by external auditors in Tanzania

RO2. To evaluate factors influencing the usage of IS by external auditors in Tanzania

RO3. To assess the impact of IS usage on financial audit process

RO4. To explore how external auditors detect e-fraud in computerised business platforms

RO5. To explore the impact of IS usage on e-fraud detection

1.3.2 Specific Research Questions

The following research questions were used to conduct the exploratory study and which formed part of interview questions:

RQ1: What is the extent of IS usage by external auditors in Tanzania?

RQ2: What factors influence the usage of IS by external auditors in Tanzania?

RQ3: How does IS usage impact financial audit process?

RQ4: How do external auditors detect e-fraud in computerised business platforms?

RQ5: What is the impact of the IS usage on e-fraud detection?

1.4 The Conceptual Framework of the Study and the UTAUT

The conceptual framework of this study incorporates three elements, namely, IS usage, factors for IS usage and post adoption impact on the audit process and e-fraud detection (figure 3.7). Thus, the conceptual framework was grounded on the Unified Theory of Acceptance and Use of Technology (UTAUT) to understand the motivation of IS usage among external auditors in Tanzania. The UTAUT is a theoretical model propounded by Venkatesh et al. (2003) which incorporates eight different models of technology acceptance and usage. The theory believes that for individuals to accept new innovation, reasons related to perceived benefits of technology, ease of use and organisational factors are important. Since 2003, the UTAUT has been widely used to investigate motivations for individuals to accept new technology such as e-commerce, e-banking, health IS and in many other fields.

Subsequently, this study used the UTAUT as a theoretical lens to explore internal factors for IS usage in the qualitative enquiry; while in the quantitative part, two variables that were relevant to the external audit environment were added. In other words, the quantitative part of the study tested six constructs as independent variables (IVs) namely, Performance expectancy (PE) Efforts expectancy (EE), Social and Organisational Influence (SOI), Facilitating Condition (FC), Clients' Factor (CF) and the Audit Professional Factor (APF). Meanwhile, the dependent variable (DV) was the Behavioural Intentions to increase the use of IS abbreviated as (BI). A detailed explanation and justification for the selection of UTAUT is elaborated in Chapter 3.

1.5 The Adopted Research Methodology

The main objective of this study is focussed on exploring the extent of IS usage among external auditors and its post-adoption impact on audit process and e-fraud detection. This objective suggests that the study is a socio-technological in nature rather than pure technological research, hence it

needs an appropriate methodology and participants fit for such an enquiry. It requires therefore, a broader comprehensive assessment of the experiences of the respondents from their personal perspectives, in their social and cultural settings (Myers, 2009). Accordingly, the study adopted a simple mixed method approach as suggested by Creswell (2009) which uses qualitative approach (interviews) as a primary enquiry and quantitative approach as a secondary enquiry to support the qualitative investigation. This type of methodological approach is referred to as a "QUAL-quant" mixed method where 'QUAL' stands for qualitative-dominant and 'quant' stands for quantitative–as a secondary data tool supporting the qualitative investigation (Creswell, 2009: pp 201). A detailed methodology of the study is discussed in Chapter 5.

1.6 Significance of the Study

There is scarcity of literature that disclosed different kinds of digital risk that require the use of IS tools and techniques in risk assessment. The significance of this study comes from the increased need to investigate technology integration within the audit practice of audit firms in order to improve the audit process and to avoid, or minimise audit risk originating from e-business dealings. The study has theoretical and practical relevance. Theoretically, the study extends the literature on the extent of use of technology by external auditors in a developing country's context (Tanzania) where the study was conducted for the first time by integrating factors for IS usage and post adoption impacts on the audit process and e-fraud detection. The findings can foster similar studies to other developing countries where e-business is gaining momentum. Furthermore, the study contributes to the theory of acceptance and use of technology (UTAUT) by including two new variables (clients' factor and the audit professional factor) which are relevant to the external audit environment. The modified model could be useful in conducting studies in other developing countries by including a large sample size of auditors so as to yield better results.

Practically, the findings of this study will provide a useful guide to auditors to evaluate their current IS usage and to determine areas that need improvement in order to increase the value of audit performance levels. Furthermore, the study could be used to encourage audit firms to intensify the use of IS in order to tap the potential values created by IS usage in auditing.

Furthermore, the results can shed some light on the need for active involvement of audit stakeholders, namely investors and the government in creating an enabling environment for IS auditing to effectively take place. To the academics, the study helps in generating future auditors who will be equipped with IT knowledge relevant for auditing e-business platforms. To auditors, the study will help to improve their auditing skills by fostering continuous professional learning through understanding advanced technological issues in auditing which the study has highlighted. Standard setters might use the study in modifying new standards that will foster IS usage; while investors/shareholders will benefit from this study by being enlightened that technology exists to analyse their financial data and that auditors can deliver superior quality audits through technology. Finally, the study can benefit the academic world in expanding the accounting and auditing research domain through integrating components of IS.

1.7 Organisation of Thesis

This thesis is organised in eight Chapters. Chapter 1, introduces the study by identifying the key gaps found in research and the justification of conducting this study. The key issue being the need to use IS among external auditors for effectiveness in audit tasks given the ever-changing nature of the business environment and system-related risks. The Chapter has also highlighted theoretical and practical significance to a group of stakeholders.

Chapter 2 is the literature review related to financial audit and IS in perspectives. Likewise, the evolving role of audit and audit objectives are critically discussed, the use of IS for auditing and the factors influencing technology usage in auditing. The Chapter further discusses the issue of e-fraud,

how it occurs, and its impacts on audit reports. Additionally, the Chapter discusses various techniques used to identify e-frauds and their impact in detecting various types e-fraud.

Chapter 3 elaborates the theoretical literature reviews that are related to technology adoption, acceptance and usage at individual and organisational levels. Precisely, technology acceptance model (TAM), diffusion of innovation (DOI), technology-organisation and environment (TOE), information technology audit quality (ITAQ), and the UTAUT theories are discussed and the selection of one theory (UTAUT) is justified.

Chapter 4 introduces a brief case study on Tanzania where the study was conducted. The Chapter highlights the economic developments, an overview of technology diffusion among users of innovation, the perceived risks caused by e-business integration and the level of external auditing in the country.

Chapter 5 discusses the methodology adopted for this study which is the simple mixed method approach. The Chapter further discusses an espoused exploratory study which used interview (qualitative data) as the main source of data supported by a questionnaire that covers two research objectives (RO1 and RO2). The justification for the chosen methodology, the sample selection, data collection, data analysis and dissemination are also discussed.

Chapter 6 presents the findings of the interview (qualitative data). The identified themes are discussed in light of the research questions. The findings discussed in the Chapter cover all the five research questions of the study.

Chapter 7 presents the findings obtained from the questionnaire (quantitative findings). The process of data analysis and presentation, descriptive and inferential statistics are included in the Chapter with their interpretation and discussion.

Finally, Chapter 8 is the conclusion of the thesis. The Chapter compares and contrasts the findings from previous studies. The key findings are reported and compared with the specific research objectives. Additionally, the Chapter discusses the contributions of the study, limitations and recommendations for future research.

1.8 Definition of the Main Terms.

1.8.1 Information Systems (IS)

IS definition in multiple contexts goes beyond the combination of hardware and software to include other contingent factors such as human resources and IT infrastructure (Ali-Akbar, 2013). However, in the context of this study, IS has been defined as a tool, used to facilitate the audit activities of an audit firm or organisation. It combines procedures, controls and auditing techniques with the technology of the IT industry, user interface, computers and sophisticated software. The software used to track transactions provides internal reporting data, external reporting data, FSs, and trend analysis (Ghasemi et al., 2011). Examples of IS tools are CAATTs which are used in audit practices.

1.8.2 External Auditor

An external auditor is an independent person (an outsider) that is responsible to oversee the activities of the client (the auditee) by assessing the FSs prepared by the management to confirm whether they are free from any material misstatements (Knapp, 2013).

1.8.3 Electronic Based Fraud (E-fraud)

E-fraud is a type of computer crime (Simkin et al., 2015) which involves the use of electronic devices sometimes with the help of an Internet to conduct an illegal act with an intention to benefit oneself. There are many kinds of e-frauds that can happen to an entity and its customers (see Newman and Clark, 2003). However, for the purpose of this study, e-fraud is any fraud that is committed through computer networks and which, if not discovered by an auditor, may lead to a material misstatement in

the FSs of an entity. In other words, e-frauds which this study considers are those that fall under the category of ISA 240 and ISA 315, which if not identified may either result into audit risk or business risk. These risks are clarified further in Chapter 2 subsection 2.9

1.8.4 E-fraud Detection

E-fraud detection is a technique that auditors use to identify any possibility of fraud to have occurred through electronic mechanisms. Generally, fraud detection (including e-fraud) is not the major responsibility of external auditors, but one of the most important part of the audit evidence (absence of fraud) because undetected fraud can result into material misstatements in FSs.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter presents a review of literature related to auditing and the use of IS. It examines into detailed elements of auditing, fraud detection and the evolving role of external auditors in the technology era. The second sub-section is about IS, types of IS and the reasons for the use of IS in audit functions. The third sub-section discusses the impact of IS on financial audit process. The last sub-section discusses the role of auditors on e-fraud, the possible ways of using IS to identify e-fraud and the impact of IS usage on fraud detection.

2.2 Financial Audit in Perspectives

The term "auditing" originated from the stewardship role where one person (principal) entrusted another person (agent) to conduct the business affairs (Porter et al., 2008). The affairs had one fundamental aim which was to yield a return to the owner by increasing his wealth (Rose and Westerfield, 2007). Conversely, during the course of the activities, the agent puts forth his personal interest contrary to that of the principal, which results in questionable behaviours to his trust. Hence, the auditor comes in as an intervening party between the agent and the principal. According to Porter et al. (2008), the definition of auditing and its scope is changing to reflect the needs of stakeholders. In the past, auditing reflected a simple role which targeted a single owner (sole proprietorship) or family businesses but the recent definitions have encompassed a wider role of auditing due to multiple ownerships of businesses (Porter et al., 2008). The evolving role of auditors and audit objectives are discussed in detail in sub-section 2.3.

Knapp (2013) defines financial audit as the process of verifying FSs in respect of the original records of the company with the sole purpose of rendering an opinion certifying that reports presented are

true and fair. Financial audit is also defined as a systematic and well-organised procedure of accurately finding and evaluating evidence with regards to stewardship assertions about economic events to establish a degree of correspondence between those reported assertions and accepted standards with the sole intention of communicating the findings to the intended users (Porter et al., 2008). The board of auditing practitioners (APB, 2010) defines financial audit as the process of finding evidence regarding any disclosures on financial reports of an entity which are sufficient to provide sound assurance on whether the financial reports are free from material misstatements. In all the three definitions, the word 'evidence' is important hence; auditing has encompassed the role of investigation by gathering evidence in order to bring about a more informed decision (Soltani, 2013). Financial audit therefore, involves assessing of policies, estimates, measures and their consistencies; adhering to specified audit regulations, gathering evidence, and critically examining assertions made by directors and other personnel who prepared FSs (Porter et al., 2008). The attention of this study is on statutory audits conducted by independent auditors.

In Tanzania, which is the focus of this study, statutory audits are mandated by the Companies Act 2002. The act requires that all companies of whatever size, whether public or private, to prepare FSs at the end of each financial period. The preparation of FSs must comply with the International Financial Reporting Standards (IFRS) and they are required to be audited by an independent auditor who is accredited to work in Tanzania. The NBAA under the umbrella of IFAC is the supervisory body of the accounting profession, auditors and audit firms in Tanzania.

2.3 The Evolving Audit Objectives: From Ticking to Clicking

Auditing is a dynamic field (Matthews, 2006). The dynamism of this profession is attributable to the environment of its practice and the audience it serves, which are audit clients and other stakeholders (Porter et al., 2008). The stakeholders in auditing are varying from single in the 1800s to multiple stakeholders at the present time. The evolving role of auditing can be categorised into three main

phases based on the features, nature of business environment and ownership, which subsequently define the audit objectives (Porter et al., 2008). The next sub-sections explain these phases.

2.3.1 Auditing of Bookkeeping

During the old times in the 1880s towards 1920s, an auditor was any trustworthy person who was well known to the owner of the business but with minimum knowledge of bookkeeping (Porter et al., 2008). According to Caglio (2003 pp. 102), the audit of the past, focussed on auditing the work of accountants when he stated "*as too traditional role whose main task was to check the books of accounts by focusing on detecting fraud and errors and to ensure the accuracy of bookkeeping records"*. It was easy to attach the role of auditors with fraud detection due to the small size of businesses and the nature of transactions performed. Most businesses were owned by individuals or families hence, most tasks performed by auditors were manual based that involved vouching and examination of the accuracy in the books of accounts. In the words of Matthews (2006, pp. 96), *"Auditing of the old days were not pure audits, majority of them for instance in the UK, were somewhat of a respectful novels and not pure inspections"*. Until the 1920s, auditing was more accountable to owners and creditors (Porter et al., 2008). The issue of honesty and proper authorisation of funds were critical. By large, the main objective of auditing was to ensure that the entity maintains a sound solvency in the undertakings (Salehi and Alipour, 2010). Mostly, the items of the balance sheets were given attention which was why it was referred to as a balance sheet audit (Kotb et al., 2012). There was little concern on verification of evidence, rather, the balancing of the books of accounts and specifically, the balance sheet items were of more concern.

2.3.2 Audit Evidence and Internal Controls

From the 1920s towards the 1960s, there was a dramatic increase in the volume of transactions among audit clients (Porter et al., 2008). Most corporations grew in size and capital which eventually increased the separation of ownership. This was also an emergence of institutional investors where

most businesses could issue shares and bonds. The emergence of institutional investors widened the scope of auditors' accountability in terms of number of stakeholders. The features of business activities in that era resulted in changes made on audit objectives. The main objective of audit became lending credibility to FSs which surpassed fraud and error, making it a secondary objective (Porter et al., 2008). Similarly, the emphasis of audit items shifted to income statements, especially profitability and revenue recognition which surpassed the audit of the balance sheet items (Porter et al., 2008).

Due to a considerable increase in transactions, the audit techniques eventually changed. Auditors relied on internal controls and sampling techniques by testing a few transactions. In principle, testing all transactions for 100 percent accuracy was impractical (Matthews, 2006). As a result, a physical observation of a few items such as assets or confirmation of accounts receivables was instead conducted as part of audit evidence. This was also the birth of a true and fair view regarding audit reports which swapped the true and accurate verification of bookkeeping (Matthews, 2006).

2.3.3 Computerised Auditing

From 1960 towards 1990, immense business expansions, mergers, takeovers, international diversification, and competition between businesses occurred. This phenomenon commanded more capital from multi-dimension investors which eventually resulted in a wider gap in ownership (Porter et al., 2008). To manage large businesses needed professional expertise which eventually widened the separation of ownership of the business and the over reliance of management to run the affairs of the business. Likewise, the number of business stakeholders also increased to include owners, creditors, customers and the general public. Accordingly, the role of auditors was adjusted to ensure that the management of the appropriate companies became accountable to all these stakeholder groups by ensuring proper/honest management in the allocation of resources (Porter et al., 2008). In addition, profitability and other corporate social responsibility (CSR) issues became important, in what was

referred to by Power (2000, pp.198) as '*the audit explosion'* which means providing both audit and non-audit services. Yet again, these phenomena adjusted further the objective of auditing by retaining lending credibility as the core objective in addition to providing advisory services to the management (Porter et al., 2008). Consequently, audit techniques were reformed and the use of computers for auditing and sampling became useful. More prominently was the birth of risk-based auditing which stressed on the need to thoroughly understand the entity and its business environment, to have an analytical review and testing of internal controls of an entity. The use of computers characterised the sampling techniques, evidence and testing control of the enterprise. Apparently, in that time-period, fraud and error were not mentioned as part of the audit objectives (Porter et al., 2008).

From the 1990s until today, radical changes in auditing have emerged largely due to increased sophistication in e-business models (Kotb and Roberts, 2011), huge corporate fraud and the collapse of many companies close to the millennium (KPMG, 2006). Due to these phenomena, a backward and forward move in audit role materialised. Lending credibility still remained as the core audit objective, when provision for advisory services was removed after 2002 corporate scandals (Porter et al., 2008). Fraud detection and reporting corporate fraud were brought back on board and assigned to specific standards (see ISA 240, ISA 315 and SAS 99). There were also increased prospects for regulatory authorities and compliance such as Sarbanes Oxley-Act, PCAOB and the UK's combined code (Porter et al., 2008). Therefore, auditors assumed the role of risk assurance service providers, meaning that they are concerned about both the audit risk and the business risk that could threaten the going concern of the enterprise (Hunton et al., 2004; Cosserat, 2004). The use of audit techniques through IS tools were recommended (Information Systems Audit and Control Association (ISACA), 1999) because different e-business models emerged where some were simple while others were complex in nature (Kotb et al., 2012). At first, audit was conducted on printed documents that were processed by computers that became known as audit around the computer (Bagranoff and Vendrzyk, 2000). Auditing around the computer was termed a less reliable means for auditing especially to pure

e-business clients because some of the computer evidence became available in read-only memory which might be irretrievable after a certain period of time (Gopalakrishuna, 2008). As a result, it became necessary to audit both the transactions as well as the systems that process transactions (auditing through the computer) to ensure effective risk assessments (Hunton et al., 2004; Bagranoff et al., 2007). Today, some audit firms are utilising IS ranging from simple to high end technologies that can perform audit in real time (Alles et al., 2008). These impending modifications in audit practices are some of what researchers have remarked "*Certainly, the work of auditing has fundamentally changed from ticking to clicking"* (Matthews, 2006, pp.88). Auspiciously, the use of IS in auditing has reported many success factors both to the users and the audit firm which will be discussed in the coming sub-sections.

2.4 Information Systems in Perspective

The definition of IS has been examined from diverse disciplines to include economics, strategic management, accounting, procurement, e-business and operations research (Melville et al., 2004). Prior researchers have defined IS beyond the combination of hardware and software by incorporating other contingent factors relevant for its application in an organisational context (Bharadwaj, 2000). Yet, others have treated IS as a tool that can be used to achieve certain organisational objectives such as enhancing operational activities of the firm (Lal and Bharadwaj, 2016). Melville et al. (2004), suggest the construct of IS based on five main concepts, namely (1) IS as a tool (2) a proxy (3 ensembles (4) a computation and (5) a nominal.

The tool view theory considers IS by measuring their intended objective. Researchers have measured the productivity improvements of IS as a tool and its enhanced relationship in generating value. The proxy view of IS theory defines IS based on its essential features and perception of users in relation to the value of IS. Researchers who opted to define IS construct based on the proxy view have considered IS as an investment by measuring it in terms of dollars per investment of stock

(Bharadwaj, 2000). Meanwhile, the ensemble view of IS conceptualises IS holistically to include human resources capabilities to generate value (Kohli and Devaraj, 2003); and the ensemble view, which is a more general approach, considers IS to include infrastructure, human resources and other intangible assets aggregated and measured against certain performance measures. The computational view considers IS as procedures computed and modelled to test systems development and other techniques. Meanwhile, the nominal view of IS conceptualises innovation by its name and not in evidences. For example, oligopolistic competitors have used IS as a factor applied on the production process by observing the stages before and after the impact. However, the computational and nominal views are uncommon is MIS research (Melville et al., 2004).

With regards to the varied concepts of IS by different researchers, this study defines IS as a tool which can aid auditors in accomplishing audit tasks. They combine procedures, controls and auditing techniques with the technology of the IT industry, user interface, computers and sophisticated software. The software used to track transactions provides internal reporting data, external reporting data, FSs, and trend analysis (Ghasemi et al., 2011). This study has adopted the IS typologies provided by (Greenstein-Prosch et al., 2008), as derived from a detailed list compiled from IFAC manuals and the Norwegian auditing profession (McKee, 2000), where 36 important technologies for auditing purposes were extracted. These technologies were factored into five components, namely (a) Ecommerce technologies (ECT) or Intruders detection technologies (b) Networking and data transfer (NADTT) (c) General office automation technologies (OAT) (d) Audit automation technologies, (AAT) and (e) Accounting firm office automation technologies. NADTT are tools which help auditors during internal and external communication of important audit reports, discussions, findings and queries (McKee, 2000). They include digital communication, internal and external networking configuration. OAT includes all relevant applications that can facilitate internal audit functions such as preparation of working papers, documentation and report writing process. Specifically, OAT includes Word processing, Excel, Emails, Internet, Image processing and e-presentation (Greenstein-

Prosch et al., 2008), Meanwhile, AAT covers all the categories of GAS and CA methodologies and tools which are relevant for auditing tasks. These tools could be used directly by auditors when auditing the clients' environment (Ahmi and Kent, 2013). Meanwhile, AFAT are specific audit tools (software) which are installed by the audit firm for special types of clients or special audit assignments (Greenstein-Prosch et al., 2008). Therefore, in this study, the exploration of IS tools used by external auditors will be discussed in light of the above mentioned categorisation.

2.5 Impact of Information Systems on Financial Audit

The word "impact" is defined by Cambridge Dictionary as *a powerful major influence, swaying, or having a strong control over something* (Cambridge Dictionary Online, Accessed on 19/12/2015). The impact of IS that this study considers is the influence which is measured based on how IS has brought changes to the financial audit when auditors use technological tools during the audit process (Abu-Musa, 2008). However, the impact of IS in auditing has been examined from two perspectives, namely (1) from the clients' systems side and (2) from the auditors' systems usage and applications. Scholars who examined the impact of IS (the auditee's systems) described the challenges brought by technology usage amongst audit clients and how it affected the audit tasks. For example, scholars identified different risk categories which originated from the complex e-business models that arguably has characterised the auditee systems, as compared to the traditional paper-based systems (Bierstaker et al., 2006; Kotb et al., 2012; Kotb et al., 2014). Hence, the main focus on this category of researchers is the description of risks threatening the audit environment especially systems-related risks.

The second category is composed of studies that examined the impact of IS based on the audit firms' systems (Banker et al., 2002; Shaikh, 2005; Abu-Musa, 2008; Greeinstein-Prosch et al., 2008; Omoteso et al., 2010). Researchers in this category looked at how IS tools are being adopted and used by auditors and suggested a variety of ways to speed up the adoption process. One of the important

methods suggested to increase the adoption process is the understanding of the challenges and opportunities in the use of IS so that responsible bodies and stakeholders could see the need to adopt technology in auditing.

One of the extensive work on the impact of IS on financial audit was done by Kotb et al. (2012), when they examined the risk brought by the use of technology among audit clients. The study contends that, IS in auditing should be viewed as an inevitable move for auditors especially for audit firms which audit e-business clients. Kotb et al. (2012 and 2013) argued that the risk-based systems brought by e-business models have posed a threat on financial auditors' knowledge. Hence there is a need for more skills in IT based in order to effectively assess risk in e-business platforms. Likewise, Vendrzyk and Bagranoff (2003) predicted the changing role of auditors when more businesses move to technology in the processing and storing of the accounting information. They argued that as more accounting information is kept in paperless, audit clients would request for additional services such as checking of computer security and other general systems control services which would need auditors to be equipped with systems-based expertise and control mechanisms. Four main classes of risks were clarified when a business uses ERP systems; namely, systems interdependency, security risks, process risk and internal control risk (Hunton et al., 2004). A suggestions to mitigate these risk categories through the use of IS was also proposed which include the adoption of technological tools to align with the nature of clients' automation.

Hence, this study finds it important to focus on the identified challenges in order to understand the auditors' pace in the use of IS in auditing. Specifically, the study explore on the current IS which auditors in Tanzania are using when performing their tasks with special focus on potential tools which can help them in identifying e-fraud. Additionally, what influences auditors to adopt technology are also examined. The next sub-section reviews the literature on available audit technologies that can help auditors to enhance audit tasks.

2.6 Relevant Technologies for Audit Purposes

There are several technologies that are available for auditors to use. The most common tools are known as CAATTs (Braun and Davis, 2003; Janvrin et al., 2009; Curtis and Payne, 2014). CAATTs come in different versions, first, as an application and also as a tool specifically to help auditors to conduct auditing in a computerised business environment (Janvrin et al., 2009). CAATTs are defined as any tool that can be used to assist auditors in performing audit tasks (Braun and Davis, 2003). They range from basic software such as MS Excel (Ahmi and Kent, 2013) to advanced audit tools such as artificial intelligence, which can be used to perform CA of highly digitalised clients (Alles, et al., 2008; Varsahely et al., 2012). Generally, CAATTs are available in five main categories which are utility software, test data, parallel simulation, integrated test facility and embedded audit modules (Porter et al., 2008). A detailed clarification of these tools and how they can assist in auditing tasks is summarised in table 2. 1.

According to Ahmi and Kent (2013), Sun (2012) and Debreceny et al. (2005), the most frequently used CAATT is the GAS which is available in modular form. GAS had been used to perform several audit tasks such as data extraction, querying, data manipulation, summarising and performing analytical tasks (Ahmi and Kent, 2013). The unique features in GAS makes users find it easy to use and learn it. However, studies on the usage of GAS have reported on average, a low usage of this unique, indispensable tool (Debreceny et al., 2005; Singleton, 2006; Ahmi and Kent, 2013). Generally, what constitutes a low usage of IS in auditing is still inconclusive. There are different factors, namely economic, social and political, as well as individual factors that contribute to a low usage of IS in auditing (Rosli et al., 2013). These factors are discussed in the next sub-section.

Table 2.1 IS Tools That Aid Auditors in Performing Audit Tasks

Types of information systems	Purpose it serves in auditing	Cited in
Utility software	It performs data processes like sorting or retrieving computer files. They are used to speed up the audit procedure.	Biestaker et al. (2001),ISACA (2009), Ahmi and Kent (2013)
Generalised Audit Software	A Software package which can be used to perform multi-audit tasks i.e. retrieving files, reading computer files, sampling, computations and comparing past and current reports. They perform data analytics, select samples and confirm accounts balances.	Biestaker et al. (2001),ISACA (2009), Ahmi and Kent (2013)
Specialised Audit Software	These are software designed to conduct a special audit. Sometimes referred to as in-house software that can be installed by an IT vendor to the audit firm on demand.	Biestaker et al. (2001),ISACA (2009), Ahmi and Kent (2013)
Parallel simulation	Helps auditors to process clients' data into auditable version that can be used in the external auditors' application.	Biestaker et al. (2001), ISACA (2009), Ahmi and Kent (2013).
Integrated test facility	It is used to test and identify dummy data sets. It also makes computations, conducts various tests for auditors to evaluate application controls.	Biestaker et al.(2001), ISACA (2009), Ahmi and Kent (2013).
Embedded audit modules	It is used to perform continuous auditing and monitoring of auditee's transactions. They can be used to detect irregularities in transactions and controls.	Ahmi and Kent (2013; Greenstein-Prosch et al. 2008).
IDEA .	It is a common category of GAS, that is used for scanning the whole population for testing, testing a 100% sample, detecting frauds i.e. fictitious claims, checking compliances etc.	Biestaker et al. (2001), ISACA, (2009), Ahmi and Kent (2013).
Audit Command Language (ACL)	It is a common category of GAS used in balancing ledgers, totalling records, sorting accounts by size, mining huge data, selecting samples for detailed testing, generating confirmations and identifying unusual transactions.	Biestaker et al. (2001), ISACA (2009), Ahmi and Kent (2013).
Statistical Analysis Systems	These are high standard CAATTs that can check clients' reliability of information from real world sources instantaneously after the transactions have occurred.	Ahmi and Kent (2013), Greenstein-Prosch et al. (2008), Rezaee and Reisten (1998), Braun and Davis (2003).
Microsoft Excel	It is a common GAS that can be used for computation of figures and data manipulation. It reduces errors and saves time in verification of reported figures. It can also be used to analyse data of varied forms.	Greenstein-Prosch et al. (2008), Banker et al. (2002), Biestaker et al. (2001).

Table 2.1 lists some of the most common IS tools that can help auditors to accomplish audit tasks. Some are advanced while others are moderate tools. For example, ACL, and IDEA were installed by large audit firms in US (Mahzan and Lymer, 2014), while Excel was reported to be widely used by auditors in small and medium audit firms (Singleton, 2006). In the study conducted by the Institute of Internal Auditors (2009), it was found that 100 percent of the surveyed internal auditors reported analysing their accounting data in Excel. Thus, Excel was named "*a must use IS tool for auditors"* (Ahm and Kent, 2013). However, a low capacity and features in Excel can make it be limited to specific types of clients' systems (Singleton, 2006). Although its capacity is limited only to lower level audit clients, always a combination of Excel with In-house applications characterise the audit tools used by most large audit firms (Braun and Davis, 2006).

In addition to the IS tools explained above, there are other technologies which can help auditors to simplify several audit tasks. Greenstein-Prosch et al. (2008) has identified 36 important technologies that are relevant for auditors (see Appendix II). They categorised technologies into those which can help auditors to perform general office activities, internal and external communications and those specifically for performing auditing tasks.

2.7 Factors Influencing the Usage of IS in Auditing

The need to use IS tools and techniques in auditing vary among countries and among audit firms within the same countries (Greenstein-Prosch et al., 2008). These variations are partly attributable to the voluntary nature of using technology in auditing under the current ISAs (Curtis and Payne, 2014), while some factors originate from individuals, organisations and the audit environment. Firstly, it is important to explain the benefits of using IS tools in auditing. According to Ahmi and Kent (2013) and Janvrin et al. (2009), there are many functions that IS (i.e GAS) can do to help auditors during the audit process. As a result, auditors will save time and resources while providing maximum

assurance in performing auditing tasks. The following are the functions of IS tools during the audit process as specified in audit standards:

i. Detection of errors and fraud
ii. Identifying items in the journal for testing
iii. Testing correctness of electronic files
iv. Confirming aging of all accounts receivables
v. Selecting a required sample from the original files
vi. Sorting items of transactions which have the same features
vii. Finding evidence regarding the effectiveness of controls
viii. Calculating the representativeness and completeness of inventories

With such advantages which IS can promise, auditors are expected to be motivated in the utilisation in order to tap these benefits, especially in the current technology era (Ahmi et al., 2014). However, auditors were reported to be reluctant and preferred their traditional audit techniques. Curtis and Payne (2014) reported that "*never will I use CAATTs in auditing*" as the highest frequency theme during an interview session with auditors from one large audit firm in the US. Such kinds of perceptions among auditors have brought about interest among many researchers in the accounting field to understand why auditors do not use audit technology irrespective of the varied potential benefits.

There are several factors that can induce individuals to use technology. These factors are broadly categorised into three groups that include personal factors, organisational factors, and environmental factors (Rosli et al., 2013). Individual factors include the perception of auditors to use and appreciate the available technology in improving the audit tasks. Meanwhile, the organisational factors are directly related to the management decision to use or not to use technology (Janvrin et al., 2009; Vasarhelyi et al., 2012; Razi and Madani, 2013). Individual factors and organisational factors are also named as internal factors because they involve decisions regarding the organisation and its

capabilities in terms of infrastructure, budgetary constraints and human resources (Rosli et al., 2013; Ahmi et al., 2014). On the other hand, external factors, also known as environmental factors, include pressure from competitors, oversight bodies (example section 404 of SOX) and the demand of the e-business environment (Kotb et al., 2012).

According to Lal and Bharadwaj (2016), internal factors to technology adoption outweigh the external factors. They argue that internal factors, generally involve cost-benefits analysis. If technology is perceived as useful in yielding a required return such as lowering costs, it will be regarded as beneficial, leading to adoption. According to Kotb et al. (2012), external pressure especially e-business environment, is the distinct key driver for technology adoption in auditing. Kotb et al. (2012) is considerably concerned of the audit quality in this technology era, where new e-business models among audit clients are constantly evolving. As a result, the demand for CA throughout the use of IS will emerge (Alles et al., 2006; Omoteso et al., 2010). The arguments among these scholars suggest that both internal and external factors can have a significant impact on technology adoption decisions.

Other factors which can influence auditors to use IS were derived from models of technology adoption such as technology acceptance model (TAM) (Vasarhelyi et al., 2012; Razi and Madani, 2013), diffusion of innovation (DOI) (Lal and Bharadwaj 2016), technology organisation and environmental (TOE) model (Ahmi et al., 2014) or I-TOE (Rosli et al., 2013) and the unified theory of acceptance and use of technology (UTAUT) (Mahzan and Lymer, 2014; Curtis and Payne, 2014; Gonzalez et al., 2012).

Contingent on the empirical data collected, culture of the country studied, and the type of auditors (internal or external), researchers reported inconsistent findings. For example, Mahzan and Lymer (2014) found that performance expectancy and facilitating condition were the most important determinants for CAATTs adoption by external auditors. Meanwhile, Curtis and Payne (2014) found that long-term budgetary pressure was mostly valuable to suggest that auditors will most likely use

technology. Likewise, Ahmi and Kent (2013) found that a combination of both internal and external factors had a strong influence on auditors' use of technology. Specifically, they found that technological infrastructure, auditors' knowledge and experience in computerised auditing, support from the management and client factors, strongly influenced external auditors to use GAS. Again, these factors differed significantly when Debreceny et al. (2005) investigated the acceptance level to use audit tools by external auditors in Singapore.

Henceforth, from studies of technology adoption and usage in auditing, a combination of individual, organisational and external factors were reported to influence the use of technology in auditing. However, some of the identified factors could not be supported hence, the question emerges as to why there is a low usage of technology in auditing even among auditors in the developed world (Debreceny et al., 2005; Wehner and Jessup, 2005; Vasarhelyi et al., 2012; Ahmi and Kent, 2013). One of the causes for a low IS usage in auditing is arguably to be the lack of expertise in using modern technology (Greenstein-Prosch et al., 2008). Greenstein-Prosch et al. (2008) found a low IT knowledge among auditors in US and Germany in at least three out of five of the IT components. Specifically, they found that many auditors had a low expertise in e-commerce technology, NADTT and AAT. Similarly, IT knowledge level among auditors in Malaysia was found to be lower than their perceived importance of technology application in the audit process (Ismail and Zainol-Abidin, 2009). Equally, Abu-Musa (2008) found a low involvement of auditors in the process of acquisition and installation of IS which resulted in a low usage of IS tools. Meanwhile, Curtis and Payne (2014) found that the voluntary nature of IS usage in auditing was a barrier to full technology adoption in auditing. They argued that if technology usage was mandatory it could intensify the pace in technology usage and subsequently auditors would learn and be competent in technology applications.

One of the biggest influence of IS usage is the management (Mahzan and Lymer, 2008). Their perception towards IS usage can limit or increase the degree of adoption and usage. However, issues related to age of management and their expertise in the use of IS in auditing were found to be a

significant hindrance in adoption decisions (Venkatesh et al., 2003). For example, it was found that old age managers had a negative attitude towards technology usage while young managers easily supported the adoption of IS. According to Mahzan and Lymer (2008), old managers have sufficient experience in auditing and hence understand the risk involved within their clients and therefore, preferred to use the personal judgement approach.

Besides that, studies have cited limitations to technology adoption to be related to cost benefits analysis (Rosli et al., 2013). Generally, managers would forecast the use of technology that is whether it outweighs the costs before implementation. In many developing countries, the use of technology can be viewed as too expensive, which may limit the adoption process (Abu-Musa, 2008; Lotto, 2014; Moorthy et al., 2011). Software ownership and licensing issues hindered management decisions to adopt GAS (Ahmi and Kent, 2013). Likewise, security issues were also reported to hinder auditors to conduct IT audits effectively because clients were more concerned about disclosing much of their data to a third party (Alles et al., 2008). According to Debreceny et al. (2005), ignorance on the part of the clients' personnel and lack of collaboration hindered IT audits to effectively take place. These factors have resulted in a slow pace to technology acceptance and usage which may have a negative impact on risk assessment and audit quality.

2.8 Utilisation of IS and its Impact on the Audit Process

The literature suggests that the adoption and utilisation of IS tools has enabled audit firms to improve the audit processes through improving the audit quality (Omoteso et al., 2008). IS simplified coordination of audit activities due to the availability and use of new and relatively inexpensive information delivery mechanisms by maintaining links with clients for value-added services and support (Banker et al., 2002). It is further argued that the utilisation of IS supports four key areas of audit processes; namely, planning, documentation, testing and communication or audit reports (Bierstaker et al., 2001; Banker et al., 2002; Omoteso et al., 2010). The use of IS tools in auditing

enabled audit firms in the US to experience a steady growth of revenue due to enhancement in risk assessment capability to their e-business clients (Vendrzyk and Bagranoff, 2003).

Studies found that non-audit services (IT based services) had increased revenue for audit firms by 70 percent (Bagranoff and Vendrzyk, 2000), which suggested that there was an increased need for their clients' use of innovations. Kotb et al. (2012) contended that the use of IS software and capability enabled audit firms to expand their products and services from auditing FSs alone into WebTrust and SysTrust assurance services. It can be argued that the utilisation of IS tools by audit firms has not only increased its revenue margin but also improved coordination of activities within the audit departments and other segments (Banker et al., 2002; Kotb et al., 2012). For audit firms with international affiliations, the use of knowledge sharing applications enabled them to link their audit tasks by fostering transparency in the audit process.

Evidence from the surveyed literature shows that the measurement criteria of IS usage and their impact on firms' performance is inconclusive. Various studies have measured utilisation of IS impacts by employing either financial measures like profitability, cost reduction or revenue recognition (Banker et al., 2002). Others have applied non-financial measures to include improved operations, customer satisfaction, competitive advantage and other market measures (Ahed and Louis, 2008) or a combination of financial and non-financial measures (see Banker et al., 2002). Non-financial measures of IS utilisation for audit value includes efficiency of operations, improving audit quality and individual auditor's performance (Banker et al., 2002; Omoteso et al., 2010). However, this study will benchmark the degree of impact of IS usage on the audit process based on the improved audit processes derived from the audit life cycle.

Meanwhile, other researchers have defined efficiency improvement in IS utilisation to include improved coordination and supervisory activities (Omoteso et al., 2008). According to Janvrin et al. (2009), the impact of IS on efficiency comes from internal and external efficiency adjustments. Internal efficiency adjustments include time and cost savings by abandoning complex manual tasks

which are time consuming and increase administrative expenses. In contrast, external efficiency stems from stakeholders' satisfaction of the audit quality and on time delivery of audit services (Ohman et al., 2012; Mohamed and Habib, 2013). It was also reported that the usage of IS in auditing narrowed the expectation gap among audit stakeholders (Omoteso et al., 2008). They argued that through the use of IS, auditors can perform several tasks by applying modern techniques in gathering audit evidence and identifying fraud easily than using manual processes. Other measurements reported include increased audit independence (Omoteso et al., 2008) and firms' competitive advantage (Kotb et al., 2012). However, studies have reported various benefits depending on the expected outcomes. In contrast, Quaddus and Achjari (2005) measured the impact of technology usage (e-commerce) in terms of the degree of contribution of IS in meeting organisational goals, and increase in customer base. It was found that the adoption of e-commerce increased the number of customers by tapping them across borders and also reduced the costs of operation.

The unique features of audit software (such as GAS) enables audit value creation by improving efficiency in analytical procedures, documentations, clients' feedback and information sharing (Banker et al., 2002; Greenstein-Prosch et al., 2008; Janvrin et al., 2009; Ahmi and Kent, 2013). The value creation of IS utilisation has been found to depend on IT systems used, firms' sizes and human resources capabilities (Greeinstein-Prosch et al., 2008; Elly and Boter, 2011). The macro level of IS utilisation success model that was developed by Melville et al. (2004), highlights the core internal and external determinants, and internal and external obstacles as important factors affecting the achievement of IS usage in any organisation. Internal and external determinants were defined as the success factors accruing to a firm as a result of using technology. Meanwhile, internal and external obstacles were the impediment that hinders firms from utilising IS in its business processes.

However, a recent study in an emerging market (Egypt) suggests that the use of audit technology in technical audit procedures varies with the size of the audit firm and auditor's expertise in IT usage (El-Sood et al., 2015). For instance, if the audit firm is a Big Four, with sufficient IT auditor

proficiency, the perceived importance of technology usage for audit process increased. In contrast, auditors from small and medium audit firms may not appreciate technology usage as important due low perceived benefits as most of them lack enough expertise in IT skills (Ahmi and Kent, 2013). As a result, they cannot overcome the IT anxiety and fail to focus on the usefulness of technology (Taylor and Todd, 1995). These factors can minimise the reported importance of IS on financial audit processes to be limited to a few respondents based on the size of their audit firm and expertise in audit technology.

In any case, this study will benchmark the degree of impact of IS usage on financial audit based on the improved audit processes derived from the audit life cycle. This part of research has yet to be empirically explored.

2.9 E-fraud and the Use of IS Tools for Fraud Detection

It is important to first discuss the general concept of fraud and its various classifications so as to link e-fraud, the role of external auditors and the use of IS tools and techniques. This is important because e-fraud as referred to in this study, is the same fraud concept but differs from the traditional offline fraud on its mode of occurrence, timing and the environment where e-fraud occurs (Jans et al., 2009). In other words, while e-fraud occurs electronically with the use of electronic devices propelled by the Internet (Simkin et al., 2015), traditional fraud occurs in the absence of these sophisticated mechanisms. Nevertheless, fraud in its totality is defined as a deliberate act of deceit that is committed by an individual to obtain an unlawful gain (Jans et al., 2009). It can involve more than one person who have intended to commit a secret act by depriving another person (or an entity) by taking away an item of value, for their own development (Davia et al., 2000). ISA 240.11 (IFAC, 2009a) defines fraud in the scope of auditing as *"An intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage"*. This definition encompasses two classes of

possible culprits, namely, internal and external fraudsters whose classifications have been suggested by Jans et al. (2009) in Figure 2.1. Furthermore, ISA 240 clarifies that the ultimate consequence of fraud must have caused a *material misstatement in FSs* which brings the need to understand the term "misstatement".

Material misstatement is defined in ISA 450.1A as *"The difference between the amounts, classification, presentation, or disclosure of a reported FS item and the amounts, classification, presentation, or disclosure that is required for the item to be, in accordance with the applicable financial reporting framework. Hence, Misstatements can arise from error or fraud"* (IFAC, 2009e). In principle, a misstatement arises due to inconsistencies between the value conveyed in the FSs against what is anticipated to be fairly presented in portraying a true and fair view (Association of Certified Chartered Accountants (ACCA), 2012). Additionally, misstatements can be real (i.e. in situations where there is clear breach of requirements of any IFRS regarding presentations, disclosures or omissions), or could be judgmental as a result of inappropriate estimation and choices of accounting procedures (ACCA, 2012). Hence, ISA 240.3 identifies two forms of fraud, namely FSF and AMF. FSF is fraud occurrences, which might falsify the truth and fairness of FS. It includes understating or overstating FSs by means of factual manipulation of the items used in preparation of FSs (Alexander et al., 2011). Likewise, FSF can happen for several motives such as enabling the entity to raise financing capital, avoiding insolvency by hiding debts and supporting equity over-valuation (Lau and Ooi, 2016). Irrespective of the reason behind FSF, generally this act is considered fraudulent and hence illegal.

On the other hand, AMF also named transactions fraud (Jans et al., 2009) as any act, which involves stealing assets of the company for personal gain (Bologna and Lindquist, 1995). Typically, AMF involves stealing cash or cash equivalents like credit notes or vouchers, stealing inventory for selling and general exploitation of the company's assets like cars and other tangible assets. Even stealing of company's data and intellectual property has also been categorised under AMF (IFAC, 2009a).

According to Jans et al. (2009 and 2010), AMF is frequently committed by lower level employees and third parties or by collaboration with customers or suppliers during the procurement process (i.e faking payments to accounts receivables). However, other management personnel and even those who are responsible with governance of the company can also commit it. In some extreme cases, top-level management have committed AMF and concealed it within FS (Bologna and Lindquist, 1995).

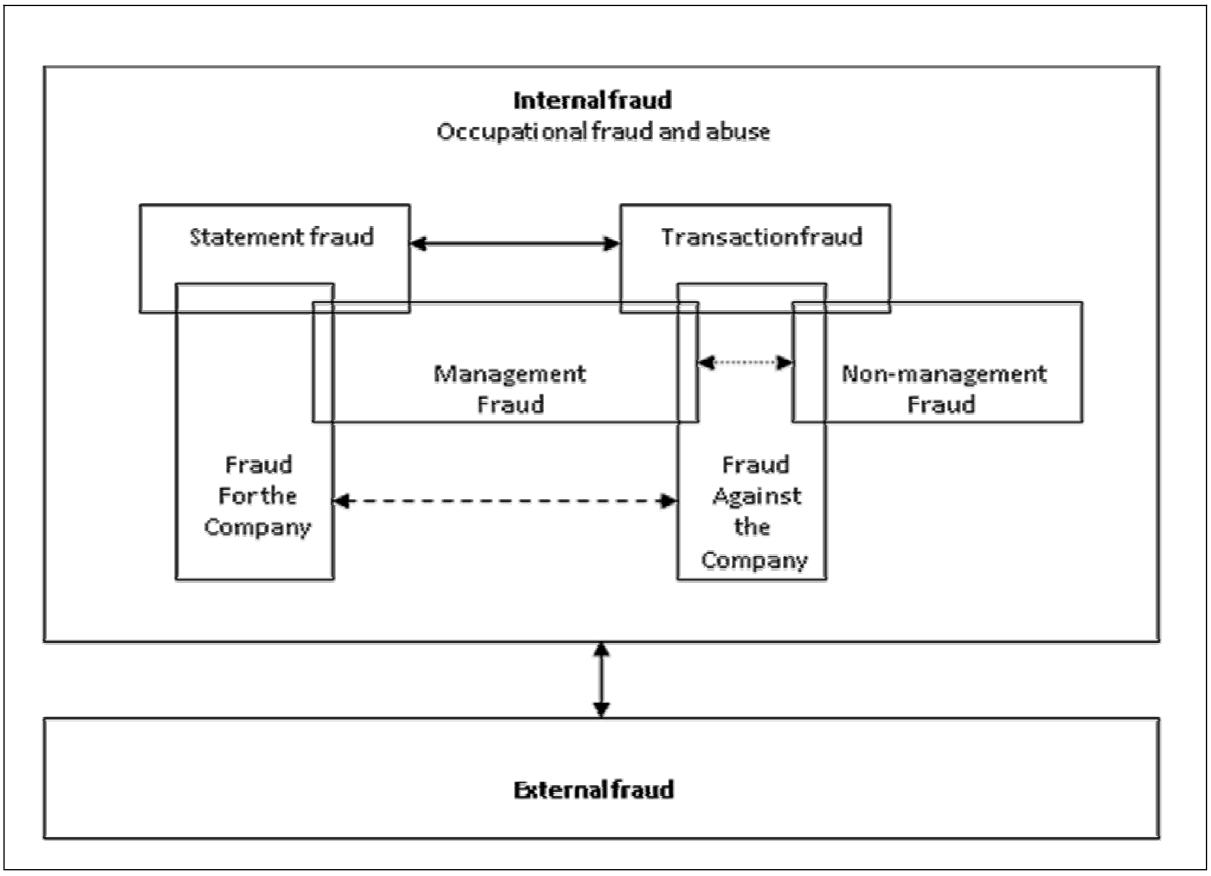
2.9.1 Fraud Classification

Bologna and Lindquist (1995) describe frauds in three main categories (a) internal fraud versus external fraud (b) fraud for the entity versus fraud against the entity, and (3) fraud committed by management versus fraud committed by other employees. Internal fraud versus external fraud is distinguished by the nature of the perpetrator in the sense that when a perpetrator is an insider to the deceived company, fraud is termed internal fraud (Bologna and Lindquist, 1995). This is different from a situation where a perpetrator is an outsider such as vendors or systems attackers, which will be called external fraud. According to Jans et al. (2009), internal fraud is similar to occupational fraud because the perpetrator has to be an internal party to the organisation in order to deprive his occupational trust. However, in some situations internal fraud has involved collaboration between an employee and an outsider such as a supplier or customer to fraud the company (Jans et al., 2009).

Fraud for versus fraud against the company can be distinguished by its motives. Fraud for the company has a motive to benefit the company while fraud against the company benefits individuals. Tax avoidance schemes or inflating earnings are examples of fraud for the company because their motives are not towards harming the company, rather to protect the existence of the entity (Jans et al., 2009). According to Bologna and Lindquist (1995), FSF are routinely committed by top management of the company because they have a direct access to FSs. On the other hand, fraud against the company involves a scheme to steal assets of the entity for personal gain. According to Jan et al. (2009), transactions fraud characterises structures for frauds against the company. According to

Davia et al. (2000), the key difference between FSF and transactions fraud is that in the former, there is no direct stealing of assets while in the latter there is. Similarly, AMF may likely lead to FSF in situations where management and top personnel were involved to commit AMF.

Management versus non-management fraud have been distinguished by the nature of the seniority of the perpetrator. According to Jans et al. (2009), management can commit both FSF and AMF while non-management employees can be restricted to only AMF/transactions fraud because they have no direct access to altering FSs. From this broad fraud classification, it is suggested that fraud is a complex issue and its examination in auditing perspectives needs boundaries (Jans et al., 2009). There are other wider categories of fraud which have not been discussed extensively by prior literature and are considered beyond the limit of this study for instance, fraud against the government (i.e. tax avoidance). The following diagram summarises fraud types more clearly.



Source**:** Jans et al. (2009)

Figure 2.1 Fraud Classification

According to Jans et al. (2009) in Figure 2.1, FSF and transactions fraud (AMF) are inter-related, which means that they might occur at the same time or one could result in the other. In some practices, transactions fraud has resulted in FSF where the culprits are part of the management intending to conceal their acts within FSs (Jans et al., 2009). Therefore, management can commit both frauds for and against the entity (Jans et al., 2009). Meanwhile, external frauds are categorised separately as a single set because they are complex and can involve multiple players.

2.9.2 E-fraud

E-fraud, also named as e-crime or online fraud (Lubua, 2014) is a subset of cyber-crime (Paula et al., 2016) that is defined as any illegal act that is committed through computer networks that can affect businesses/individuals when they have linked their information processes on web-based or the Internet (Kotb et al., 2012). E-fraud was also defined in the context of mobile transactions fraud as a deliberate action carried out by players in the mobile transaction ecosystem targeted to derive gain (in cash or e-money), and/or refuting other players revenue and/or damaging the reputation of other stakeholders (Mercy and Rafe, 2017). They pointed out the risk factors that make mobile money vulnerable to fraud and their corresponding fraud typologies to be product risk, channel risk, agent risk, customer risk, system risk and regulatory risk.

According to Simkin et al. (2015), e-fraud occurs due to weaknesses in computer systems where a particular weakness becomes well known to a few individuals who installed the system and hence have access to it; or those who constantly use the particular system for a long time. It was reported that inadequate internal controls systems to prevent data hacking, insufficient audit processes, deprived corporate control structures, inadequate fraud education to employees, and absence of whistle-blowing mechanisms are the fundamental contributors to e-fraud ecosystems (Mercy and Rafe, 2017).

E-frauds have cost businesses huge losses both in the developed and developing countries. In the US, e- fraud is estimated to cost businesses one trillion dollars each year (Simkin et al., 2015). In a report issued by PwC (2014) regarding global fraud, it was found that fraud statistics have been on the rise and fraudsters targeted mostly computerised sectors. The report further found that banks and other financial institutions were the most targeted sectors where the attackers were interested to steal cash and sensitive information by attacking the systems infrastructure of retail banks and stealing monies through technological tools. Similarly, ACFE (2006) reported businesses losing five percent of the total revenue each year due to fraud from both internal and external fraud. Similarly, a survey on businesses by PwC (2007) found businesses in the US suffered at least a loss of $2.42m due to fraud. The report further found that the extent of fraud loss was proportional to the size of companies. In other words, large companies suffered huge losses as compared to small companies.

The extent of external fraud occurrence has also been alarming. Telecommunication (telecoms), insurance and banking fraud (mostly credit cards) were among the common external frauds reported on the rise (Jans et al., 2009). Brockett et al. (1998) found 10% of all insurance claims were fictitious while the national insurance crime bureau (NICB, 2008) estimated that 20 billion worth of automobile insurance claims were fictitious. In the banking sector, a total of $10 billion cash was lost from visa and MasterCard worldwide (Bolton and Hand, 2002). Additionally, studies show that fraud has increased post millennium as compared to the past (Hua et al., 2008), a phenomenon that can be linked with the increased use of technology where multiple players to fraud can cause fraud incidences to upsurge (Simkin et al., 2015). Table 2.2 shows a highlight on reported fraud in the UK before and post millennium.

In developing countries, the Africa Cyber Security report found that Nigeria suffered the highest loss of $550 million, while Kenya suffered $174, Tanzania $85 million, Ghana $50 million and Uganda $35 million (Paula et al., 2016). The telecom industry in Kenya estimates fraud losses due to mobile wallet fraud to be around 2-3% of mobile money revenues each year. At the same time, phishing,

illegal SIM Swaps, identity theft, advance fee scams, false transactions, DOS attacks, and mobile money and agent malpractices are becoming common e-crimes in the country (Muchiri, 2016).

In South Africa, digital crimes (banking fraud) are constantly on the rise. Delinquents are surfacing in line with trends in technology which has resulted in an 'even cat-and-mouse game' between criminals and online security experts (Luke, 2018). Despite the fact that many banks are revitalising their apps, some complicated scams succeeds to penetrate security systems of many banks in South Africa and manage to commit fraud through various loopholes (Luke, 2018). This is an indication that traditional fraud detection mechanisms are still practiced in these African countries and which do not align with the speed of online culprits who increasingly evolve new techniques to commit fraud.

In the Gulf region, online culprits have committed fraudulent acts in e-banking, auction trading, and e-commerce to profit from illegal cash while plundering on low perceived knowledge and carelessness of online users and employees of organisations (Alanezi and Brook, 2014). Among all the countries in the Gulf region, Saudi Arabia had the reported largest rate of Internet penetration of 62% and also experienced the largest growing number of online frauds (Alanezi and Brook, 2014).. Nevertheless, little is known on how auditors are detecting such frauds to ensure that financial statements are free from material misstatements due to digital frauds.

Table 2.2 Frauds statistics in the UK for a period of 20 years from 1987- 2007

Source	**Fraud numbers**	**Actual figures in million**
KPMG (1997, 2001) reported fraud for period between 1987-2000	885	£4,177
KPMG (2004)	174	£329
KPMG (2005)	222	£942
Yirrell (2007)	277	£837

Source: Porter et al. (2008)

Table 2.2 shows that in a period of 13 years (1987-2000), a total of 885 fraud cases were reported, which is equivalent to 68 cases per year (885/13). If these number of cases are compared with the subsequent years (i.e 2000-2004), it would show an increase of 150% of fraud cases. Likewise, the

statistics from 2004 to 2007 in Table 2.2 reveals an upward trend in fraud cases. The interpretation of these fraud statistics is similar to that of KPMG (2006, pp.123), when they cited that "*fraud cases had worsened on post millennium and since then it has never gone down*". These fraud statistics suggest three important issues. First, fraud has a direct relationship with an increase in technology. In the 1980s towards 2000s, technology had not advanced as it had after the millennium. It is argued that as technology increases, the avenues for committing fraud also increase and so do the modes of committing it (Biestaker et al., 2001; Simkin et al., 2015).

Second, as technology increases, fraud prevention mechanisms become weak over time since the traditional techniques may not be applicable in computing business platforms (No and Vasarhelyi, 2017). Third, as technology increases, fraud detection mechanisms become weak over time, potentially due to a low technology usage to align with the pace of perpetrators. It therefore becomes imperative for auditors to adopt appropriate technological mechanisms to align with the nature of e-business processes.

Besides the frequency of fraud occurrences, what is more startling than the figures is the question of "who is committing fraud". Prior studies on fraud incidences in the corporate world found that most fraud incidences were occupational related, which involved accountants and top-level managements (Crites, 2008). According to Crites (2008), the level of accountants committing fraud was 30% while that of top-level management was 20% of the entire sample. In some incidences, fraud involved collaboration between IT experts and accountants to commit fraud. Similarly, a study conducted by Ernst and Young (2000) found that 82% of corporate fraud from the surveyed companies was committed by company employees. It was also found that the management of the companies committed 33% of the total fraud. A more recent study found that top-level managers committed 40% of large fraud cases in the UK with a value of £350 million (KPMG, 2006).

E-fraud was also found increasing in developing countries. A recent report from Kenya Cyber Security (KCS) found that e-fraud was on the rise and threatening investors in the banking sector and the economy of Kenya (Kigen et al., 2014). The report found that mobile banking fraud, which is one of the leading businesses in Kenya, had increased by 25%. Similarly in Tanzania, mobile banking fraud was found on the rise by 39% in a period of five years (Lubua, 2014). This makes it important for auditors to learn and be equipped with IT skills especially on how to detect fraud in this digital era (Braun and Davis, 2003; Janvrin et al., 2009; Simkin et al., 2015). According to Aminiria et al. (2015), strong detection mechanisms can act as preventive measures in the long run. This is possible because when perpetrators are aware that their acts will be discovered, eventually they will reduce committing the acts.

2.9.3 Modes of Committing E-Fraud

Hopwood et al. (2008) clarified five major modes of e-fraud commonly found in the computerised environment, namely, manipulation of input control systems, direct alteration of files, stealing data, disruption and alteration of programmes. Input manipulation can be committed by disgruntled employees by abusing their power to alter important settings and sometimes divert the IP instructions to some innocent people. At times, such employees can tap and modify accounting files and even tamper and divert audit trails to confuse investigation (Hopwood et al., 2008). According to Crites (2008), occupational frauds committed by IT experts may take long to be detected unless strong controls mechanisms are properly in place.

In manipulation of files which occurs in an accounting information system, normally, each employee is assigned a specific password or username credentials such that whenever they log in, a trace can be seen in terms of time, location, computer number and so on. However, there are IT fraud experts who can manipulate and alter the system by making changes within the file storage. Audit trails in such situations cannot be relied on because it will be difficult to detect any irregularities (Hopwood et al.,

2008). Meanwhile in stealing data, each company keeps valuable data and information which can only be accessible by a few top-level personnel. Such information could be in the form of a formula or marketing strategies that, if stolen, could create a huge loss to the company. However, there are insiders who can tamper with IT systems and steal such information. Audit trails regarding that information must be computer based because normal audit trails may not identify such a leakage of information (Hopwood et al., 2008). Similarly, sabotage may happen in the form of some files being deleted completely, alterations and or physical damage such as burning or stealing a whole system or even corrupting it. Normally, sabotage can destruct evidence of fraud. Any disgruntled employee can sabotage the company but according to Crites (2008), sabotage is mostly committed by top-level employees and management.

In alteration of programmes, fraudsters can attempt to alter the settings and programmes such as in payroll or accounts receivable settings. This is very common in insurance frauds where compensation can be made upon claims (Hopwood et al., 2008), even in dividend payments, when a particular amount needs to be paid on a specified period. When a programme has been altered from its source, traditional audit trails may fail to unveil the fraudulent activity. Besides many incidences of corporate fraud, e-fraud has taken several other forms. Newman and Clark (2003) conducted a study on e-fraud that were committed across the globe and identified different categories as shown in Table 2.3.

Table 2.3 Fraud in Computing Environment

E-fraud	Explanation
Electronic funds transfer fraud	They target information system and intelligence database of banks. Irrevocable transfer of funds, usually offshore, extremely difficult to prevent, especially when perpetrators typically use fictitious identities (Chapman and Smith, 2001).
Hacking	They target specific IS or intelligence. They are the greatest known computer crimes. Hackers have broken into bank systems in Los Angeles, the LA Police Department, Scotland Yard, etc.
Cross-border crime	They target customers. An example, Boy buys a DVD player on Amazon auction site, wires money to seller in Moldova. Never receives items. Finds out that many others have been victimised as well. Amazon partially reimburses victim. The auction website is a transitional target for the fraudster.
Credit card fraud	A cross-border crime, which targets customers by invading the credit card systems of any bank. An example, 2 Britons from Wales who hacked into e-

	commerce websites in the USA, UK, Canada, Thailand and Japan and stole credit card information of 26,000 accounts. (Wales, 1999)
Accounting fraud	Overriding information system fundamental to the computerisation of buying and selling of shares, buying and disbursement of fund by evasion of payment approval procedures, and several mechanisms that utilise opportunities surrounding the absence of paper trails in computerised records. The Enron and WorldCom scandals are instances of hi-tech accounting fraud.
Money laundering	Intrusion of the banking system by organised delinquencies, using electronic non-banks on transmission of illegal cash and cyber-banking, and many other refined techniques.
Denial of service attacks	An attack of services to the network of a company by means of throwing a virus into the systems. A malicious virus can target to bring down the company or steal cash from the company by confusing investigation.
Investment fraud	Fake banks that use the web as an intermediate target to set up fraudulent websites. These bogus companies promise to turn iron-ore rocks into gold, and many more. (Wyatts and Edward, 1999).

Source: Newman and Clark (2003)

The level of computer crime depends on the nature of loopholes and online products to steal.

In a developing country, the following categories of e-frauds were identified as shown in Table 2.4.

Table 2.4 E-fraud that were Reported in Kenya

E-fraud	Explanation
Insider Threats	Malicious activity committed by employees by probing systems for unapproved contact. They hack other user's access rights and break the systems for a variety of reasons including monetary gains and competition.
VoIP PBX Fraud	International call users: hackers increase unlawful access to the company's PBX phone system and make profits from calls that they make to international premium rate numbers, leaving behind huge debts for the company to pay.
Phishing	Attacks mobile banking agents and customers pretending to be genuine staff and prompting customers to reveal their personal details and passwords. If they attack many customers with huge amounts of cash, the liquidity situation of the bank could be affected.
SIM swap Fraud	Cleverly-organised syndicates involving Safaricom officials, M-Pesa agents and fraudsters. Fraudsters hack ID cards and SIM cards of subscribers by swapping their lines and steals huge sums of cash from multiple customers and agents.
Phishing Fraudulent	Fraudsters sending fake SMS to customers and agents of mobile money services pretending to be working from service providers companies. They hacked into Safaricom server and use the SMS alerts systems to send texts telling customers to send money so as to receive certain gifts or promotion tickets.
Mobile Money Fraud	Crimes on mobile phone banking customers. The fraudsters are too innovative and are very fast at finding loopholes in new controls implemented by merchants' banks and mobile company customers. If they attack many customers with huge amounts of cash, the liquidity situation of the bank could be affected.

Source: Kigen et al. (2014)

Studies conducted by Galetsas (2007) reported that businesses fail to report the actual crime figures in fear of losing public reputation, customers and prospective investors as they will perceive the company's security system as weak. Due to that fear, thousands and even millions of cash due to e-frauds have gone unreported, making companies stagnant in growth (Mercy and Rafe, 2017). However, the impact of e-fraud to a business could be severe. Some business harms might result into a general business collapsing, for instance, a virus contagion thrown onto the business systems could spread out to the major systems of a company, resulting in closure of the business and laying off of all employees (Newman and Clarke, 2003). As a result, huge economic stagnant will feature its way if multiple businesses are

affected. This is what the chairman of KPMG-Australia mentioned in his statement "*fraud in the computing platform, is a business risk rather than a technical risk. It can take away everything*" (KPMG, 2005).

2.9.4 The Role of Auditors in Relation to Fraud Detection

The role of auditors in detecting frauds is emphasised in the new standards such as ISA 240, ISA 315 and SAS 99 (see IFAC, 2009a; IFAC, 2009b, AICPA, 2006). The pressure for auditors to take fraud as one of their important responsibilities started a long time back in the late 1980s where 28 out of 30 savings and loans that filed for bankruptcy in the US, received clean audit opinions just before their filings (Wyden, 1995). Largely, the public was infuriated that the independent auditors were unaware of the financial indecencies and required the auditor to take a more pro-active part in looking at the FSs (Farrell and Franco, 1999).

Even more, the media, politicians and influential commentators played the role to enforce fraud detection as one of the important roles of auditors and that was mostly the pressure for setting SAS 82 (Farrell and Franco, 1999). SAS 82 required auditors to design and execute an audit to attain reasonable assurance about whether FSs are free of material misstatement due to errors and frauds. It marked the first time for AICPA to use the plain word "fraud" in its standards, contrary to the past when the more modest word "irregularity" was used (Farrell and Franco, 1999). SAS 82 further listed forty-one risk factors that can lead to FSF and AMF and required auditors to consider them when designing an audit plan (AICPA, 2002).

Similarly, in the UK, the minister for corporate and consumer affairs, Howard John Winston expressed a high expectation and trust by the public on auditors in the fight against corporate fraud, urging them to assume full responsibility in identifying fraud (Porter et al., 2008). The SEC Director in the US expressed a similar viewpoint when he indicated *"the commission*

looks at auditors to fight fraud. The commission with its limited resources must rely heavily on the accounting profession to perform its tasks diligently and responsibly. In short, auditors are the first line of defence (Walker, 1999; in Porter et al., 2008; pp.143). Thus, both IFAC and AICPA became the front-liners to preserve investors' funds from fraudulent activities and to restore the professional credibility. In 1988, the AICPA issued SAS No.53 'The auditor's responsibility to detect error and irregularities'. The role of auditors in relation to fraud was reinforced further when SAS 82 was issued as a revised SAS 53. Unlike SAS 53 which incorporated errors as well, SAS 82 dealt with fraud issues only as a matter of importance. The standard required auditors to adequately design the audit in a way that it can obtain a sound assurance that the financial reports do not contain material misstatements due to fraud. The standard further provided auditors with a list of possible fraud risk factors that may constitute a possibility for fraud to exist which includes incentives, opportunities and rationalisation.

In 2002, SAS 82 was superseded by a new standard, SAS 99. SAS 99 which is still in operation has widened further the level of auditors' role in fraud detection. The standard requires auditors to practise a professional scepticism (a questioning mind) whenever they are in any audit engagements. This requirement was not there in the preceding two SASs. According to Ramos (2003), *"SAS 99 requires auditors to consider abundant extended grounds of techniques to detect fraud. They will collect evidence and contemplate a lot more information in assessing fraud risk than ever before. There is a potential turning point of how auditors think and perform an audit*". (Ramos, 2003 as cited in Porter et al., 2008 pp.165). The expanded role of auditors in SAS 82 and subsequently SAS 99 is what was referred to by Wyden (1995) as "*putting well-armed auditors back where they belong."*

On the international arena, in 2001, IFAC set ISA 240 'fraud and error' which was revised in 2004 *'Auditor responsibility to consider fraud in an audit of FS'* which is closely similar to SAS 99 (AICPA, 2002). The standard:

(a) Sets the limits for fraud detection and puts the prime responsibility to the management but provides auditors with requirements to clearly plan the audit in such a way that if significant fraud has been committed by the management, auditors should have a likelihood of detecting it unless it has been cleverly well-concealed.

(b) Requires auditors to plan, perform and evaluate their audit work in order to have a reasonable expectation of detecting material misstatement due to fraud.

(c) Provides circumstances conducive for fraud to happen, also referred to as fraud risk factors, namely incentives or pressure, opportunity and rationalisation.

(d) Emphasises on professional scepticism at every stage of the audit. The standard requires auditors not to rely on the past integrity of behaviours of individuals but rather to continuously focus on professional scepticisms on the possibilities of material misstatements due to fraud (para.12-14, A7-A8)

(e) Requires audit teams to discuss situations on each possible grounds especially on how and where the auditees' financial reports could be prone to fraud and the possible forms of fraud occurrences. During their discussion, the standard urges auditors to consider the possibility of management involvement in the process of concealing fraud including the top-level management (ISA 240 para.15).

One important point to note in the standard is para 11A which requires auditors to consider how and where the company's FSs may be susceptible to material misstatements due to fraud, how management could perpetrate and conceal fraudulent FSs and how the entity's assets

could be misappropriated. The fact that AMF can be both physical and intangible assets suggests that the role of auditors in the computing business platforms cannot be narrowly conceived (Flint, 1988). Indeed, e-business systems have changed the entity's risk profiles and augmented prominence of security and system reliability as these might threaten the going concern of the entity (Kotb and Roberts, 2011). The fact that fraud risk in computing platforms consists of multiple players with complex modes of occurrences means that auditors must be equipped with techniques and tools to assess system infrastructure risk, application risk and business process risk (Kotb and Roberts, 2011). This also means that auditors must check the systems that process information, network security, encryption, firewalls, digital signatures and password validation (Kotb et al., 2012). It is argued that if traditional audit methodologies continue to be used to audit computerised clients, significant risks may go undetected (No and Vasarhelyi, 2017). This calls for the need for audit change, skills change and the use of IS tools and techniques in the audit processes for effective risk assessment in the digital business environment (Kotb et al., 2012; Kotb et al., 2013).

2.9.5 Is Identifying E-fraud the Role of Auditors?

E-fraud as used in this study is any fraud occurring through digital means. In other words, it involves fraud in the e-business world that cannot be seen by the bare eyes and has multiple modes of occurrences. As noted in the earlier sub-sections, fraud in its totality, irrespective of its mode of occurrence (whether online or offline), is an illegal act that can be committed by one or more individuals, and for the act to be called fraud, it must be intentional (IFAC, 2009a). Furthermore, ISA 240.2 describes fraud, which falls within the role of auditors by stating that *"it should have impact on material misstatement in the FSs"*. However, the standard does not differentiate between fraud occurrences or the timing of the act (i.e electronic or traditional) and this is because audit objectives are still the same whether the

entity conducts its economic activities in the electronic environment or manual systems (Biestaker et al., 2001). Hence, this suggests that some e-fraud falls within the category of ISA 240 (for example, deletion of an account in a bank in order to steal cash for an entity or an employee fraudulently creating a fictitious account so that he/she can steal cash of the entity).

Meanwhile, other e-fraud falls under the classes of risks identified in ISA 315.32A known as business risks (IFAC, 2009b). In principle, business risks are those that may adversely affect the entity from attaining its objectives. For example, an incompatible IT process that might result in potential risk in business processes such as a fault in the entity's payments system can result in the loss of major customers of the business through credit card fraud. The nature of e-fraud (i.e. credit card fraud, DOS, hacking, mobile money fraud, etc.), can result in adverse effects on several customers, causing liquidity problems to the company. Hence, the literature and the contents of the ISAs suggest that ISA 240 and ISA 315 can explain well the link between e-fraud and the role of auditors.

Furthermore, e-fraud can have both audit risk and business risk consequences. By definition "*Audit risk is the risk considered at assertion level when the auditor expresses a clean audit opinion that FSs presented a true and fair and they do not contain material misstatements when in fact there is at least one or more items of material misstatements as auditors might not have detected a material error or fraud during the audit process (Knechel, 2001; CICA; 2003).* Hence, audit risk is a combination of detection risk, inherent risk and control risk (IFAC, 2009c). Detection risk is the chance that an auditor will not find material misstatements relating to an assertion in the FSs of an entity through substantive tests and analysis. In other words, detection risk will make an auditor to conclude the absence of material misstatements when in fact there are (ACCA, 2012). Inherent risk is the risk caused

by an error, fraud or any omission in FSs due to a factor other than a failure of control. In a FS audit, inherent risk is most likely to occur when transactions are complex or in situations that require a high degree of judgment with regards to estimations and disclosures (CICA, 2003). Control risk is the probability that a material misstatement exists in an assertion for the reason that either a misstatement was not prevented from entering the entity's financial information or it was not detected and corrected by the internal control system of the entity.

Meanwhile, business risk is the risk facing the company from achieving its objectives. ISA 315.4 defines business risk as '*the risk resulting from significant conditions, events of circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives'* (IFAC, 2009b). A list of these risk categories are shown at the end of Appendix in ISA 450. Three of them are identified as most relevant for this study, namely (1) going concern and liquidity issues including loss of significant customers (2) inconsistencies between the IT strategies of the entity and its business strategies and (3) changes in the entity's IT environment. The nature of e-fraud largely involves taking away assets of the entity (mostly cash), hence, making AMF more dominant in the e-business environment (Cosserat, 2004). Besides that, e-fraud has involved third parties like systems hackers and intruders, making the impact of e-fraud beyond AMF to include threatening the whole business survival. Hence, most e-fraud falls under business risk because they might threaten both the company's survival, customers and the economy at large (Newman and Clarke, 2003).

Henceforth, e-fraud can be embedded within either audit risk or business risks but largely embedded within the business risk category. This is why Power (2000) views the role of auditors as a more complex role contrary to what outsiders perceive it as merely 'giving their opinions regarding FSs'. Before giving their opinions, auditors go through several checks,

tests and procedures to confirm the absence of harm or any possible intentions to harm the well-being of the entity (Bagranoff et al., 2007). The process of checking the entire systems of the company and identifying possible threats embedded within the systems is what is known as risk assessment (Hunton et al., 2004). During risk assessment, auditors check the authenticity of both IT general controls and application controls.

IT general controls are those that apply to all systems components, processes, and data for a given organisation or IT environment (Hunton et al., 2004). The objectives of IT general control are to ensure the proper development and implementation of applications, as well as the integrity of programmes, data files, and computer operations (Bagranoff et al., 2007). On the other hand, application controls are controls over the input, processing, and output functions. They contain items such as guarantee to the accuracy, validity and completeness of input data; and confirming the internal processing yields the expected results (Hunton et al., 2004).

2.10 Various Techniques and their Impact on E-fraud Detection

Mooney et al. (2000) reported a list of IS tools that can help auditors to perform a variety of tasks including e-fraud detection. However, fraud identification, particularly internal fraud is perceived as a judgemental task that can involve both a suspicious ground and insider's information (Sacks, 2014). To further understand the mechanisms to control internal fraud, the association of fraud examiners (ACFE, 2006) recommends that auditors use the fraud triangle for corporate occupational frauds. Other mechanisms include chances, tips, and reliance on strengthening internal control systems. Similarly, prior researchers have recommended CA methodologies and other data mining techniques. These mechanisms and approaches, including potential weaknesses and impact on e-fraud detection are discussed in the next sub-sections.

2.10.1 The Fraud Triangle

The fraud triangle model (Cressey, 1973) proposes that fraud incidences occur in the presence of three main factors, namely motive, rationalisation and opportunity. Motive is the most aggressive factor that makes someone steal, which can range from personal reasons as well as group motives. Social class fitting or family problems may cause one to steal without thinking twice of its implications (Skillicorn and Vats, 2007). Rationalisation is the determination within oneself, which creates a feeling that stealing is a normal act (Jans et al., 2009). Meanwhile, opportunity is the availability of power to steal from among the resources available within someone's reach and supervision. Opportunity to commit fraud has also included self-assurance of not being detected. One important influence under opportunity to steal is the assurance to conceal fraud with the anticipation that nothing bad will happen at least for a certain period of time (ACFE, 2006). Hence, understanding the fraud triangle is considered an important step in detecting fraud, irrespective of the mode of occurrence (ACFE, 2006, Jans et al., 2009). The fraud triangle was also considered as a behavioural analysis technique to fraud detection as it involves learning the behaviours of individuals working for the organisation (Stanton, 2012).

In using the fraud triangle as a detection tool, Skillicorn and Vats (2007) suggest for auditors to consider the following questions; (1) how would an employee rationalise committing a fraud? (2) Are there strategies within the organisation that promotes ethical behaviour? (3) Are there possibilities for collusion among employees in committing fraud? (4) Were incentives offered for one to commit fraud? Generally, the fraud triangle can show auditors some clues for fraud to occur. However, studies have argued that identifying management fraud can be very challenging especially with the use of ordinary audit procedures since there is knowledge deficiency regarding the features of management fraud (Kotsiantis et al., 2006).

Although the fraud triangle model is a predominant framework in understanding fraud occurrences and fraud risk factors, it falls short of empirical validation on its effectiveness (Boyle et al., 2015). Furthermore, Kotsiantis et al. (2006) enlightened that most auditors lack sufficient experience that is essential to facilitate them to detect fraud as managers could intentionally attempt to mislead auditors. Hence, it becomes crucial to realise innovative and enhanced mechanisms to discover and deter fraud specifically in computerised platforms.

2.10.2 Chances, Tips and Internal Control Mechanisms

A study by PwC (2007) reported chance mechanisms as fraud detection tool. The report found that insider information and whistle-blowing had substantially helped several companies to receive tips regarding fraudulent activities, mostly internal fraud. Likewise, ACFE (2006) suggested that companies install anonymous hotlines for receiving calls and tips following fraudulent events that had already happened or are about to take place. In their survey, they found a 50% median reduction in fraud losses for companies that had installed anonymous hotlines as compared to those that did not install them (ACFE, 2006). In other words, those companies that did not have any hotlines suffered substantially higher median losses. A recent PwC survey found that anti-fraud controls were the most successful detection techniques that exposed 19% of frauds, followed by tips and whistle-blowing which uncovered 16% of internal frauds (Brian, 2018).

In contrast, a study by Ernst and Young (2006) that surveyed company representatives regarding fraud detection mechanisms reported in favour of strong internal control mechanisms as the key determinant in fraud detection. The study reported in favour of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework of 1992. The study praised the COSO as the single most effective internal control system due to its requirements that defines internal control in the form of three main features, namely (1)

value and efficiency of the procedures (2) consistency in financial reporting and (3) agreement with applicable principles. The applications of the three identified features were contended to have a higher possibility in curbing both transactions fraud and FSF (Jans et al., 2009). Hence internal control has been relied on both as a tool for prevention and detection of fraud (Ernst and Young, 2006). However, a recent survey found that internal audits had detected only 15% of the total fraud, slightly below behavioural techniques such as tip-offs and whistle-blowing (Brian, 2018).

To sum up, the most widely used measures to detect fraud are tips, chance, inside information and reliance on internal control systems. However, technical researchers in auditing have critically argued contrary to relying exclusively on these mechanisms (Jans et al., 2009). For instance, tips and insider information could not be fully reliable in the long run, the reason being that tips are more inclined to corporate culture or society. As a result, it may not particularly be predicted in most business environments. Consequently, it cannot be used as a permanent technique in fraud detection. Contrary to over reliance in internal control systems to detect fraud, Jans et al. (2009) and Skillicorn and Vats (2007) argue further that since the same people who design the system can decide to override it, it makes the whole process of fraud detection a complex issue. Especially, in the technological environment where multiple players to fraud can be involved, a combination of approaches needs to be instigated to include CA and data mining techniques. These techniques are also supported by other researchers in audit technology (Cosserat, 2004; Alles et al., 2008; Jans et al., 2009; Amirinia et al., 2015; No and Vasarhelyi, 2017). The following sub-section discusses CA and data mining as detection tools for fraud occurring in the e-business environment.

2.10.3 Continuous Auditing (CA)

CA was mentioned among the five top most emerging technological concerns for 1999 requiring audit practitioners to consider during FSs audits in the e-business environment (Helms and Mancino, 1999; Cosserat, 2004). CA is defined as a mechanism that can allow independent auditors to conduct audit of FSs instantaneously after the transaction has taken place and issuing reports on demand (Chiu et al., 2014). Hence, CA is a computer-based audit that uses advanced computerised-based techniques to perform the audit in real time (Alles et al., 2004; Alles et al., 2008). Both internal and external auditors can perform CA but in a situation where clients are concerned about giving sensitive information, CA can be done internally by involving internal auditors (Omoteso et al., 2008; Gonzalez et al., 2012; Sun, 2012).

Prior studies contended CA as an appropriate technique in modern auditing due to its duo capability to act as a detective and preventive mechanism in protecting the entity's information (Omoteso et al., 2008). As a detective tool, CA can perform tasks similar to verifying 'historical' records by looking for audit evidence during the audit process. Similarly, as a preventive mechanism, CA acts as a block to the existence of errors and fraud by applying various IS tools and techniques including artificial intelligence technologies to function as Continuous Intelligent Online Validation (CIOV) (Omoteso et al., 2008).

In the use of CA to control fraud, Alles et al. (2004) proposed the use of a black box (BB) log file which would be available in the form of read-only memory (ROM) organised by a third-party (i.e. an independent auditor). The BB would be recording actions, communications and interactions between auditors and the management particularly in respect to their choice of audit metric and models. Meanwhile, Varsahely and Halper (1991) proposed the CA methodology to audit in a paperless environment using various modern technologies. The

model was tested at AT&T laboratories and proved efficient in producing instant, accurate results. Similarly, Rezaee (2002) suggested building automated auditing capabilities by using GAS, Extensible Continuous Audit Language and intelligent agents to effect CA application. Meanwhile, Onions (2003) recommended a CA paradigm on debt covenant through a web-based technology; and Shaikh (2005) proposes the use of generalised audit software over the Internet (GASI) in auditing a loan account in a bank. He argued that GASI is an easy to use technique and Certified Public Accountant (CPA) auditors need not rely on IT specialists.

The main barrier to conducting CA is the cost implication that investors may not be ready to pay (Omoteso et al., 2010). Irrespective of the costs issues, CA is the single most technique that researchers in audit technology have come to conclude as the solution to maximum risk assessment in the e-business platforms (Rezaee at al., 2001; Alles et a., 2006; Omoteso et al., 2008; Varsahelyi and Romero, 2014; No and Varsahelyi, 2017). However, the adoption of CA methodologies at the global level found a majority of adopters to be in emerging CA stages and few at maturity but none had reached full CA stage (Varsahelyi et al., 2012)

2.10.4 Data Mining Techniques

Data mining is a procedure which uses arithmetical procedures with the help of artificial intelligence and machine-learning techniques to select and distinguish valuable information and consequently, gain understanding of the patterns in a large digital databank (Carminati et al., 2015). According to Ngai et al. (2011), the data mining technique can enable auditors to be sure of the intention behind a fraudulent transaction by finding sufficient indications of fraud from the existing data using particular scientific data processing procedures.

Data mining is defined as ‘a process of discovering patterns from a substantial quantity of data automatically or at least semi-automatically by converting the patterns into meaningful

results which can lead to fraud detection (Almeida et al. 2009). The critical objective of employing data mining to fraud detection is to generate a model that can tag a record, an individual or an enterprise as being deceitful. This is because data mining techniques have advanced taxonomy and ability to forecast events and occurrences as being fraudulent or not (Kirkos et al. 2007).

There are three main data mining algorithms, namely (1) decision trees technique (DTT), (2) neural networks (NN); and (3) Baysian beliefs networks (BBN). DTT is a tree-like arrangement of main and sub-branches through a point of intersection known as a node. These trees can be established through machine-learning systems of main and sub-attributes. The main attribute (i.e. node/branch) signifies an assessment on the attribute and each sub-branch denotes the outcomes of the test (Stanton, 2012). The arrangement is then used to categorise a formerly invisible item by inspecting the quality values against the splitting nodes of the decision tree. The items of the nodes can be in the form of sales figures against expenditure, debt to equity ratio, total assets to liabilities and so on (Kirkos et al., 2007). The main advantage of decision trees is that they offer an understanding of the cause and effect of a fraudulent event in form of '*IF-THEN'* taxonomy (Stanton, 2012). Decision trees are commonly utilised in credit cards, car insurance and company frauds (Ngai et al., 2011). Prior studies reported the accuracy rate of applying DTT to be 73.6% in classifying FSF (Kirkos et al., 2007) and 90.6% accuracy was found in identifying high-risk companies (Amirinia et al., 2015).

Meanwhile, NN is a system that auditors can use to identify fraud through a system of inter-linked processing units or neurons. Each link in an accompanying item is assigned an arithmetical value known as "weight", which is summed-up after receiving signals from other connected neurons (Kirkos et al., 2007). The neurons send alerts if the combined feedback

signal strength goes beyond a specified threshold. The key benefits of NN are that they can handle inconsistent data and are suitable alternatives for ambiguous specification problems (Ngai et al., 2011). Studies found that the use of NN in classifying FSF had high accuracy values of 80% (Kirkos et al., 2007).

The last cluster of data mining is the BBN. BBN is technology-based fraud detection through a Bayes law, which measures a degree of beliefs for an event to be categorised as fraudulent or not (Kirkos et al., 2007). The Bayes law is based on a list of conditional dependencies between subclasses of aspects using a directed compounded graph (DCG). In the DCG, each node signifies random variables and omitted boundaries encrypting a conditional independent variable (Ngai et al., 2011). BBN is mostly adopted in credit card, insurance and corporate fraud detection by permitting a depiction of dependencies among subsets of attributes tested on a large cluster of data (Ngai et al., 2011). The use of BBN reported the accuracy of classifying FSF by a large margin of 90.3% (Kirkos et al., 2007).

Ngai et al. (2011) conducted a study related to financial fraud detection, particularly the application of data mining techniques. Through gathering data from 49 articles available from 1997 to 2008, the study established four common categories of online fraud, which were (1) bank linked financial fraud (2) indemnity based fraud, (3) fraud in shares and bonds, (4) extra financial related frauds. It was also reported that logistic models, NN, BBN and DTT were the most dominant data mining techniques used in detecting insurance and credit card fraud.

Similarly, Sharma and Panigrahi (2012) found that BBN, decision tree systems and NN were effective means in detecting accounting frauds. Meanwhile, Amirinia et al. (2015) found that among all the data mining techniques, NN were the best approach in detecting fraud in high-risk companies with 90.6% detection accuracy. For credit card fraud, Zareapoor et al. (2012) proposed a fraud detection model called Certain Design Criteria which can detect credit card

fraud from a large cluster of users. Meanwhile, for online banking frauds solution, Carminati et al. (2015) proposed a banksealer support scheme which uses data mining techniques to help auditors in identifying anomalies within customers' transactions. *"A Banksealer is a method which uses a mixture of cutting-edge data mining and arithmetic techniques to rank digital-based transactions according to their risks of being fraudulent"* (Carminati et al., 2015, pp.176). Through inserting the software to monitor daily customer transactions, the techniques were proved to be 98% accurate in fraud detection (Carminati et al., 2015).

In curbing internal occupational frauds, Boyle et al. (2015) proposed a fraud diamond model in dealing with internal CEO frauds. The model uses algorithm and machine learning to detect occupational fraud. Meanwhile, Jans et al. (2010) proposed the internal fraud risk (IFR) reduction model. The model can curb IT related frauds that are common to business segments with frequent large cash flows and a known history of occupational frauds. The model extended the fraud triangle elements (Cressey, 1973), particularly the opportunity to commit fraud in an IT environment. A descriptive rather than a traditional prediction data mining was presented in the model with multivariate latent clustering algorithm. The practical trial of the model proved 98% accuracy in fraud detection within one of the top 20 banks in Europe (Jans et al., 2010).

Likewise, Van-Vlasselaer et al. (2015) proposed the APATE model, an automatic e-fraud detection mechanism and a solution to credit card fraud. The model detects fraud in two ways, namely (1) identifying anomalies by tagging customer-spending history and (2) by using online network-based characteristics to tag the time used in the suspicious transaction. The findings of the model test reported effective results by a wide margin of 98%.

2.10.5 Forensic Audit

Popoola et al. (2014) suggest the inclusion of forensic auditing knowledge, skills and mind-set to auditors following the increase in e-fraud, money laundering and terrorism financing. Forensic auditing is an IS based tool which can assist auditors to investigate the causes and effects of a potential fraudulent event or systems interruptions that could lead to the significance of intentional activities to fraud the entity (Popoola et al., 2014). Forensic auditing encompasses the detection and recovery of electronic information that was purposefully erased (Cosserat, 2004). In conducting forensic auditing in the computerised environment, an auditor might be required to use part of the forensic audit procedures including linking e-mails of workers, their user names and log-in-times, probing for duplicate transactions on receipts and payments, scrutinising the order of transactions to ascertain any unlawful involvement; and skimming lists of providers, customers, and movements of merchandise (Cosserat, 2004).

Similarly, forensic audit can involve the use of emails and social media to trace communication between the suspected culprits by tagging the emotional state of the sender when composing the message (Keila and Skillicorn, 2005). It is suggested that the use of verbs such as 'I, we and my', would indicate that the sender was associated in the act. Meanwhile, the use of verbs such as 'except, but and without' could suggest a fictitious story as fewer of such words imply 'a lesser cognitive complex story' (Keila and Skillicorn, 2005). A fictitious story would further suggest a guilt sub-consciousness sensed by the culprit hence providing a clue on the possible involvement in the committing of fraud (Stanton, 2012).

In a recent study, Jans et al. (2010) identified fraud prevention and detection mechanisms in e-business platforms. The study recognised the most used techniques in detecting both internal and external fraud. However, they mostly related to external fraud and the use of data mining

techniques. A summary of the literature on detection techniques and the type of e-fraud are listed in Appendix III. It can be seen from the Appendix that all the studies were on detection mechanisms, except Fuzzy rules which have both detective and preventive measures (Sanchez et al., 2009; Estevez et al., 2006).

Meanwhile, fraud prevention is argued as a technical task to perform, hence, the literature suggests that strengthening detection mechanisms can act as preventive measures of fraud in the long run (Boyle et al., 2015). Therefore, studies conducted by Jans et al. (2009) and Ngai et al. (2011) highlight three important points, namely (1) most academic studies focussed on external fraud as compared to internal fraud which might suggest that external fraud is complex due to possible involvement of multiple players, (2) FSF was found to be not the number one fraud category, rather transactions fraud was; and (3) the commonly used technique in fraud detection was data mining. The use of data mining as a detection method is contrary to the suggestions in the audit literature which stress on internal control systems that do not include technological tools (No and Vasarhelyi, 2017). Hence, it was suggested that a consideration within the audit standards be made mandatory to use technological mechanisms because fraud detection can involve more than one technique (Jans et al., 2009; 2010).

However, the limitation noted by this study is that all the mechanisms to detect e-fraud are silent of mobile banking fraud which is currently on the rise among many developing countries in Africa including Tanzania (Rumanyika, 2015; Paula et al., 2016). Regardless of the fact that most literature on e-fraud detection is from the developed countries, this situation leaves a gap for technology vendors and academics in audit technology. It was reported that mobile banking fraud is a threat to users of banking services and also to the growth of businesses in many developing economies (Paula et al., 2016). There is need for audit plans and specific tools to audit these products and to detect fraud in these platforms at the early

stages before the harm multiplies. However, contrary to advanced tools for fraud detection, other studies suggested simple technological tools to detect fraud and also to automate audit functions. The tools are listed below in Table 2.5.

Table 2.5 Software that Can Assist Auditors to Perform Different Functions

Software that supports fraud detection and fraud management	Software that supports automation and audit functions
ACL;	**PANEL A**
IDEA;	ADM Plus; Audit Leverage;
Financial Crime Investigator;	Audit Master Plan
WIZ Rule;	Auditor Assistant; Auditor's Software Toolset;
DATAS for IDEA;	Auto Audit SE; Auto Audit 2000; Expert choice;
The Analyst's Notebook;	Management Audit Ltd; Pentana Tracker;
Veris Social Security;	Pinpoint; Work Force 2.0
Number Validation Services;	**PANEL B** (security checking tool)
SSNDTECT;	i. Active Security
Auto Fraud Investigation	ii. Consul/Enterprise Audit+ Audit
	iii. Database Scanner
	iv. Internet Scanner
	v. System scanner
	vi. Real secure
	vii. Netre con
	viii. Ps Audit

Source: Mooney et al. (2000)

2.11 The Adoption of IS tools in Auditing in Developing Countries

The literature review suggests that the use of IS for audit purposes is still a new phenomenon for most developing countries and even less technological tools are used to detect e-fraud. This is because most developing countries are late adopters of innovation while their developed countries counter-parts are the pioneers of any new technology that becomes available on the market (Miah and Omar, 2012). Cost-benefits factors and macro-economic infrastructures have contributed to slow adoption of new innovation to many developing countries (Miah and Omar, 2012). This is also true with the case of IS usage in auditing.

The literature review search from standard journals shows that few studies in developing

countries have examined the adoption of IS tools and techniques in the audit environment (see Appendix I-B). While the Middle East and Asian countries have slightly been explored, only three African countries have been studied on this area, namely Egypt (El-Sood et al., 2015; Kim et al., 2016), Nigeria (Ebimobowei et al., 2013) and Zimbabwe (Nugi, 2011). Even then, for Zimbabwe, the study is more on critical review of challenges and opportunities for IT audit adoption and not an empirical study. The remaining discussion shows a glance of literature on technology usage in auditing for the Middle East, African countries and Tanzania in particular.

In the Middle East, Saudi Arabia is the leading adopter of Internet with a penetration rate of 62% (Mansour, 2016). It is reported that the Saudi government and Saudi organisations have advanced steadily in the use of technology into their economic dealings and business processes (Al-Fehaid, 2003; Abu-Musa, 2008; Razi and Madani, 2013; Mansour, 2016). Meanwhile, the pace for IS usage in auditing was reported as low due to various factors which are mostly related to organisational readiness. Razi and Madani (2013) found that external pressure had no impact on the adoption decision of audit technology among Saudi organisations rather, organisational factors and perceived benefits were found to be reasonably good predictors of IS adoption intentions. Similar findings in Saudi Arabia revealed that internal auditors lacked sufficient expertise to assess IT-related risks due to lack of perceived benefits by firms' management to involve internal auditors in system development and acquisition issues (Abu-Musa, 2008). The lack of inclusiveness potentially resulted in low perceived benefits of using technology, hence, leading to a slow adoption of IS tools.

Meanwhile, in the external audit environment in Saudi Arabia, a few variations on motivation for technology adoption were reported. The most significant factors for audit technology

usage were sufficient qualified audit staff to audit computerised clients, suitable audit methodology and the strength of internal control measures in the auditees' systems (Al-Fehaid, 2003). It was further reported for a possibility of increased audit risk in IT environment due to adoption of IT-based accounting systems by audit clients. The authors suggested the need for audit clients to increase training of staff on IT-related risk, upgrading the accounting systems and also to strengthen the internal control measures (Al-Fehaid, 2003). This is also consistent to establishing a deterrent mechanism with prevention, detection and remedy to online fraud through a General Deterrence Theory (GDT) that involved various stakeholders of online services (Alanezi and Brook, 2014). It was contended within the GDT if applied appropriately, it could reduce online fraud from individuals as well as organisations in Saudi Arabia.

In other parts of the Middle East (Jordan), researchers validated the UTAUT to understand individual factors for CAATTs adoption (Mansour, 2016). The study findings revealed that performance expectancy and firm's facilitating conditions influenced CAATTs adoption decisions. The remaining UTAUT variables (social influence and efforts expectancy) were found not to be statistically predictors for CAATTs usage. These findings were totally the opposite of the most recent findings on GAS usage among Egyptian audit practitioners (Kim et al., 2016). It was reported that perceived ease of use and perceived benefits highly influenced GAS usage. It would be expected that since the two countries (Jordan and Egypt) have similar cultural environment, the results could be the same. These inconsistent findings suggest further research is needed to validate the UTAUT in other developing countries.

Meanwhile, in Asian countries (Malaysia), two studies predicted TOE and I-TOE factors to explain the adoption of CAATTs by internal auditors and external auditors respectively (Ahmi et al., 2014; Rosli et al., 2013). In the lens of increased e-business and e-government activities and processes, the scholars explored the technology-based auditing practices to align

with the nature of increased automation in accounting and reporting. They predicted that for a smooth adoption of IS in audit practices in Malaysia, clients-related factors, competition, auditing oversight factors as well as individual and organisational factors are important. However, the two studies proposed hypothetical models that are yet to be empirically validated.

In another study, the impact of IS on internal auditing practices among SMEs in Malaysia was examined (Moorthy et al., 2011). Five key areas that IS impact internal auditing processes were identified; namely, control environment, risk assessment, control activities, information communication and monitoring. The findings revealed that IT had totally changed how data are being processed and stored from manual to electronic data processing and urged internal auditors' responsibility must increase to ensure that management understands the risks caused by IT in delivering strong internal control measures.

Meanwhile in Taiwan, the adopted TAM behavioral model revealed that the usage of GAS in internal audit environment was minimal (Huang et al., 2008). Reasons related to the high cost of implementation and long-learning curves highly affected the low usage of GAS. A similar study in Taiwan revealed that system functions, data processing, and technical support from vendors were the significant factors for CAATTs usage (Lin and Wang, 2011). However, the selection of efficient audit software was dependable on the cost of the system, its stability, data processing accuracy, and technical support from vendors. These differed findings reported from the same country suggest inconclusive results on possible motivating factors for IS usage in audit practices.

A more recent study on GAS usage by audit practitioners in Indonesia revealed that all the Big Four firms and 43% of mid-tier firms used commercially available audit software, mostly ACL or IDEA (Widuri et al., 2016). In addition, office-related applications (Microsoft Word

and Excel) and In-house software were also reported. As for what influenced the usage of GAS by external auditors, the study documented environmental factors to be highly influential on GAS usage such as availability of IT-skills in the market, clients' related factors, support from professional regulatory authority and availability of GAS in many languages. Similarly, the motivation for adoption of cloud-based services among Indian firms was found to be easy to use interface, experience, expertise of the cloud service provider and support from top management (Lal and Bharadwaj, 2016).

In Africa, studies have reported businesses in Botswana adopting e-business and the government going fast into e-government while education institutions adopting e-learning platforms (Nugi, 2011). Irrespective of the fast IT adoption, the assurance services from the financial audit perspective were reported as sluggish. The main reason was insufficient IT audit expertise for both private and public sectors. Several on-going strategies by the governments of Botswana and the Big Four Audit firms were concerned in funding CPA training and conferences in addressing IT challenges to the auditing profession (Nugi, 2011). IT audit methodology is important in assessing the controls risks in digital audit engagements (Omoteso et al., 2010). Subsequently, a public-private partnership was proposed in uplifting the ICT knowledge by sponsoring auditors to study IT-audit techniques.

Meanwhile, in Egypt, the perceptions of the usage and importance of IT audit tools were examined by involving both the Big Four and Non-Big Four international audit firms (Al-Sood et al., 2015). The findings reflected a highly perceived importance of using audit technology in technical and administrative procedures, specifically, to assess fraud risk components in the clients' IT systems. Firm-tailored audit software, Microsoft Office, ACL, IDEA, Communication tools and Infrastructure tools (wireless and remote network) were the reported IS tools used by the selected audit firms (Al-Sood et al., 2015). However, the

importance of audit technology was relatively higher for those in the Big Four firms, as compared to auditors from the Non-Big Four firms.

Likewise, a study in Egypt documented perceived ease of use as the most significant factor for GAS usage (Kim et al., 2016), while co-worker, supervisor, or organisational factors through perceived usefulness were also significant predictors. These findings are consistent to Ebimobowei et al. (2013) in the Nigerian context where the UTAUT variables were significant predictors for CAATTs usage. Irrespective of inconsistent findings reported from developing countries, it can be concluded that for smooth IS adoption in auditing, both internal and external factors are important.

The literature review search from audit technology journals shows that Tanzania is less represented in this area. However, a glance of IS usage is provided by Lotto (2014) regarding the impact of technology on internal auditing effectiveness. Through a purposive sampling which targeted internal auditors from organisations that had integrated technology into their business processes, it was revealed that the internal audit practitioners in Tanzania lagged behind in effective use of IT to support their duties (Lotto, 2014). Factors which contributed to the hindrance in IT usage included lack of top management support which was referred to as 'a *critical problem'*, inadequate training programmes, lack of involvement in IT development and poor budgetary to the internal audit departments. These results are similar to Abu-Musa (2008) who examined the extent of technology integration in the internal audit activities among Saudi organisations. These studies suggest that in some countries internal auditors are not given enough space to acknowledge the need to integrate technology into their audit methodology. Partly, this could explain the increased risk in digital environments in Tanzania and elsewhere, as the culprits are motivated by the perceived low prevention mechanisms (internally) to stop their acts (Jans et al., 2010; Alanezi and Brooks, 2014). This

also justifies the need to understand the external auditors' counter-parts on the move to use technology for audit purposes and for fraud detection in particular.

It is also important to note that culturally, Tanzania is categorised as a collectivist country with high power distance as opposed to individualistic western countries with low power distance (Hofstede, 1984). This categorisation of a country has an impact on the business culture and the way of life including technology usage among individuals and businesses. Cox and Khan (2017) reported a positive relationship between individualism and innovation performance, while power distance and uncertainty avoidance were negatively related to national innovation performance. This can partly explain why little research is done on the extent of use of IS by external auditors in Tanzania. Due to these cultural differences, it is anticipated that some reported findings between Tanzania and other counties might differ significantly as to what influences the usage of IS.

Besides that, the economic power of Tanzania is also different from many countries in the world, or even those of some of the African continent. For instance, countries like Nigeria, South Africa or Egypt have a much higher GDP as compared to that of Tanzania (IMF, 2016). Studies have reported a positive strong relationship between IT usage and GDP growth of a country (Cho, 2007). Specifically, the number of industries in the economy and income per capita increased significantly with the use of IT (Cho, 2007). With the low GDP and per capital income of Tanzania, coupled with it being an agricultural-dependent economy (Mbelle, 2004), this also could partly explain the low-level of IT-based research in the country and specifically on the external audit environment. Again, due to this factor (low economic power), the study anticipates different results between Tanzania and other countries regarding the usage of IS in the audit environment. Additionally, Tanzania being a member of the IFAC as well as World Bank-grant-recipient, there could be some institutional pressure for audit

firms to improve audit quality by adhering to ISAs and other international reporting requirements (World Bank, 2005). The pressure to report issues and compliances can result in adoption of audit technology at the firms' levels to meet the expected standards of various stakeholders while little perceived benefits could be recognised by the individual majorities.

In conclusion, the literature review shows that fraud has increased with the increase in technology integration in business processes. The IT integration has further increased the level of audit risk especially fraud which is posing threats to growth and survival of business portfolios. Meanwhile, the usage of IS tools by auditors in many countries is reported as low. Reasons related to organisational readiness, personal reasons such as IT expertise, cost-benefits issues and external factors were found to influence the adoption decision. However, the reported findings for IS usage in auditing were inconsistent between countries and even within organisations in the same countries (see Huang, 2008; and Lim and Wang, 2011). In all the countries studied, African countries were highly unrepresented in this area and Tanzania had very scanty of information. Consequently, this study has examined the usage of IS, factors for IS usage and post-adoption impact on the audit process and e-fraud detection. A further justification for conducting this study has been discussed earlier on in subsection 1.2.

2.12 Summary of the Chapter

This Chapter has reviewed the literature on financial audit, the evolving role of auditors and audit objectives and the use of IS tools for audit purposes. Similarly, the Chapter has discussed different tools that can help auditors to audit computerised environment and also to detect fraud. Lastly, the impact of IS usage on the audit process including various techniques in identifying fraud in computing business platforms were discussed from various sources. The next Chapter discusses relevant theories to underpin this study.

CHAPTER 3

THEORETICAL FRAMEWORKS UNDERPINNING THE STUDY

3.1 Introduction

The nature of this study is multidisciplinary and takes a combination of auditing, technology usage and fraud in one concept. As such more than one theory is necessary to underpin the underlying research objectives. Generally, the selection of a theory relies on the choice of a researcher, relevance of the theory in relation to the research objectives, and the problem under study (Creswell, 2009). Therefore, this study reviews several theories in technology adoption, acceptance and usage.

3.2 Theory of Reasoned Action (TRA)

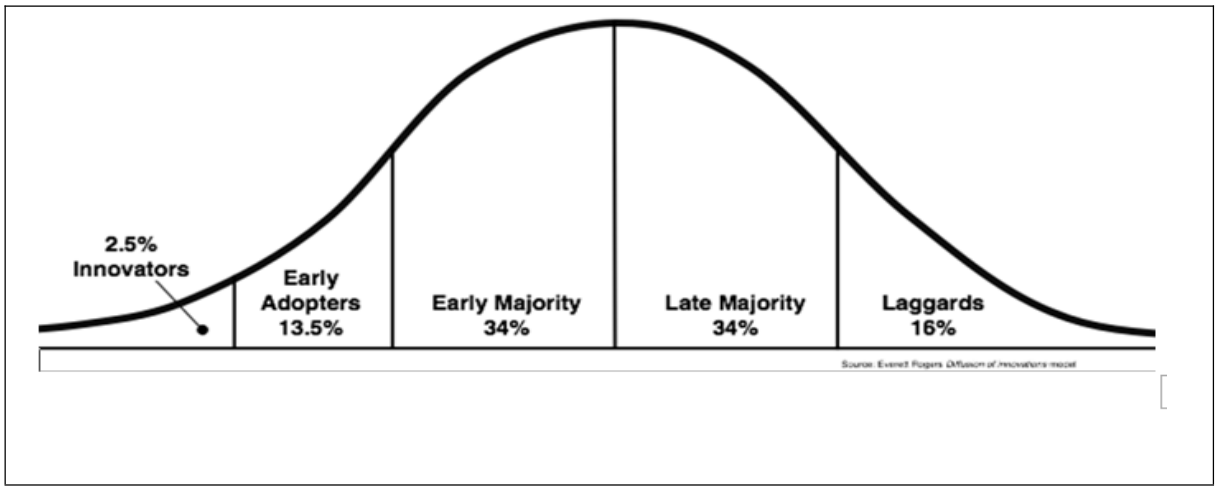
TRA is one of the popular theories that was developed in the 1960s by Martin Fishbein and later on expanded by Fishbein and Azjen (1970) and Ajzen (1991). The theory has its origin in psychology. The fundamentals of the theory are based on understanding people's behaviour, beliefs, intentions and attitudes towards implementing change. The theory proposes that an individual's intention to perform a behaviour in question is a factor of that behaviour. Intentions are suggestions of difficulties and willingness to try and the amount of effort they forecast to apply in order to achieve the behaviour (Ajzen, 1970). Thus, the theory believes that in order to determine one's intentions, two factors are important, namely (1) attitude towards the behaviour and (2) subjective norm (Ajzen, 1991). In using these two factors to determine the willingness to adopt change, TRA gained fame in management information systems (MIS) research. Studies have used TRA in examining pre and post-adoption use of technology by measuring the determinants of adoption and its outcomes (Khalifa and Shen, 2008; Nor and Pearson, 2008; Grandon et al., 2011). TRA could be a suitable theory to

underpin this study however, it is not the best-opted theory because in the external audit environment, the use of IS does not only depend on attitudes and beliefs of individuals. There are other external factors which might demand users to use technology as a necessity (Kotb et al., 2012), irrespective of their personal attitudes and belief of the outcomes of technology.

3.3 Diffusion of Innovation (DOI)

DOI is one of the oldest models of technology which was started by Rogers in early 1962 and later on expanded by Rogers (2003). The model provides explanations related to how, why, and the extent in spreading of new ideas or innovation over time in different cultural settings. DOI defines diffusion as the progression by which technology is transferred through specific channels in a social structure by considering four elements, namely (1) presence of new technology, (2) proper dissemination channels, (3) time, and (4) social system (Rogers, 2003). Although the four factors are the main drivers for the theory, capital availability (human capital and cash) are the sole factors to determine when and whether to adopt innovation (Rogers, 2003). Specifically, DOI states that individuals and groups will reach a decision to adopt new innovation based on five conditions, namely (1) relative advantage, (2) comparability, (3) complexity, (4) triability and (5) observability. Relative advantage is the point where new technology is perceived superior than the old norm it replaces. Compatibility is the extent of value generated from the use of new innovation. Complexity is the extent of difficulty or ease to understand and or use new innovation. Meanwhile, triability is the extent to which the innovation can be tested before adoption takes place, and observability is the extent on how the new technology is perceived in providing concrete outcomes.

Furthermore, Rogers (2003) pointed four main groups of adopter of innovation to include (1) innovators, (2) early adopters, (3) early majority, (4) late majority, and (5) laggards.



Sources: Rogers, (2003)
Figure 3.1 Technology Adoption Stages

The interpretation of Figure 3.1 is that innovators are the actual ventures or risk takers. They take risk in using the new ideas by placing it to the market. They tend to spend their resources with positive outcomes in mind to profit from innovation. Few people can be risk takers, thus, this group tends to have few players. Early adopters take the new idea and start using it after learning from the innovators. Similarly, they are few in the beginning because many are still uncertain on how things will turn out after adoption (Rogers, 2003). The early majority are the third category of adopters of innovation. They become many in number as they are convinced of the positive outcomes of using innovation. Meanwhile, the late majority are the late comers in accepting technology. They can be many depending on success outcomes they observe from the early majority. Therefore, they tend to accept innovation in large numbers after fully being convinced of its perceived benefits. Lastly, the laggards are the most recent category of users of innovation. They are fewer in number, not risk takers and hence, they fear to lose their invested cash through adopting change. Therefore, they will remain practising the traditional techniques in their activities, irrespective of the benefits of innovation.

In e-business, DOI gained fame and has been used as a single model to study the extent use of IS to businesses at both pre and post adoption (Fuchs et al., 2010, Vicente and Lopez, 2009;

Yuan et al., 2003). Other researchers in e-commerce have combined DOI with other models to understand drivers of e-commerce players. For example, Cheng and Cho (2010) combined DOI with the Theory of Planned Behaviour (TPB), while Zhu et al. (2006) combined DOI and TOE. Besides that, DOI could be useful in this study as it shows the adoption stages and the key ingredients in the adoption process. However, it has not been used to study technology acceptance in external auditing. This could be partly due to its main cited limitations that the theory has focussed more on personal behavioural factors that do not take into account external factors and organisational support, which are key drivers in adopting change (Berwick, 2003; Stone, 2004.) Within this limitation, the study does not consider DOI as the most appropriate theory to use.

3.4 Technology-Organisation- Environment (TOE) Model

TOE is a more recent model of technology adoption that was developed two and a half decades ago (Tornatzky and Fleisher, 1990). The model states that 'the process of implementing new innovation is influenced by three factors, which are (1) technology, (2) organisation and (3) environmental factors'. Under technology, the model refers to the needs for both internal and external availabilities of technology such as equipment, the Internet and other infrastructures to implement innovation. Under organisational factors, the model refers to both human resources capabilities, management readiness, formalisation and the extent of centralisation of the organisation structure; while environmental context referred to all macroeconomic factors such as competitions, customers, size of the industry and regulatory framework that supports the use of technology (Tornatzky and Fleisher, 1990).

TOE has been widely used in pre-adoption of technology to study e-commerce adoption by small and large e-commerce players. TOE has also been used as a one model or by combining it with other models to study the intensity of value added by technology adopters on post

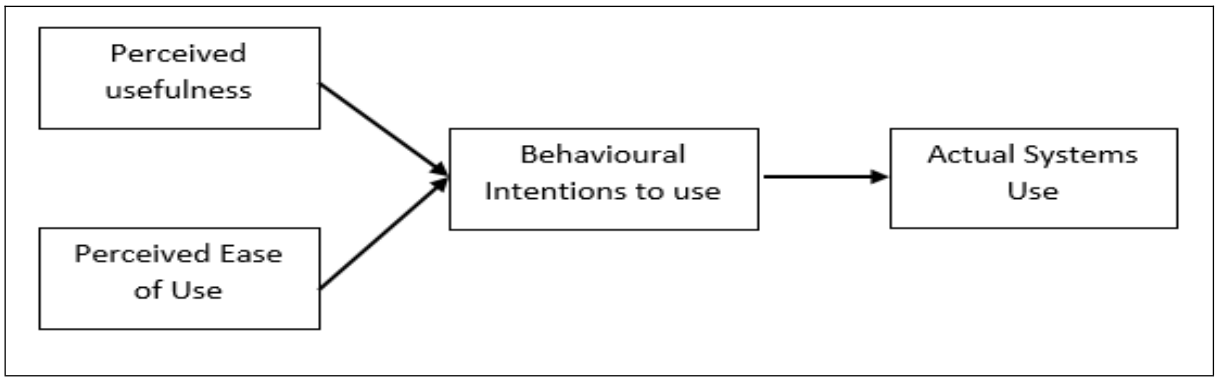
adoption of technology by SMEs (Gibbs and Kraemer, 2010). Salwani et al. (2009) and Zhu and Kraemer (2005) combined TOE with resource based view (RBV) while Zhu et al. (2006) combined TOE with DOI to understand drivers for technological adoption by e-commerce users. Among the most influential factors cited when using TOE model included perceived benefits and external pressures which have been reported to have more influences into e-commerce adoption (Zhu and Kraemer, 2005; Salwani et al., 2009; Gibbs and Kraemer, 2010).

From the reviewed literature, it was concluded that TOE model has not been used widely to study IS adoption in auditing. This could be partly due to its unit of analysis which is the organisation (Gibbs and Kraemer, 2010; Rosli et al., 2013). The organisation being the determinants of the sample size, makes the use of TOE in understanding adoption of technology in auditing very difficult, due to the small number of audit firms in many developing countries. There is also a high likelihood of lack of access to the audit firms and a low response rate due to the busy work environment (see low responses from Kotb et al., 2012; and Ahmi and Kent, 2013). Thus, the demand for TOE which needs decision-makers as a unit of analysis could be difficult given the small number of auditors (partners) in Tanzania.

3.5 Technology Acceptance Model (TAM)

TAM is a common model which supports the facts on how users reach a decision to accept and use new technology. TAM is an extension of the TRA model, which derives theoretical concepts that are essential determinants to use new technology (Davis, 1989), which are beliefs, behaviours and attitudes. The model was later on expanded by Venkatesh et al. (2003). TAM states that "as soon as workers are exposed to a new technology, two factors are important to drive their choice of usage, namely (1) perceived usefulness (PU) and (2) perceived ease of use (PEOU). PU is the degree at which one believes that applying a certain

system will improve his job performance. PEOU is the extent to which a person believes that by using a new innovation, he would be free of additional efforts (Davis, 1989).



Source: Davis et al. (1989)

Figure 3.2 The Original TAM Model

The model argues that when new technology is perceived as easy to use, subsequently users will perceive it as beneficial to the particular task, leading to a change of individual behaviour which triggers the actual usage (Davis et al., 1989; Venkatesh et al., 2003). The main criticism in TAM that is cited on its validation of the model is that it used students as participants in adopting e-learning (Curtis and Payne, 2008). Another limitation is the failure to put into consideration external factors allowing researchers to make a self-selection of external variables that might impose a self-selection bias (Van Raaij and Schepers, 2008). Irrespective of its criticisms, TAM has gained popularity in the field of IS including e-commerce, e-accounting and auditing. TAM has also been combined with other theories such as DOI or TPB in the field of MIS (see Cheng and Cho, 2010; Hung et al., 2011).

In a recent study on models of technological adoption, Korpelainen (2011) conducted an exploration research to find the most widely-used models in business and management research. The study used qualitative content analysis by tagging articles between 1990 and 2010. The findings revealed that TAM was the most popularly used model, followed by TRA and DOI. The justification for the wide use of TAM as compared to other models, was

arguably its simplicity, clarity, reliability and practicality of the factors involved (Korpelainen, 2011).

Table 3.1 Number of Citations in the Use of Models of Technology Adoption in Business and Management

	Model	Author	Citations
1.	Single Models		
	TAM	Davis (1989)	869
	TRA	Fishbein and Azjen (1970)	502
	DOI	Rogers (1983)	497
	UTAUT	Venkatesh et al. (2003)	109
	TPB	Azjen (1991)	331
2.	Combined Models		
	TRA +TAM	Davis et al. (1989)	195
	TPB + TAM	Taylor and Todd	144
	TRA +DOI	Karahana et al. (1999)	100
3.	Replications and extensions		
	TAM (replication)	Adam et al. (1992)	74
	TAM2 (extended TAM)	Venkatesh and Davis (2000)	129

Source: Korpelainen (2011)

The weakness in Korpelainen (2011) is that only papers published in English language and available in English journals were reviewed. There is a probability that the list could have changed if journal papers published in other languages were included. It can be argued that the findings reported are only acceptable in the condition of language as a determinant for the sample selection.

In audit technology, TAM was used to study the adoption and usage of CAATTs, GAS and CA by internal auditors (Huang et al., 2008; Kim et al., 2009; Varsahely et al., 2012; Razi and Madani 2013). However, from the literature summary (see Appendix I) TAM has never been used to study the adoption of technology in external auditing. This could possibly be due to its

measurement variables which are inclined towards two main factors only (PU and PEOU) without considering management or environmental factors. The usage of technology in the external auditing can be influenced by both internal and external factors (Ahmi and Kent, 2013). Hence, TAM may not be a suitable theory to underpin this study.

3.6 Information Technology Audit Quality (ITAQ) Model

Havelka and Merhout (2008) conducted a study to investigate attributes that constitute Information Technology Audit Quality (ITAQ). The study gathered several items through a triangulation of data sources. The gathering of such items involved a large sample from a diverse business background and auditors of different levels working within manufacturing industries, telecommunications and financial institutions who regularly used technology in their processes. The findings reported that for an IT audit quality to be effective, six items are vital, namely, audit organisation, client organisation, target process, audit methodology, audit personnel and IT knowledge. According to Havelka and Merhout (2012), these factors stand as the predictors in ensuring IS audit quality. They argued that the identified factors are multi-dimensional and can be used to understand both internal and external audit quality.

However, this study does not consider using ITAQ model because its validation was dependent on data from internal auditors. Factors for the use of IS by internal auditors may be different from those of external auditors because internal auditors are employees of the organisation while external auditors are employees of an independent audit firm. Furthermore, the model is still new and has no popularity. The factors which were validated in only one setting might produce reliability problems especially when tested in a developing country's context.

3.7 Towards a Proposed Theoretical Framework for the Study

Several models of technological adoption have been discussed above and their graphical depiction shown. There is no single model that can be used precisely and fits another study when replicated to a different population (Venkatesh et al., 2012). Each model has some flaws; therefore the use of more than one model or combining variables from different models has been used in prior studies. It has been observed that in audit technology literature, researchers have adopted various styles in the use of models and theories. Some have attempted to develop their own models (see Havelka and Merhourt, 2008, Ahmi and Kent, 2013), while others have adopted theories by making some changes to suit particular settings (see Razi and Madani, 2013; Mahzan and Lymer 2014). However, the researcher must always present a justification for such a decision (Creswell, 2009).

Table 3.2 A summary of technology theories used in auditing

Model	**Elements in the model**	**Target**	**Scope in auditing**
TAM	o Perceived usefulness o Perceived ease of use	Individuals	Internal auditors
UTAUT	o Performance expectancy o Efforts expectancy o Social influence o Facilitating conditions o Moderators (age, gender, experience and voluntariness)	Individuals	Internal +External Auditors
TOE	o Technological factors o Organisational factors o Environmental factors	Organisation	I-TOE, not validated
DOI	o Relative advantage o Compatibility o Triability o Complexity o Observability.	Individual	Nil
ITAQ	o Audit methodology o Audit organisation o Client organisation, o Target process, o Audit personnel	Individual& Organisation	Internal +External Auditors

It can be seen from Table 3.2 together with the summary of the literature in Appendix I that out of 18 studies on technology adoption in auditing, 8 used UTAUT, 4 used TAM, 2 used

ITAQ and 1 used technology task fit. It is also noted that 12 studies examined the use of IS on internal auditors and only 3 examined factors of IS usage by external auditors (Janvrin et al., 2009; Ahmi and Kent, 2013; Curtis and Payne, 2014). On the other hand, UTAUT has been used to study the adoption of technology by both internal and external auditors while TAM has been used on the internal auditors only. These statistics influenced the decision for selection of a theory for this study. Specifically, the study chooses UTAUT as theoretical lens to underpin objective 2 which aims to explore the perception of auditors on the factors motivating the use of IS. Further justification for the adoption of the UTAUT is discussed in the next sub-section 3.8.

Likewise, from the theoretical literature review, it can be concluded that the most widely used models in auditing technology are TAM and UTAUT (see Appendix I). Out of 18 reviewed papers on technology adoption in auditing, 9 studies used UTAUT, 4 used TAM, 1 used ITAQ and 1 used technology task fit, while 1 study, the authors developed their own model. It is also noted that out of 18 reviewed studies, 12 investigated the use of IS on internal auditors while 5 examined factors for technology usage by external auditors (Debreceny et al., 2005; Janvrin et al., 2009; Ahmi and Kent, 2013; Curtis and Payne, 2014; Pedrosa et al., 2015). While TAM has been used to understand technology acceptance by internal auditors, UTAUT has been used to study the adoption of technology by both internal and external auditors. The decision for the use of a theory for this study has been influenced by these statistics. This study finds that UTAUT is the ideal theory to use in understanding "why" external auditors in Tanzania use IS. However, the study adopts it by adding two other factors from prior literature (audit clients factor and the audit profession factor). Hence, objective 2 of this study will be underpinned by this theory. Specific justifications for selecting UTAUT are clarified in the next sub-section.

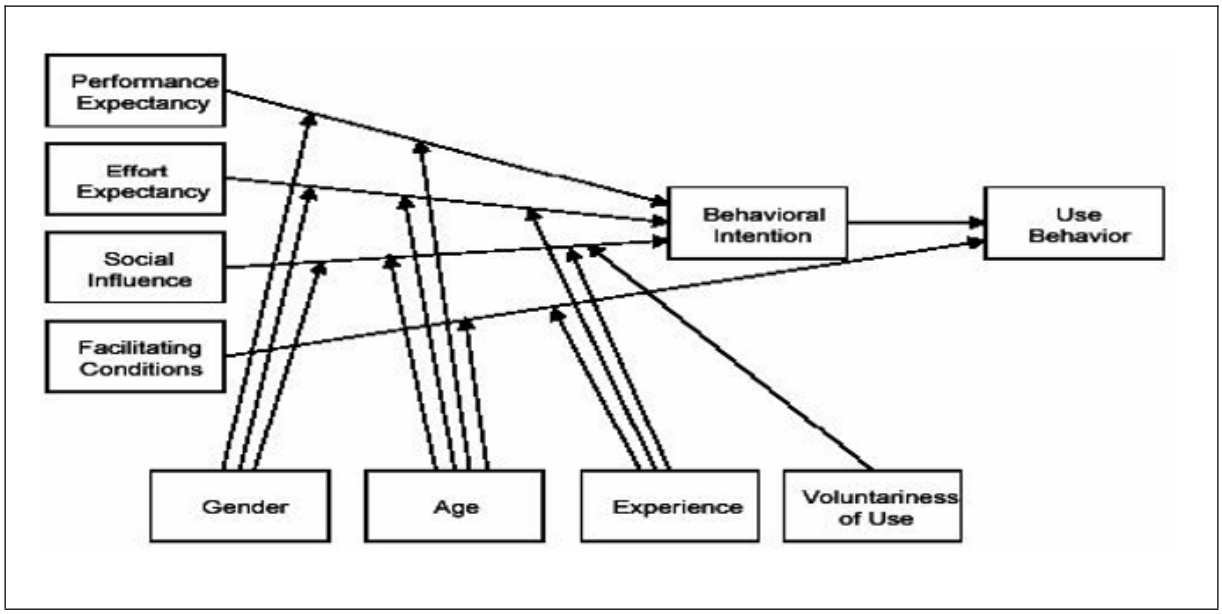
3.8 Unified Theory of Acceptance and Use of technology (UTAUT)

UTAUT is one of the models in technology adoption that has combined factors from eight different theories including TAM, TPB, TRA, Motivational Model (MM), theory of PC use, DOI, and social cognitive theory (SCT) (Venkatesh et al., 2003). The factors identified from the eight theories were modified into four factors which were termed as constructs. They are (1) performance expectancy, (2) effort expectancy, (3) social influence and (4) facilitating conditions. In addition to the four constructs, the model includes gender, age, experience and voluntariness as moderating factors that impact the behavioural intention (BI) to use technology.

Table 3.3 UTAUT Elements

Element	Definition	Constructed from
Performance Expectancy	The extent at which a person believes that using technology will support him to improve job performance	TAM-Perceived Usefulness TAM2-Extrinsic motivation DOI-Relative Advantage
Efforts Expectancy	The degree of ease related to the use of technology	TAM -Perceived Ease of Use Complexity
Social Influence	The degree to which a person perceives important what others believe he should use the new innovation	TPB-Subjective Norm TRA-Social Factors and Image
Facilitating Condition	The degree to which an individual believes that organisational and technical infrastructure exists to support the use of the system	DOI-Perceived Behavioral Control Facilitating conditions and Compatibility

The relationship between the UTAUT variables are explained in figure 3.3 below.

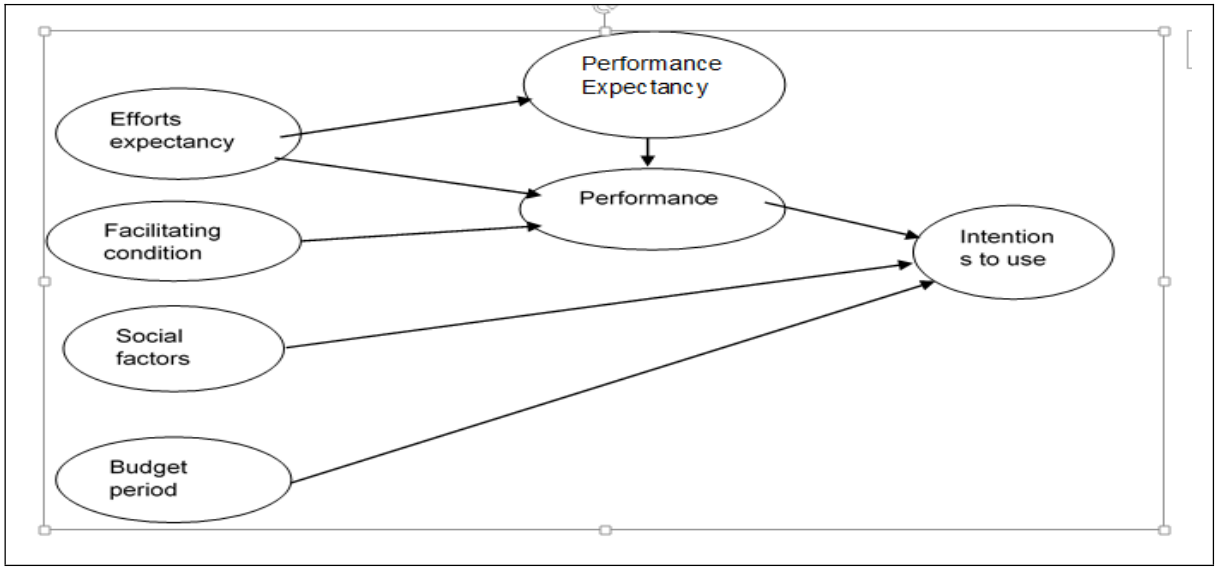


Source: Venkatesh et al. (2003)

Figure 3.3 The Original UTAUT Model

Besides combining eight different models, UTAUT is in fact the most recent theory as compared to other models of technology adoption. The items specified in previous theories of technology adoption include individual perceptions of technology use (usefulness and easy to use), organisation, and availability of resources which have all been captured in UTAUT. Therefore, UTAUT has by far outperformed other models of technology adoption (Curtis and Payne, 2014). Furthermore, in the auditing field, UTAUT was used to test adoption of IS to both internal and external auditors. Gonzalez et al. (2012) used UTUAT to explore the use of CA by auditors across the globe. Janvrin et al. (2009) and Curtis and Payne (2014) both adopted the UTAUT model to examine the acceptance of IS (CAATTs utilisation) by external auditors in the US. In these studies, varied items of UTAUT were added and replicated and in some instances the model was reconfigured to fit a particular setting (*see* Curtis and Payne, 2014). Therefore, in a developing country such as Tanzania where technology is still in its infancy and little is known, the use of a ready model can easily predict the application of the factors identified by making a starting point into the exploration.

One of the main strengths cited in the use of UTAUT is that its empirical validation through a cross-sectional study produced results with a validity of 70% (Venkatesh et al., 2003). However, this study adopted the UTAUT model by considering its four main constructs and one moderating variable (voluntariness) while adding two new factors that were deemed important in the external audit environment. Likewise, Curtis and Payne (2014) conducted an empirical study by applying the UTAUT model to investigate CAATTs adoption by external auditors in the US. The study reconfigured UTAUT with one additional construct, 'budgetary period'. The findings revealed that CAATTs adoption was significantly influenced by social factors. The results further showed that firms with longer term budgetary plans were more likely to adopt new technology than short period budgetary firms. The second findings revealed that the use of modern tools improves productivity and value of audit processes, such as identifying fraud hence, reducing costs of litigation. The new revised model is shown in Figure 3.4.



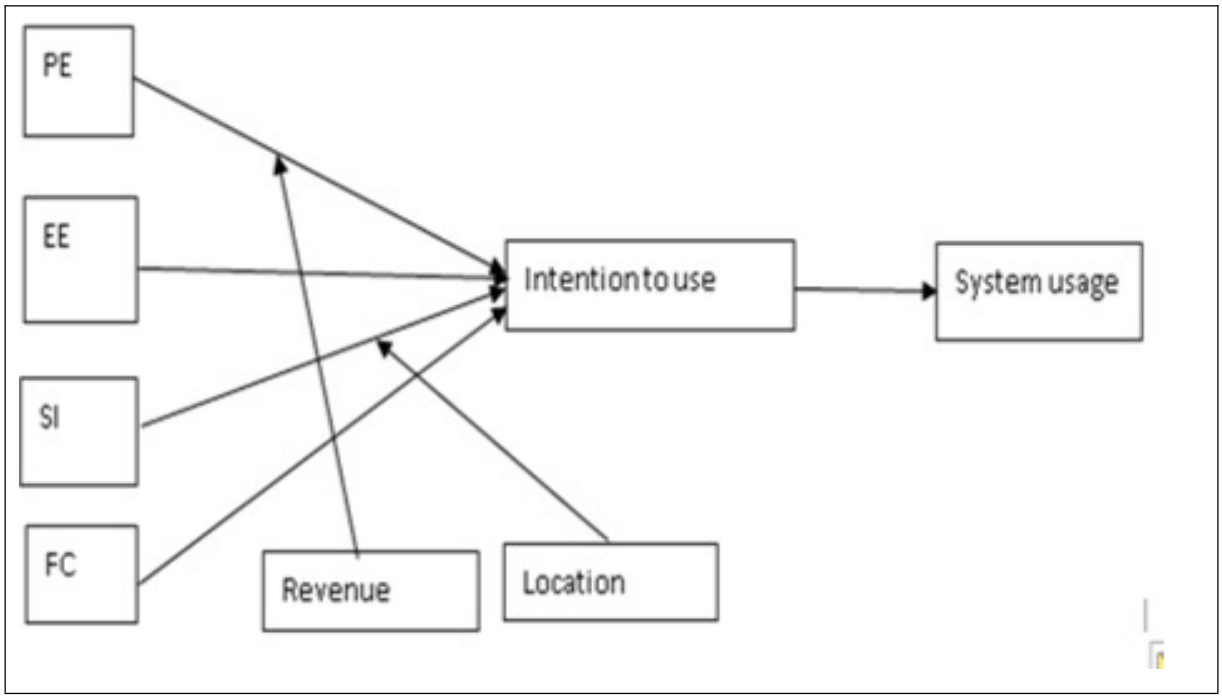
Source: Curtis and Payne (2014)

Figure 3.4 Modified UTAUT- A

Prior to that, Curtis and Payne (2008) applied UTAUT to understand CAATTs utilisation decisions by firms' managers in the public accounting firms. The study used another

constructs 'risk preferences' in addition to individual characteristics. The findings revealed that risk-seeking managers were more likely to adopt new technology irrespective of any budgetary constraints as compared to managers who were risk-averse.

Similarly, Gonzalez et al. (2012) used UTAUT to investigate the use of technology by auditors. The study modified the model by including two moderators, 'annual revenue' and 'geographical location'. The proposed model is as shown below:



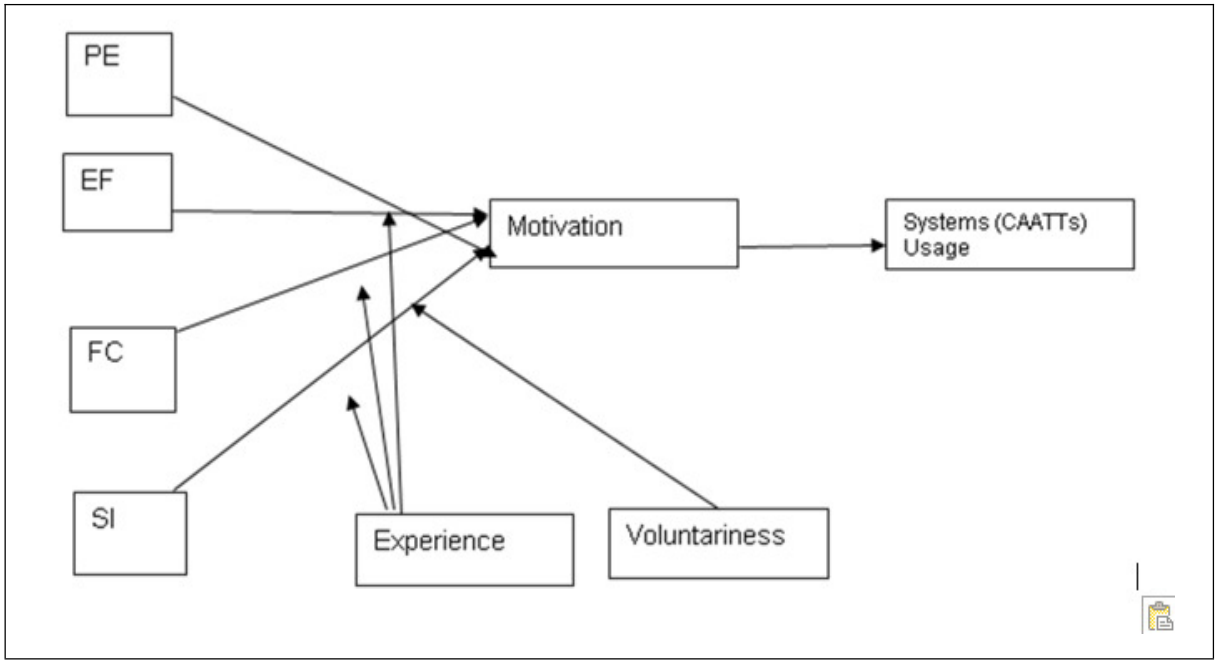
Source: Gonzalez et al. (2012)

Figure 3.5 Modified UTAUT-B

The findings in Gonzalez et al. (2012) reported a 44% model significance in predicting the intentions to use the systems. Irrespective of acknowledging the benefits of using CA methodologies, auditor's use of the techniques was abnormally low. In regard to the specific factors within UTAUT model, the study revealed that efforts expectancy and social influence were the two significant predictors in determining the use of CA. The findings further revealed that annual revenue was a significant moderator of performance expectancy while geographical location was a significant moderator for social influence. The findings of

Gonzalez et al. (2012) highlights that geographical location can produce different results of the same UTAUT variables, which resulted in a contribution of a new variable, '*geographical location*' to the model.

Other researchers who used UTAUT include Diaz and Loraas (2010) and Mahzan and Lymer (2014). Diaz and Loraas (2010) found that efforts expectancy (perceived easy to use) had a strong and significant impact in influencing the use of technology by junior auditors. In particular, it was found that as technology features became difficult to learn and understand, it affected other factors indirectly such as perceived benefits, social influence, budgets and attitudes. However, when technology became easy to learn, only individual factors were affected. However, Mahzan and Lymer (2014) found that PE and FC were supportive predictors of system usage but EE and SI were not strongly supported. The study added an important lesson to be learned, that it is the systematic moderation of UTAUT variables by replacing BI with '*motivation*'. The new proposed model appears as follows:



Source: Mahzan and Lymer (2014)

Figure 3.6 Modified UTAUT -C

Recently, Venkatesh et al. (2012) expanded the UTAUT model by incorporating three more variables to the original UTAUT in studying the use and acceptance of technology by online consumers. The new model added hedonic motivation, price value and habit. The individual characteristics of gender, age and experience moderated the relationship while experience was dropped. The findings revealed that the 'intention to use' variable increased to 74 percent while the actual technology use increased from 46% to 52%. These results highlight that UTAUT can be moderated, replicated and extended and still can produce significant results.

Henceforth, this study found it relevant to use the main variables of UTAUT in addition to other two variables (client's factor and audit profession factor) from the prior literature. The moderating variables of age, gender and experience were also excluded. The decision to drop these moderating variables was reached after the interview stage, when it was found that a majority of auditors were males of a certain particular age group. In fact, Tanzania has been categorised as a masculine country (Hofstede, 1984), which believes in males as decision-makers. As a result, the norms of the societies believed in educating boys more than girls, which resulted in extremely few educated females including accountants and auditors. Meanwhile, age and experience were also left out due to their small impact on the main variables, as reported in prior studies (Gonzalez et al., 2012; Curtis and Payne, 2014; Mahzan and Lymer, 2014).

3.9 Hypothesis Development and Proposed Theoretical Model

Since the study adopted a simple mixed method approach, it becomes imperative to develop hypothetical predictions for the factors that influence IS usage (RO2) the most. Additionally, the study explored to understand how the use of IS could help to improve the audit process and in identifying e-fraud, thereby minimising audit risks (RO3, RO4 & RO5). Hence, the proposed conceptual framework incorporates the elements of UTAUT as internal factors with

two other variables as external factors. Similarly, the impact of IS usage on the audit process and e-fraud detection are also incorporated and summarised within the model, but will be explored deductively through the interview data. The next sub-section discusses the hypothesis for the factors influencing the IS usage in answering RO2.

3.9.1 Performance Expectancy

Performance expectancy is the degree at which an individual believes that using new technology would enhance job performance (Venkatesh et al., 2003). Among the specific measurement constructs of performance expectancy are improved job performance, quick task accomplishment, increased productivity, personal monetary gain, and efficient in saving time and cost. It is argued that IS usage has a high possibility of achieving audit value and other benefits such as eliminating computational errors and simplified audit procedures (Banker et al., 2002). For instance, the use of technology such as GAS and data analytics modelling can aid auditors in identifying fraud easily where manual techniques cannot guarantee audit effectiveness (Ahmi and Kent, 2013, Curtis and Payne, 2014; Mahzan and Lymer, 2014). Similarly, through the use of software such as caseware, lotus notes and the Internet, audit procedures can be minimised, leading to saving time and efforts (Omoteso et al., 2008). The use of Extensible Business Reporting Language can reduce errors in manual computations, enhancing working papers preparation, documentation and cross referencing (Biestaker et al., 2001, Banker et al., 2002). Furthermore, the use of IS simplifies the searching of clients' files from a well-maintained database allowing knowledge sharing, hence improving the quality of report and decision-making (Banker et al. 2002). The use of audit software enables audit managers to analyse large data, hence simplifying audit review and report writing.

To sum up, the use of IS can lead to improved efficiency and effectiveness of audit procedures, thus benefitting both auditors and the audit firm (Ahmi and Kent, 2013). This

study predicts that if external auditors perceive IS as being better than using predecessor manual techniques, they are expected to have positive intents to use it. Through the survey part of the data, it is posited that:

H1: Performance Expectancy positively influences Behavioural Intentions to increase the use of information systems by external auditors

3.9.2 Efforts Expectancy

Effort expectancy is defined as the degree of ease to use technology (Venkatesh et al., 2003). The ease comes from three main parts: additional time of training (learning curve), understanding the application of the technology and the ability to become skilful. If technology is difficult to learn and apply, auditors may fear that the new adjustments will likely take a long learning curve and may negatively affect the usage behaviour. In contrast, if technology is perceived as easy to apply, auditors will use it more frequently in many aspects of the audit process (Chiu et al., 2014).

The main role of auditors in today's digital environment involves investigating both irregularities in transactions and the systems that transmit information (Gonzalez et al., 2012). In assessing risks in such environments, auditors will have to use computer applications with specific enabling technologies, some of which may be complex to use. Some statistical tools such as neural networks, intelligent agents or data mining are some IS that are recommended in auditing a computerised platform (Gonzalez et al., 2012, Chiu and Varsahelyi, 2014; Carminati et al., 2015). In using such methodologies, auditors will not only have to attend extra training but also use their extra time and efforts to learn. Anything that may have to consume extra time, resources and increased learning curve, may likely be perceived as undesirable to new system adoptors (Kim et al., 2009). Diaz and Loraaz (2010) found that

efforts expectancy significantly affected how auditors learnt new technology. As technology became more difficult to learn, it affected several other factors such as budgetary pressure, social influence and attitude. However, when new technology was easy to learn, it only affected individual factors such as self-efficacy. Other studies found that auditors were confident in learning new technologies and did not find the need to consult IT experts (Hunton et al., 2004). In light of prior literature, it is anticipated that a positive perception in system usage will be anticipated by auditors when a software is easy to use and promises to shorten the learning curve. The study hypothesises that:

H2: Efforts Expectancy will positively influence the Behavioural Intentions to increase the use of information systems by external auditors

3.9.3 Social and Organisational Influence

Social influence is the degree to which a person perceives important to use technology due to influence of colleagues, supervisors and management (Venkatesh et al., 2003). Social influence includes all the people important to one's career and who can influence one's decision in using technology. Such people are mentioned in the UTAUT to include work peers, supervisors and senior management (Venkatesh et al., 2003). Social influence is a construct that has originated from TRA (Fishbein and Azjen, 1970), which takes into account the issues of image and subjective norms. Image is the prestige that individuals can feel when using innovation in the presence of others. Subjective norm is the inherent attitude that a person will have regarding what his or her peers will view of him in using innovation (Fishbein and Azjen, 1970).

It is argued that group peers, colleagues and management are important in persuading and supporting individuals to use innovation. The use of IS influenced auditors' roles, creating

duo roles in auditing and the need to acquire additional IT skills (Vendrzyk and Bagranoff, 2003). As such, auditors who had excellent use of technology had higher chances of promotion and increased pay (Omoteso et al., 2010). Similarly, management support may come as a result of financial support and cost of training to speed up technology adoption process (Ahmi and Kent, 2013; Curtis and Payne, 2014).

It was reported that organisational support influences auditors' decision to use IS both in mandatory and voluntary adoption (Janvrin et al., 2009). If top management perceives the use of technology as useful, their intention to use increases, resulting in adoption of technology. Huang et al. (2008), Gonzalez et al. (2012 and Razi and Madani (2013) found management support having a significant influence in the acceptance of CAATTs by auditors. Similarly, Curtis and Payne (2008) found a positive influence of peers, superiors/supervisor in auditors' use of technology. It is contended within UTAUT that the sole decision to adopt technology comes from peers, supervisors and superiors in a defined seniority (Venkatesh et al., 2003). It is from these personnel chain that a decision can be made on behalf of the organisation. Their commitments to support the system usage and approval of funds are the important decision tools to the adoption of IS. The study postulates that:

H3: Social and organisational influence positively influences the Behavioural Intentions to increase the use of information systems by external auditors

3.9.4 Facilitating Condition

Facilitating conditions are defined as the degree to which an individual believes that organisation and technical infrastructure exists to support the use of technology (Venkatesh et al., 2003). Technological infrastructure includes both internal and external technology where the firm can utilise its use. Internal technological factor is the availability of equipment

(computer hardware and software) and installation costs (Ahmi and Kent, 2013). Meanwhile, external technology capability is the reliability of vendors in supplying the required technological peripherals on demand. Technological infrastructure also includes manpower competence within the organisation. According to Vicente and Lopez, (2009), technology competence is the ability of the firm to assess, integrate, and use new technology. Thus, firms with a good legacy of human resource capabilities in innovation are more likely to utilise IS as compared to organisations that have less IT competent manpower.

Another aspect in facilitating condition is system compatibility. Compatibility is defined as the extent to which advance in technology is perceived reliable with the existing principles and needs (Wan et al., 2013). At the firm's level, technology compatibility is related to systems software availability to suit the needs of the adopters. In auditing, compatibility is the ability of audit firm's tools to be compatible with the software of their clients. For example, the clients' IT system could be different from the available software used by the audit firms. If this happens, it may hinder external auditors' use of IS (Curtis and Payne, 2014). Prior studies have reported that the ability of audit firms' software to meet data manipulation needs were found to be significant determinants for the use of IS in auditing (Mahzan and Lymer, 2008). With mandatory auditor rotation after every three fiscal years, a constant change of software could make audit firms reluctant to installs particular software for each client in fear of additional costs. Additionally, prior scholars in technology adoption have argued that there existed a strong relationship between technology adoptions and existing IS infrastructures. As such, well-established infrastructures, compatibility, and manpower in systems can influence a firm to adopt and use innovation (Alam, 2009; Zhu et al., 2006). Given the scope of the audit firms that this study has targeted (i.e large and medium audit firms), it is anticipated that they have sufficient technological ability to influence IS usage. Hence, it is hypothesised that:

H4: Facilitating condition will positively influence the Behavioural Intentions to increase the use of information systems by external auditors.

3.9.5 Clients' Factor

The UTAUT model does not include audit clients' influence on the acceptance and use of technology. This factor is adopted from prior literature of IS adoption by external auditors (Ahmi and Kent, 2013). Clients' factors can be in the form of complexity of clients' IT environment, complexity of clients' e-business environment, the size of clients' business and the volume of clients' transactions. Other elements include the strength of clients' internal control system and the level of audit risk (Ahmi and Kent, 2013). Meanwhile, Debreceny et al. (2005) found that the use of CAATTs by external auditors would depend on the strength of the internal control system of their clients. When clients' internal controls systems were strong, less work would be needed by external auditors hence they would use IS infrequently. Meanwhile, Omoteso et al. (2010) reported a strong internal control mechanism in the UK businesses that resulted in low CA usage by external auditors. However, in developing countries where internal control is not strong enough (Ramachandran et al., 2012), external auditors will be anticipated to use IS more frequently to test IT related controls. Furthermore, Bierstaker et al. (2001) argued that the more complex the clients' systems are, the more likely audit firms will be motivated to adopt technology for risk assessment. However, in the transition period of IS adoption, it was found that some auditors were still using traditional audit approaches concurrently with technology-based tools audit when auditing in e-commerce environments (Varsahely et al., 2012).

However, the need to assess risks of e- fraud may arise as a necessity for auditors to use IS irrespective of perceived complexities in clients (Jans et al., 2010). This could be possible where the level of audit risk is deemed high and manual techniques cannot guarantee

effectiveness in risk assessment (Ahmi and Kent, 2013). Similarly, ISAs recommend auditors to use IS tools and techniques (*see* ISA300) to identify the level of audit risk such as control risk and inherent risk (Pedrosa et al., 2015). It is anticipated that when auditors conduct audits in computerised clients who are more automated with large volumes of transactions (i.e banks in Tanzania), they must use technological tools. Consequently, the study predicts that clients' factors would influence the use of IS by external auditors. It is hypothesised that:

H5: Clients' factors will positively influence the Behavioural Intentions to increase the use of information systems by external auditors.

3.9.6 Audit Professional Factor

The audit profession requires auditors to adhere to standards, rules and regulations so as to remain compliant (i. e documentation and record keeping). It is reported that the use of IS enabled auditors to remain compliant easily as compared to manual systems (Ahmi and Kent, 2013). For instance, the use of office applications such as word and excel can facilitate storage of clients' records in many formats which can easily be retrieved whenever they needed. Besides that, both IFAC and AICPA standards require auditors to ensure transparency, accountability and independence. Again, these requirements can easily be achieved when auditors use IS (Bierstaker et al., 2001; Ahmi and Kent, 2013). Furthermore, several audit firms have adopted technology from their international affiliates for consistence in auditing and reporting. These firms can only recoup the cost of the investments if the tools are used in the audit tasks (Bierstaker et al., 2001). In the Tanzanian context, several audit firms have international affiliations and it is anticipated that they use similar audit methodologies or software for consistency. Besides that, the NBAA and BOT require audit firms that have reliable technological infrastructure to conduct the audit of banks, as they anticipate them to use technology during audit engagements. Therefore, this study expects that IS usage by

external auditors will be motivated by the pressure from local and international audit authorities as well as the available audit methodology to use. The study hypothesised that:

H6: Audit professional factor positively influences the Behavioural Intentions to increase the use of information systems by external auditors.

3.9.7 Moderator: Voluntariness

Currently, the use of IS in auditing is still voluntary. It was argued that voluntariness has contributed to a slow pace of IS adoption by auditors (Curtis and Payne, 2014). Notwithstanding the substantial benefits of IS in audit effectiveness and efficiency, studies reported that the adoption of CAATTs was slow (Ahmi and Kent, 2013). The reason behind the slow technology adoption was due to a lack of mandatory adoption. Curtis and Payne (2014) identified this deficiency and researched on factors influencing the adoption of IS (CAATTs) under a voluntary setting. The findings revealed that budgetary pressure was the main factor that influenced the use of IS under voluntary utilisation. Since budgetary pressure is related to management decision, it will affect the social influence of the UTAUT variable. Hence, it is hypothesised that:

H7: Voluntariness will positively moderate social and organisational influence

3.9.8 Other Moderating Variables (Age, Gender and Experience)

Apart from Voluntariness, the UTAUT uses other three moderators which are age, gender and experience. However, in determining what moderators to use, a particular stage of technology adoption and the nature of respondents are important. In this study, the three moderators were dropped from the model after interviewing 13 external auditors. It was observed that most of the respondents were young and 85% of them were males. Similar results were observed on

the factor of experience where some respondents had experience in auditing while others in IT audit, which makes it difficult to determine which 'experience' variable is to be considered.

Therefore, after the preliminary results, the study dropped age, gender and experience as moderators. However, the variables still remained on the questionnaire and were tested on hierarchical regression for any additional effect on the six main IVs. The dropping of these factors is in line with the work of other researchers (Kim et al., 2009; Sun, 2012; Gonzalez et al., 2012; and Curtis and Payne, 2014). Similarly, after the interview was conducted, 'voluntariness' to use technology was also dropped as it was mentioned that the use of IS was mandatory and some respondents clarified that the use of technology was in fact part of their daily work (see R2, R5; R8 in Chapter 6).

A proposed conceptual framework for the study

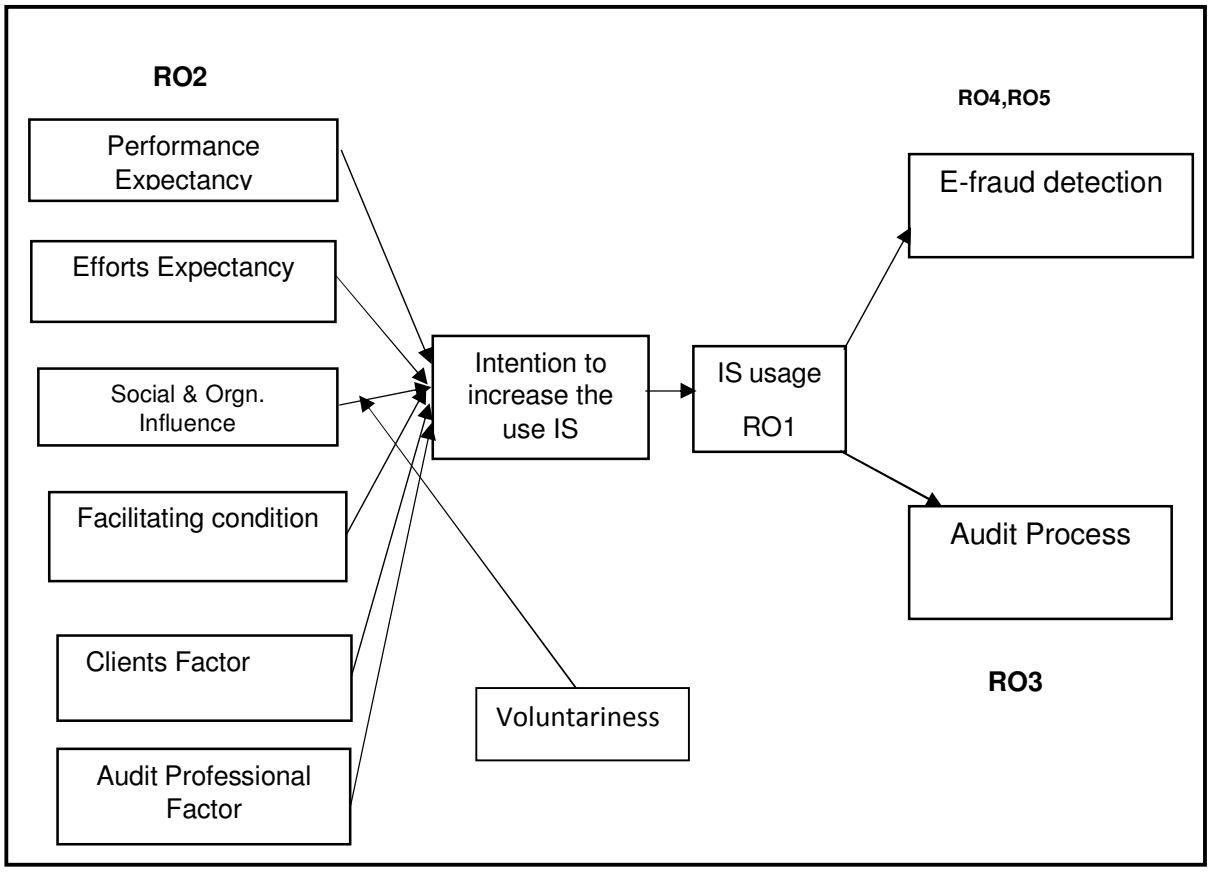


Figure 3.7 Proposed Conceptual Framework of the Study

3.10 Linking the Conceptual Framework with the Research Problem

The first two Chapters have highlighted the changing nature of conducting business from manual into e-business platforms. In e-business, buyers and sellers do not physically meet, rather, the use of technologies characterise the exchange of goods and services (Kotb et al., 2013). When more business dealings become automated and paperless, auditors must also change and conduct auditing through the use of technologies (Bierstaker et al., 2001; Alles et al., 2008). Nonetheless, the extent of technology diffusion itself is not clearly known for most audit firms in developing countries. Even more, the perception of auditors regarding the use of technology is also unclear. This brings the exploration of the state of technology usage among external auditors in Tanzania. The following research question becomes relevant:

RQ1. What is the extent of IS usage by external auditors in Tanzania?

After establishing the state of technology usage, there is need to understand why auditors use IS. In other words, it is to verify the reasons for the adoption of technology. In understanding these reasons, several opportunities and challenges can be inductively and deductively addressed which are important for several groups of audit stakeholders. Prior research has proposed reasons for technology acceptance and usage, which still suggest inconsistent findings. By building understanding from the literature sources and models of technology acceptance especially the UTAUT, the study will establish the most significant factors applicable in a developing country's perspective. The following research question was posited:

RQ2: What factors influence the use of IS by external auditors in Tanzania?

After establishing the drivers for IS usage, the study investigated its impact on audit functions especially the audit process. The audit process is composed of five phases, namely, engagement, planning, execution, gathering audit evidence and reporting the audit findings. In the computerised environment, external auditors are expected to automate their audit procedures for effective auditing (Kotb and Roberts, 2011). Besides that, there are technological tools and techniques that are available for auditors to automate audit procedures (Ahmi and Kent, 2013). Specifically, the study examined how IS has impacted the financial audit process which is the ultimate goal of the audit firm. Grounded on previous studies which reported positive results of technology usage in other fields such as e-commerce (Gibbs and Kraemer, 2010; Gunasekaran and Ngai 2005; Maswera et al., 2008), manufacturing (Barua et al., 1995), banking (Aliyu and Tasmin, 2012), insurance (Lee et al., 2007), healthcare (Bardhan and Thouin, 2013) and hotels and hospitality (Gonzalez and Gidumal, 2016); IS could be viewed as useful in fulfilling audit objectives and improving the audit process. However, there is lack of empirical evidence in investigations in this area of study. The following research question was advanced:

RQ3: How does the use of IS impact financial audit process?

Finally, the study extends the impact of IS on auditor's responsibilities in relation to e-fraud detection. E-fraud in this study is any irregularity that can be committed by either internal or external party to the entity and which falls under ISA 240 and ISA 315. The harm caused by e-fraud can be mild or severe. Mild e-frauds might result in audit risks by causing a material misstatement in FSs at the assertion level (CICA, 2003). An example of this is a deletion of an account in the bank in order to steal cash from the entity, manipulation of data records, using computer programmes to camouflage the true nature of transactions; hacking into an entity's systems to steal or manipulate business information, and unauthorised electronic transfers of funds (Cosserat, 2004). Therefore, the auditor is anticipated to apply proper techniques to determine factors that might increase e-fraud in the entity's e-business systems and then identifying them (Kotb et al., 2012).

On the other hand, a severe case of e-fraud is the business risk, which means there is a possibility of a large fraud that might threaten the survival of the portfolio. An example of this is an attack on the credit card systems or online payments systems of an entity where multiple customers can be affected (Ngai et al., 2011). Indeed, this kind of e-fraud can threaten the liquidity of the company by posing a danger to the '*going concern'* theory of the company (ACCA, 2012). Prior studies proposed the use of technological mechanisms to identify such fraudulent attempts (Jans et al., 2009; Simkin et al., 2015; Stanton, 2012). These technological tools range from simple to high end technologies of different kinds (Janvrin et al., 2009; Jans et al., 2009; Ngai et al., 2011). However, it is not clear how auditors in Tanzania detect e-fraud in computing business platforms which is reportedly gaining momentum in the country. This leads to the following research question:

RQ4: What techniques do external auditors use to detect e-fraud in computerised businesses?

E-fraud has occurred in the developed world as well as in developing countries. In the developed world, credit card, insurance and telecommunication frauds are the leading e-fraud affecting businesses (Jans et al., 2009). Meanwhile, in developing countries, specifically those in the EAC (Kenya, Uganda, Rwanda and Tanzania), the utmost e-frauds on the rise are the mobile banking frauds (Lubua, 2014; Masamila, 2014; Kigen et al., 2014; Rumanyika, 2015; Paula et al., 2016). Hence, in exploring the impact of technology usage to identify these fraud occurrences, the following research question is posited:

RQ5: What is the impact of IS usage on e-fraud detection?

In addition, there are 7 other questions to the interview guide which were supportive in understanding the state of technology usage and its impact on the audit process and e-fraud detection.

3.11 Summary of the Chapter

This Chapter has reviewed theories related to technology adoption, acceptance and usage. Specifically, TAM, DOI, TRA, TOE, ITAQ and UTAUT were briefly discussed in the Chapter in terms of their application, strength and limitations. Any of these theories could fit the nature of this study. However, the study finds UTUAT a more ideal theory because it incorporates features from eight different known validated models of technology adoption. The Chapter has also proposed a conceptual framework which comprised the five (5) research objectives. The next Chapter is a brief case study about Tanzania where an overview of economic development, technology diffusion and external audit environment in the country is discussed.

CHAPTER 4

A CASE STUDY OF TANZANIA

4.1 Introduction

This chapter presents an overview of the economic reforms in Tanzania and the state of technology usage and external audit practices. This chapter is important as the understanding of the economic situation and technology diffusion in Tanzania can be related to the findings presented in Chapter 6, 7 and Chapter 8.

4.2 Demographic Features of Tanzania

Tanzania is a developing country located on the south-eastern part of the African continent. The country is estimated to have a population of 47.25 million people (2013 census), with an estimated size of 945,203 square kilometres including areas under inland water bodies in the Indian Ocean (Tanzania National Bureau of Statistics, 2014). The geographical peculiarity of Tanzania makes it a member of two sub-regional blocks: (1) The East African Community (EAC) and (2) the Southern African Development Community (SADC). According to recent statistics on the economic growth of countries measured by their GDPs, Tanzania was named the second fastest-growing economy in Africa and among the 10 fastest-growing economies in the world (IMF, 2016). Similarly, in the global peace index report, Tanzania was named among the most peaceful countries in the world, ranking the 10th position in Africa (Qorro, 2017).

From the geographical peculiarity and the peace ranking, Tanzania has enjoyed a steady economic growth from foreign investors who are attracted by the peaceful and business-friendly environment (Tanzania Investments Centre, 2015). The growth rate of the Tanzanian

economy from 2009-2016 has remained steady at an average of 6.9% with small upward fluctuations (IMF, 2016). This growth rate has been achieved through its natural resources rich biodiversity of flora and fauna. The major economic sectors which contribute to the GDP are telecommunication companies (telecoms), banks, energy and mining (IMF, 2016). Furthermore, Tanzania is one of the exporters of tanzanite, gold, diamond, and agricultural products such as tea, coffee, cotton, cashew nuts and sisal.

4.3 Economic Reforms in Tanzania

Tanzania obtained its independence of colonialism from the British in 1961. Shortly after independence, the country named itself a socialist economy in the sense that all assets and resources became publicly owned (Hyuha and Ndulu, 1990). In 1967 a resolution was passed through the Arusha declaration which resulted in nationalisation of private-owned enterprises. As a result, the private sector was shut down and a macro-economic model aimed to strengthen the public sector was formed (Moshi and Kilindo, 1990). In early 1985, Tanzania started making significant adjustment programmes which created a move from a socialist economy (or Ujamaa) to an open market economy (IMF, 2009). Such a transition resulted in significant economic reforms that made domestic and foreign investments to flow back into the country (Hyuha and Ndulu, 1990). Among the fruits of the economic transition was the opening of doors to the market economy, the removal of price controls, elimination of restrictions on agricultural products and the restructuring of the financial sector (Pratt, 1999).

In the year 1996, the first stock market was opened in Dar es Salaam and called the Dar es Salaam Stock Exchange (DSE), followed by the Tanzania Private Sector Foundation (TPSF) in 1998 (IMF, 2009). The two organisations were sought as a solution to take the lead in the social economic development of the private sector (Mbelle, 2004). Since the move of nationalisation in the 1960s, private investors have not gained full confidence to put in huge

capitals, hence the stock market is still small. Currently, there are only 26 registered companies in DSE, 12 of which are financial institutions (DSE, 2016). Besides that, there are 37 large companies but not listed, some are state owned and others privately owned. There are also 865 private companies registered in the TPSF (TPSF, 2014). All these companies undergo a statutory audit at the end of each financial period.

4.4 The State of ICT in Tanzania

The use of the Internet for commercial purposes in Tanzania started in 1996, ahead of the government ICT policy (Oreku et al., 2009). Tanzania implemented her first National ICT Policy in the year 2003 with the aim of: "*being the hub for technological innovations*" with a vision of *speeding up the provision of better, faster and reliable facilities to the community through the usage and implementation of technology"* (Tanzania National ICT Policy, 2003). Since the implementation of the ICT policy, individuals, companies and the government increased adoption of technology in their departments and ministries (Genuchten et al, 2012). The growth rate of technology usage in Tanzania reached 450%, between 2000 and 2015 (Lubua, 2014). The growth rate was attributable to the increased competitions among businesses within and across borders. Due to the Internet barriers, the easiest way to use technology among individuals in Tanzania is through mobile phone devices. It is estimated that 84% of the Tanzanian population owns mobile phones, in absolute terms, 39.8 million people (TCRA, 2015). Apart from individuals, businesses both large and small, private and public institutions are active users of technology. As such, technology users in the country can be categorised into three groups: (1) services sectors (led by financial institutions and telecoms), (2) public institutions (public sector-or the government); and (3) other private sectors combined (small, medium and large companies) (Oreku et al., 2009). The private sector is further sub-divided into the agricultural sector, logistics and manufacturing sectors.

The extent of technology usage tends to differ with the size of the company, its customers and the nature of the activities conducted. Generally, ICT adoption in Tanzania is used for several purposes such as e-business, e-banking, e-government and e-learning (Genuchten et al., 2012). These are elaborated in the next sub-sections.

Table 4.1 Penetration of ICT in Tanzania

Size of ICT market	**Penetration rate**
Mobile subscribers (mobile customers SIMs) (000)	39, 800
Mobile penetration (nominal-due to high multiple SIM ownership)	65%
Population coverage mobile network	89%
Internet service providers	32
Internet users (000)	7,600
Registered IT&T companies	98
Broadcasting service providers	46

Sources: TCRA (2015)

Table 4.1 shows the extent of ICT penetration in Tanzania where the use of mobile devices for various economic activities and e-payments is becoming dominant. The mobile phone subscribers of 39,860,000 people, is a trend which is expected to increase by 5% each year with the size of broadband penetration (TCRA, 2015). The advanced use of ICT in the telecom industry, which has grown steadily to provide financial inclusiveness to the marginalised rural population, is also gaining momentum (Rumanyika, 2015). In the year 2000, Internet users were 50,000 but in 2015, the number increased to approximately 7,600,000 people (TCRA, 2015). These statistics show a motivation for individuals and companies to adopt technology in the country. However, there are barriers hindering the growth of ICT to its full potential. According to Rumanyika (2015), the hindrances include slow Internet, network interruptions, power outages and deficiency of knowledge among technology users. However, these challenges are some of the issues addressed in the ICT

agenda in transforming the country into a global competitive nation by 2020 (National ICT Policy, 2003).

4.4.1 E-government

The government of Tanzania is utilising e-government in several of its ministries, departments and local governments. Recently, the government of Tanzania has introduced e-procurement and e-payments in the ministries. From the year 2013, the Tanzanian government changed from cash to accrual accounting with a subsequent installation of a software called EPICOR that is used to process and store all government financial data (Tanzania e-government strategy, 2013). The resulting benefits or e-government include reduced corruption, enhanced transparency, convenience, revenue growth, and decrease in government spending (Dewa and Zlotnikova, 2014). Furthermore, Tanzania Revenue Authority (TRA) made it mandatory for all SMEs to install electronic fiscal device (EFD) in storing their financial data for efficiency in tax monitoring. A positive impact on the use of the EFD was reported in terms of revenue collection (TRA, 2014). However, a lack of awareness and trust in electronic means of payments was a hindrance among users of the device (Mandari et al., 2017).

4.4.2 E-Learning

Many Tanzanian universities have launched e-learning platforms to improve learning delivery and efficiency by establishing platforms where students can access materials on-line (Kisanga and Ireson, 2015). Study materials are kept in the form of CDs for both audio and video, including for students to view their results online rather than using the traditional manual systems. Furthermore, many students have e-mail addresses and are able to use search engines to look for materials in various ways which were not possible a few years ago. The wave of e-learning is sweeping across not only in universities but in other higher institutions of learning

which has resulted in better service provision and better outreach (Essellar and Lishan, 2013). This does not only impact on students learning, but also on many work practices for the academicians as well as other professionals including accountants and auditors.

4.4.3 E-Business

Most businesses in Tanzania have adopted e-businesses (Oreku et al., 2009). Financial institutions are the leading adopters on this area of e-business (Nicholaus and Venkatakrishnan, 2013). Banks are using various software to process and store their information. There has been an integration of banking services between banks and telecoms, where a customer's mobile phone is directly linked to his bank accounts, enabling him to transfer cash from either way. Other areas where e-business has developed is insurance services, tour guide, hotels and air ticketing (Nicholaus and Venkatakrishnan, 2013). There is also an increase in international trade between Tanzania and other countries as a way of embracing the inevitable globalisation, where e-commerce (i.e business to consumer) transactions are completed overnight. For example, purchasing of cars and other merchandise abroad through online systems are some of the recent achievements in e-business (Mwaikali, 2014).

4.5 The Tanzanian Financial Sector

According to the IMF (2016) country reports, the financial sector in Tanzania has experienced a considerable structural change as compared to post independence period. Back to its history, the banking activities in Tanzania were initiated by the colonialists, particularly Germany (Pratt, 1999). From 1919, the British Empire introduced more banks in the country and by-laws were enacted from the British Banking Laws. However, in the year 1967, after Independence, the Arusha Declaration announced the nationalisation of privately owned

banks where all banks became publicly owned (Pratt, 1999). From the early 1990s under the Nyirabu Commission, several structural changes emerged in the banking sector which resulted in the setting of new laws on the banking business such as the Banking and Financial Institution Act (BFIA) of 1991, which was amended in 2006 (Nyaga, 2014). Notwithstanding the contribution of the BFIA 1991, it did not include any item on e-banking. The main reason was that ICT had not yet ventured into the market and so financial institutions were still operating on traditional manual practices over the counter (Nyaga, 2014). However, the trend of e-banking was propelled by the introduction of ICT and the Internet in the country in the year 2003. According to BOT (2014), there are 58 registered banks in Tanzania. These include 15 large banks, 24 medium banks, 16 regional and 3 Non-Banks Financial Institutions. In additional to traditional banking facilities, there is a rapid growth of e-banking with services embedded in the telecoms. The telecoms in Tanzania provide a variety of banking services as well through mobile phones for inclusiveness of the formerly un-banked rural population (Masamila, 2014). The mobile banking services have extended its investment in both local and foreign currencies within 5 EAC member states (Rumanyika, 2015).

Furthermore, there is a growth of automatic teller machines (ATM) and card-less services which were not available in the past. Currently, a customer can withdraw cash sent through a mobile phone to any bank without necessarily having a bank account (Lubua, 2014). The leading banks with e-banking services are CRDB, NMB, Exim, and Postal Bank (Rumanyika, 2015). It is estimated that 70% of the population use mobile money services with a significant improvement of mobile banking businesses at 94.36%, in the year 2012 (Rumanyika, 2015). This growth is contributed by the increased number of large bank subscriptions for both mobile (SMS) and other traditional banking services. The increased usage of technological services in the country gives rise to new products invented by both banks and telecoms. For example, mobile phone customers are encouraged to deposit a certain amount of cash for a

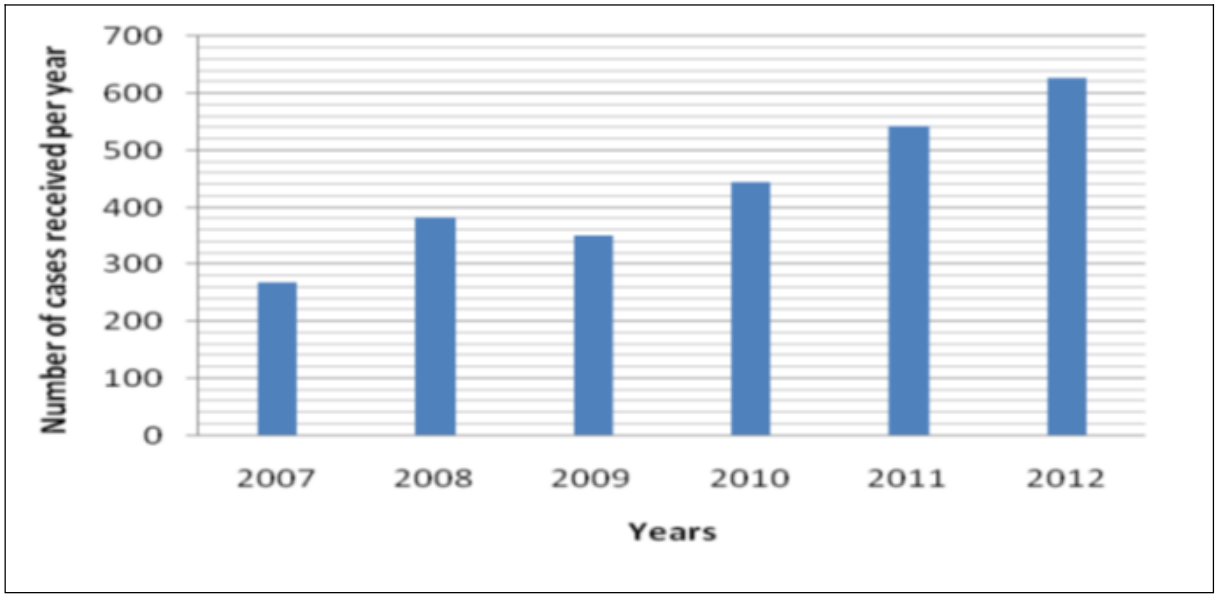
week, a month or several days in a month at an interest rate. There are also other products issued to customers such as insurance compensation services, funeral services, borrow credit and pay later with interest, top-up credit directly from a bank account, etc. It was reported that in 2012, a total of 1.7 trillion Tanzanian shillings were transacted through mobile money (Ndulu, 2012). This is a huge volume of transaction that can attract fraudsters from both within and outside the e-banking sectors.

It is imperative for the Tanzanian context to include telecoms in the banking sectors because they are using e-banking (mobile banking) in a manner that is argued to have a larger frequency in transactions with a large geographical coverage as compared to traditional bank account customers (Lubua, 2014; Rumanyika, 2015). Traditional banking account holders are only 15% of the total population as compared to 70% mobile banking account holders (Rumanyika, 2015). In addition to such e-banking services, there are several government services and payments that take place through online payments, such as government taxes, charges and other levies, which are paid directly through mobile money services, sometimes with embedded banks.

4.6 Mobile Banking Risks in Tanzania

Every good development comes with some challenges. The high rates of technological adoption by users and customers of e-banking and mobile money ecosystems means opening wide doors for fraudsters. There is a higher risk atmosphere in the e-banking system particularly when other information technology and telecoms (IT & T) products are used simultaneously as with the case in Tanzania (Paula et al., 2016). The increased risks on both sides are as follows: (1) risk on the side of a customer- any bank employee or even an outsider can hack customers' information and transfer cash from one account to another mobile phone and then destroy off the new mobile number that has been used to effect a fraudulent

transaction; (2) individual banks are losing huge cash, for example, it was reported that mobile banking fraud within three consecutive years had increased by 39% from 265 to 673 cases (Lubua, 2014) with some single incidence costing several million dollars in cash terms (Rumanyika, 2015). In one incident, it was reported that a total of 7 billion Tanzanian shillings (approximately $4.4 million) was tapped from numerous customers of Exim Bank due to collusions between employees and external IT hackers, making it one of the largest ever cyber-bank robbery in Tanzania (Ihucha, 2014). As a result, banks must refund their customers, creating loses to investors and (3) There is a possibility that governments are losing millions of tax revenue due to cash leakages under such complex cyber-crimes (Paula et al., 2016). Hence, there is a need for intervention between various stakeholders in the issue of mobile banking fraud occurrences. Lubua (2014) reported the following statistics of mobile-banking frauds as shown in Figure 4.1.



Source: Lubua (2014)

Figure 4.1 Mobile Banking Frauds in Tanzania.

Figure 4.1 shows an increase in fraud cases committed through mobile banking, a growing and dependable means of paying and receiving cash in Tanzania. In 2007, there were less than

300 cases which dramatically increased to more than 600 cases in 2012. Therefore, studying the impact of IS among players of risk assurance providers (auditor), becomes both imperative and timely. Fraud occurrences in cyber systems are an issue of concern to all stakeholder-groups involved in e-business dealings as they can affect individuals as well as the economy (Newman and Clark, 2003). However, external auditors have a higher chance to detect and report frauds to shareholders and the management. External auditors are selected for this study because of two main reasons. First, the absence of a single study for Tanzania in investigating this category of auditors makes this study important so as to know how new technology is perceived by auditors and what techniques and tools are used to detect fraud in computing business platforms. Second, in recent studies it was revealed that large e-frauds in the financial sectors involved either collusions of IT experts, employees or external systems attackers (PwC, 2014). It was further found that about 30 per cent of banking frauds were occupational-related, committed by accounting employees (ACFE, 2006), and 20 per cent were committed by top-level management or executive employees (Crites, 2008, KPMG, 2006; Ernst and Young, 2010). In light of such a possibility, the issue of independence, skills, due care and competence become important; and external auditors are superior in exercising such attributes (Alleyne and Howard 2005).

4.7 Regulatory Authorities in the Financial Sector in Tanzania

There are two main regulatory authorities in Tanzania for financial sectors and online transactions. The Central bank of Tanzania known as Bank of Tanzania (BOT) is the regulatory authority for financial issues. The BOT is the overseer of activities of financial institutions in the country including registration, monitoring and evaluation (BOT, 2014). The BOT does the monitoring in conjunction with DSE. All banks in Tanzania must have internal control systems in place. This is in accordance to the Banking and Financial Institutions (BFI)

Act for compliance and monitoring purposes (BOT, 2014). The BFI Act also obligates all banks to have a printed audit agreement that develops and monitors the management of the internal control role in the banks (Ramachandran et al., 2012). The availability of such mandates in the banking sectors implies recognition of the role of internal and external auditors. On the other hand, all cyber-related issues are regulated by the Tanzania Communication and Regulatory Authority (TCRA) which was formed in 2003 under the Postal and Communication Act (TCRA, 2015).

4.8 The Accounting Regulation and External Audit Environment in Tanzania

The accounting and auditing profession in Tanzania is under the authority of the NBAA. The NBAA, which is also a member of IFAC, was established in 1973 to regulate financial reporting in the country (NBAA, 2015). The board is also responsible for setting standards and monitoring certified public accountancy (CPA) examinations in the country. Most of its members are affiliated to recognised accountancy bodies such as the American Institute of Certified Public Accountants (ICPA), ACCA and CPA Kenya. As of 31 December 2015, the NBAA had a membership of 1,887 fully certified accountants, out of that, 553 held practising certificates to perform audits (NBAA, 2015). The registered auditors are those who are at least senior auditors who hold a certified public accounting professional qualification such as CPA or ACCA and above. The following is a summary of external auditors' positions and the duration for promotion to another level which was extracted from the company returns of one of the Big Four operating in Tanzania.

Table 4.2 Bands in Promotion for Auditors

Assistant Auditor	**Senior Auditor**	**Manager**	**Senior Manager**	**Associate Manager**	**Associate Director**	**Partner**
3 Years	3 Years	3 Years	3 Years	3 Years	3 Years	Forever
AA1	SA1	M1	SM1	AM1	AD1	Top Rank
AA 2	SA2	M2	SM2	AM2	AD2	
AA 3	SA3	M3	SM3	AM3	AD3	

Source: EY Business Manual (2012)

Table 4.2 shows that to qualify as a senior auditor (SA), a newly recruited auditor (AA) must undergo a compulsory training of up to three years, while at the same time studying for a CPA/ACCA qualification. Upon successfully passing professional qualification examinations including other internal and external training, the audit trainee becomes an SA level 1 (SA1). SA1 is a position that will be held for 3 years. Upon successfully passing various internal practical assessments, the SA will be promoted to Manager Level 1 (M1), in which he/she will stay for a maximum period of 3 years before he/she becomes a Senior Manager (SM). After three more years, the SM becomes an Associate Director (AD) and eventually a Partner.

4.8.1 Audit Firms in Tanzania

There are 189 registered audit firms in Tanzania, which are authorised to provide audit services (NBAA, 2015). The audit firms are categorised under small, medium and large firms. This categorisation depends on affiliation (international or local), number of partners and resources capabilities to conduct the audit (NBAA, 2015). For instance, to get a certificate as a large audit firm, the firm must have at least 3 registered partners, 50 and above number of employees and satisfactory resources capabilities to provide audit services (NBAA, 2015). Most internationally-affiliated firms are registered as large audit firms. Audit firms in Tanzania are allowed to audit not only private businesses but also various government departments, and ministries. All government audits are conducted in conjunction with or with the approval of the Chief Auditor General (CAG).

A majority of the audit firms in Tanzania (70%) are situated in Dar es Salaam, while 30% are situated in other regions. There are also 21 audit firms that are specifically selected and authorised by the BOT to conduct audit of banks and financial institutions in the country. The list of authorised audit firms is available on the BOT website at www.bot.go.tz/banksupervision. The mandate to select statutory auditors to audit financial institutions is at the discretion of the BOT because the sector is considered more automated and risky, hence, it needs assurance of resources on the part of the audit firms.

The Big Four accounting firms have branches in Tanzania. They conduct rotational audit of all the listed companies in DSE, including large unlisted private companies, financial institutions and several government departments. According to the Report on Observance of Standards and Codes (ROSC) (2005), the BOT and the DSE have placed a lot of trust and reliance on the external audit assurance for compliance, statutory and effective audit. Until 2005, there was no legal liability against auditors or audit firms reported in Tanzania (ROSC, 2005). This could be an indication that the audit environment is well managed by the authorities concerned in the country and also auditors are striving to adhere to professionalism.

However, ROSC (2005) reported that many audit firms in Tanzania, especially small and some medium firms were detaching from using technology for audit purposes even when some of them were auditing computerised clients. The report questioned the audit quality produced by some of those firms, urging for NBAA to be strict on its regulatory role to ensure compliance on audit standards and procedures. Therefore, it became necessary for the BOT to select a few audit firms to audit banks and financial institutions on the merit of IT capabilities. Unfortunately, there is still little research that investigated the extent of technology adoption among small audit firms in Tanzania since 2005 which calls for further research.

4.9 Summary of the Chapter

This Chapter has highlighted the historical reforms of the Tanzanian economy including the banking reforms in the country with the focus on technology diffusion. The situation of the banking environment and challenges associated with modern banking systems were also discussed. The Chapter has also highlighted that both banks and telecoms are working in conjunction to provide mobile banking facilities which makes the banking environment more complex and therefore prone to cyber-related frauds. Finally, the Chapter discussed the aspects of external auditing, the role of the BOT and TCRA in monitoring financial and cyber-related issues. The next Chapter will discuss the espoused methodology appropriate for this study.

CHAPTER 5

RESEARCH METHODOLOGY

5.1 Introduction

This Chapter explains the methodology used to explore the way in which external auditors embrace IS and how IS has impacted on the financial audit process and detection of e-fraud that are material to FSs. There are four (4) specific research questions which the study advanced in Chapter 1. A comprehensive research approach is necessary to get answers to the logical questions of the study in the form of what, why, and how (Merriam, 2009). The research design adopted for this study should meet these prerequisites. Similarly, the Chapter describes the scope of the study, sample and sampling procedures, pilot study and data collection. Finally, the Chapter describes data analysis, validity, reliability and ethical considerations during the research process.

5.2 Research Design: The Mixed method Approach

This study adopted a cross-sectional concurrent mixed method approach, by combining both qualitative and quantitative approaches. However, the primary method that guided this study was the qualitative design which is denoted by the word 'QUAL', while the quantitative method denoted by the word 'quant' was used as a secondary database to support the qualitative enquiry (see figure 5.1). In other words, a deductive approach dominated the method of enquiry where all the five (5) research questions were included in the interview guide and appropriately analysed through thematic coding. Meanwhile, one research question (RQ2) was answered using both interview and survey data in order to validate the UTAUT model and to find the most significant factors for IS usage from a larger sample size of respondents.

According to Onwuegbuzie and Collins (2007), the mixed method research design can be conducted for varied reasons but mostly for: (1) expansion of original idea, (2) initiation of a new idea, (3) development of a theory, (4) complementarity of the findings and (5) triangulation of data. In this study, there are two (2) central reasons that influenced the researcher to prefer employing a mixed method approach over a single research method (mono-method) approach. First, the nature of the research problem (Creswell, 2009), which addresses multiple issues to be investigated and which needs responses from two groups of respondents (i.e, managements/IT experts and other external auditors who participate in audit assignments). Hence, the use of mixed method research design can offset limitations characterised from the use of a single method (Teddlie and Yu, 2007; Creswell, 2009). Second, the mixed method approach provides the opportunity to triangulate, compare and contrast the results obtained from qualitative and quantitative data (Collins et al., 2006; Teddlie and Yu, 2007; Creswell, 2009). Hence, it leads to a stronger evidence and reliability of the findings.

Likewise, the mixed method research design can either be sequential or concurrent (Creswell, 2009). A sequential mixed methods strategy involves gathering and analysing both qualitative and quantitative data in different time periods. Meanwhile, a concurrent mixed method design involves collecting and analysing qualitative and quantitative data at the same timeframe. Thus, this study adopted a concurrent mixed method design by collecting qualitative data followed by quantitative data at the same time period (nine months). The reason for using the concurrent mixed method approach is due to the timeframe of the thesis completion at the University of Nottigham Malaysia Campus (UNMC). The UNMC policy requires students to submit their completed thesis by the end of the 3rd year. Another reason is the cost constraints because cash allocated for this project was assigned to a fixed budget.

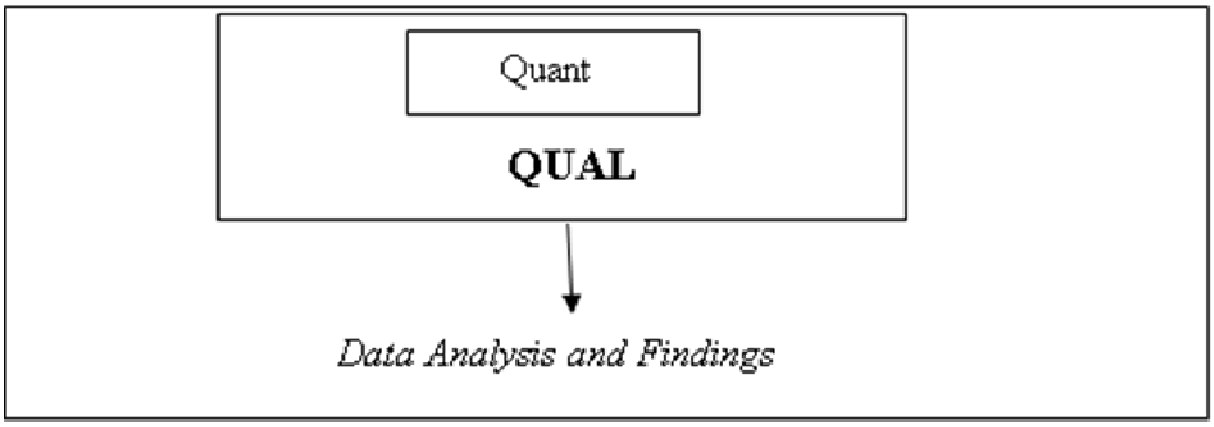
A concurrent mixed method research is further divided into three formats, namely, (1) concurrent triangulation, (2) concurrent embedded and (3) concurrent transformative design (Creswell, 2009). The three concurrent mixed designs differ according to their weight and reason for their mixing (Tashakkori and Teddlie, 1998; Creswell, 2009). Table 5.1 summarises the three concurrent mixed method designs based on their similarities and differences.

Table 5.1 Summarised Concurrent Mixed method Strategies

	Concurrent triangulation	**Concurrent Embedded**	**Concurrent Transformative**
Timing	Collect Qual and Quan data at the same period.	Collect Qual and Quan data at the same period.	Collect Qual and Quan data at the same period.
Weight	Gives weight to both Qual and Quant data. Can be rigid on Quant or Qual; but commonly uses Quant as the main research paradigm (Teddlie and Yu, Creswell, 2009).	Chooses either QUAL or Quant to be the primary data source and either one can be a secondary source. Is flexible in the selection of Qual/Quant combination.	Can opt for either concurrent triangulation or concurrent embedded strategy.
Practice	To study same group of people such as 200 managers from 200 organisations (i.e 20 of them are interviewed) to support the Quant findings.	To study different levels/groups in a given population (eg. managers and subordinates; or teachers and students). To nest the secondary method (Qual or Quant) so as to support the primary enquiry.	Used in critical theory, advocacy (i.e to study gender, race or disability) to facilitate inclusiveness in change process. Can combine practices from triangulation and embedded concurrent strategies.

Source: Teddlie and Yu (2007) and Creswell (2009).

Table 5.1 shows the similarities and differences of the three concurrent mixed method strategies. While their similarity is in the timing of the data (i.e, both collect qualitative and quantitative data at the same time frame), their differences are in the weight and practice. In other words, each strategy allows researchers the flexibility to mix data by dominating one aspect (either qualitative or quantitative data) based on the nature of their studies and respondents. This study adopted a concurrent embedded mixed method strategy where qualitative method (interviews) dominated the research enquiry and quantitative data (questionnaire) was used to support the qualitative enquiry. Fig. 5.1 shows a composition of the mixing for the research design adopted in this study.



Source: Creswell (2009)
Figure 5.1 Concurrent Embedded Mixed Method Design

As shown in fig.5.1, the primary method that guided this study was the qualitative design which is denoted by the word 'QUAL', while the quantitative method denoted by the word 'quant' was used as a secondary database to support the qualitative procedure. According to Creswell (2009) and Tashakkori and Creswell (2007), the embedded mixed method can be used for two reasons: (a) to study different groups or levels in an organisation such as top-level managements and other employees at the same time, where the top-level managers are interviewed and other employees are surveyed through a questionnaire, and (b) to study part

of a quantitative phase that cannot be quantified. According to Morse (1991), "*a concurrent embedded mixed method allows qualitative researchers the opportunity to embed some aspect of quantitative data to supplement the explanation of the sample"* (Morse, 1991 as quoted in Creswell, 2009:214).

Accordingly, this study used the mixed method design as shown in Figure 5.1 for two reasons: (1) the nature of the research questions explores a combination of problems which need information from both the expertise (IS experts or/and Partners/Directors) and other auditors who are involved in audit engagements (2) the nature of the problem identified in the third and fourth research questions (RQ3 and RQ4) cannot be quantified as the study seeks to assess how IS might be useful to external auditors in identifying e-fraud that can be a cause of distortion to the auditor's opinion. Therefore, the study interviewed some of the external auditors who had more expertise in IT and e-business risks while others were randomly studied through a questionnaire to respond to the less technical questions (RQ1 and RQ2).

5.3 Research Scope

This study focussed on the use of IS by external auditors by understanding the factors motivating them to use IS, how IS impacted the audit process and confirming that material e-fraud did not occur, which may distort audit opinion. Therefore, the study focussed on external auditors who audited banks and financial institutions. The easiest way to access this group of auditors was to visit the website of the BOT where a list of audit firms that were allowed to audit banks and financial institutions was displayed. The list was accessed at www.bot.go.tz/banksupervision. The list showed that there were twenty-one (21) audit firms that were allowed to audit banks and financial institutions. The reason for considering auditors who audited banks and financial institutions is because most banks in Tanzania have automated their accounting systems and also in some banks, mobile banking fraud was

reported (Lubua, 2014, Masamila, 2014; Rumanyika, 2015). Similarly, the study considered auditors who were situated in only one city (Dar es Salaam) for two (2) reasons. First, Dar es Salaam is the largest city in Tanzania and also the centre for economic development and innovation. As such, it represents IT growth of both government and business entities in the country (Lotto, 2014). Second, more that 70% of all audit firms are situated in Dar es Salaam (NBAA, 2015). However, clustering the population by region would be the best method of selecting respondents for this study which would eliminate biasness in the sample (Kumar et al., 2013). Therefore, the study acknowledges a possibility of lack of representativeness of auditors from other regions of Tanzania.

5.4 Population and Sample

Population is defined as a sum of a given items of interest in a particular investigation (Zainudin, 2012). It contains the people or group of interest to the investigator (Silverman, 2010). This study considered auditors as a unit of analysis. However, it was also important to consider respondents from different audit firms during the interview session so as to widen the understanding of the types of IS tools they used in the audit process. As such, the study interviewed 13 auditors from 12 different audit firms that were allowed to audit banks and financial institutions in Tanzania. All the auditors involved in the audit process were considered appropriate for this study because they can evaluate the usefulness and benefits of using IS during the audit process (Ahmi and Kent, 2013). However, how IS can be used to detect fraud and how it has improved the audit process overtime required an expert opinion such as an IS auditor (IT expert) or a partner/director/manager who had enough working experience to understand the nature of their clients' e-business integration and the risk components in the e-business environment (Kotb and Roberts, 2011).

Meanwhile, the word 'sample' is defined as a unit of analysis which is a representative of a given population (Zamalia, 2008). As the population is basically expected to be larger than the sample size, sampling the population becomes a vital procedure in a mixed method study in order to guarantee reasonable representativeness of a given population (Hair, 2010). According to Onwuegbuzie and Collins (2007), sampling is important to both quantitative and qualitative enquiries because it assists to enlighten the value of inferences made by the investigator that would reflect on the fundamental conclusions. Thus, in quantitative enquiry, a good sampling technique can enhance estimation or prediction of a fact or an outcome from a large population (Hair et al., 2010). While in a qualitative enquiry, sampling enhances information for generalisation of ideas (Onwuegbuzie et al., 2004; Teddlie andYu, 2007).

Similarly, for qualitative studies, a sample should not be too large neither too small. If a sample size is too small it may bring problems in attaining data saturation, hypothetical saturation or produces information idleness (Sandelowski, 1995; Denzin and Lincoln, 2005). Yet, an overly large sample may create problems to carry out an endless case focussed analysis (Onwuegbuzie et al., 2004). Most qualitative studies adopt a purposive sampling while quantitative studies adopt a random probability sampling, whereas mixed method studies tend to adopt both purposive and random sampling strategies (Teddlie and Yu, 2007).

Prior studies have proposed specific sample sizes for both qualitative and quantitative studies. In quantitative-correlational, causal and experimental studies, Onwuegbuzie et al. (2004) proposed a minimum of 64 and 82 participants for one-tailed and two-tailed hypotheses respectively. Meanwhile, for qualitative studies such as case study-based research, a sampling of 3 to 5 participants is recommended (Creswell, 2002). Likewise, in phenomenology enquiries, the number of interviewed participants is suggested to be ≤ 10 (Creswell, 2007); while Morse (1995) proposes interviewees to be ≥ 6 in number. Yet, in grounded theory, Strauss and Corbin (1998) and Creswell (2007) suggest interviewing fifteen (15) to thirty (30)

people; and for ethnography, the number is suggested to be around thirty (30) to fifty (50) individuals in a cultural setting (Strauss and Corbin, 1998).

However, Strauss and Corbin (1998) and Teddlie and Yu (2007) contend that samples in qualitative researches should be determined by data saturation and not necessarily a precise fixed number of respondents. Accordingly, when conducting this study, the viewpoints from different researchers were considered so as to produce a reliable sample size acceptable in a mixed method design. Table 5.2 displays a summary of the scope, unit of analysis and the nature of the intended respondents.

Table 5.2 Scope, Population and Sample of the Study

Scope	**Unit of analysis**	**Characteristics**
Auditors who audit banks and financial institutions.	Auditors who participate in audit engagements.	IS-experts/Directors/Partners Audit seniors, Managers and Juniors

Table 5.2 verifies that the main criterion for selecting appropriate respondent for this study was if the auditor audited banks and financial institutions. Meanwhile, the unit of analysis was the specific auditor who was involved in the audit assignment. Again, auditors of different positions and experiences were appropriate to answer RQ1 and RQ2, while RQ3 and RQ4 needed expert opinion. The targeted respondents were accessed by contacting the specific audit firms through a recommendation from three important people who knew the researcher. The recommendation facilitated the collection of data, building rapport and in identifying the appropriate respondents to be interviewed (Silverman, 2013).

5.5 Sampling Procedures

Sampling procedure is the process of choosing a portion or section that stands as a representative of a total population (Onwuegbuzie and Collins, 2007). In mixed methods

research designs, the sampling process will involve a selection of units of analysis through both probability and purposive sampling strategies (Teddlie and Yu, 2007). In purposive sampling strategy, which is a qualitative strand, does not necessarily require a sample to be representative of a population, rather, it also considers the saturation of the data (Collins et al., 2006; Teddlie and Yu, 2007). Saturation of data is a qualitative measure of a stopping point of data collection which is established by the researcher that the data has attained adequacy and quality to support the study (Collins et al., 2006).

Meanwhile, a probability sampling contained in a mixed method can follow a representativeness of the group to be studied. According to Curtis et al. (2000) and Onwuegbuzie and Collins (2007), some form of generalisation naturally arises in equally quantitative and qualitative investigations. Quantitative investigators are inclined to create *"arithmetic generalities, which comprise generalising results and inferences from a sample of a population"* (Curtis et al., 2000, pp.1002). In contrast, several qualitative academics are inclined to create *"analytic generalisations that can be applied to a wider theory on the bases of fitting with general constructs"* (Miles and Huberman, 1994). For instance, qualitative researchers make a case to case generalisations based on theoretical power (Curtis et al., 2000; Miles and Huberman, 1994).

According to Teddlie and Yu (2007), a concurrent mixed method sampling design involves a simultaneous selection of components of analysis for both probability and purposive sampling. Accordingly, scholars have outlined 24 sampling structures contended to be equally applicable to qualitative and quantitative studies, which fall into two broad classes; namely, probability and non-probability sampling (Onwuegbuzie and Collins, 2007). Probability sampling is a sampling procedure that employs random methods in selecting a sample in order to allow an equal chance to each segment of the population to be chosen (Zainudin, 2012;

Zamalia, 2008). For instance, simple random sampling, systematic, stratified, cluster and multistage cluster sampling are some of the common probability sampling procedures used in management research (Onwuegbuzie and Collins (2007).

In contrast, non-probability sampling (or qualitative sampling) procedure is frequently used implicitly in a situation where it is impossible to apply a probability sampling procedure (Kumar et al., 2013). Hence, a non-probability sampling technique does not provide an equal chance for the items in a population to be chosen. In other words, it is useful to apply a non-probability sampling where the results of the study are only pertinent to the specific individuals and do not need to essentially replicate the entire population (Zainudin, 2012). Nonetheless, the use of non-probability sampling has limitations; for instance, (1) it could influence a potential bias in the way the sample is selected and (2) sometimes a lack of representativeness of a population may hinder generalisations of the findings (Zainudin, 2012; Zamalia, 2008). Convenience sampling, snowball sampling and purposive sampling are some of the common non-probability sampling techniques that researchers have used in management and social sciences research (Collins et al., 2006; Teddlie and Yu, 2007; Onwuegbuzie and Collins, 2007).

In research designs that encompass a form of mixed method of data collection, Onwuegbuzie and Collins (2007) suggest a sampling scheme that will involve more than one stage. The use of simple random sampling, stratified random sampling, cluster, systematic or multi-stage purposive random sampling schemes are some of the recommended sampling techniques appropriate for most mixed-research strategies (Onwuegbuzie and Collins, 2007; Creswell, 2009). Consequently, this study adopted a multistage-purposive random sampling (MPRS). MPRS is defined as "*a process of selecting settings or groups, and/or individuals as a representative of a sample in more than one phase*" (Onwuegbuzie and Collins, 2007, pp. 287). In the first phase, a purposive sampling selection is conducted and in the second phase,

a random sampling selection of respondents is performed (Onwuegbuzie and Collins, 2007). The reason for adopting a MPRS technique is because both qualitative opinion and statistical generalisations are essential to determine the perception and motivation of external auditors in the use of IS and its impact on the audit process and e-fraud detection.

Furthermore, the study utilised a parallel connection of mixed-sampling strategy. According to Onwuegbuzie and Collins (2007), a parallel connection sample is a mixture of sample that is drawn from the same population of interest but in two different groups. The first group is aimed for qualitative data and the second group is aimed for quantitative data. In this study, two groups of auditors were involved in a parallel manner. First, a small sample of technical and experienced auditors who provided technical information regarding IS usage by answering questions related to 'what' (type of technology is used), 'why' (they need to use IS, including challenges and opportunities), and 'how' (IS usage impacted the audit process and in e-fraud detection).

Second, a large sample size that composed of other auditors who were not included in the interview session, but who provided information by selecting one answer from a Likert scale in relation to their motivations to increase the usage of IS. The respondents who were interviewed were not allowed to participate in the quantitative data collection in order to eliminate the possibility of bias in their responses (Tashakkori and Teddlie, 1998). Henceforth, the researcher visited the NBAA website and found a list of registered accounting professionals upon which the Quantitative sampling of the respondents was based on. It was noted that the NBAA had nine (9) categories of memberships who were registered and recognised as active members. The following list was accessed as of 30th December 2015.

Table 5.3 Active Professional Memberships Registered by NBAA

	Certification	Abbreviation	Members
1.	Fellow Certified Public Accountants	FCPA	146
2.	Fellow Assistant Certified Public Accountants	FACPA	123
3.	Certified Auditors in Public Practice	CA-PP	553
4.	Associate Certified Public Accountants in Public Practice	ACPA-PP	387
5.	Associate Certified Public Accountants	ACPA	1,074
6.	Temporary Certified Public Accountants in Public Practice	TCPA-PP	26
7.	Temporary Certified Public Accountants	TCPA	135
8.	Graduate Accountants	GA	3,756
9.	Approved Accountants	AP	242

Source: NBAA (2015)

Most of the listed members in Table 5.3 had their affiliation (employers) and their addresses. Any of these professionals could be employed and worked as external auditors and/or audit trainees. However, this study considered only the CA-PP 553 (category 3 on the list) who are employed and working as auditors in public practice. Since it was not possible to establish the exact number of auditors working within the selected audit firms (as all of them are registered as private associate entities), the study estimated 553 to be all the active auditors registered within the country and who are practising auditors. However, this number excludes auditors who are employed by international audit firms as expatriates who were expected to be few. Hence, a sample size for quantitative enquiry was estimated from Krejcie and Morgan (1970), as shown in Table 5.4. It can be established that a population of 500-550 corresponds to a sample size of 217-225, thus it is considered an appropriate sample size for respondents in answering RQ2. The study distributed 300 questionnaires randomly to auditors in the twelve (12) audit firms upon the completion of the interview data collection process.

Table 5.4 Defining Sample Size and Population

P	N	P	N	P	N
65	56	220	136	480	214
70	59	230	140	500	217
75	63	240	144	550	225
80	66	250	148	600	234
85	70	260	152	650	242

"P" stands for population and "N" stands for sample size.

Source: Krejcie and Morgan (1970)

5.6 Data Collection

Data collection for this study was conducted in a mixed approach. According to Creswell (2009) and Collins et al. (2006), mixed methodologies are noble because they provide investigators with sound results better than mono methods. Furthermore, they help to counterbalance the flaws in applying a single method (Tashakkori and Teddlie, 1998). As a result, data collected through qualitative enquiry, enriches the study with descriptive data quality while quantitative data enable the study to ascertain observable findings (Creswell, 2009). Therefore, mixed method design reassures data triangulation from a number of sources, hence it improves on value, reliability and strength of data (Kemper et al., 2003; Collins et al., 2006; Teddlie and Yu, 2007). Data collection of this study was predominantly based on primary sources; specifically, interviews and questionnaires. Interviews data (qualitative data) were collected first, followed by quantitative data (questionnaire).

Before the commencement of data collection, it is a requirement at the UNMC that all studies conducted which involve human characters must pass through the ethics committee for assessment. After the assessment process, the feedback is given to the researcher to proceed to data collection. Hence, all the interview questions and questionnaires were submitted to the Reseach Ethics Committee (REC) at Nottigham University Business School (NUBS) on 18th January 2016 and was assigned the submission number REC-NUBS-2016-03. The REC at

NUBS provided comments in order to improve the quality of questions to ensure that no harm would likely occur from both parties, i.e.the researcher and the respondents.

Ethical issues were stressed throughout the process of data collection. Silverman (2010) suggests for researchers to hold an identification and a letter of introduction from the research funding or the affiliated institutions. In order to ease the access to the audit firms, a letter of introduction was requested from the UNMC, introducting the researcher as a bonafide PhD student. Besides that, annonimity was stressed in all the data collection stages (interview and questionnaire). Furthermore, respondents were informed verbally and in writing on the first page of the questionnaire that they had the right to withdraw at any time from the interveiws and from filling the questionnaires. The next part elaborates on the process of collecting qualitative data, which is the main enquiry method of this study.

5.7 Qualitative Data Collection

Qualitative data collection can be conducted either through individual interviews, focus groups, observations or action research (Tracy, 2010). However, due to time constraint associated in analysing multiple sources of data, this study used individual interview as the main source of qualitative data. Interview is defined as a verbal exchange of information between two or more people for an intended purpose (Silverman, 2010; Creswell, 2009). According to Bryman and Bell (2011), interview is a talking data and a common method of conducting qualitative enquiries.

During the interview process, one person (a researcher) asks questions to another person (a respondent) while the former takes notes of what the latter says (Tracy, 2010). According to Merriam (2009), it is imperative to collect interview data where behaviour, emotions, and understanding reality are difficult to observe. According to Silverman (2010), interview is important when an investigator intends to explore the respondents' feelings rather than their

awareness. And according to Yin (2009), interviews are important when the study investigates issues which are complex and on-going. The unique feature in using interviews as a data collection tool is the opportunity of collecting and analysing data concurrently. In other words, a researcher can analyse data at the same point when he/she listens from the respondent (O'Leary, 2004).

Interviews can be conducted based on single-person or focus group discussion (Silverman (2010). Focus group involves more than one person (normally between 3-5 people) (Silverman, 2010), while single face-to-face interviews can be conducted by exchanging ideas between the researcher and the respondent. Furthermore, interview can take place in several forms: (1) face-to-face, (2) telephone or (3) email interviews. Besides that, interviews can be unstructured or semi structured. Unstructured interviews are when questions asked are free flowing without a formal standardised order of asking questions (Tracy, 2010). On the other hand, semi-structured interviews are where questions are pre-arranged and asked to respondents in a conversational manner, not necessarily following the format of the questions, but all questioned are asked to the respondents.

This study used semi-structured face-to-face interviews to thirteen (13) external auditors. The use of semi-structured interviews allowed flexibility in the way the questions were asked, not necessarily following the arrangements of the interview guide (Silverman, 2010). The researcher probed respondents and allowed the flow of a conversation in a natural way while remaining focussed on the subject matter to ensure all questions were answered (Silverman, 2010). Each response was considered as a separate case except in a situation where it was necessary to interview two people (i.e in firm L), where the partner invited a fellow partner who was an IT specialist to accompany him during the interview session.

The researcher had set two criteria for the respondents in order to ensure worthiness of information provided. First, respondents must be at least managers. On average, most audit managers must have worked for at least 7 years with the audit firm (Ernst and Young, 2012). Second, respondents must have been involved in auditing computerised clients. Hence, the researcher prepared the interview questions based on the key concepts which were identified from the literature and which formed part of the research questions. In essence, the interview questions composed of four main parts: (1) the demographic features of the respondents and audit firm, (2) the usage of IS, (3) the impact of IS on the audit process and on e-fraud detection; and (4) the complexity of the audit clients' environment.

In preparing interview questions, it is important to break questions into sub-parts so that respondents can understand what they are being asked (Denzin and Lincoln, 2005). Thus, the research questions were simplified into smaller parts and a total of 12 questions were developed and written in a chronological order and used as a guide during the interview sessions (see Appendix V). The process of collecting interview data started on 1st March 2016 until 15th April 2016. In another stage, the researcher approached a few auditors who were willing to provide extra clarification with the intention to validate their transcripts before the commencement of the coding process. The process of data validation was conducted between September and October 2016.

5.7.1 Interview Protocol

In tracking all relevant information from the respondents, the researcher carried a notebook, a pen and an audio recorder. Silverman (2013) suggests researchers to contact influential people who can help get access to the organisations as a way of building rapport especially for interviews. This is because it can be very difficult to get access to the organisation which might delay the process of data collection. Accordingly, the researcher contacted a few

individuals who were well known to the researcher in order to ease the process of getting access to the audit firms. The staff introduced the researcher to the appropriate people who fit the set criteria for interviews. At first, the researcher explained to the colleagues about the purpose of the research and the nature of the respondents that could provide relevant details to the questions related to IS usage in external auditing. There were three people who assisted the researcher to gain access to the respondents' premises and they were assigned names as X, Y and Z.

Ms X was a former master student at UNMC, who has been working for many years with one of the leading banks in Tanzania. Due to her experience as a banker, she had contacts with external auditors who audited banks and introduced the researcher to a number of external auditors. Mrs Y was a government employee in one of the ministries as a Principal Accountant. Due to her vast experience in working with external auditors (as the CAG does partnership audit with audit firms), she knew several external auditors. Hence, she introduced the researcher to a number of mangers and partners. Finally, Mr Z was a partner and owner of one of the audit firm. Although he was not ready to be interviewed, he introduced the researcher to a number of his fellow partners who accepted to be interviewed. A recommendation from the three mentioned contacts greatly simplified the process of getting access to the audit firms and in building rapport with the informants. However, the main challenge was to get appointments for interviews because the targeted respondents were very busy, especially the partners. Nonetheless, the researcher managed to get appointments with 12 respondents, and one of the respondents invited a fellow partner during the interview session, making a total of 13 respondents.

The researcher was aware that in collecting qualitative data, the issue of adequate sample size was not so important, rather, the quality of the data, the nature of the respondents and

generally data saturation were more important (Denzin and Lincoln, 2005). Therefore, the researcher used two criteria to determine the stopping point which constituted the sample size of the interview data, namely (1) the exhaustive nature of the answers from the respondents; and (2) the quality of information obtained. Besides that, the researcher considered suggested samples from other qualitative scholars in order to foster reliability, generalisability and transferability of the findings. The researcher based on a suggestion from Creswell (2009) who proposed that phenomenology studies to have a number of three (3) to ten (10) respondents. However, after interviewing the 10th respondent, the answers were somehow not as anticipated and the researcher decided to add 2 more respondents. After interviewing the 12th respondent (12a and 12b), data saturation was reached where no new information was obtained. The repetitions of the already spoken words related to types of software used in auditing did not bring any new information (Denzin and Lincoln, 2005). Hence the researcher started to focus on the shared themes that were reported.

The researcher ensured adherence to privacy of respondents' data and anonymity. The use of mock names or initial names and letters is recommended in order to eliminate harm to individuals and organisations (Thorpe and Holt, 2011). Therefore, the researcher abbreviated the word 'respondent' as R1, R2 and so on to denote respondents who were interviewed and arranged them in a chronological order according to how they were approached during the interview sessions. This arrangement helped the researcher to track records of narratives to be included in the findings.

Prior to commencement of the interviews, the respondents were informed that they could withdraw any time during the interview process, which made them feel relaxed to provide information. Similarly, in reducing subject error, subject bias and observer error, the respondents were encouraged to give answers according to how they felt instead of suggesting

words for them (Thorpe and Holt, 2011). Furthermore, the researcher allowed the respondents the time to speak freely without much interruption.

On average, each interview lasted one hour and 5 minutes (1:05 hours), except with three respondents R1, R5 and R11 who showed extra interest in the topic and consequently gave more detailed information. R11 was an old experienced partner in the Big Four who had interest in technology evolution in auditing, the conversation between the researcher and R11 lasted approximately two and a half hours (2:35 hrs.). Meanwhile, the interview sessions with R1 and R5 lasted 1:30 hours and 1:20 hours respectively. The researcher patiently listened to the explanations from all the auditors and later on sorted the information according to the themes of the central research problem and created the remaining data under 'emerging themes' (Silverman, 2010). Most of the interviews took place at the auditees' premises, except for interviews with R3 and R6, who preferred to be interviewed during lunch time in an arranged restaurant to avoid interruptions in the office. A majority of the respondents were males and only two were female respondents which could suggest that there are fewer female auditors in Tanzania as compared to males.

5.7.2 Piloting the Interview Questions

Before the interview questions were sent to external auditors, it was necessary to conduct an initial study in order to reduce the risk of asking questions which are unclear to respondents (Thorpe and Holt, 2011). Piloting the interview questions started on 20th February 2016. The researcher conducted an initial study with seven people, four were university lecturers in accounting and three were external auditors. The respondents were assigned mock names (Kiemi, Yuda, Ntui, Mato, Manoni, Hussein, and Ramadhani), so as to differentiate them from the respondents of the main study. The four (4) university lecturers (Kiemi, Yuda, Mato and Ntui) were not experts in audit technology field but were teaching accounting and

auditing. They were also aware of the on-going adoption of technology in business and the mobile banking fraud issues happening in Tanzania where they could reflect the problem of concern. The major task of the academics was to help in checking the logic and flow of questions and to correct the grammar and jargons of the terms used.

On the other hand, the three (3) external auditors were the experts and targeted group of respondents. They helped the researcher to respond to the questions to ensure that what has been asked is clear to the respondents. For example, Mr. Manoni, was an experienced partner who had worked for one of the Big Four audit firms in Tanzania for 15 years. He had just opened his own audit firm three years ago which was operating as a small firm. He used his past experience to suggest improvements to the interview questions, while he was giving clarifications for the questions asked. Similarly, Mr. Hussein and Ramadhani were both external auditors with 10 and 8 years of working experience respectively. While Mr. Hussein works for Firm B, Ramadhani was working with a large local audit firm. They were both audit managers. The piloting interview with Manoni was conducted at his office while the other two auditors, Hussein and Ramandhani were conducted outside their offices. All piloted interviews were audio recorded, transcribed and saved into the researcher's personal computer. It was observed that all the interviews lasted almost between one hour and one hour fifteen minutes (1.00 -1.15 hours).

The pilot interview session exposed the researcher to conversational abilities to reflect on personal clarity of speaking, listening and also to observe the total time taken in the interviews. Furthermore, the pilot study helped to check the coherence of inquisitive interrogations for each RQ on IS usage in auditing and to ensure that the language was suitable and clear (Thorpe and Holt, 2011). Besides that, the pilot testing helped to identify the initial flow of themes while observing the new emerging themes and also to develop familiarity with transcribing qualitative data.

During the piloting meetings, it was noted that some questions were ambiguous and required to be re-phrased. It was observed that two respondents took time to understand and kept asking for more explanations. For example, Mr. Manoni suggested re-phrasing the word 'e-fraud' because he perceived it as not a familiar term and instead to use the term 'online fraud' which is a common term for auditors. One auditor and the two lecturers suggested using the word 'technology' instead of the word 'information systems', citing a possibility of confusing the term with the MIS. The suggestions were noted and the researcher became mindful whenever the two terms were mentioned, their meanings were clarified or the more familiar alternative terms were used. Advocated by De Vaus (1993: 54), "*conducting preliminary interview tests is to minimise risk"*. Thus, the initial study was conducted and it facilitated the enquiry by minimising methodological risks in the overall main study.

5.7.3 Practising Brackets

Crotty (1996) defined bracketing as an attitude of disallowing personal views, beliefs, assumptions and experiences to dominate data collection. The researcher adopted bracketing practices by setting questions that engaged external auditors in the discussion. Each respondent was given time to explain in own words, phrases and examples on what they considered necessary on each question. The researcher set aside her own feelings but at the same time cross-checked them, whereas hesitations and prospects were noted in the memo to reflect the respondents' views (Merriam, 2009). However, it was not possible for the researcher to vision respondents' explanation and involvements "*without observing it from a starting point"* (Fischer, 2009 pp. 584). This means that the researcher did not totally detach her own awareness and experiences as the data developed but rather opted to be vigorous and open to her own perspectives that arose to ask clarifications on what the respondents offered.

Likewise, the researcher practised constant contemplative bracketing, which means re-evaluating prior information and re-reading it in light of fresh knowledge (Fischer, 2009). The transcripts were checked, re-checked and cross-checked to find details of the researcher's own views, words and experiences to see the likelihood of their influence on the overall data (Merriam, 2009). Upon close scrutiny, the researcher accepted that her own assumptions, words and direction did not influence her transcriptions of what the respondents mentioned. After that, the transcripts were revised to increase the value on what they said about the use of IS, the impact of IS on financial audit process and in e-fraud detection.

5.8 Qualitative Data Triangulation

Data triangulation is a situation where more than one source of data is used to improve confidence in research outcomes (Creswell, 2009). In this study, the researcher identified respondents who had varied experiences in auditing. Some had worked with international audit firms while others had worked with local firms. Furthermore, their skills and expertise also differed significantly. While some had accounting specialities, others were IT specialists, yet, others were engineers and computer sciences specialists with additional accounting knowledge. The researcher compared the experiences and expertise of the respondents in order to get the point of similarities and differences. The different audit experiences and knowledge background is what the researcher considered as one of data triangulation on the part of qualitative data.

Additionally, the researcher engaged a practical data triangulation in the form of field notes, interviews and questionnaire responses to compare and contrast the findings. This is what the researcher referred to as a mixed-data triangulation. Besides that, a number of times, the interviews were reviewed to appreciate the intricacies of the respondents and to develop a comprehensive understanding of their meanings. In a position wherever each method of data

collection gives reasonably similar results, it is considered to have attained validity (Teddlie and Yu, 2007).

Furthermore, while in the process of data collection, analysis, interpretation and writing up of the thesis, the researcher cross-validated data by re-reading the transcripts, listening to the saved audio recorded interviews and revising field notes, memos and quotes of the respondents so as to support the interpretations. Similarly, the websites of the audit software were visited in order to confirm the names of the software so as to avoid any misspelling. Likewise, other websites were also visited such as the ISACA Tanzania local Chapter so as to confirm the enrolment of membership into IT governance issues as was mentioned by the respondents. Moreover, the researcher asked for comments from the respondents (validation of data) after writing the results so as to apprehend a polished perspective from the auditors and to identify any subject error, observer error and researcher's own prejudice (Merriam, 2009). Overall, triangulation of data facilitated the researcher to corroborate the data and to apprehend scopes of shared phenomenon.

5.9 Transferability, Validity and Reliability

Transferability refers to the relevance of the study beyond the reported findings by the researcher (Merriam, 2009). In other words, it is the validity of the reported findings if the same study is conducted to another context whereby *"the original researcher does not know the population"* (Lincoln and Guba, 1985, pp. 298). In practice, transferability and generalisability sound similar to the art of knowledge sharing or testing the results to another setting. Hence, the researcher employed thick narratives to detail the framework and research findings and left the reader to contemplate the level of confidence before determining whether to apply the findings to another context (Maxwell, 2005). Furthermore, the respondents and

research locations were cautiously selected so as to enable reviewers to apply the results to another environment (Merriam, 2009).

Reliability has been referred to as dependability, stability and worthiness of the study findings, which is defined as the ability to produce the same results if the same study is repeated by another person (Lincoln and Guba, 1985). According to Merriam (2009), reliability is the first criteria for a good quality research. According to Lincoln and Guba (1985), reliability is the ability of the researcher to convince spectators that the research findings are worthwhile for consideration. It is about the consistency of the findings for others to replicate based on detailed novelty research (Merriam, 2009). In this study, reliability was considered through the use of data triangulation strategy and examination of the work by members of the supervisory committee by sharing the transcripts and consulting to confirm the stability of the findings.

Likewise, the researcher constantly visited the websites to confirm other information such as the names of the software that were mentioned during the interview, in order to avoid mistakes in naming the mentioned technologies. Furthermore, the researcher submitted her first paper in a conference and presented it to a large audience which was composed of experts in audit technology to check the stability of the results for comments and questioning. At the conference the researcher received useful feedback and suggestions to improve the reported findings. Furthermore, the researcher documented all field notes, memos, diary entries and transcripts for inspection by her supervisors whenever they were needed so as to enhance reliability of the findings of the study. Similarly, the reliability of the quantitative data was examined through Cronbach alpha, whereby statistical tests of the variables revealed high internal consistency which suggested that the data were appropriate and further analysis could be conducted. Also, the survey questionnaires were adopted from reliable sources and

were piloted before they were sent to the respondents. This process ensured the reliability and the validity of the reported findings.

5.10 Quantitative Data Collection

Quantitative data were collected through the use of a questionnaire which started after a short interval from qualitative data. The questionnaire was used as a secondary data source to support interviews. Zamalia (2008) defines a questionnaire as a list of questions written in a proper chronological order based on the concepts under investigation. The questionnaire is usually addressed to the respondent asking him/her to read, interpret and provide answers based on his/her own perception (Malhotra, 2009). While some questionnaires are open ended, some are closed ended. Open-ended questionnaires provide open space for respondents to explain in detail their own views based on the questions asked. Meanwhile, closed-ended questionnaires do not provide space for further explanations, rather respondents are asked to rate the items according to the degree of measurements. The unique value of using questionnaires is the anonymity of the respondents which makes them provide answers freely as compared to interviews (Silverman, 2010). Another advantage is the large number of responses which provides greater opportunity to generalise the results to a larger population (Zamalia, 2008).

In this study, the researcher used a closed-ended questionnaire as data collection tool. The reasons for using closed-ended questionnaire include (1) the ease in asking the questions, (2) it promotes uniformity in asking the same questions, (3) the ease in administering questions; and (4) it eliminates bias from the interviewer's point of view (Zamalia, 2008). The questionnaire had three sections: section one was the demographic characteristics of the respondent, section two was the organisational profile, and section three was the IS usage. Due to the fear of validation of the questionnaire items to a new setting (Tanzania), the

questionnaire was adopted from two main sources. The first and second part of the questionnaire was adopted from Ahmi and Kent (2013), when investigating the adoption of GAS by small and medium audit firms in the UK. The last part of the questionnaire was adopted from the UTAUT model (Venkatesh et al., 2003), when the items were refined to fit the external auditing context as were modified by Curtis and Payne (2014). The reason for adopting these two sources of questionnaire was their high loading on reliability test which in both cases, they had Cronbach Alpha of more than 0.7, which suggested a high internal consistency (Cohen, 1998).

According to Hair (2010) and Zamalia (2008), questionnaires can be administered through different ways: (1) self-administered questionnaire, (2) posted questionnaire, (3) Internet-based questionnaire, (4) telephone questionnaire; and (5) email. This study used the following methods to deliver the questionnaires to the respondents, namely (1) self-administered questionnaire, where printed copies of the questionnaires were given to the respondents in person, (2) email questionnaires- which were sent to the auditors after getting their email addresses from their workplace; and (3) online questionnaires which were prepared though Qualtrics. However, the researcher distributed most of the questionnaires in person and through connections with friends who were working with the audit firms. It was necessary for the researcher to distribute the questionnaires in person in order to encourage feedback and to reduce delays in data collection which characterises most survey-based studies (Zamalia, 2008).

It was observed that external auditors were extremely busy and most of them delayed in returning the questionnaires. As a result, it delayed the process of collecting quantitative data through emails and Qualtrics. Hence, the researcher travelled from Malaysia to Tanzania so as to administer the process of collecting the questionnaire responses. By December 2016, 117

responses were collected. Due to time constraints, the researcher closed the process of data collection and focussed on data analysis. The questionnaires with missing values were eliminated and the remaining 106 were considered appropriate for further analysis.

5.10.1 Piloting the Questionnaire

Before the questionnaires were sent out, the original version was given to fellow PhD students at the UNMC. The purpose of doing this was to share their experience and to get their opinion on the accuracy of language and the number of pages in order not to produce an excessively lengthy questionnaire. After receiving their comments, the researcher fine-tuned the questionnaires to be ready for piloting. At another stage, the questionnaires were given to six (6) accounting lecturers in two different universities in Tanzania. Three (3) were from a private university and three (3) from a public university. The purpose was to get a varied opinion on the adequacy of the questions and whether they would be clear to an average respondent. At first, the researcher had included a few open-ended questions but the lecturers involved in the pilot study proposed that the researcher remove the open-ended questions because the interview method was also used, it should enable the open-ended questions to be clarified. Finally, the final questionnaire was completed and sent to external auditors for the final piloting because auditors were the ultimate intended sample to provide answers to the questions.

The piloting of the questionnaires to the auditors started on 18th April 2016 where 25 external auditors were asked to fill in the questionnaires. This process was administered on a personal basis in order to receive ready comments and not to delay the process of distributing the final questionnaires. A total of 20 questionnaires were received well filled and some were with written comments. For example, it was recommended to change the flow of the arrangements of the questions to capture the use of IS, followed by the benefits of using it and finally the

reasons for using IS (i.e the items of the UTAUT model) should come at the end of the questionnaire. Further comments were suggested on the numbering of the items inside the boxes for consistency. Upon receiving the piloted questionnaires, a Cronbach Alpha test was conducted to see whether the items were measuring the same factors. The items which had the lowest loadings were suggested to be removed. However, the pilot test showed that all the items scored at least 0.7, which is acceptable for internal validity (Cohen, 1998). The results of Cronbach Alpha are shown below in Table 5.5.

Table 5.5 Reliability Tests for the Pilot Study

Factors	**Cronbach Alpha**	**No. of items**
Performance expectancy	0.844	5
Efforts Expectancy	0.792	5
Social and Organisational factor	0.957	5
Facilitating Condition	0.951	5
Audit Clients' Factor	0.843	6
Audit Professional Factor	0.922	3
Behavioural Intentions to use IS	0.939	3

Finally, the questionnaires were distributed to the auditors and also uploaded into Qualtrics. Qualtrics is an online platform for uploading questionnaires. Meanwhile, some of the questionnaires were emailed to auditors based on their emails that were found on the NBAA website. The NBAA website displayed the names of the auditors, their qualifications and affiliated employers. The first batch of questionnaires (200) was sent to the auditors on 29th April 2016. One of the biggest challenges in using questionnaires as a data collection tool is the delay in the responses (Zamalia, 2008). In order to speed up the process, two weeks after distributing the questionnaires, the researcher sent a reminder to the respondents. After two months another reminder was sent. The second batch of questionnaires (100) was sent on 5th

June 2016. Until December 2016, a total of 117 questionnaires were received. The researcher then started entering the data into SPSS software version 23.

5.10.2 Research Variables

Variables are aspects (Creswell, 2007), statements (Hair et al., 2010), concepts or social occurrences (Zamalia, 2008) that a researcher can identify when conducting investigations. Variables can be categorised into four: (1) independent variables (IVs), (2) dependent variables (DVs), (3) moderating variables (MVs) and (4) mediating variables (M-Ds) (Hair et al., 2010; Field, 2013). The first two are very common and are used in numerous investigations, while the latter two are uncommon and mostly used in advanced studies (Kumar et al., 2013) to test further existence of relationships. An IV is an attribute that impacts DV (Creswell, 2007; Zamalia, 2008); it is a variable that does not rely on anything except itself. In fact, an IV is the one responsible in bringing changes on the DV (Field, 2013).

The IV for this study was denoted by a combination of factors that influences the use of IS by external auditors. These factors are categorised into internal (organisational factors and individual factors) and external factors. Specifically, IVs (which are identified in RQ2) include: performance expectancy, efforts expectancy, social and organisational influence, facilitating condition, audit clients' factor and the audit profession factors. When a variable is composed of multiple statements or concepts which can test the same aspect, it is called a construct (Hair et al., 2010). The IVs used in this study are in the form of constructs predicted to measure the same items. In contrast, a DV is the final outcome caused by the variation as a result of manipulations of the IVs (Hair et al., 2010). In other words, a DV portrays the predicted value of the experiment being measured (Zamalia, 2008). The DV in this study is denoted by the intentions to increase the use of IS.

To sum up, the study through objective 2, predicts that the intentions to use/increase the use of IS can be achieved as a result of changes in the IVs (performance expectancy, efforts expectancy, social and organisational influence, audit clients' factor and the audit professional factor). Figure 5.2 shows a schematic relationship between the IVs and the DV in answering the second RQ.

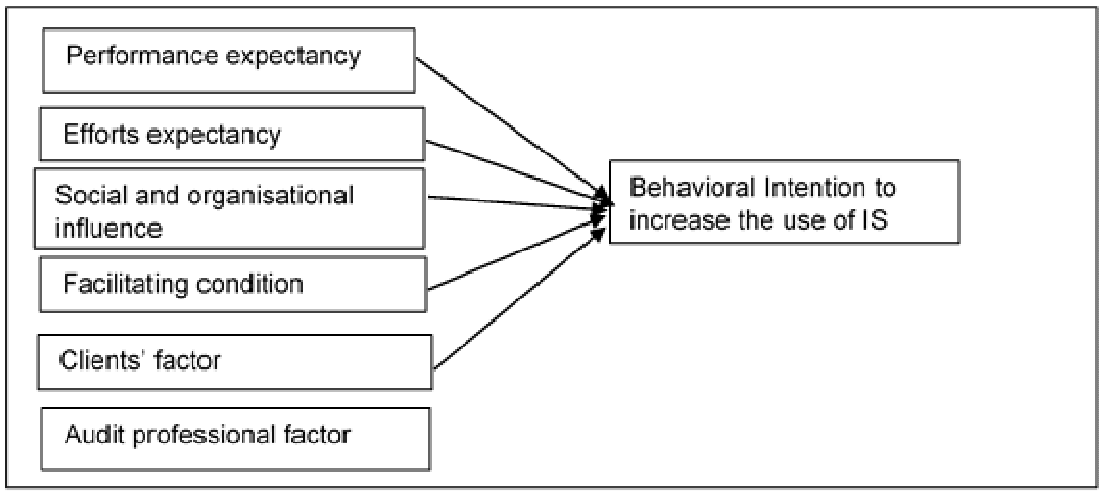


Figure 5.2 Schematic Relationship between IV and DV

In addition to the predicted relationship, there is one MV existing between the two IVs and DVs. According to Field (2013), a MV is a variable that affects the strength of the relationship between the IVs and DVs. According to Hair et al. (2010), a MV is a variable that "obstructs" or "modifies" the association between the IVs and DVs.

Nonetheless, in order for an MV to show the effect of IV on the DV, there must be an established significant relationship between the IV and DV prior to the inclusion of the MV. As a result, the inclusion of the MV amidst the IV and the DV could show the impact by either increasing the relationship beyond the initial prediction or decreasing it (Kumar et al., 2013). In assessing the effect of the MV on a modest model: first, the IV need to affect the DV, second, the MV must affect the DV, and third, there must be an interactive effect which is the product of the MVs and IVs (i.e. MV multiplied by IV) on the DV (Field, 2013). In this

study, a MV is voluntariness to use IS. The study predicts that as technology usage remains to be on a voluntary basis (not mandatory), there should be a change on the effect when social and organisational factors are involved as IVs. In order to test for the effect of the MV (Voluntariness) amidst social and organisational factor (IV) and BI to increase the use of IS (DV), a sequence of regression determination should be executed in stages. At first, the IV and DV will be regressed, second the MV will be regressed against the DV, and third, regression will be conducted for the interactive effect amidst IV and MV alongside DV (Kumar et al., 2013). Figure 5.3 shows a schematic illustration between an MV (Voluntariness to use IS) amid the IVs and DV.

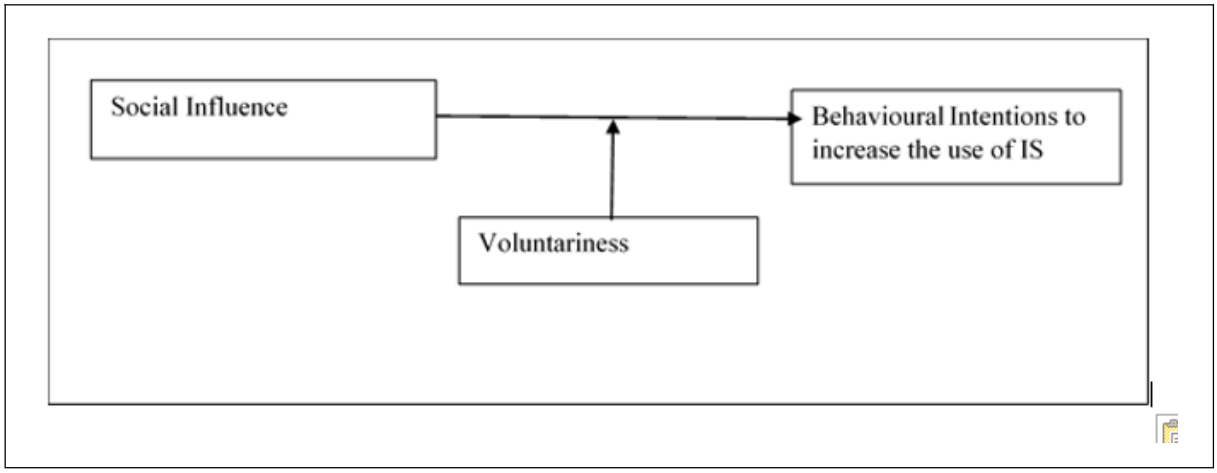


Figure 5.3 A Schematic Relationship between IV, MV and DV

5.10.3 Data Measurements

In quantitative investigations, data measurement is an important step as it provides the basis on the reliability and validity of concepts (Field, 2013). In order for the measurement to be acceptable as predictable constructs in research, they must be consistently used, measured and accurate (Zamalia, 2008). Validity and reliability are the two terms that are used in assigning measurements and which are linked to good predictable findings. In numerical techniques, reliability is the uniformity of dimension, stability and accuracy of measurement throughout

the research process (Field, 2013) while validity is acceptance of what the researcher intended to predict (Field, 2013; Zamalia, 2008).

In many quantitative studies, researchers use four main measurements namely, nominal, ordinal, interval and ratio. Nominal is the least frequent scale used in numerical studies as it denotes a letter or a number assigned to identify a particular class or category. For instance, in gender, males could be assigned number 0 while female assigned number 1 (Field, 2013). The central tendency that can be used to describe a nominal value is the mode. Meanwhile, an ordinal scale permits the ranking of items in a chronological order by which data can be sorted. The central tendency used to measure ordinal scales are the mode and median. In addition, an interval scale arranges items of responses on the basis of their magnitude, either in increasing or diminishing order. Mode, median, mean and standard deviation can be computed using the interval scale (Field, 2013).

In standardising respondents' data, the questionnaires were designed to include nominal, ordinal and interval scales. Nominal and ordinal scales include the profile of the respondents (i.e gender, age, qualification, experience, etc.) Likewise, the type of organisation and the type of technology used were all scaled in nominal and ordinal data. Meanwhile, interval, being the most common scale that is used in most quantitative management research (Field, 2013; Kumar, 1999), has characterised the remaining largest portion of the questionnaire. A five-point Likert scale was used in ascending order with (1) denoting strongly disagree, (2) disagree, (3) neutral, (4) agree; and (5) strongly agree.

5.11 Data Analysis

This study has used a mixed method strategy where both qualitative and quantitative data were collected. The interviews data were analysed in themes while the questionnaires data

were analysed using descriptive and inferential statistics such as mode, mean, standard deviation, EFA, and regression. The next sub-section explains the process of analysing qualitative data, followed by the quantitative data analysis techniques.

5.11.1 Qualitative Data Analysis-Thematic Analysis

Thematic analysis is a procedure used by researchers in qualitative enquiries to infer raw data into making sense (Silverman, 2010). It is an imaginative presentation of data gathered through interviews or any recognised texts associated to the study (Merriam, 2009). Thematic analysis includes labelling the manners in which patterns are established, connected, defined and applied (Creswell, 2007; Silverman, 2010; Thorpe and Holt, 2008). In thematic analysis of texts, the collected data are clustered according to common themes that describe the communality of respondents in relation to the main issues being asked (Thorpe and Holt, 2008). As advocated in Creswell (2007, p. 244) "*thematic analysis entails scholars to examine the data for explicit themes by grouping information into large groups of concepts and elaborating evidences that substantiate the themes"*. Hence, grouping the communalities in themes resulting from the text data needs rigorous and intellectual understanding from the researcher. In other words, the interpretations depend on the researcher's instinctive understanding of the findings (Creswell, 2007).

In order to ease categorising themes, the researcher used NVivo software version 10 to create, code and store groups of data within the main topics of investigation. The Nvivo software fosters quick, efficient and transparent procedures in categorising themes which can be shared by a group of other researchers (Bazeley and Jackson, 2013). At first, the interview transcripts were cleaned to remove repetitions and less weighted words, which could not alter meanings to the answers. Secondly, the cleaned transcripts were uploaded into the Nvivo software whereby the researcher created a new project which was assigned a name 'IS in auditing' and

saved it on the desktop. The process of uploading the data into the software is called 'importing data from an external source' (Bazeley and Jackson, 2013). Third, the researcher created nodes based on the selected topics/themes identified from the research questions. A node is a container that stores the items/words/phrases from the process of coding. Meanwhile, coding is a process of gathering materials by topics or themes (Bazeley and Jackson, 2013). Therefore, five main themes were identified namely, (1) Usage of IS tool, (2) factors for use of IS, (3) Impact of IS on audit process; and (4) How auditors detected e-fraud; and (5) Impact of IS usage on e-fraud detection. The remaining spoken narratives which were beyond the scope of this study were kept under 'emerging themes' (Silverman, 2010). The emerging themes were (1) clients' business complexity (2) adoption of E-government in Tanzania and (3) challenges in the use of technology in the external audit environment. The emerging themes were used in publishing research papers.

Generally, Nvivo categorises nodes in two ways which are (1) parent nodes; and (2) child nodes (Bazeley and Jackson, 2013). A parent node is a container that carries the general theme of the research question. On the other hand, a child node is a container that carries sub-items of a parent node that explains a specific item. Hence, each of the identified themes for this study represented parent nodes. The researcher dragged and dropped words, sentences and paragraphs from the transcripts into the child nodes to act as a back-up of what has been said on the particular theme. For example, in the parent node 'Usage of IS tools', the researcher identified types of software used according to their functionalities and were codes as child nodes (see Appendix X). A summary of the IS tools was represented in pictorial form (tree-maps) according to the number of references mentioned in the transcripts (see Figure 6.1). The same procedures were done to the remaining themes. The findings of the detailed interview data analysis are reported in Chapter 6. The following table (Table 5.6) shows the demographic data of the interviewed respondents.

Table 5.6 Profiles of Interviewed Respondents

Respondent	Sex	Firm	Position	Experience and Education
R1	Male	A	Managing Partner-FA	B.Com (Accounting), MSc, CPA (T), 15 years audit experience.
R2	Male	B	Associate Director-IS-A	BSc (Electronics), CISA, CFE, 13 years audit experience.
R3	Male	C	Senior Manager-FA	BCom (Accounting), CIMA, 8 years audit experience.
R4	Male	D	Manager-FA	BBA, ACCA, 7 years audit experience
R5	Male	E	Senior Manager-IS-A	BSc (Computer Science), CISA, CPA (T) 8 years audit experience.
R6	Male	F	Associate Manager-FA	BBA (Accounting), CPA (T) 9 years audit experience.
R7	Male	H	Manager-FA	BBA (Accounting), CPA (K), 7 years audit experience.
R8	Female	I	Senior Manager-IS-A	BSc, CISA, 9 years audit experience.
R9	Male	J	Partner-IS-A	BSc (Engineering), MSc, CISA, ACCA, 16 years audit experience.
R10	Female	K	Associate Director-IS-A	BSc (Computer Science), MBA, ACCA, CISA, 15 years audit experience.
R11	Male	L	Country Managing Partner-FA	ATEC, MSc (Auditing), MBA, CPA (T), 21 years audit experience.
R12a	Male	M	Managing Director-FA	BCom, MBA, PGDA, CPA (K), CPSP-K, CPBC, 19 years audit experience
R12b	Male	M	Partner-IS-A	BSc (Computer Science), CISA, CPA (K), 13 years audit experience.

Note: R= Respondents; FA-Financial Auditor; IS-A = Information Systems Auditor

Table 5.6 shows that eleven (11) respondents were males and two (2) were females. The respondents' working experience in auditing was ranging between 7 and 21 years; had Bachelor Degrees in Business or Computer Science and Engineering with professional certification in either CPA or Certified Information Systems Auditor (CISA) qualifications. Most of the respondents had CPA (T) and CPA (K) while 3 had a UK accounting qualification (ACCA). The qualifications of the respondents are in line with the description in

the changing nature of using technology in auditing which requires multiple skills (Seeburn, 2013; Kotb and Roberts, 2011).

5.11.2 Quantitative Data Analysis

The Quantitative data were analysed in the form of descriptive and inferential statistics. Descriptive analysis is part of a statistical analysis of data set which can help a researcher to summarise patterns of a sample as a representative of a given population (Malhotra, 2009). Descriptive statistics can be analysed based on three patterns: (1) those that measure frequency of occurrences, (2) those that measure the central tendencies and (3) those that measure the variations (variability) (Zamalia, 2008). The first category includes histograms, percentages and normal distribution patterns. The second class includes mean/average, median and mode, while the last class includes range, variance and standard deviation.

According to Sekaran and Bougie (2010), mean is the most common measure of central tendency. Hence, the following figures were used as suggested by Sekaran and Bougie (2010) in interpreting answers from different mean scales: (1) a figure of 1.00-2.33 implies low mean score, (2) a figure of 2.34-3.66 implies medium; while (3) figures of 3.67-5.00 imply high mean scores. Meanwhile, reliability tests were used to check the accuracy of internal validity dimensions that were performed to all constructs after entering the data into SPSS. The most common test of internal validity is the Cronbach Alpha (Field, 2013; Malhotra, 2009). The following values are recommended for Cronbach Alpha scales: (1) values of 0.70-1.00 implies high reliability, (2) values of 0.60-0.69 implies moderate reliability; while (3) values range of 0.00-0.59 implies low reliability (Field, 2013; Malhotra, 2009).

Furthermore, the study conducted advanced statistical analysis to infer the sample of the population. The importance of performing inferential analysis is to generalise the findings using statistical power to confirm variations in relationships (Zamalia, 2008). Morever,

inferential statistical analysis helps to recognise a correct variance and consequently rejecting a null hypothesis (Field, 2013). A research test lacking sufficient statistical power might result in potentially making a Type II error by suggesting a rejection of the null hypothesis when essentially a significant relationship exists (Malhotra, 2009). Hence, the appropriate inferential statistical analyses for this study are the Analysis of Variance (ANOVA), correlation and regression.

ANOVA was used to identify interactive effects between variables, between and within the groups; hence, providing confirmations for further complex propositions (Field, 2013). Specifically, one-way ANOVA was applied to relate the means on the perceptions of respondents regarding factors influencing the usage of IS. Additionally, a number of hierarchical regressions were performed to determine additional effects after adding demographic variables (age, gender and experience in computerised auditing, professional affiliation, auditor type and IT skills).

Besides ANOVA, a correlation analysis test was conducted to determine any relationship among the individual variables. Some variables may suggest a positive relationship, others negative, yet, some may have no relationships (Field, 2013). The most common tool to run a correlational analysis test is the Pearson Product Moment Correlation (Malhotra, 2009). In this study, the relationship between IVs (factors influencing the use of IS) and DV (BI to increase the use of IS) was examined to establish its association in a linear approach. When testing correlational analysis, the magnitude and direction of the relationships are the two essential items to note for interpretation (Filed, 2013). As such, the following benchmarks were used to interpret Pearson values (r): (1) when r = 0.00-0.40, it implies a low relationship (2) when r = 0.50-0.70, implies a moderate relationship, and while (3) r = 0.80-1.00 it implies a high relationship (Cohen, 1998).

Finally, a regression analysis was performed to predict a relationship between the IVs and the DV. In other words, a researcher can observe one IV at a time against the mean value of a DV while other IVs are held constant (Malholtra, 2009). In this study, regression analysis was performed to formulate an equation that characterised the best prediction of factors influencing the use of IS. It was predicted after running a factor analysis, that several factors would emerge confirming similar loadings and labelled as one item ready for a regression analysis. From the regression equation, the emerged predictors were used for interpretation and analysis. The coefficient of determination (R^2) was used to establish the goodness of fit of the overall significance of the regression model (Field, 2013). The following measurements for R^2 were used for interpretation of the strength of the regression model: (1) 0.00-0.40 weak effect (2) 0.41-0.70 moderate effect and (3) 0.80-1.00-strong effect size (Field, 2013).

Table 5.7 Summary of Research Objectives, Variables, Data Measurement and Data Analysis of the Study

Objective	**Research Objective**	**Variable**	**Measurement**	**Data Analysis**
RO1	To explore the extent of IS usage by external auditors in Tanzania	Qualitative: the types of software and applications used	Nominal data and Qualitative data	Descriptive and Qualitative data
RO2	To evaluate factors influencing the use of IS by external auditors	IV = PE, EE, SOI, FC, CF and APF. DV = BI to increase the use of IS	Interval (5-point Likert Scale)	EFA, Correlation Regression and Qualitative data
RO3	To investigate the impact of IS on the financial audit process	n/a	n/a	Qualitative data
RO4	To explore how external auditors detect e-fraud in computerised business platforms	n/a	n/a	Qualitative data
RO5	To investigate the impact of the IS usage on e- fraud detection	n/a	n/a	Qualitative data

5.12 Should Hypotheses/Propositions be Used to Predict the Outcome?

There is incongruity among scholars on the meaning and uses of the terms 'hypothesis' and 'proposition' and when the two are used interchangeably or simultaneously, they create even more confusions (Cooper and Schindler, 1998). Usually, propositions are used to predict the outcomes of the study of qualitative enquiries while hypotheses are used to predict the results of the quantitative investigations, laboratory work and experimental studies (Morse and Field, 1995). By definition, a proposition is a statement on existing concepts for which no experimental test is available, rather, is based on observable phenomena; while hypothesis refers to a condition where a prediction is formed to speculate an end result of an experiment or when a proposition is presented for empirical validation (Cooper and Schindler, 1998: 43). The two definitions suggest that both proposition and hypothesis have one common factor which is 'prediction of a possible answer (either true or false) to a specific scientific question'.

Since the main concern of this study is to answer questions related to 'why' and 'how', rather than 'when or how much', it becomes relevant to use research questions to stand as propositions to find in-depth explanations that will result in generating new knowledge based on the respondents' own experiences (Morse and Field, 1995; Cooper and Schindler, 1998; Merriam, 2009; Silverman, 2010). Besides that, it is argued that proposition development follows a very positivist view of research; hence, it is rather at odds with the interpretivist nature of qualitative research which has characterised the largest part of this enquiry (Minichiello et al., 2008). The study therefore, used research questions to stand as propositions as discussed in subsection 3.10 which is in line with previous studies in audit technology (see Vendrzyk and Bagranoff, 2003; Kotb and Roberts, 2011; Seerburn 2013; Widuri et al., 2016; No & Vasarhelyi, 2017).

To summerise, the study used the literature review to identify the gap in research and to formulate research questions that guided the investigation as elaborated in subsection 3.10. Hypotheses were developed in the 2nd research question only to complement the findings especially to test the modified UTAUT. It can be concluded that this study has adopted a partly pragmatic methodological stance to make it more communicative yet simple to understand by an audience from various research backgrounds.

5.13 Questionnaire Development

The questionnaire for this study composed of three main parts. Part one captured the demographic features of the respondents and audit firms, part two explored the usage of IS, and part three focussed on the reasons for the usage of IS tools.

5.13.1 Organisational Profile

The profile for the audit firms under study is important for inclusion in the questionnaire. The details can help to understand the evolving organisational awareness in the use of IS. Two types of organisations were targeted for this research namely, large and medium audit firms. This is because the use of technology can be more expected among medium and large audit firms as compared to small audit firms (Greenstein-Prosch et al., 2008).

5.13.2 Date of Establishment

The time frame for the organisation's existence is important. Newly formed audit firms will be associated with scanty practical knowledge of the audit risk involved in the digital environment while highly experienced audit firms can provide more evidence on the challenges in the computing platform as the client's business environment keeps changing. For example, Greenstein-Prosch et al. (2008) found that recently formed audit firms had less market experience with clients whereas experienced audit firms such as the Big Four, had a

variety of market experience with frequent multiple engagements. These differences can have an impact on how the audit firms use technology.

Table 5.8 Structure of the Questionnaire

No	Constructs	No of Items	Data Measurement	Source of Reference
1	Demographic data of respondents	10	Nominal (Multiple Choice)	• Ahmi and Kent (2013) • Venkatesh et al. (2003) • Curtis and Payne (2014) • Janvrin et al. (2009) • Greenstein-Prosch et al. (2008) • Kotb and Roberts (2011)
2	Organisational profile	2	Nominal (Multiple Choice)	
3	Usage of IS	4	Nominal (Multiple Choice)	
4	Benefits of using IS	9	Interval 5-point Likert Scale	
5	Performance expectancy	6		
6	Efforts expectancy	5		
7	Social and organisational influence	5		
8	Facilitatng condition	5		
9	Clients' factor	6		
10	The audit professional factor	3		
11	Behavioural intentions to increase the use of IS	3		
Total Number of Items		**58**		

5.13.3 Demographic characteristics of Auditor

(i) Age of Auditors

Prior studies reported a relationship between age of auditors and the use of IS (Kim et al., 2009; Sun 2012). For example, Sun (2012) found that the IS usage is frequent among auditors of a young age as compared to old aged auditors. This could be partly attributed to the fact that the younger generation are more prone to using digital devices faster and are more eager to learn because they are born in the digital age as compared to mature/older auditors.

(ii) Gender of Auditors

The gender of the auditors can have an influence on the use of IS. Mahzan and Lymer (2008) found that female auditors used technology more frequently as compared to male auditors, while Debreceny et al. (2005) found that males used IS better than female auditors. These studies show pragmatic evidence as such; this study has included gender into the questionnaire intending to predict an influence to occur by running hierarchical regression.

(iii) Experience of Auditors

Auditor experience has a relationship with IS usage. Mahzan and Lymer, (2014) found that more experienced auditors are less likely to use technology as compared to less experienced auditors. This is so partly because an experienced auditor has more understanding of the clients' business environments and can easily use judgemental approach to spot areas of weaknesses due to his knowledge in the varieties of internal control of different businesses. Likewise, Huang et al. (2008) and Razi and Madani (2013) found that audit partners and managers used IS more frequently as compared to junior auditors.

(iv) IT Knowledge of Auditors

Auditor's knowledge is another important factor that can affect the use of IS. Hunton et al. (2004) and Brazel (2008) reported that IT expertise in auditing is important in influencing the decision to use technology. Meanwhile, Stoel at al. (2012) found auditor IT knowledge an important factor in ensuring IT audit quality.

(v) Professional Affiliation

Auditor specialisation is an important factor in influencing the use of IS. According to the International Education Practice Statement (IFAC 2006), the knowledge component of

auditors in a digital environment must have a mixture of business-related knowledge, including emerging IT issues. Hence, some auditors were reported to have only CPA while others had CISA, yet others had both CPA and CISA qualifications (Hunton et al., 2004). As reported by Brazel (2008), effective digital risk assessment can be achieved when auditors exhibit expertise in both knowledge areas. Hence, professional affiliation will be predicted to have an effect on usage of IS beyond the identified IVs.

(vi) Auditor Type

The type of auditor, whether financial auditor or IS auditor can have an impact on IS usage behaviour. Studies documented that IS auditors used technology more frequently than financial auditors, while Hunton et al. (2004) reported that both auditors had same confidence in the usage and understanding of IS. Hence, it was necessary to include the item into the questionnaire to predict its impact beyond the main six identified variables.

5.13.4 Response Rate of the Questionnaire

The study sent two hundred (300) questionnaires to the external auditors between 29th April and December 2016 and received an overall response quantity of one hundred and seventeen (117). The sorting of responses was conducted to identify missing items. The breakdown of the responses from the questionnaire is shown below on Table 5.9.

Table 5.9 Breakdown of Survey Response Rate

Phases	**Questionnaires sent out**	**Received questionnaires**	**Percentage**	**Not received**	**Percentage**
1st round	200	62	31%	138	69%
2nd round	100	55	55%	45	45%
Total	**300**	**117**		**183**	

From the response rate obtained in Table 5.9, the study conducted data cleaning in order to identify responses which had missing values and those which showed inconsistent patterns. During the process of entering the data into SPSS, it was observed that some of the respondents had filled parts of the questionnaire while others had not filled certain parts of the questions. These were removed in order to eliminate distortion of the data.

Table 5.10 Missing Data in the Questionnaire

	Number of Responses	**Percentage**
Filled up to page No.6	106	89%
Filled up to page No. 5	5	4.1 %
Half-way filled Questionnaires	4	3.3%
Did not fill some items in a questions	3	2.6%
Total	117	100%

The study considered the questionnaire response (106) that were filled in from page 1 to page 6 as relevant for analysis. Table 5.11 shows the grouping of respondents according to seniority to reflect the types of auditors who provided the information.

Table 5.11 Response According to Seniority

	Number of Responses	**Percentage**
Partners	2	1.9%
Managers	37	34.9%
Seniors	59	55.7%
Junior	08	7.5%
Total	**106**	**100%**

The sample size might seem to be small for a generalisation, but it represents 47.1% of the recommended sample size (225) and it also represents 19.8% of the registered auditors in

public practice which is 553 (NBAA, 2015). The analysis of the data from the questionnaires is presented in Chapter 7.

5.14 The Value of Mixed method Research: a Message for Future Researchers

Mixed methods research is a growing field of methodology that has been practised for nearly 70 years (Creswell & Plano Clark, 2007); but attained its prominence in the late 1980s. The approach is increasingly used by a growing number of researchers in social sciences, business and clinical health (Creswell, 2007; Creswell & Plano Clark, 2007; Dunning et al., 2008). In fact, the number of dissertations and theses with keywords "Mixed methods" increased from 3 in 1984 to 2,538 in 2013 (McKim, 2017). Some studies affirmed that the increased use of mixed methods is partly motivated by the perceptible deficit of quantitative methods (O'Cathain et al., 2007).

The increase in mixed methods research justifies the question of determining the perceived value of mixed methods research compared with mono-method/single method which uses either quantitative or qualitative data. Among the most cited values of mixed methods research includes increased validity of the findings and assisting with creation of new knowledge such as identifying new variables (Hurmerinta-Peltomaki and Nummela, 2006). Similarly, studies found that the use of a mixed methods approach increased a sound and comprehensive understanding of the phenomenon than studies that used a single/mono method approach (Creswell, 2007). Furthermore, it is argued that studies that used mixed method approach received higher academic citations as compared to studies that used single method approach (Molina-Azorin, 2011).

For future researchers who wish to use the mixed methods approach, we suggest that they consider two important issues. First, researchers need to have sufficient time to conduct mixed methods research (Creswell & Plano Clark, 2011). Since both qualitative data (i.e

interviews, documentaries, observations etc) and quantitative data (i.e. survey) will be used, additional time is essential in collecting and analysing the two data sets. However, researchers can consider recruiting research assistants to speed up the process of data collection especially survey data (McKim, 2017). Collecting survey data does not necessarily need the presence of the researcher especially if the respondents understand the language used in the questionnaire. In contrast, collecting interview data needs the presence of the researcher in order to probe for clarification of the issues and also to observe verbal emotions of the respondents (Silverman, 2013). Similarly, analysing a mixed methods data needs expertise in both quantitative and qualitative methodology (Creswell, 2007). This includes learning software for data analysis such as Nvivo and SPSS, understanding the meaning of the figures and interpretation of the final results. Since data analysis is the core part of the research findings, it is highly advised for mixed methods researchers to identify earlier the tools they will use during data analysis before commencement of data collection process (Creswell, 2007).

The second point to take note when using a mixed methods studies is the additional resources (funding) that will be required to accomplish various tasks (Creswell & Plano Clark, 2011). Typically, researchers in mixed methods studies will need additional funding for additional supplies and additional space to interview informants or administer a questionnaire. Likewise, additional cash budget is essential to pay assistants who lend a hand with data collection and or data analysis processes. These additional costs might be very low if a mono-method approach (i.e. qualitative approach) is used.

In respect to this study, interview data were collected first followed by questionnaires. This approach is applicable mostly when little or no literature exists on the phenomenon of concern (Yin, 2009), as was the case with IS usage among auditors in Tanzania. However, for

future researchers who want to take this approach, the best and common approach in mixed method research is to collect survey data first, analyse the quantitative data then conduct interviews later (Creswell, 2007). This approach can help to triangulate the results and also explain any inconsistencies arising from the two data sources better by getting clarification from the informants.

5.15 Summary of the Chapter

In this Chapter, the study explained the research design used for the data collection, the approaches and the analytical process of the empirical data generated. The study adopted a cross-sectional concurrent mixed method design where data were collected in two short intervals. Both interviews and questionnaires were used as tools for data collection. Interviews were used as the main enquiry tool that covered all the four research objectives while questionnaires were used as a secondary source. The next Chapter presents qualitative findings.

CHAPTER 6

QUALITATIVE FINDINGS

6.1 Introduction

This Chapter explains the findings obtained from qualitative data which were collected through interviews. The Chapter has four sub-sections based on the research questions as shown in Chapter 1. The first sub-section describes the current level of IS usage by external auditors in Tanzania, highlighting the types of software and applications that were used, the efficiency and benefits of using a particular software. The second subsection presents the findings related to the factors of IS usage by external auditors, where the study used the UTAUT as a "theoretical lens" to explore internal factors for IS usage. The last two sub-sections present the impact of IS usage on the audit process and on e-fraud detection.

6.2 What is the Extent of IS Usage by External Auditors in Tanzania?

One of the objectives of this study was to explore the types of software and applications that were used by external auditors and how they facilitated various audit activities. All respondents (R1-R12) reported that they used various IS tools which include those that are meant to accomplish office-related tasks and those that are specifically meant to conduct audit activities. Table 6.1 summarises the specific types of software and applications used by external auditors.

Table 6.1 Types of IS Tools Used by External Auditors in Tanzania

Type of software	**Frequency (N= 12)**	**%**
Audit Command Language (ACL)	6	50%
Interactive Data Extraction and Analysis (IDEA)	3	25%
Physical Configuration Audit Software (PCAS)	2	17%
Engagement Management System (EMS)	5	42%
Pro-Audit	2	17%
Specialised Audit Software (SASoft)	2	17%
Teammate	4	33%
GAMX	1	8%
Auto-Audit	2	17%
Ethical Hacking tools	5	42%
In-house-software	4	33%
Others (UIE data collector)	2	17%
MS Excel	12	100%
MS Word	12	100%

Note: Audit firms used more than one software

The most frequently used audit software was ACL which was used by half (50%) of the respondents (R1, R2, R5, R8, R9 and R10). Two respondents reported that the use of ACL facilitated the process of data analysis by mining huge amount of data, summarising, detecting missing sequences, errors and spotting unusual patterns in transactions (R2 and R9). Furthermore, the interview findings showed that using an advanced audit software such as ACL facilitates interrogations of the data, predicting risk occurrences by checking outliers in a given set of electronic accounting records (R9 and R12b). The tool can display signals to auditors by showing where problems might have occurred, enabling them to concentrate on such areas rather than assuming risk to have occurred in all transactions (R9).

Furthermore, the use of ACL helped auditors to visualize the trends in data where the movement of events were observed in pictorial form (R2, R9 and R10). For example, if the curve for September appeared not to be straight, it indicated an abnormality in that period

(R9). Hence, auditors may choose to focus around those periods instead of assuming that the big risks have occurred everywhere. This saves time and assures effectiveness in risk assessment. One respondent, a partner from the Big Four commented "*The use of ACL can help us by showing a pictorial view of how the trends have been like for the whole period and help us to spot where the risks can be suspected rather than assuming risks in all the months" (R9).* Hence, the use of ACL does not only facilitate data analysis but also in risk assessment. It was also established that this tool was more useful in auditing large automated clients with multiple products.

One of the IS tools which was similar to ACL, was IDEA (sometimes referred to as Caseware-the name of the software vendor). IDEA can be used to export data files from clients' records in various formats such as spreadsheets, database, PDF, ERP systems and plain texts (R12a). The tool has in-built access to several audit functions such as fraud detection mechanisms, summarising data, stratification of sampling, auditing the entire population and the Bedford's Law (R12b). The Bedford's Law is a technique of identifying fraud from a series of transactions by observing a significant digit which is always suggested to be small (R12b). For instance, when assessing possible fraud occurrence on cash withdrawals, the last digits are expected to be zero. It was stated that if auditors discover that the Bedford's law has been violated in the transactions, it can be an indication that there is possible risk of fraud, and this would make auditors change their audit strategies (R12a).

Furthermore, three respondents who used IDEA (R6, R7 and R12a), reported that, the tool can be used to visualise data, pinpoint trends and outliers. It was further reported that, IDEA, was used to audit large clients, mostly banks due to the nature of transactions, i.e. complexity and high risks. R12a commented "w*e use IDEA to audit banks, definitely because they have voluminous transactions, complexity and also the level of fraud is high. IDEA is one of the tools that we use to command the Bedford's law which checks the relationships of digits*

which can help to identify frauds such as in ATM cash withdrawals". Therefore, the study found both ACL and IDEA were the most frequently-used tools in auditing large clients. According to one of the respondents who had experience in using both ACL and IDEA, the main difference between the two IS tools is that ACL is more popular than the latter (R2). In contrast, IDEA has better navigation boundary, high file conversion levels, can work well with multiple tables and can append files more efficiently as compared to ACL (R2).

The third most popular software was found to be PCAS, and was used in two medium-size audit firms. It was mentioned that the PCAS software has in-built ISAs which guide auditors during the audit process in relation to standards and codes of conducts (R3). PCAS also helps auditors design, implement and review controls, assess and identify risks and in addition prepare an audit report. Two respondents who used PCAS clarified that the tool has limited capacity in auditing small and some medium clients, who use technology in limited activities (R3 and R4). However, R4 clarified that PCAS was used in conjunction with MS Excel but his audit firm was in transition to purchase new software because the firm wanted to move from medium to becoming a large audit firm.

Other tools such as Teammate, Pro-Audit, SASoft, Auto-Audit and GAMX, were used by large, international audit firms. For instance, GAMX was used by one of the Big Four audit firms; and the partner clarified that the tool has in-built functionalities that incorporated the audit life cycle from planning the audit to reporting the findings (R11). Furthermore, GAMX had the capacity to upload the clients' data for auditing which permitted collaboration among auditors. For example it allows managers to assign a coaching note to junior auditors regarding the way the assignment needs to be performed (R11). However, in data analysis, the audit firm could choose between ACL, MS Excel, or In-house software depending on the nature of client and the needs of the specific audit.

On the other hand, Pro-Audit and SASoft were among the less frequently used software only mentioned by one respondent (R1). The respondent clarified that the audit firm had first installed SASoft; and being inadequate, they later added Pro-Audit as it was regarded with better capability in analysing data as compared to SASoft.

Other audit tools that were common are Teammate and EMS that were mentioned by 33% and 45% of the respondents respectively. It was mentioned that Teammate was used as a management systems aimed to help auditors undertake all facets of the audits. Two respondents who frequently used Teammate (R2 and R8), clarified that the tool can enable auditors to produce valuation reports, assign resources, create, accomplish and track audits through electronic working papers mechanisms. For example, auditors can take the whole of the system of a bank, upload it into one of the IS tools and audit it conveniently at the audit firm's premises or any other convenient location. Hence, Teammate was one of the tools that was used as a platform to export clients' data ready for auditing. R2 commented: *"We have Teammate which is used for data analytics procedures by uploading client's data and then we conduct the audit"*.

Meanwhile, EMS, which is known as 'engagement management system', is composed of several other tools which can be used in different situations. Contained in EMS are analytical tools, documentation tools, and share ware systems that can enable communication of the audit findings. One respondent, an audit partner clarified that *"In our firm [firm I], we have EMS tool which is an integrated system with several analytical tools that we can use for communication" (R9).* The interview findings further revealed that, through the use of these tools, auditors can link their activities in an internal online platform where they can present the audit activities.

The interview findings further indicated that the use of Teammate and EMS software can facilitate the conducive platform for audit engagement. The IS tools have additional implements that dictate the circumstances for what tools to be used. For example, Teammate can have up to 150 diverse audit tools which can be used to conduct various audit processes (R2). This asserts the extent of sophistications that system vendors can provide in order to facilitate audit activities. Nevertheless, the use of Teammate and EMS were found in large audit firms only.

Besides that, all respondents (R1-R12) reported using Microsoft Office packages for office-related tasks. Although these tools were used in many activities, auditors in large audit firms did not consider them as audit software but basic tools that can be used to conduct multiple tasks. Three respondents (R2, R4 and R8) mentioned that MS Excel was an important IS tool due to its ability in handling multiple tasks such as documentation as well as data analytical-related tasks. Excel was used to analyse data in small and medium clients, even though other large audit firms still used it in data analysis to clients who were less automated (R2 and R8). A few respondents (R3, R4, R7 and R12a) mentioned that Excel was a user-friendly tool that auditors understood easily as compared to other complex audit software. However, it was reported that Excel has limited functions as compared to other analytical tools such as ACL or IDEA which makes it less useful in the long run. On the other hand, MS Word was used in limited audit activities, mainly for preparation of working papers for a few audit firms. Additionally, MS Word was also used in writing final audit reports and engagement letters.

6.2.1 The Choice of Audit Software

Respondents were further asked to clarify on what affects their choice of one software over the other and whether there were any audit tasks that would be handled manually. Interview findings revealed that audit software had different capacities and audit firms may opt to use

one software over the other depending on a number of factors, namely (a) the volume of transactions that the client accumulated over a period of time, (b) the level of the client automation, (c) perceived electronic risks, (d) cost of the software, (e) purpose of the audit tasks; and (f) compatibility of the software between the clients and that of the audit firm.

A few respondents (R2, R9, R10 and R12a) clarified that in a situation where the client had voluminous transactions with higher level of automation, audit firms would use a higher level of audit software when analysing data. In such a situation, ACL and IDEA were mostly used. On the contrary, when the volume of transaction was moderate, with low or moderate level of automation or a combination of manual and automation, the use of audit software for auditing purposes would be minimal and auditors would use MS Excel (R1 and R12a).

Respondents further clarified that due to high costs of acquiring audit software, availability of funds dictated the type of software to be used. This asserts the importance of NBAA to categorise audit firms as small, medium or large, based on their resources capabilities including IT which also dictated the types of clients they should take in (R1 and R11). All large audit firms used commercially available software which was both advanced and expensive as they were guaranteed of the costs to be compensated by their clients. Meanwhile, some medium audit firms could not afford expensive audit software and they used PCAS which was sponsored by the NBAA or sometimes Excel (R3). This finding suggests that IS usage varied according to firm sizes and resources capabilities.

Lastly but not least, the interview findings advocated that when clients' software was not compatible with the audit firm's software, the audit firm would choose to use a lower version of a software such as MS Excel which was reported as friendlier to most accounting software (R2). For example, two respondents (R3 and R4) mentioned the reason why they used MS Excel extensively was because most of their clients had their data processed and installed in

Excel and Pastel which was easy to upload their data in Excel and save them therein for auditing.

The respondents were further probed whether there was any audit task that had to remain entirely in manual processes. It was stated that the use of IS in auditing was becoming more prevalent. However, three respondents (R1, R8 and R9) clarified that the use of IS can be considered vital in data analysis of large computerised clients but still in some other instances the use of manual techniques was valuable. One respondent, a partner from the Big Four (R11) clarified that computers have a capacity of recording accounting transactions, providing support on data analysis and presenting in many formats but computers cannot make judgements. For instance, if the results from the software show that the clients' systems aren't secured enough, the judgement comes from auditors to decide and change the strategies by not relying on computers. The use of manual techniques such as interviews and interrogations to ascertain the truthfulness of the computed data becomes essential (R11). This clarification asserts the importance of human judgements over machines and rules out the myth that technology can overtake human thinking (Bostron, 2015).

6.2.2 Ethical Hacking

As organisations transfer most of their critical activities to the Internet, delinquents have more chances and motivation to the access of the entity's data via web-based applications. This necessitates audit firms to use additional IS tool and techniques when auditing web-based clients to check for possible unauthorised access to clients' information. This study found that 42% of the respondents conducted penetration testing through the use of IS tools and techniques known as "*ethical hacking"* (R2, R5, R9, R11 and R12b). Ethical hacking are IS tools that can be used to conduct a specialised audit to the clients' systems by checking vulnerability of the client's data to e-fraud and to establish the integrity of the figures

presented in the financial reports (R5, R9 and R11). The interview findings found that auditors were trained to become system hackers (legally accepted), who could hack the clients' systems with the purpose of providing solutions to systems securities. It was mentioned that for hacking to be considered ethical, it was essential for the hacker (audit firm) to get consent of the clients to investigate their systems and network in an effort to identify possible security-related risks (R11). The respondents further clarified that the BOT requested auditors of banks to perform penetration testing at least once a year and to provide a separate report on data safety and vulnerability of banking systems (R9 and R12). Four respondents (R9, R10, R11 and R12b) supported the above by mentioning that, they performed ethical hacking at least once a year to their bank clients.

6.2.3 Discussion on the IS Usage

All in all, the findings revealed that audit firms in Tanzania have made steady progress from manual auditing to computerised platforms by using different IS tools. In the last five years, many audit firms were using MS Excel in their audit assignments, but recently many have shifted to higher levels of IS. A combination of commercially-available software and internally-developed software were found to be used. The IS usage facilitated risk assessment procedures by checking outliers, plotting trends of transactions, fraud detection, report writing, computations and spotting unusual transactions among others. Hence, this study managed to categorise the IS tools into four main categories: (i) those that are entirely related to audit tasks or audit automation technologies (AAT) (ii) those that are related to general office related activities (OAT) (iii) those that are related to specialised audit tasks such as E-commerce technology (ECT)/intruders' detection technologies (IDT) and (iv) those that facilitated audit tasks by interlinking the audit functions in one platform (NADTT).

The IS tools that are related to AAT include ACL, IDEA, SASoft, PCAS, GAM-X, Pro-Audit and Excel. Similarly, the IS tools that are related to OAT include all categories of Office applications such as MS Word, Excel and Access while the tools which are related to specialised audit tasks (i.e ECT), include ethical hacking tools. Likewise, Teammate, EMS, Emails and other Work-related messengers are the facilitators to a smooth platform for audit functions to take place and this study categorises them under NADTT.

Figure 6.1 shows that the most frequently used IS tools are AAT. In essence, the common AAT were ACL and IDEA, which are both associated with advanced software applications. They are mostly referred to as commercially available software where researchers in audit technology have categorised them under GAS (Ahmi and Kent, 2013; Widuri et al., 2016), which is also a subset of CAATTs. The technology typology in Appendix II, highlights that ACL and IDEA can be used to balance ledgers, total records, sort accounts by size, mine huge amounts of data, select samples for detailed testing, generate confirmations and identifying unusual transactions (Greenstein-Prosch et al., 2008; Ahmi and Kent, 2013). In a developing country such as Tanzania, if audit firms make use of ACL and IDEA, it might suggest that the pace to embrace technology in external auditing is increasing. This is because these tools are essential in auditing large automated clients with voluminous of transactions.

Interview findings also suggest a possibility of huge volumes of transactions and risky environment among audit clients, which need auditors to use ACL or IDEA tools to effectively analyse their data. Past scholars contended that installing audit software could be expensive and needed availability of resources (Rosli et al., 2013). Thus, the cost-benefit analysis in using software by audit firms is anticipated to be compensated by the auditees through increase of audit fees. This opens a discussion for another area of research to establish whether IS usage in auditing has a relationship with increase in audit fees.

Besides the above mentioned, five auditors (R2, R5, R8, R9 and R10) reported using EMS. EMS is integrated in management systems which have several embedded in-built analytical tools that can be used in different situations within the computerised-based clients (R8 and R9). This study found reasonable to categorise EMS under NADTT that helps in levelling flexible communication among auditors in different audit engagements. This is because EMS can provide a platform for auditors to display, amend and share their working papers for discussions and viewing by others. In the new ISAs, transparency in the audit process is emphasised. One way of maintaining transparency is by discussing audit evidence, tests and findings before the final report is signed by the partner (Banker et al., 2002). Likewise, the use of EMS can foster independence within the audit engagement. Hence, the use of this software amongst external auditors in a developing country can suggest that audit firms are keen to comply and keep with best practices in auditing.

Furthermore, the use of IS by auditors needs to fulfil the intended objectives and the fitting of the technology within the environment (Goodhue and Thomson, 1995). Therefore, the use of Microsoft office package which was used by all the respondents (although to limited activities), suggests that this tool is needed to accomplish several office-related tasks. This study categorised Microsoft office package under one group of OAT which can assist auditors in the preparation of audit reports, documentation and accomplishing of initial audit procedures such as preparation of working papers, computations and data analytics (Simkin et al., 2015). The use of Excel can as well aid auditors to convert a client's data into alphanumeric so that they can manipulate it either via standard functions or auditor-programmed functions (Ahmi and Kent, 2013; Widuri et al., 2014). Therefore, Excel is a unique tool that can be used to perform multiple tasks.

Lastly but not least, the study found that ethical hacking tools and techniques were used to check system vulnerability of clients. As a result, the tools provided for protection and

detection of systems-related faults and fraud. Ethical hacking has several strategies of tools which can be used to crack passwords, to attack electronic files of the entity and user accounts, to identify the IP discourse of the target systems and to scrutinise configuration faults (Ajinkya et al., 2010). Although respondents did not clarify the specific tools that they used for security reasons, studies have mentioned some of the IS tools used in ethical hacking to include LC4, John the Ripper, Brute Force, Port scanners, Dictionary Attacks, and WebInspect (Smith, 2002; Juneja, 2013; Danish and Muhammad, 2011). Through the use of ethical hacking tools, it was mentioned that not only attackers can be identified but also the entity's systems can be protected. Although ethical hacking is a long term technique that has been used in IT field and computer science to check systems vulnerabilities and websites, its usage for external auditing purposes remained limited. Hence, by reporting the usage of ethical hacking in the external audit environment in Tanzania and its perceived importance when auditing bank clients, it remains one of the main contributions of this study.

In summary, this study found that the usage of IS tools and techniques for external auditing in Tanzania is gaining momentum. New refined external audit tools are being used to perform various audit-related tasks. There are some audit clients in Tanzania that cannot be audited without the use of IS and one of which are banks; while others are insurance companies and telecoms. Audit firms were using more than one software depending on different factors such as the extent of clients' automation, risk components and availability of budgets to use advanced audit tools. Although some software were single, others were integrated platforms with embedded audit procedures to ease the audit tasks. The following figure (figure 6.1), shows a summary of IS tools as reported by respondents. Instead of categorising them as GAS/CAATTs, this study has grouped them according to their functionalities. It is important to note that figure 6.1 was as a result of the coding process through Nvivo software. The

larger the size of the box indicates the frequency of the items being mentioned in the transcripts.

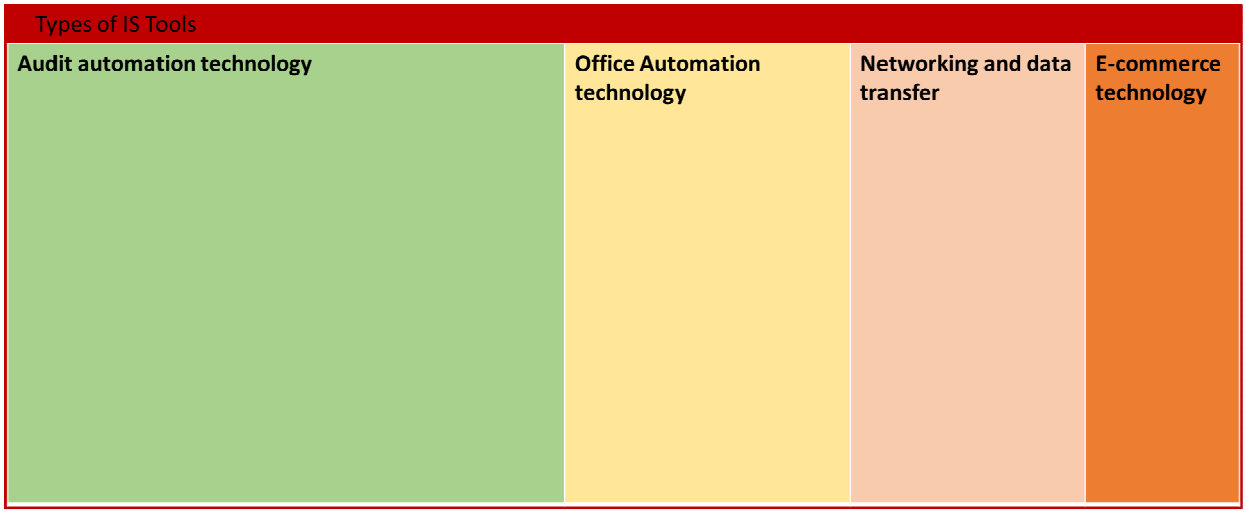


Figure 6.1 Thematic Coding on Types of IS Tools

6.3 What Factors influence the Usage of IS by External Auditors in Tanzania?

This study also intended to understand whether the usage of IS by external auditors is influenced by internal factors or external pressure and to compare and contrast with prior studies conducted in other countries. Given this perspective response, the study found that the factors could be categorised into two groups, namely, internal factors and external factors. The internal factors include perceived benefits of the user (auditor) and perceived benefits from organisational perspective. Meanwhile, external factors were divided into three, namely, clients' factors, the audit professional factors and other factors that emerged from the interview transcripts.

Table 6.2 summarises specific aspects of the factors that were identified from the interview transcripts where the study extracted 18 aspects marked them as 'highly influential', 'somewhat' or 'less influential'. As identified in table 6.2 below, 'Highly influential' means the aspect of the factor was mentioned by at least fifty percent (50%) of the respondents, 'somewhat influential' means the factor was mentioned by at least 30% to 49% percent of

respondents while 'less influential' represented aspects mentioned by less than 30% of the respondents which is consistent to Widuri et al. (2016).

Table 6.2 Factors of Using IS by External Auditors in Tanzania

Factor category		Usage factors	Highly influential	Somewhat influential	Less Influential
External factors	EF1	Client's IT intensity	✓		
	EF2	Client's products complexity	✓		
	EF3	Minimise audit risk	✓		
	EF4	Clients' e-business integration	✓		
	EF5	Size of the client's business	✓		
	EF6	Pressure from regulators	✓		
	EF7	Ready audit methodology to follow	✓		
	EF8	Accountability		✓	
	EF9	Competitive advantage			✓
Internal Factors	1F10	Simplified tasks & saving time	✓		
	1F11	Flexible work environment	✓		
	1F12	Organisational efficiency		✓	
	1F13	Audit effectiveness		✓	
	IF14	Ease supervision		✓	
	IF15	Management pressure		✓	
	IF16	Relevance to task		✓	
	IF17	Availability of resources		✓	
	IF18	Monetary gain		✓	

Note: EF = External factor, IF = Internal factor

6.3.1 External Factors

The interview findings showed that external factors were the main motivators for IS usage by external auditors in Tanzania. Factors related to the clients' nature of automation and the perceived increased risky environment, highly influenced auditors to use audit tools. Table 6.2 shows that majority of items labelled 'EF' were 'highly influential' with exceptional of a few items EF8 and EF9 which were 'somewhat influential' and 'less influential' respectively. In contrast, all internal factors labelled as 'IF' were either 'somewhat' or 'less influential' with the exceptional of IF10 and IF11.

The external factors that were mentioned to influence IS usage the most were related to the audit oversight body and clients' related factors. More than 50% of the respondents perceived

that the use of IS was important by considering the external factors surrounding the auditees' environment as the main driver. The next sub-section discusses the specific items in detail as was clarified by the respondents.

(i) Clients' IT Intensity

IT intensity is defined as the extent of usage of technology among businesses where some may opt to use ordinary technologies while others use advanced systems. The usage of advanced systems among audit clients were found to be common in multinational companies and banks, who were reportedly using Limo software, SAP, Sage, Sun System and other ERP systems (R1, R7 and R12a). Meanwhile, local businesses were reported using IT to a lesser extent and even the types of software that they used were also simple such as 'mind your own business' (MYOB), Tally, Pastel and Excel (R1, R7, R9 and R12a). Thus, it was stated that when clients used advanced software to process information, audit firms purchased appropriate software that aligned with the nature of their clients' IT systems in order to ensure audit effectiveness. One respondent, a partner in a large audit firm, delineated "*for us here we believe that technology doubles every one year, and as auditors we must adjust with the trends in technology to align with the business world (R9).* This perception clarifies that auditors are aware of the dynamic technological world and are prepared to align their practice to suit their auditees' usage.

In addition, auditors were trained on how to use audit firm's software and also the software of their clients (R2; R9; R8 and R11). This also shows the suggested importance of accounting academics to include elements of e-business and IT into the accounting curriculum in order to reduce time and resources in training auditors (R9, R11, R12a and R12b). To summarise, the usage of IS in the external audit was motivated by the clients' IT usage. The variable was considered most important by all respondents (R1-R12b) to the extent that one of them

commented: *"In fact most of our clients are using information systems in one way or another. So it is difficult for us to continue using manual audit systems" (R8).*

(ii) Clients' E-Business Integration

E-business integration is the extent of the audit client's environment to incorporate Internet or other electronic systems into their business processes. It includes online payments systems, IT outsourcing for data storage and other electronic based products and services. In most African developing countries including Tanzania, where the Internet is a barrier to e-commerce, mobile phones are used extensively to make payments for goods and services instead of credit cards. Hence, it was mentioned that the type of e-business model opted by an audit client dictated the usage of IS tools and also the type of software to be used by the audit firm. To elaborate this, several respondents (R1, R2, R8, R9, R10, R11 and R12a) clarified a situation why they needed to use IS pointing to the integration of embedded products between telecoms and banks in offering mobile money services.

It was mentioned that the e-banking business model created a new business environment which was difficult to audit without IS tools due to the level of computerisation (R9; R10). R9 stated: "*So I would say, without technology, it is impossible now to audit certain clients who are computerised particularly in banks and telecoms".* It was further mentioned that where auditors were recruited to audit banks and realise that they do not have an IT system they would resign; as it would be difficult to confirm whether things were okay. Hence, increasingly, auditors find it completely impossible to audit financial institutions or telecoms that do not use IT systems in processing its FSs at higher levels of automation (R11).

The interview findings also revealed that, not only the private sector was computerised, but also the government of Tanzania had moved into e-government by adopting business integrated financial management system (BIFMS) (R11). The adoption of BIFMS implies

that "*the government accounts are fully computerised and became more or less on par with the private sector"* (R11). Subsequently, a few respondents (R5; R9; R11) mentioned that they conducted audit with/for Chief Auditor General (CAG) due to scarcity of IT resources in the government departments. Therefore, it becomes imperative for audit firms and auditors to adopt and use IS tools for auditing both computerised private and government departments (R11).

(iii) Clients' Product Complexity

Products' complexity is the extent to which the auditee may have multiple products embedded within the entity's business line that have varied treatments. Common examples of businesses that were cited to have complex products were banks and telecoms where some respondents referred to as *"very complex to audit"* (R9, R10, R11 and R12a). One respondent (R9) gave examples of bank audits and how complex it was to confirm revenue earned from interest income and other derivatives. He cited the level of interest rate fluctuations within the year and its impact on the computations of revenue at the end of the financial period. He stated that in the last five to seven years, it was very simple when auditors approached banks during engagement because most banks had only savings accounts, current accounts and fixed deposit accounts. Fixed deposit accounts and savings accounts had a rate of interest which was uniform while current account holders did not pay interest (R9). Therefore, it was easy and straightforward for auditors to ascertain the level of interest income by re-computing and confirming the figure with that recorded in the FSs. However, in recent years, everything had changed because banks' clients have the right to negotiate the interest rate where there is no fixed prices attached to specific products. Thus, the complexity in products' flexibilities needed time and skills in IT and ISA/IAS to understand treatment of such items. The partner commented: *"Unless we use IS tools and techniques, the auditing of some of these products are very complex and it is a challenge"* (R9).

It was further mentioned that, *n*ot only interest but also derivative contracts are challenging to audit because they are recorded at different rates based on the buyers' negotiation ability and the market prices. Another respondent commented: "*Some of businesses certainly have complex products, for instance banks are more complicated; first, in terms of the level of computerisation and secondly their products have become different from what auditors were used to in the past. It is difficult now to audit them without using technology"* (R10). These findings suggest that the use of IS tools is influenced by the complexity of the clients' products.

Another respondent (R5) clarified that most IT auditors are important for telecoms and banks due to their nature of products. He mentioned that banks have several branches and products such as electronic cash transactions, ATMs, interactions between banks and mobile money services, interaction between banks and Maxmalipo (a point of sale systems) and other points of sale services and agents scattered across the regions. Hence, it becomes a must for auditors to use IS during audit in such environments.

Another industry that was mentioned as having complex systems was telecom because they were IT users by default (R2, R8, R9, R10 and R11). One respondent explained an example of complexity when confirming revenue earned in a telecom client when a customer buys a prepaid top up credit. The respondent clarified the challenges involved especially in ensuring that the computed revenues adhered to IAS. He commented: *"When you buy a voucher (prepaid credit), of 10,000 and load it in your phone, it is not called revenue, according to IAS 18; until you make a call. So if you used 2,000, that is revenue while 8,000 is deferred revenue which is a liability. So, that process is very complex to identify for the whole sample and because the products are complex, the environment is complex, we had to respond by using IS tools like ACL and other tools" (R2)* These examples elaborate the complexities in products embedded in clients' systems where the analysis can be simplified through using IS

tools and techniques. Other clients that were equally mentioned as increasing automation were insurance, hotel industry, air ticketing, and pension funds (R1, R2 and R7).

(iv) Size of Clients' Business

External auditors conduct audit of different business sizes both in terms of capital, customer base and the frequency of transactions. Large businesses are more inclined to generate large amounts of transactions per given period of time as compared to small businesses. All respondents (R1-R12) reported that the size of the business of their clients and the volumes of transactions dictated the usage of IS tools. It was stated that IS can simplify the process of data analysis and ensures that the optimal sample size was estimated which could not be achieved using manual techniques (R2, R8; R10). Again, it was found that most large banks, telecoms, pension funds, some insurance companies and all companies registered on DSE were considered large in terms of volume of transactions that necessitated auditors to use IS when analysing their data (R3, R9 and R12a). For instance, the usage of data analytics tools was emphasised by R9 and R11 as a move to audit in cloud platform where some of their clients had saved vast amount of data into third parties. It was mentioned that Tigo and Vodacom (telecoms) generated millions of transactions per day and had outsourced some of their functions and stored their data in clouds (R9). Even though the trend of cloud computing for businesses in Tanzania is still pre-mature, one respondent, a partner from the Big Four perceived the future for audit technology to be intense and inevitable where more companies opt to process and save their information into cloud system. He stated: *"where more businesses use cloud computing, increasingly, this trend will command auditors to use IS whether we like it or not"* (R11). In contrast, where a business is small, the volume of transactions is small and the extent of competitiveness is low, the usage of technology becomes limited to a few audit tasks such as documentation and reporting (R12a).

(v)Minimising Audit Risk

Audit risk is the possibility of an auditor to issue a clean audit opinion when in fact there could be at least one or two items of material misstatements undetected by an auditor. It was mentioned the main causes of audit risks in a computerised environment are poor IT control mechanisms of the clients, low level of IT skills of the clients and of the external audit teams and inappropriate audit methodologies in assessing risks (R11). The interview findings also revealed that the extent of audit risk is considered higher when an audit client has automated its financial activities, which necessitates auditors to conduct audit of the systems first before conducting substantive testing on transactions (R2, R11 and R12a). It was stated that the most efficient way to minimise audit risk is to use IS tools and techniques to predict risk occurrences and to test electronic-based controls including testing the computer systems that process information (R12a).

All respondents (R1-R12b) mentioned that banks are the most risky environments to audit than any other businesses in Tanzania that needs the use of IS tools to conduct audit through the systems, rather than a traditional auditing around the computers due to perceived high risky environment. An Associate director from one of the Big Four explained how she perceived the risky environment when auditing mobile money transactions, the most risky platform that is gaining momentum across EAC (R10). She perceived mobile money an East African product which is prone to risks of fraud and has no audit program. She stated*: "I mean mobile money is an example of a risky environment and I normally tell people mobile money is an east African product where you cannot find a checklist or an audit program anywhere. It is a highly risky business and there is a lot of fraud which people have experienced"* (R10). She further stated that, the audit of such risky products needs the use of technology. Thus, knowing that occurrence of fraud or errors in accounting records questions the credibility of the financial reports, and because IT is the one that processes financial

transactions, generates financial reports, it is also a motivation for auditors to use IS tools for effective risk assessment (R9 and R11). It was further mentioned that increasingly, auditors are using tools like ethical hacking as part of audit objectives because of the complication of the level of risk of fraud. The increased use of IT tools and ethical hacking enables auditors to detect fraud and mitigate risk. As R9 commented *"we are aware that we cannot be effective without the use of technology. The use of technology can help us manage our audit risk or at least minimise it"*.

On the contrary, one respondent clarified that if auditors are not using technological tools, there is huge risk of failed audits. That is why regulators are increasingly putting up rules – which require the use of IT. For example the BOT shortlists auditors who are approved to audit banks and one of the criteria for shortlisting is that the audit firm uses technology (R11). He commented "*If you do not use technology, they disqualify you"*. So, as much as audit firms are authorised by the NBAA, BOT always authorises very few firms after ensuring that they have a capability to audit IT systems, because now without IT, it is impossible for auditors to confirm the audit was effective (R11).

Furthermore, respondents explained the concept of garbage in and garbage out, which means a computer error that could be programmed by the user which makes it important for auditors to use IS tools to test the systems for possible errors before the audit commences (R5 and R12a). In addition, it was mentioned that as much as the system processes the information, it is prone to programing errors. Some systems could be intentionally incorrectly programmed to fraud the entity, while others could be due to management pressure. It is due to this possible risk that R12a clarified the impossibility for auditors to claim that FSs are presenting a true and fair view without auditing the systems. The usage of IS provided a higher level of assurance that the system was secure (R12a). As a result, it provided the comfort to auditors that the five attributes of data are in place. R12a commented: "W*e need to test the system to*

ensure that all the five components of data are okay". The attributes were mentioned to include accuracy, completeness, reliability, confidentiality and preciseness (R12a).

(vi) Pressure from Regulators/Oversight Bodies

The audit oversight can be categorised into local and international. The local audit oversight in Tanzania is the NBAA, which supervises the audit profession and evaluates their practices on a regular basis (R3, R7; R11). Among the aspects that the NBAA emphasises is the compliance to ISA, and audit best practices including independency, transparency, documentation and methodical way on how the audit is conducted. One respondent (R11) mentioned that when the NBAA visits the audit firm's premises, they sample a few files, check the procedures to assess how managers audited the juniors and how the partners were involved in the audit process. Six respondents (R1, R3, R5, R9, R11 and R12a) reported that the NBAA was the main motivator for the usage of IS because they emphasis on compliance to standards and the easiest ways to remain compliant is to use technology. If the NBAA finds that the audits did not adhere to the best practices in audit; or supervisors were not fully engaged in the audit process, they can terminate the licence of the audit firm (R11).

It was further clarified that the NBAA puts pressure on all audit firms including small firms to have a methodical way of documenting audit evidence using technology. R11 remarked: "*The mother motivator for us to use technology is regulator. Regulator wants us to use technology whether we like it or not; forcefully. The NBAA found that small firms had no methodical way of documenting their work. So they forced them to apply a certain computerised tool which is now mandatory for local firms".* It was further mentioned that only the NBAA assert pressure on auditors to use IS, they also provided support for audit firms on the adoption process. For instance, the NBAA negotiated an affordable vendor of audit software (PCAS) so that even small audit firms could afford it (R3 and R4). Hence,

through the use of the advocated software, the NBAA does not want to find box files kept by audit firms anymore (R3, R7 and R11). This asserts the importance of the audit oversight body to be strict on compliance issues through their emphasis on audit firms to use IS tools.

The interview findings also revealed that another imperative for auditors to use IS was compliance to the IFAC standards. The IFAC standards require auditors to preserve and retrieve audit evidences for up to six years. Hence, it becomes impossible to achieve all the requirements of IFAC as far as the audit process is concerned in the absence of using IT (R3, R9 and R11). R11 clarified further that the IFAC standards require that an audit needs to be planned before it is executed. It also requires that the audit work by juniors is reviewed by a senior. In other words, the audit must be composed of a layer of junior auditors, seniors and supervisors. So it is realised that for a reviewer of audit quality to be able to review audit falls and confirm that the audit was planned before auditors executed the work, and supervisor really reviewed the work on a timely bases, "*it actually requires the usage of IT tools otherwise it can be difficult to achieve stamping"* (R11). It was clarified that stamping is a compliance process through the use of tools, evidencing that auditors followed appropriate procedures and standards in doing their work and supervisors were actively involved throughout the audit process (R11).

(vii) Accountability

Three respondents (R5, R9 and R11) reported that they used IS for accountability purposes. Although this aspect was 'somewhat influential', it showed an importance attached by some respondents on increased accountability to investors' resources through the use of IS. It was mentioned that, increasingly, auditors are learning IT skills like CISA in order to be more effective in the audit assignment (R9). It was mentioned that the IT profession would make auditors understand better the client's environment which is the first requirement of ISA

when auditing a computerised client (R11). To clarify more on accountability, R11 referred the interviewer to the ISACA local Chapter (Tanzania) to show the increased enrolment of CPA accountants in acquiring additional IT skills such as CISA.

Furthermore, the respondent explained that in the years 2003-2005, the ISACA local Chapter in Tanzania had very few members but recently the trend is showing "*a skyrocketing increase in membership"* (R11). This study visited the website of ISACA-Tanzania local Chapter at http://www.isaca.org/chapter9/tanzania and found that in 2003 there were only 33 memberships; however, in 2016 the affiliations had mounted to 337 which is equivalent to 900% increase in thirteen years. These findings are an indicative that the audit profession in Tanzania is striving to learn IT skills so that they can benefit from its usage to foster accountability. The secondary data also revealed that Tanzania was the fourth country in Africa to open the ISACA local Chapter after South Africa, Nigeria and Kenya. ISACA is a world-wide organisation which is involved in training IT auditors and all IT governance-related issues. Likewise, R9 clarified that the current NBAA syllabus has included IT which aims to enhance a CPA auditor to become an IT expert so as to bridge the knowledge gap for technology usage in auditing. However, the respondents were not sure of the extent of technology inclusion in the syllabuses for Tanzanian universities which calls for further studies on this area.

(viii) Readily Available Audit Methodology

The usage of IS by external auditors was 'highly influenced' by the presence of an audit methodology which had incorporated the audit procedures, making it inevitable for auditors to use IS tools. Six respondents (R2, R5, R8, R9, R10 and R11) reported that their audit firms were using either an internally-developed software or a global audit methodology software which was integrated across their affiliated audit firms. Again, the presence of such a

software means that the necessary audit procedures from planning, working papers, gathering evidence, testing to reporting, are already incorporated within the software (R5 and R11). In other words, auditors who were employed in these audit firms used IS more frequently as compared to auditors in other audit firms. One respondent, a senior manager from a large international audit firm, mentioned that they were using a global audit methodology which provided them with various guidelines on how to do an auditing in an accounting system, such as checking IT general controls around the particular system, security on the servers and so on (R5). He stated: "*our audit guidelines have eight procedures, other organisations [audit firms] may have six, but ours is international, so the procedures are the same as the ones used in German, in UK, or elsewhere and are benchmarked with best practices in IT".*

Meanwhile, another respondent, a partner from one of the Big Four mentioned that they have their in-house software which gives them the guidelines on auditing computerised clients (R11). At the same time he clarified that his audit firm does not create any new audit software, but simply request from their mother audit firm. In some instances, they may reject some of the audit tools which are more advanced to use in a country such as Tanzania. He stated: "*Big Four are supported by their global organisation which conduct research on IT and any technology that comes out they already have it. So we don't create anything new. We receive software and our methodologies are the same, even sometimes we say this [software] is not relevant for our environment"* (R11). The findings from R5 and R11 highlight that the use of IS tools can be influenced by the availability of ready audit methodology and software to use.

(ix) Competitive Advantage

The motivation to use IS tool in the external audit environment was 'less influenced' by competitive advantage factors. Only two respondents (R9 and R11), both partners in the Big Fours mentioned competition as one of the motivations for IS usage in their audit firms.

Irrespective of the aspect to receive little ranking, the observation from the secondary data revealed that all the 12 surveyed audit firms had websites and had advertised extensively their products which included IT consultancy services. The secondary data and the findings from the two respondents highlight that audit firms used IS to remain competitive but a majority of the informants did not consider competitiveness as a threat to their customer retention or profitability.

6.3.2 Internal Factors

This study used the UTAUT as a theoretical lens to probe respondents to get clarification on the factors for IS usage. Hence, the UTAUT factors were considered internal factors as they are related to 'individual's perception and that of their work colleagues, supervisors, management and organisation (Venkatesh et al., 2003). The interview findings revealed that the benefits in using IS tools can be categorised in two ways: (1) benefits from users and (2) benefits to the organisation. The next sub-sections explains these factors as were emerged from the transcripts.

(i) Simplified Tasks & Time Saving

All respondents (R1-R12b) agreed that the usage of IS in auditing simplified audit tasks from manual computation to technology based. For example, by using MS Excel, IDEA or ACL, auditors can save time and efforts needed to verify clients' information. Unlike the use of manual systems where auditors were using calculators to compute relevant accounting balances or ratios, the use of IS tools has simplified audit tasks for data analysis and risk assessment. One of the respondents, an associate director shared: *"by using the software like ACL, I can get a transaction of a bank, let's say Stanbic Bank, I can do the analysis for the whole transactions from January to December within one hour; I can identify high risky areas and in five minutes I can get all the duplicate transactions*" (R2). The clarification from

this respondent conforms that the usage of IS has the ability to simplify the process of data analysis because computers can be programed to do work in an easier way than manual techniques (R11). The computations and confirmations of accounts balances can be done easily though IS tools and so it saves time from manual routine in traditional paper-based audit techniques (R1 and R3). Even though this study had used a mixed sample from medium and large firms, still these aspects were among the factors mentioned as 'highly influential' by auditors in all firms.

(ii) Eased Supervision

Furthermore, respondents reported that they used IS tools and techniques because they facilitated supervision activities. The presence of tools could help them view the work of one another and simplified the work of supervision from juniors, managers to partners. A few respondents (R2, R5, R7, R8; R9 and R11) mentioned that technology usage is becoming paramount in the audit process due to its unique nature of simplifying the work of supervision. A senior manager mentioned *"now I can supervise multiple work much easier from any engagement locations and can make a follow up when a project will be completed" (R7).* Furthermore, the use of technology enables managers to see real time work through the use of tools such as work-related messengers, which enable auditors to communicate online (R11). Moreover, with globally affiliated audit firms, supervisors may be situated in different countries, but still collaborate with others by sharing their expertise (R5 and R11).

(iii) Monetary Gain

The interview findings revealed that the use of IS in auditing had the advantage of increased salaries for users who were conversant with both IT and accounting. Three respondents (R1, R9 and R11) who were all partners, reported that the use of IS in the external auditing has higher chances of increasing remuneration for the respective auditors. They clarified that the

current technology era where most accounting data is stored electronically, needs auditors to have multiple knowledge and IT is one of the preferred knowledge because it is expected that technology increases every year (R9). Another respondent added that today the audit of FSs is highly reliable on the systems that process information. So, if auditors test the system and find it ineffective, the auditors can resign as it will be impossible to promise assurance when the system is not reliable (R11). Hence, checking the reliability of the system is the work of the IT expert or IS auditors, and paying an IT expert is very expensive. As a result audit firms have opted to hire most of them instead of using them as consultants. It was mentioned that, "*in the past, audit firms concentrated on auditing certified public accountants, but now, increasingly, a certified public accountant with additional skills like CISA is highly preferred versus a traditional CPA accountant, and that commands a higher pay" (R11).* These findings suggest that the use of IS in the external audit environment needs accounting with additional IT skills. A composition of both can make an individual auditor to have high chances of increased pay thus motivating them to use and learn IS.

However, two respondents (R2 and R8), who were both IS auditors, mentioned that they received the same amount of pay as their co-workers who had CPA only. They mentioned that the criteria for recruitment and promotion were either an IT-related affiliation such as CISA or CPA. These contradicting findings suggest that the UTAUT variable of social influence might produce a pragmatic inference when statistically tested in the external audit environment.

(iv) Flexible Working Environment

The interview findings revealed that users of IS reported enjoying a flexible working environment. The use of IS removed the routine for auditors to report at work early in the morning. Instead, auditors could do their work from anywhere, at the client's office, on

transit or at home (R2, R5 and R11). The use of laptops which audit firms had bought for their employees to use during engagement (R11), facilitated flexible working environment which in turn motivated auditors to enjoy using IS. In fact, flexibility did not only occur to individual users (auditors) but it was also a motivation for the organisation. It was reported that the use of IS enabled audit firms to share information with other auditors through shareware applications. For internationally affiliated firms, an audit task could be performed in Tanzania while a supervisor (partner) could be situated in Nairobi or South Africa (R5). The flexible working environment did not only ensure effectiveness, but it also allowed knowledge sharing among the audit teams (R11).

(v) Relevance to Task

A few respondents (R2, R5, R8 and R9) mentioned that IS usage was influenced by its relevance to their task. Most IS auditors and IT specialists were likely to use IS frequently as compared to financial auditors. Based on snowball selection of respondents, IS auditors were preferred to provide deep information. Hence, this group of respondents considered 'relevance to task' as a motivation for IS usage due to the nature of the daily tasks they performed. For example, R2 and R8 mentioned that IS usage constituted part of their daily job as they were only involved in the audit of computerised clients when assisting financial auditors to check the security of the systems before the audit commenced. R8 stated: *"these are the tools we use in our daily activities. They are part of doing our job without which we cannot do our job* (R8). Meanwhile, R2 also mentioned that he audited only computerised clients and the usage of IS tools and techniques were part of his daily routine. Most respondents did not mention 'relevance to task' as a motivator or a factor to influence their audit practice.

(vi) Audit Effectiveness

A few respondents (R9, R11 and R12a) mentioned that the use of IS was necessary to attain audit effectiveness. For most respondents, audit effectiveness referred to the absence of error, fraud and irregularities, and issuing a report reflecting the fair view on financial records. One respondent, a partner (R11) clarified the usage of IS tools to foster audit effectiveness by citing his worries that if they completed the audit and later on found that errors or fraud ought to have occurred without being detected during the audit process, would amount to their demise as an audit firm. He commented: "*Shareholders would sue me for being incompetent"*. Hence, the use of IS tools was important for effectiveness to protect the reputation and survival of the audit firm.

Another partner clarified his concern on effectiveness during the audit process and the implication to his audit firm. He stated: "*even a fraud for example, which ought to have been captured, within the audits is fair, then I have not been effective and I will fail as an audit firm. I will perish because shareholders will sue me for failure to detect that fraud" (R9).* Therefore, the use of IS was regarded important to facilitate detection of fraud and errors and so as to avoid litigation costs.

(vii) Organisational Efficiency

A few respondents (R9, R5, R11 and R12b) reported that achieving audit efficiency was another motivation for using IS tools and techniques. It was mentioned that audit firms are looking for means of achieving audit objectives more using less resources (R11). It was reported that due to cost reduction strategies and maintaining profitability level, audit firms must find a way to compensate the costs by reducing time frame of completing an audit assignment. Hence, the use of IS tools was important for cost reduction purposes. An audit

partner commented, "*If we have to retain our profitability, we must embrace technology" (R11).*

(viii) Availability of Resources (IT Resources, Training etc)

The usage of IS tools was influenced by the resources availability of the audit firms. The interview findings revealed that respondents from audit firms that had installed IT infrastructures and invested in IT human resources mentioned this variable as influential compared to those from audit firms with less or fewer IT manpower. A majority of respondents reported to be influenced by the availability of resources due to the nature of the sampled respondents which mostly were from large and medium audit firms. When firms have invested in technology, they can only recoup the investments by extensive use of it. Hence, it can be concluded that the use of IS tools and techniques was influenced by the availability of IT resources within the audit firm.

(xi) Management Pressure

The interview findings further revealed that audit firms were putting pressure for their employees to use IS (R9, R11 and R12a). Even though the extent of usage differed between audit firms, the basics of the usage which was relevant for compliances and accountability, made the management put its emphasis for the usage (R11). Four respondents (R9, R10, R11 and R12a) who were all partners, mentioned that they invested millions of cash in training their employees to ensure that they apply the skills to perform audit procedures smoothly. Meanwhile, three respondents (R4, R5 and R8), mentioned that they have received adequate training in IT so that they can apply their skills to improve the audit process. This is an indirect evidence that after training, auditors must use their skills though the usage of IS tools or the software that are available. Furthermore, the pressure from the oversight body stresses the management, which in turn puts pressure on their employees to use IS tools. Since half of

the respondents who were partners mentioned that they put emphasis on their subordinates to learn and use IS for organisational efficiency. Hence, the huge investments in IT and training could be an indirect emphasis for beneficiaries (trainees) to use IS tools.

6.3.3 Discussion on the Factors for IS Usage

The second objective was to establish the factors for IS usage by external auditors. The interview findings revealed that external factors were the most influential factors, namely, the nature of the clients' business which integrates IT into their processes. Secondly, the influence from the oversight body, which puts pressure for audit firms to use IS tools to ensure adherence to ISA and audit best practices. The NBAA was found to be at the forefront both in speeding the adoption of IS and also to support audit firms by suggesting a cheaper audit software which enhanced audit activities for many audit firms. It was mentioned that even small audit firms had to use IS for documentation and working papers because the software simplified adherence to ISA. The role of NBAA in IS adoption and use is worth implementing by other national audit standard bodies in order to speed up the adoption of IS.

Apart from the external factors, the UTAUT was used to reflect the usage of IS tools at individual level. The interview findings revealed that perceived benefits at personal and organisational levels were valued differently. However, simplified supervision, ease of computations and communication of audit evidence, were the most influential factors for IS usage. Meanwhile, the organisational factors revealed that audit efficiency and effectiveness were 'somewhat influential'.

From the interview findings, this study has managed to categorise all the aspects into two main variables, namely, internal and external variables. The external variables, were found to be too general, thus, the study further categorised them into client's factors, the audit professional factors and other external factors (i.e. competitive advantage). Meanwhile, the

internal factors which composed the UTAUT variables, were also categorised into two main factors, namely, perceived benefits (individual users of IS) and perceived benefits (audit firms). This classification emerged due to the varied types of respondents that were selected which composed of managers and owners of audit firms (partners). Figure 6.2, displays a tree map of the factors influencing IS usage based on coding process in Nvivo. Again, the larger the size of the box, the more frequent it appeared in the transcripts.

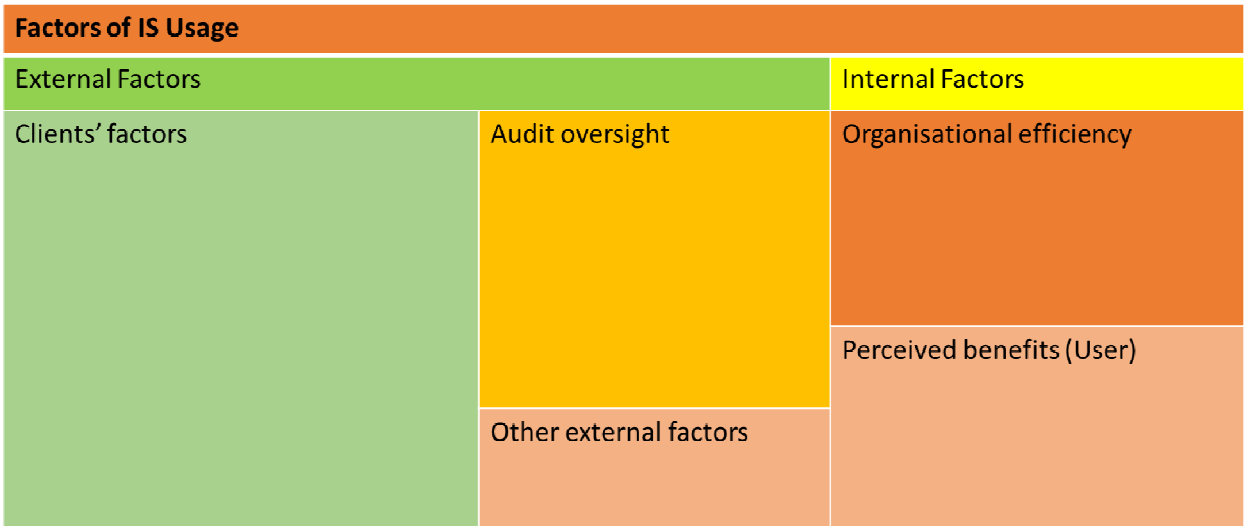


Figure 6.2 Thematic Coding on Factors Influencing IS Usage by External Auditors

6.4 What is the Impact of IS on Financial Audit Process?

The third objective was to assess the implication of IS usage on financial audit process in order to determine the extent of IS diffusion and how it facilitated the audit process. The audit life cycle is composed of planning, execution, documentation, gathering evidence or testing and report writing. IS tools such as ACL, IDEA, SASoft, Pro-audit, GAMX and so on, are used to achieve audit objectives and to enhance the audit process. The interview findings revealed that IS had impacted the audit procedures differently. The following sub-section discusses these aspects as was described by the interviewed respondents:

6.4.1 Planning and Audit Team Composition

Audit Planning involves allocating appropriate resources including manpower based on the nature of the audit assignment. The interview findings revealed that unlike in a manual environment where a partner would select the audit teams from among financial auditors, in a computerised environment, audit teams are composed of both financial auditors and IS experts to effectively audit the systems as well as transactions (R2, R8, R9 and R11). The IS experts check the IT environment and ascertain its extent of complexity and security that would permit the financial auditor to rely on the systems that process information. In a situation where the level of audit risk is assumed to be high, the audit team would require more IT experts and other specialists such as IT fraud examiners (R9 and R11). A partner in a large international firm clarified that "*it has become imperative for audit firms to develop additional skills outside the traditional audit"* (R11). In contrast, if the system is just used to post transactions with few electronic transfers of cash, few individuals (two or three), who have access to the system, it becomes economical for the financial auditor to just audit the transactions directly without the assistance of an IT expert (R5, R11 and R12a).

6.4.2 Documentation of Audit Work

As businesses are gradually relying on paper-less processes and documentation, audit firms are expected to also move to automated systems (Bierstaker et al. 2001). Accordingly, more than fifty percent (50%) of the respondents mentioned that they were in the process of transforming to automated working paper mechanisms and storage of information. It was revealed that a main benefit of automated working papers is that data can be shared easily via emails, work-related messengers or other remote access software (R8 and R11). Past years' audit working papers are integrated with the recent years' working papers without difficulties. In circumstances where a client is still keeping financial data on hard copies, scanners can be

used to convert the information into an electronic presentation. For safety reasons, several backups are maintained electronically at various storage locations. This practice has significantly reduced the cost of storage of working papers which could not be achieved in manual documentation systems (R2, R9 and R11).

The interview findings further revealed that six audit firms did not have to develop audit programs. It was clarified that the audit software has embedded both audit procedures and authoritative guidelines from IFAC standards, NBAA and other regulators (R11). For the internationally affiliated audit firms, the audit programs were developed by their mother organisations and embedded within the audit software. The practice has significantly simplified the audit procedures. For instance, a partner in one of the Big Four commented "*in a practical audit, after completion of CPA training, a junior auditor who is not yet exposed to IFRS would realise the applications of the accounting standards automatically as he starts doing the audits because it is something that they work with daily within the audit system"*. (R11).

6.4.3 Audit Testing

The interview findings reported that between 60% and 80% of audit clients were using some kind of enterprise computing platform (R1 and R12a). This, therefore, means that paper-based trails and mechanism check points that were formerly normal for an average audit firm, are accessible in an automated form. Thus, it becomes critical for auditors to have an in-depth understanding of the clients' systems so as to audit through the system. For instance, during reconciliation of client's financial data, auditors used software to pull the client's records for verification (R2 and R5). Audit standards also require that, if clients use IS to process and store data, the IS platform must also be audited (R11). Hence, testing of sophisticated controls like firewalls, encryption of sensitive information, passwords, and authentication of

automated data and signatures becomes important (Bierstaker et al., 2001; Kotb and Roberts, 2011; No and Vasarhelyi, 2017). Consequently, respondents mentioned that they have implemented a risk-based audit methodology that focused on analytical review, testing of IT controls and reduced substantive testing (R9, R11 and R12b). Similarly, the use of software such as ACL, IDEA, GAMX and so on, has helped auditors to improve the audit tasks by auditing through the system especially in high computerised clients (R2, R5, R8 and R11). Testing of one hundred percent of data can be performed on some businesses with high compliances like banks, insurance companies, telecoms and health where audit software can probe for repeated invoices, identical transactions and false claims (R11 and R12a).

6.4.4 Execution of the Audit

The computerised environment of the clients has changed the way the audit is conducted. The interview findings revealed that the IS auditor first checks the IT general controls around the system after which the financial auditors perform transaction audits by relying on the tested controls by the IS auditor (R2, R5, R9 and R11). In a situation where the controls in the systems are confirmed to be ineffective, further verification of the system is performed, after which auditors will contact the management for clarifications and confirmations to see whether the management is aware of the situation (R5). In rare, extreme cases the audit firm would resign and recommend the client to change the auditor if the system is believed to be unreliable (R5 and R11).

The nature of financial audit has now enshrined into understanding of a client's business (R2, R8; R11). It was clarified that the auditors' methodologies are converging with the changes of the clients' environment (R9 and R11). It therefore means that for computerised clients, manual audits cannot be applied (R11). Additionally, IFAC standards require auditor to use technology to achieve efficiency and to be effective in performing audit assignments. It was

stated that since audit software can select, scrutinise, and analyse large data sets, it has improved efficiency in the audit process (R9 and R11). For instance, audit processes such as reconfirmation of accounts balances, aging of accounts receivables, and recognising of outliers in transactions might be conducted on the whole population instead of a sample (R2 and R5). However, such a procedure is desirable but not practiced because the notion of audit relies on efficiency on the side of the audit firm (R11). The audit of the entire population may produce high level of audit effectiveness but may be inefficient because "*the needs justify the means"* (R9). It was therefore reported that the nature of audit clients in Tanzania does not require a verification of the entire population due to cost-benefit issues (R5, R9 and R11).

6.4.5 Communication and Information Sharing.

The interview findings revealed that the use of IS has enhanced the sharing of information among auditors when they are working in different audit locations. The use of software such as EMS has shareware applications where the work performed by each auditor can be seen by others. The updated and deleted work can be viewed by others, hence, enabling transparency and knowledge-sharing among the team members. For instance, if one auditor is working with payables' database and another one with receivables, the work can be viewed and shared by all (R11). Furthermore, a manager can leave a coach note on how the juniors need to improve and also the audit findings can be discussed by the team members through shareware applications which was not possible in the past (R9). In the new ISAs, transparency in the audit process was emphasised and one of the ways to foster transparency is to discuss the audit reports internally before being signed by the partner. Subsequently, a few respondents (R2, R5, R8 and R9) reported using audit software (EMS) for communication purposes to produce a group consensus or opinion. Meanwhile, another respondent mentioned using work-related messengers to discuss the audit report at various stages (R11).

6.4.6 Report Writing

The interview findings revealed that the use of IS tools has facilitated the report writing process and allowed audit firms to issue reports on time. Basic IS applications such as MS Word and Excel enabled the preparation of the audit reports and sending them to the clients. Furthermore, audit firms are able to rectify errors, make adjustments and issue the corrected version of the report in a very short period of time (R1, R3; R4 and R7).

6.4.7 IT Consulting Services

Several respondents (R1, R9, R10 and R11) reported that training in IT related issues was among the important priorities for audit firms. Auditors were given internal training or sent abroad to acquire additional IT skills necessary for their working environment. The purpose of training in IT was to enhance human resources development so as to ensure that audit effectiveness is achieved (R7, R9 and R11). As auditors become more technologically proficient, additional consulting services will emerge (Bierstaker et al., 2014). Thus, Auditors provide extra services to their clients such as risk management and cybersecurity services. The provision of such services enables the clients to be updated on the various risks categories that might threaten their information and learn mitigation strategies (R9; R11 and R12b). Subsequently, auditors assist their clients in designing assessable objectives and performance indicators that can be electronically monitored through enterprise computing. The use of IS tools and techniques facilitates auditors to utilise their extra time in assisting clients to assess business risks as part of FSs audit.

6.4.8 Discussion on Impact of IS on Audit Process

The third objective was to assess the implication of IS usage on financial audit process which is the core business of the audit firm. The interview findings highlighted that IS usage has

implications on the audit process from planning, execution, audit testing, documentation and report writing. The use of IS tools has enhanced these audit procedures differently. Figure 6.3 shows a summary of answers from the response based on the coded items as they appeared on the transcripts. It was found that some of the respondents stated that their audit firms had computerised their audit procedures while others were in the process of converging. The use of IS tools and techniques has necessitated for auditors to acquire additional skills in IT which is becoming useful in providing extra services to their clients. In turn, auditors are saving time and efforts, ensuring safety of clients' data, while increasing revenue to the audit firms by providing additional IT related services.

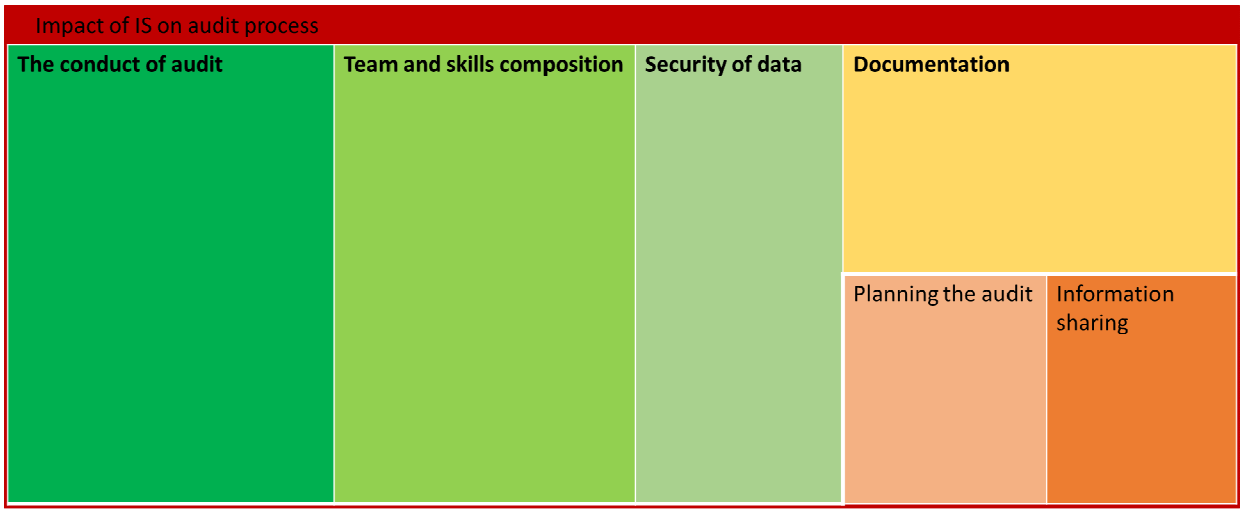


Figure 6.3 Thematic Coding on Impact of IS on Financial Audit Process

Figure 6.3 displays sub-themes as they emerged from the transcripts. It was revealed that the use of IS has positively impacted the audit process. The common items that were mentioned are shown in the figure above to include how the audit was conducted, teams' composition and security of data, documentation, planning the audit and reduced level of audit risk.

6.5 How do Auditors Detect E-fraud?

The fourth objective intended to explore how auditors detected fraud that occurred in computerised platforms. The interview respondents explained five main aspects when

identifying e-fraud in the computing environment, namely (a) understanding the clients' business and IT environment, (b) identifying the areas of weaknesses, (c) including an expert, (d) adjusting the audit methodology; and (e) using penetration testing. The details of these procedures are explained in the next sub-headings.

6.5.1 Understanding the Client's Business/IT Environment

The respondents mentioned that in tackling e-fraud, auditors must first abide with the requirements of IFAC audit standards which require them to visit the clients and understand their IT environment before they start doing the audit. In other words, they must establish the extent of the clients' IT platform and assess the integration of online transactions and financial reporting. When auditors find that the company uses IT to conduct online banking or online orders, the auditors are obliged to be aware that fraud might have occurred through online transactions. It becomes important for the auditors to develop their audit methodology and techniques to make sure that it is capable of detecting material online fraud (R9 and R11).

After having understood the IT environment of the clients, the auditors would establish whether it is necessary to bring additional specialists in the audit process, which is also an ISA requirement (R11). Furthermore, auditors will predict the chances of frauds to have occurred, the possible areas and mechanisms of frauds to occur, which is also an important aspect of the audit process (R9).

6.5.2 Risk-Based Audit and Professional Scepticism

The second aspect involves auditors checking the potential of inherent risk, the mitigating control along that risk and testing their effectiveness (R5, R9 and R11). In complex environments such as banks, auditors would take extra precautions by suspecting what might go wrong, which is called risky-based audit (R5). For instance, if a cash transfer from one system to another is not tallying, a question mark is attached to the transaction which forms

part of the controls. It was stated that IT general controls give auditors the surety of mitigating risks (R5 and R11). So, auditors usually identify the risk and then test controls and their effectiveness.

Another important aspect is to practice professional scepticism during the audit process (R9 and R11). Scepticism is a questioning mind that auditors practice by suspecting possibilities of fraud to have occurred. The respondents reported that they continuously practiced professional scepticism during the audit process, in what they called '*what could go wrong'* (R9; R11 and R12a) which is the ability of auditors to know that in case fraud occurred, it would occur through channels A, B or C (R11). The respondents further clarified the three most common channels for e-fraud to occur. The first one is through stealing passwords (R5 and R11). R11 further explained that staff members can be used to access the system to send monies illegally to a third party. Hence, auditors must check security systems to ensure that passwords authorisation is done by one personnel instead of many authorised people.

The second possibility of e-fraud to occur is through unauthorised users who initially had access to the clients' system (R11). In order to predict such a possibility, auditors must audit the procedures in termination of the top personnel who had access to the entity's database and sensitive information to ensure that they cannot use their power to fraud the entity when their services are terminated. The third possible channel of e-fraud is through public areas. A malicious virus can be loaded into the computer system without the knowledge of the company. The virus can be capable of stealing passwords from staff and send them to a third party. The third party (a culprit) can use the password to access the client's system and commit fraud (R11). Therefore, auditors must check several other things to ensure that the clients' systems are secured from any unauthorised users (R5).

Another respondent, an associate director (R10) clarified that e-fraud can be committed by an external fraudster who worked for the system vendors of a particular software. Since the fraudster may have the knowledge of the software, he can attack the systems and commit online fraud from far. She stressed the importance of company management to frequently change passwords to ensure no loopholes in the systems to fraud the entity. She stated: "S*ometimes people forget to change passwords, so if a hacker is in Russia, and knows Oracle's default accounts are ABC, and knows the password, he can hack into the system. And it is also possible for someone to guess the systems defaults and succeed to attack the systems and commit fraud"* (R10). However, based on her experience, she perceived internal fraud as the major threat to their clients' systems as compared to external fraud.

The respondents were further probed on how a company can create a system that prevents passwords from being stolen from users. A few respondents (R2, R5, R9 and R11) mentioned one reliable method which is to have an anti-virus updated on the system. A partner from one of the Big Four clarified that "*if a company has an up-dated anti-virus on their system, the chances of passwords being stolen by a third party without the company knowing are zero"(R11).* He further mentioned that anti-virus software will always prevent virus infection to computers, and so auditors develop audit tests to assess whether the company has fully-updated anti-virus software in the first place. Auditors must examine the entity's systems, checking the installed anti-virus and the date it was last updated. It was stated that the modern anti-virus get regular, automatic updates, unlike the out-dated anti-virus. Furthermore, auditors would check what controls were activated during the financial period by testing them (R2 and R9).

Another aspect is to check whether employees are fraud conscious. It was mentioned that a fraud-conscious employee will never accept to share a password (R5). When auditors test the

possibility of employees' awareness, they want to identify whether clients are aware of how fraud may occur online, and whether they have control mechanisms that will address frauds. An audit partner explained that situation by saying: *"the objective of that can have a mix impact to test the effectiveness of a client to be aware of how fraud may occur online and secondly, whether the client has control mechanisms that will counter fraud if it occurs, it should get stack somewhere"* (R9).

6.5.3 Adjusting Audit Methodology

If auditors test and discover that some of the control measures to prevent e-fraud are not effective, for example, after testing the password system and discovering that the system has loopholes such as employees sharing passwords, it would imply that the system does not work, or that the entity does not have preventive controls in place (R5, R9 and R11). Hence, auditors would conclude that chances are that fraud may have occurred and the management is not aware of that. The next step auditors could take is to adjust their audit methodology. For instance, if the prior audit procedure required a sample size of 10%, the sample size would be increased to 80% or sometimes auditors would check the entire population (R11).

6.5.4 The Use of Forensic Expert

After confirming the occurrence of e-fraud, auditors would consult forensic experts (R5 and R11). A forensic expert is an investigator who examines the extent of fraud and its impact on the entity's FSs. The forensic expert team is composed of IT expertise, law and accounting expertise to be capable of measuring the extent of damage and be able to gather the required evidence to be presented to the court of law (Popoola et al., 2014). There are several IS tools that can be used in forensic audits such as test data, parallel simulation and other data mining techniques as was highlighted in the literature. However, five respondents (R2, R5, R9, R10

and R11) mentioned that forensic audit was uncommon as they perceived Tanzania as a relatively safe environment. Other respondents further mentioned that auditors have not experienced serious cases of huge e-fraud that required forensic investigation (R5 and R11).

6.5.5 The Use of Penetration Testing

The last procedure is to conduct penetration testing to check possibilities of unauthorised access to the entity's system. The details of this have already been discussed in sub-section 6.2.2. It was mentioned that increasingly, penetration testing/ethical hacking is becoming an important technique for auditors when auditing high risky clients such as banks (R9, R11 and R12a). It was further clarified that through the use of penetration testing, several IT related faults, unauthorised access and frauds were uncovered and reported to the management.

6.5.6 Discussion on E-fraud Detection Procedures

In identifying e-fraud, it was essential for auditors to comply with ISAs procedures such as understanding the client's IT environment and assessing if the risk is higher or minimal. If the risk is large, auditors would bring in IT and forensic experts to be among the team members. Nonetheless, the use of risk based audit procedures and professional scepticism were mentioned as the most important aspects and which are also part of requirements in the ISAs. However, auditors have also adopted extra techniques such as penetration tests or ethical hacking by hacking the client's IT system to check for any unauthorised access to the entity's database. Table 6.4 displays thematic coding on the procedures used by auditors in identifying e-fraud. It should be noted that these procedures were mostly explained by IT experts and some few partners.

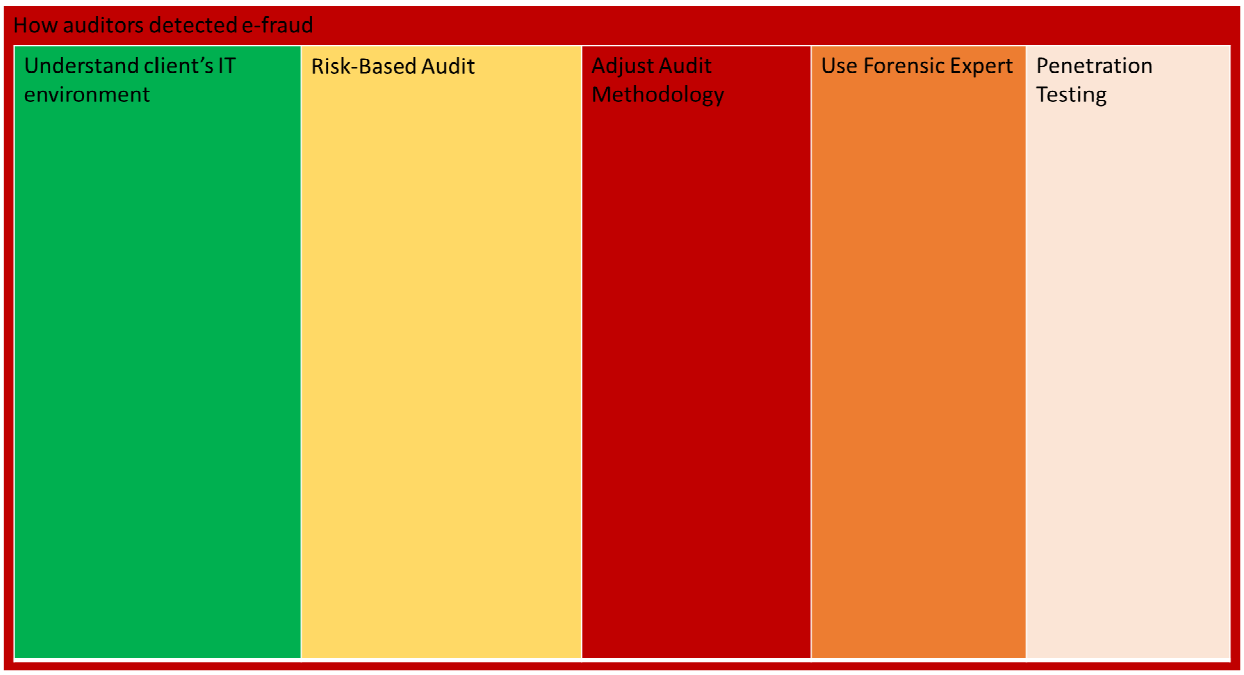


Figure 6.4: Thematic coding on how auditors detected e-fraud

6.6 What is the Impact of IS on E-fraud Detection?

The last objective was to assess the impact of IS on e-fraud detection. The interview data demonstrated two areas where IS has reported positive impacts in relation to fraud detection. These include increased fraud detection and reduction in FSF. These are elaborated further in the next subsections.

6.6.1 Increased Fraud Detection

Three respondents (R9, R11 and R12a) agreed that there has been an increasing trend in fraud detection when auditors started using IS tools and techniques. R11 clarified that such an increase in e-fraud detection should not be interpreted as the increase in fraud, rather as a signal that auditors are improving the audit quality by disclosing the culprits. Likewise, R9 explained that increasingly, auditors have managed to detect fraud in computing platforms especially in banks and telecoms because the two are purely IT-based clients where the culprits were motivated to attack the systems and steal money.

The interview findings further revealed that when auditors increased the use of IS tools and techniques, it conveyed a signal to their clients that auditors are now more effective in detecting fraud, as a result, it has deterred new frauds from occurring. R11 commented *"clients now realise that auditors are more effective, so, it is deterrent for them to cause new frauds"*. Meanwhile, R12a further delineated that when auditors started using technology, they have detected more frauds than they could before. He explained that in the beginning, the fraud curve would increase but eventually it will start diminishing as auditors increase using IT to detect loopholes that curb frauds.

6.6.2 Reduction in Financial Statements Fraud (FSF)

Similarly, a partner in one of the Big Four clarified that technology usage in auditing has a positive impact on FSF. He stated that since auditors started using IT tools, increasingly, that work has deterred FSF, which has two implications: first, auditors have become effective in identifying frauds since clients have also identified frauds easily, the level of FSF has declined. Second, he mentioned that through the use of fraud statistics, [i. e before and after IT adoption] when auditors started using computers the levels of identifying frauds have increased, which means the effectiveness in the audit procedures by using IT tools has improved the audit process. Subsequently, it has improved on the way auditors detect frauds. He commented: "*So, auditors are now able to identify frauds even in areas they were unable to identify in the past, consequently, the number of frauds identified has increased while FSF has declined* (R11). However, due to time constraint, this study did not find the data (company reports) to measure before and after IS adoption so as to establish a statistical reduction in FSF as what the respondents have mentioned. This is suggested as a gap in future research.

Finally, the interview respondents mentioned that the use of ethical hacking to do penetration testing was one of the techniques which helped greatly to detect unauthorised access for employees to commit fraud (R9; R11 and R12b). The BOT was also praised for requiring that all audit firms that audit banks to issue a report on systems security every year, which has further ensured the safety of banks' information and customers (R12b). Similarly, the BOT was further commended for its stringent measures in selecting audit firms based on their IT capability to audit computerised clients instead of allowing any businesses to select their independent auditor. This tendency has ensured that pure IT based clients (i.e financial institutions) are audited by large audit firms or medium firms that have sufficient IT experts and IT infrastructure to provide quality audit (R11). He commented "*as much as audit firms are authorised by the NBAA, BOT always authorises very few firms after ensuring that they have a capability to audit IT systems, because now without IT, there is no way that you can confirm the audit was effective"*.

6.6.3 Types of E-fraud Detected

Respondents were further probed whether they detected any e-fraud through the use of IS tools. The interview findings highlighted that auditors identified different types of transaction fraud that occurred in e-business platforms because culprits were interested in stealing electronic cash and cash equivalents. Three respondents (R2, R5 and R10) reported that the kind of irregularities happening in computing business platforms are IT related. R10, an associate director, gave an example of mobile banking fraud, citing its modes of occurrence which mostly include collusion of IT administrators. She mentioned that external hackers are now becoming common in the Tanzanian environment and most of them use loopholes which were not addressed on time. She further clarified that her audit firm detected some of these

frauds through the use of ethical hacking tools and discovered that some administrators had abused their rights and committed online frauds.

In addition, she commented on the complexity of mobile banking fraud, saying that there are tens of telecoms that are linked to the banks' systems; and administrators (and IT experts) collude differently with outsiders through the use of sim-swap systems to commit frauds. She further clarified that sim-swap is a fraudulent act where an IT administrator could temporarily stop the functioning of a sim card from the owner for some time and uses particulars of the account holder to make illegal cash transfers (R10).

Although R10 believed that, identifying fraud is not their mandatory responsibility, at the same time she explained about identifying repeated invoice numbers through running scripts on ACL. She stated that it is an easier way to check frauds and errors when any payment has been repeated more than once, and they have managed to identify a few of such fraudulent acts. However, she commented that online fraud that is happening in the Tanzanian environment can be mitigated through basic controls which are in place without necessarily applying advanced IS tools and techniques. She remarked *"online fraud incidences are there but I believe they are still manageable"* (R10). In other instances, auditors identified the risk through dysfunctional controls (R5). A dysfunctional control is a control that does not mitigate the intended risk which requires auditors to seek explanations from the management.

Another respondent (R8), an IT expert, reported that internal fraud was discovered but in a limited number of their clients where the culprit had changed system configuration to commit fraud and managed to pass illegal cash transfers in the form of money laundering (R8). She stated that money laundering is uncommon act but the impact of a single transaction can have adverse effects on both the entity and the economy.

Meanwhile, R1, a partner, mentioned that through detecting weaknesses in the IT systems of their clients (hotel client), they identified fake hotel bookings which were aimed to inflate earnings. It was discovered that the indicated paid up hotel bookings were in fact not paid. Meanwhile R7 clarified that the online fraudsters are very clever because they study the systems and check their weaknesses and discover how to play with the numbers. He commented that the remedy to e-fraud is training auditors to be ethical hackers who can identify and correct loopholes in the entity's systems.

In contrast, R11 reported that the extent of e-fraud in the country is becoming common, and he foresees a worse situation in future due to two reasons. The first reason is the quality of users of IT, who mostly come out of universities when they are not IT savvy. He cautioned that even if companies have got the best systems, the users of those systems are not highly technical savvy. That is why it is common for people to share passwords because they do not know the risks attached to sharing passwords (R11). The respondent gave an example of a situation where an employee (a culprit) in one of the largest hotel, caused millions of cash to go missing via online transfers through sharing passwords. He stated *"In one of the hotels we audit [hotel X], an employee had stolen money using a shared password. The investigation was conducted but it could not catch the thief because everybody knew the password of the other!"* This highlights a low understanding of the sensitivity of passwords given to a few individuals in the organisation as a means of strengthening internal control systems.

The second reason was related to the nature of people who commit online fraud by taking advantage of their victims' low understanding of IT related issues. He stated "*advanced delinquents who commit e-fraud are preying on people in developing countries like Tanzania who have embraced technology but do not have high level of technological knowledge of their users"* (R11). As a result, it makes these countries vulnerable to external hackers. He

compared the IT skills gap between Tanzania and developed countries where children start learning IT in primary schools.

Two other respondents (R2 and R5) reported identifying fake payroll systems that were used to pay employees. They mentioned that the use of ACL helped in identifying the addresses of employees by attaching them to the names of each person on the list. Meanwhile, R12b reported that through the use of IDEA, they managed to detect fake cash withdrawals that were not made by the owners. He clarified that the use of technology can make errors or fraud stay for a long time undetected, making the fraudster enjoy the systems for a period of time. However, he explained that through the use of IDEA to apply the Bedfont's law in identifying unique patterns in cash withdrawals, it enabled auditors to identify fraudulent cash transactions. Similarly, he perceived that the fraudulent activities are uncommon to most of the clients that they audit.

Meanwhile, R8 reported that they identified internal fraudsters who used programs to transfer very small amounts of cash from the accounts of users to another account which was created to fraud customers. She stated *"the IT guys discovered that the fraudster was conniving with senior managers to transfer small amounts of cash from the accounts of customers to another illegal account"* (R8). Even though the respondent believed that fraud occurrence is not a systems issue but a human activity, she reported that the IT experts managed to identify some frauds through audit software.

Meanwhile R2 explained the situation where an IT expert who was working in a treasury department in one of the largest banks in Tanzania was discovered creating an account and using it to transfer only US dollars of small denominations. The sum of cash stolen in the fake dollar account had reached $10,000. However, the fraudulent account was discovered later by a group of IT experts from his audit firm and was reported to the management.

Similarly, he clarified another scenario where they had identified an IT expert collaborating with other employees to create fake accounts, transferred money and then deleted those accounts. The fraudsters had managed to create seven different accounts in 2 years. When the scenario was discovered by auditors, it was found that it involved collusion between IT experts and the senior management who had authority in the organisation (R2). He further clarified that the clients' systems save all changes of the new created accounts including those that were deleted. He mentioned that the culprits may not be aware of where such changes occur unless they audit the server of the client's system.

Most of the respondents mentioned that they identified e-fraud through the use of penetration testing, also known as vulnera-penetration and ethical hacking. Three respondents who were partners (R9, R11 and R12b) commented that increasingly, auditors use ethical hacking techniques to check whether the client is vulnerable to internal and external attacks. If the auditors succeeded in penetrating the system, they confirm the possibility of fraud to have occurred. The details of the tools used to conduct ethical hacking have been discussed in sub-sections 6.2.2 and 6.2.3.

Lastly but not least, the respondents were asked whether they used CA methodologies as a fraud detection mechanism. Earlier scholars, as highlighted in Chapter 2 sub-sections 2.10.3 and 2.10.4, have argued that CA has detective and protective mechanisms to computer-related fraud in real time. In essence, CA involves the auditing of the entire population and not mere sampling so as it is able to detect fraud easily because all the items of the transactions are audited and included as a population. However, the interview findings revealed that CA was not used by external auditors in Tanzania. It was stated that clients may not be in the position to pay for CA due to its cost implications (R5, R9 and R11). R11 further clarified that one of the aspect of audit is efficiency to the audit firm. When an audit has to be done by involving all the population, it may not be efficient as the time and

manpower needs to be paid and the audit firms would provide effective services bearing in mind efficiency. He further explained that using CA in Tanzanian environment is unnecessary as they [audit firms] can manage the risk components surrounding the environment through the use of the IS tools and techniques available without necessarily changing their current audit methodologies. He commented *"Using CA for the Tanzanian environment would be like using a big stick to kill a fly" (R11).*

A few other respondents (R2, R9 and R10) mentioned that even if there are incidences of online fraud, they are manageable and can be mitigated through the existing mechanisms without necessitating the use of CA. Likewise, three respondents (R2, R7 and R12b) who had worked with the Big Four in neighbouring countries within the EAC mentioned that e-fraud occurrence in Tanzania is minimal as compared to that committed in the neighbouring country of Kenya. R7 clarified that due to high online fraud incidences in Kenya, the Kenyan Cyber Law has made it mandatory for IT audit to be conducted and to produce a report on systems' security of the client even if the entity used only one computer to transact a few online activities (R7).

6.6.4 Discussion on Impact of IS on E-fraud Detection

The 5th and last objective aimed to explore the impact of IS on e-fraud detection. The respondents explained various types of e-fraud detected using IS tools and techniques. Auditors used IS tools to curb e-fraud such as a penetration testing. Penetration testing is a procedure whereby auditors try to commit online fraud to see whether it will be successful. Afterwards, they provide the client with a report, detailing weaknesses and strengths of the system and suggestions to remedy the weaknesses. The same report would be used by auditors to make judgements about the audit because the result of the testing will inform auditors whether the system is effective so that they can rely on a small sample size. In

contrast, if the system is vulnerable to hacking, it means that the risk of fraud is high, and the risk that the numbers are not correct is also high. Therefore, auditors would dig deeper followed by additional investigations on fraud. If an e-fraud was discovered, auditors would consult a forensic expert who would dig the matter for further evidence to be produced to the court of law.

The types of frauds that were discovered using IS tools include IT related faults, unauthorised access by a terminated senior employee, stealing and misuse of passwords, opening fake accounts and transferring cash therein, transferring cash in small denominations from different customers and mobile banking-sim swap fraud. Other e-frauds were fake hotel bookings, payroll fraud and repeated paid invoices among others. The use of IS tools and techniques reduced FSF as the culprits became aware that auditors are effective in IS usage, hence, it deterred new frauds from occurring. Even though the fraud curve would show an upward trend in the beginning, it would eventually start diminishing as auditors gain experience of the clients' risk profile and also in using IS tools and techniques. To sum up, the interview findings revealed that the usage of IS tools and techniques have the ability to detect e-fraud by sensing unusual transactions and unauthorised access to the entity's system.

However, a few respondents believed that e-fraud happening in the Tanzanian environment is minimal and can be managed by strengthening controls that are in place rather than using advanced IS tools and techniques as was suggested in the literature. Hence, the use of CA and data mining were found not practiced by external auditors. This finding is contrary to suggestions of past scholars who recommended the use of advanced CAATTs and data mining techniques to spot frauds in computing business platforms (Jans et al., 2009; Ngai et al., 2011). This is because most respondents perceived the use of advanced tools as unnecessary in Tanzanian environment and felt that the risk profile of their clients can be

managed by their current audit methodologies. Instead, the use of ethical hacking tools was found important to auditors who audited risky clients especially banks. The use of ethical hacking restored auditor confidence that the client's system was safe especially in a situation where auditors did not manage to penetrate the client's system.

These findings are contrary to earlier studies in the UK where ethical hacking techniques were rated with a low mean value mostly in testing security of the clients' websites (Kotb, et al., 2012). The differed findings might be due to the strength of internal control systems of many businesses in the developed world which makes it unnecessary for auditors to use additional IS tools and techniques for auditing purposes (Debreceny et al., 2005). However, the results are consistent to El-Sood et al. (2015) who reported external auditors in Egyptian firms using audit technology mostly in risk assessment. The variable '*IT usage for risk assessment'* exhibited a high perceived importance with mean value of 4.65. Similarly, the importance of audit technology for fraud review was also rated as pretty important.

In any case, this study suggests that audit organisations should increase investments in technologies for fraud detection so as to identify systems related faults that can result into e-fraud. In fact, the new fraud dimension is systems-related that calls for assurance in IT infrastructure, security and business processes rather than substantive testing of transactions (Kotb and Roberts, 2011). Thus, if auditors continue to practice traditional methods of testing controls, significant risks may go undetected (Stanton, 2012; Vasarhely and Romero, 2014; No and Vasarhelyi, 2017). Figure 6.5 shows the coded themes on the impact of IS on e-fraud detection as were summerised from the Nvivo software.

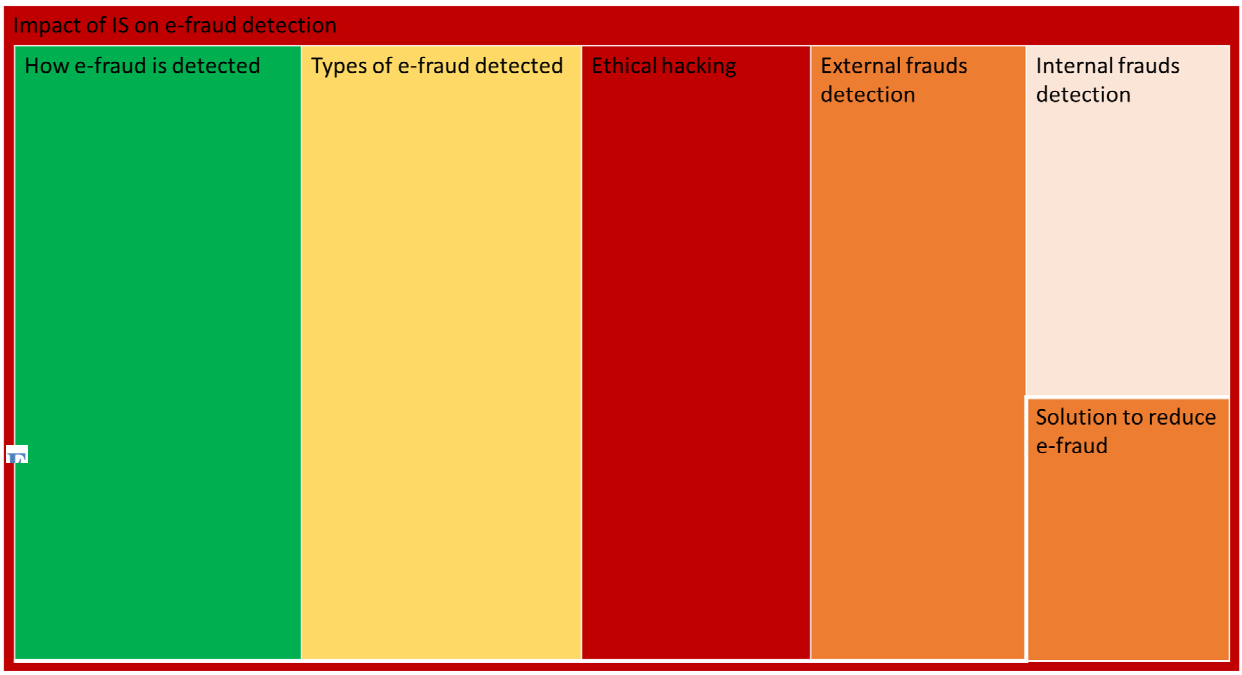


Figure 6.5: Thematic Coding on Impact of IS on E-fraud Detection

Figure 6.5 shows the summerised themes as were emerged from the Nvivo software when anlysing the interview transcripts. The responses that were similar and coded in one category include detection techniques, types of e-fraud detected, the use of ethical hacking for fraud detection, external and internal fraud and finally the solution to e-fraud. Again, the larger the size of the box, the more the number of references that emerged from the transcripts.

6.7 Summary of the Chapter

This Chapter presented the findings from qualitative data that were collected through interviews to answer all the five research questions that were proposed in Chapter one. It was revealed that external auditors in Tanzania used different IS tools and techniques. Both internal and external factors influenced the use of IS but external factors, especially clients' related factors were found to motivate the usage of IS the most. It was found that IS usage had improved financial audit process and enabled auditors to detect frauds even in the areas that they could not manage to detect them in the past. Various IT related frauds were discovered using IS tools and techniques, and subsequently, IS usage had reduced FSF while

making e-fraud detection more prevalent. The next Chapter presents quantitative findings which aim to answer the 2nd research question through a larger sample size of respondents by statistically testing the UTAUT.

CHAPTER 7

QUANTITATIVE FINDINGS

7.1 Introduction

This Chapter presents the quantitative study findings from the data collected through a questionnaire. The Chapter is presented following one study objective (Objective2), which intended to predict the most significant factors for IS usage by external auditors in Tanzania from a larger sample through the adopted UTAUT. However, the Chapter will also present a brief overview of the IS usage on a few items as were composed on the questionnaire in answering the research question 1. Similarly, the procedures and techniques used for data screening and analysis are presented to reflect the methods that the study employed in this section of data analysis. The Chapter is divided into five sub-sections. Sub-section 7.2 is the demographic features of the respondents, sub-section 7.3 is the IS usage, 7.4 is factors influencing IS usage, 7.5 is results and interpretation and lastly, 7.6 is summary of the Chapter.

7.2 Demographic Features of Participated Firms and Respondents

The demographic factors that were captured in the survey questionnaire included type of audit firm, gender, age, working experience, IT skills and education levels. The details of demographic factors are shown in table 7.1. The results from the data exhibited that 74.5% (n=79) were from large audit firms and 25.5% (n=27) were from medium firms.

Table 7.1 Profile of the Participated Audit Firms

Firms Category	**N**	**Percentage**
Large Audit Firm	79	74.5%
Medium Audit Firm	27	25.5%
Total	**106**	**100%**

Furthermore, the study findings reflected the demographic details of the individual respondents with the aim of determining the nature of employees that were at the firms to establish their gender, age, education levels, experience and professional certification. The study employed these details to establish whether they have any impact on the usage of technology and improvement in audit efficiency and performance as other studies have found in the past. For instance Chou and Pearson (2011) and Kiabel (2012), in their studies found that demographic factors have both positive and negative influences on the usage and adoption decisions of technology. As indicated in Table 7.2 the results from the demographic findings showed that there were more male than female respondents with a percentage score of 85.8 (n=91) as compared to 14.2% (n=15) of female respondents. It can be concluded that the external audit profession in Tanzania is majorly dominated by males. The respondents' age also had variances as per the study findings. The findings indicated that the majority of respondents with 73.7% (n=78) were at the age brackets between 25-34 years. It can be concluded that most audit firms in Tanzania prefer to hire young individuals who are ready to take on tasks with flexibility even though they are expensive to maintain and retain (Miiro et al., 2016).

With employees' working experience, the findings showed that 51.9% (n=55) of the respondents have audit experience of between 6 and 10 years, whereas, 57.5% (n=61) of the respondents have 0-5 years of computerised auditing while 33.1% (n=35) have 6-10 years of computerised auditing and this could suggest that the respondents are relatively experienced in the audit profession and in audit technology. In addition, in the aspect of technological skills, the study used "very good'', ''good'', "adequate'' and "basic" as a 4-point scale. From the data results, it was indicated that 42.4% (n=45) rated their overall IT skills as very good, whereas 55.7% (n=59) were under the level of good and 1.9% (n=2) were in the category of adequate skills for using technology in audit practices.

Lastly, the study findings exhibited that in terms of the education levels of respondents among the audit firms in Tanzania, a majority were Bachelor degree holders at 83.0% (n=88), 6.6% (n=7) were masters degrees and the remaining 1.9% (n=2) were diploma holders while 8.5% (n= 9) joined the firms through the use of professional certificates only. Nevertheless, the respondents were affiliated to different accounting and audit proficiency that ranged from CPA, ACCA and CISA. The study results showed that 53.8% (n=57) of respondents had CPA qualification, 21.7 % (n=23) had CISA, 21.7% (n=13) had ACCA qualification and 7.5% (n=8) were fraud examiners and certified risk information system and control experts. The overall qualifications of the respondents suggest that the audit tasks comprised of a team of multiple expertise of financial and IT audit specialists which are consistent with prior studies (Brazel, 2008; Greenestein Prosch et al., 2008; Hunton et al., 2004, Seeburn, 2013; Vendrzyk and Bagranoff, 2003).

Table 7.2 Summary of the Respondents' Profile

Item	N	%
Gender		
Females	15	14.2%
Males	91	85.8%
Age		
18-24 years	2	1.9%
25-34 years	78	73.7%
35-44 years	21	19.8%
45-54 years	4	3.7%
55 and above	1	0.9%
Audit Experience		
0-5 years	23	21.7%
6-10 years	55	51.9%
11-15 years	17	16.0%
16-20 years	9	8.5%
21 years and above	2	1.9%
Computerised Audit Experience		
None	3	2.8%
0-5 years	61	57.5%
6-10 years	35	33.1%
11-15 years	7	6.6%
21 years and above	0	0%
IT skills		
Very good	45	42.4%
Good	59	55.7%

Adequate	2	1.9%
Basic	0	0%
College Education		
Diploma	2	1.9%
Bachelor Degree	88	83.0%
Master	7	6.6%
PhD	0	0%
Others*	9	8.5%
Professional qualification		
CPA	57	53.8%
CISA	23	21.7%
ACCA	13	12.3%
Others**	8	7.5%
Others***	5	4.7%
Total	**106**	**100%**

Note*: Direct entry from Accounts Technician (ATEC) to CPA without college education.
Note**: Respondents with more than on qualifications (i.e CISA and CPA/ACCA).
Note***: 3 Certified Fraud Examiners (CFE) and 2 Certified Risk Information Systems and Control (CRISC).

7.3 The Usage of IS

One of the objectives of the study was to establish the IS usage among external auditors in Tanzania. The study findings reflected that the respondents answered the items of the questionnaire and its sub-sections. The items of the questionnaire included whether or not they used IS, the time they adopted technology, whether IS usage was mandatory or voluntary, the types of IS tools used and finally the benefits resulting from the use of IS tools. The findings in table 7.3 reflected that there was pressure from the management to use IS tool. In other words, IS usage was not voluntary, but only 4.1% (n=4) of the respondents indicated that IS was voluntarily used and this can be supported with evidence that the IS usage among the selected firms could be due to the size and nature of the clients that they audit. These results are consistent with prior scholars (Janvrin, 2008; Appiah and Nketiah, 2014; Naibei et al., 2014) who found that large and medium audit firms make extensive use of IS tools for their audit work. These findings are also consistent with Greenstein-Prosch et al.(2008) and Al-Duwaila and Al-Mutairi, (2017) who found that large audit firms have a big number of clients who can afford to pay the fees consistently for the services rendered. Meanwhile, the mandatory use of IS tools among the respondents could be justified with the need to achieve

efficiency and effectiveness of auditing performance levels (Vasarhelyi, et al., 2010; Widuri et al., 2014).

Table 7.3 IS Usage and Voluntariness

IS usage	Frequency	Percentage	Mandatory	Frequency	Percentage
Yes	106	100%	Yes	102	95.9%
No	0	0%	No	04	4.1%
Total		**106**		**106**	**100%**

In addition, the study further examined the period by which the firms have been implementing the IS. The findings revealed that 77.3% (n=88) of the respondents rated that their firms implemented IS for more than 5 years while 12.3% (n=13) of the respondents did not know the time period at which their firms started using the software and 10.4% (n=11) of respondents indicated the firms were using IS for the period between 2 and 5 years. From these results, it can generally be taken that IS usage has been embraced among audit firms in Tanzania to transform their performance levels as shown in table 7.4. However, in the interest of this study, users of IS should note that adoption of technology without enough qualified staff and training practices cannot yield enough expertise among workers in the usage of technology (Jarvinen, 2012; Alkebsi et al., 2016;).

Table 7.4 Number of Years since Adoption of IS Tool

	Frequency	Percentage
I don't know	13	12.3%
Less than 2 years	0	0%
2 to 5 years	11	10.4%
More than 5 years	82	77.3%
Total	**106**	**100%**

Also, the study examined the type of IS tools (applications and software) used by the audit firms and the results reflected that they employed more of ACL and IDEA as per table 7.5 below. These findings are consistent with prior studies (Curtis and Payne, 2014; Bierstaker et al., 2014; Subaryani et al., 2017) which found ACL and IDEA the most frequent tools used

by external auditors. Yet, other IS tools which the respondents mentioned include EMS, Pro-Audit, AS2, In-house, PCAS and Auto-Audit.

Table 7.5 Types of Software Used by External Auditors

Type of tool used	Frequency	Percentage
ACL	26	22.7%
Active Audit	4	4.1%
Excel	4	4.1%
Excel, ACL**	12	12.4%
Excel, IDEA**	13	13.4%
Excel, In-house**	15	15.5%
IDEA	22	18.8%
Other***	9	19.2%
Total	**106**	**100%**

Note: ** indicates the use of more than one audit tools in the firm.
Other ***EMS, Pro-Audit, AS2, In-house, PCAS, GAM-X Auto-Audit.

Furthermore, the study examined the perception of the respondents on the benefits of using IS. The study used 9 items of the survey tool with a 5-point Likert scale that ranged from 'highly disagree' to 'highly agree'. Interestingly, the findings showed that respondents perceived IS tools as beneficial to all the items whereby the lowest mean was 4.24 'improved responses to risk' and the highest mean was 4.51 'saving time and efforts'. Similarly, the standard deviations showed a low mean difference on all scores, suggesting that the data are dispersed closely around the mean as indicated in Table 7.6. This finding suggested that the external auditors '*highly agree'* that IS usage is important in fostering audit activities. The findings are also in line with Vasarhelyi and Romero (2014) who found that technology integration in audit firms and supports given to users improved the usability of IS and at the same time increased technology adoption.

Table 7.6 Benefits of IS Usage

	N	Min	Max	Mean	Std. Deviation	Variance
BEN1-to reduce errors	106	4	5	4.44	.499	.249
BEN2-reduce manual computations	106	4	5	4.43	.498	.248
BEN3--saving time and efforts	106	4	5	4.51	.502	.252
BEN4-simplified retrieval of clients' data	106	4	5	4.49	.502	.252
BEN5-simplified preparation of working papers	106	4	5	4.52	.502	.252
BEN6-improved data monitoring	106	4	5	4.37	.485	.235
BEN7-enhanced information sharing	106	2	5	4.38	.798	.637
BEN8-easy to identify fraud	106	2	5	4.34	.675	.455
BEN9-Improved responses to risk	106	1	5	4.24	.519	.639
Valid N (listwise)	106					

7.4 Factors Influencing the Usage of IS

This objective used quantitative techniques to validate the proposed model where the UTAUT was adopted to predict the most significant factors using a larger sample size. Since the study established a statistical relationship to occur between dependent and independence variables, it was necessary to check for parametric assumptions to ensure that the data fit the intended analytical procedures. Therefore, the study started with data cleaning and screening tests which are discussed in the next sub-section.

7.4.1 Data Screening

Prior to data analysis the important steps for data cleaning and screening were carried out as per requirements of quantitative study techniques (Odom and Henson, 2002). The survey questionnaires that were not answered from the start to the end were eliminated to avoid missing values in the process of data analysis (Wolf et al., 2013; Desimone et al., 2015). Since the study adopted questionnaires from previous studies, the researcher distributed three hundred questionnaires to arrive at the required big sample of respondents that is required for using statistical techniques for data analysis (Osborne and Costello, 2004; Mundfrom, 2007;

Knofczynski and Siddiqui, 2013; Desimone et al., 2015). However, only 106 of the received questionnaires were adequately completed and considered appropriate for further analysis.

7.4.2 Checking for Parametric Assumptions

Since the study considered using regression technique in predicting a relationship between variables, it was essential to confirm that the received sample size was sufficient as suggested by quantitative researchers (Hair et al., 2010; Wolf et al., 2013). It is suggested that a minimum sample size sufficient for linear regression is dependable on the number of variables and complexity of the model (Wolf et al., 2013). While Hair et al. (2010) suggest a minimum sample size to be measured based on the number of variables per respondents in the ratio of 1:5 but preferably 1:10; a Monte Carlo simulation suggest that any sample size between 30 and 460 is adequate for both first and second order regression (Structural Equation Modelling) (Wolf et al., 2013). However, they further recommend that for a better statistical power, a sample size of 100-250 is adequate for both 1st and 2nd order regression. In any case, this study considered the suggested sample size from O'Brien and Scott (2012) in estimating a minimum sample size for regression. They suggest it to be calculated as (50 + 8m), where m is the number of IVs which in this study is 6. Hence, the minimum required sample size was established to be 98 (i.e 50+8X6), thus, concluding that the 106 questionnaire responses are adequate for regression analysis.

In quantitative studies, checking for outliers and normality of data are also important pre-requisites (Hair et al., 2010; Field, 2013). Outliers can result in increased error term and considerable distortions of parameter and statistical estimates (Ghasemi and Zahediasl, 2012; Pallant, 2007). Hence, this study checked for both univariate and multivariate outliers. Univariate outliers were tested through 'explore' command from descriptive statistics to detect cases with extreme values or abnormal patterns (Pallant, 2007; O'Brien and Scott,

2013). It was observed that no item was an extreme value hence retaining all predictors for further analysis. Similarly, outliers in the form of multivariate were examined through Mahalanobis D2 test and the analysis reflected that the highest score value was 10.319 (Table 7.7). The requirement for using Mahalanobis is that a bigger samples threshold for the value should be higher than 3.5 or even 4 (Balasubramanian et al., 2016; Pallant, 2007). It can therefore be concluded that all the cases surfaced from Mahalanobis values were found with significant scores and unique in combination rather than one single variable (Pallant, 2007; Siddiqui, 2013).

Accordingly, seven transformed variables were tested with α set at 0.01. The degree of freedom in this case was the number used to test and identify the outliers through approximant test of the statistical significance (De Leon and Carrière, 2005; Hair et al., 2010; Balasubramanian et al., 2016;). Similarly, to verify and confirm the attained scores of Mahalanobis D2 test, Cook's distance (Cook, 1977) was employed to identify the possible multivariate outlier. According to the rule of thumb for Cook's degree, values above 1 may cause latent difficulties (Cook, 1977; Tabachnik and Fidell, 2013). In this study, the maximum value for Cook's distance was 0.150, reaffirming that no major multivariate outliers were present (Table 7.7).

Table 7.7 Residue Statistics

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	3.8320	4.9448	4.3899	.29380	106
Std. Predicted Value	-1.899	1.889	.000	1.000	106
Standard Error of Predic. Value	.036	.117	.067	.017	106
Adjusted Predicted Value	3.8165	4.9575	4.3906	.29653	106
Residual	-.68985	1.01921	.00000	.35243	106
Std. Residual	-1.929	2.850	.000	.986	106
Stud. Residual	-1.978	2.947	-.001	1.007	106
Deleted Residual	-.72544	1.08948	-.00064	.36810	106
Stud. Deleted Residual	-2.008	3.066	.003	1.018	106
Mahal. Distance	.087	10.319	2.972	2.054	106
Cook's Distance	.000	.150	.011	.023	106
Centered Leverage Value	.001	.098	.028	.020	106

a. Dependent Variable: BI

Furthermore, Skewness and Kurtosis tests were performed to establish whether the data met the assumptions of normality of distribution. As a rule of thumb, Skewness and Kurtosis tests should be close to plus/minus 2 and 4 (Pallant, 2007; Ary et al., 2010; Field, 2013). The results showed that the minimum value for skewness was -2.149 and the maximum was 2.608 while Kurtosis values were 1.092 and 2.412 for minimum and maximum values respectively. It can be concluded that the data are slightly right skewed but approximately normally distributed and within the acceptable threshhold (see Appendix VI). Furthermore, a Shapiro Wilkis test ($p>.05$) (Shapiro and Wilki, 1965; Razali and Wah, 2011) revealed that the data were approximately normally distributed for all the variables. Shapiro Wilkis which is a statistical measure of normality distribution of data showed alpha values of above .05, which results in acceptance of the null hypothesis on the normality of population sample, suggesting that further parametric analysis can be conducted (Razali and Wah, 2011). The SPSS output results are shown below in Table 7.8.

Table 7.8 Normality Tests

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	**Df**	**Sig.**	**Statistic**	**Df**	**Sig.**
PE	.146	106	.213	.785	106	.702
EE	.270	106	.105	.827	106	.593
SOI	.179	106	.137	.453	106	.212
FC	.241	106	.200	.753	106	.155
CF	.274	106	.415	.855	106	.239
APF	.369	106	.167	.730	106	.703
BI	.368	106	.199	.687	106	.112

a. Lilliefors Significance Correction

7.4.3 Exploratory Factor Analysis (EFA)

EFA was employed to test whether the indicators fit within the identified constructs since some of the factors were adopted and modified from different sources. Specifically, conducting EFA facilitated the reduction of the factors and also confirming the grouping of items with similar characteristics (Pallant, 2007; Kumar et al., 2013). The principal component factor analysis with VARIMAX rotation was employed to evaluate the factor loadings and to identify the underlying influences of the variables. Eigen value and factor loading of > 1.0 and 0.40 respectively were set as benchmarks for inclusion of items in its expected factor (Osborne, 2015; Yong and Pearce, 2013). Items that were uncertain and did not converge to their expected factor or had multiple loadings were eliminated as per the recommendation of using EFA technique (Yong and Pearce, 2013). A total of seven (7) factors were extracted. However, items PE6, EE2 and SOI2 loaded poorly on their intended factors, while CF4 had multiple loadings. Subsequently, the 4 items were dropped and EFA was re-run and the results reflected that there was significant correspondence among the constructs as displayed below in Table 7.9.

Table 7.9 Exploratory Factor Analysis

	1	2	3	4	5	6	7
PE1	.043	-.107	-.020	.122	-.138	**.814**	.005
PE2	-.248	-.091	-.095	-.049	-.153	**.725**	.045
PE3	-.061	.100	-.077	.192	.076	**.718**	.077
PE4	-.019	-.183	-.065	-.006	.013	**.585**	-.149
PE5	-.062	.076	-.043	-.082	.033	**.826**	-.061
EE1	.425	-.168	.152	.250	**.773**	-.051	-.049
EE3	.065	.071	.244	-.087	**.679**	.002	.055
EE4	.336	-.048	.107	.154	**.746**	-.009	-.017
EE5	-.023	-.199	.207	. 025	**. 681**	-.210	.285
SOI1	**.779**	.105	-.022	.218	.210	.013	-.142
SOI3	**.634**	-.122	.529	.199	.331	-.080	.128
SOI4	**.879**	-.091	.212	.019	.165	-.060	.059
SOI5t	**.777**	.137	-.207	-.104	.284	-.018	.065
FC1	.098	.017	.026	.005	-.056	.015	**.843**
FC2	.413	.056	-.129	.005	.139	-.017	**.653**
FC3	.349	.021	-.120	.004	-.099	-.029	**.718**
FC4	.201	-.201	.061	.061	.281	-.052	**.701**
FC5	.274	.009	.134	.056	-.088	-.068	**.874**
CF1	.247	**.806**	.351	.266	.099	-.014	.121
CF2	.118	**.856**	.335	.060	.018	-.037	-.105
CF3	.117	**.806**	.395	.137	.131	-.056	-.078
CF5	.016	**.726**	-.171	-.183	-.321	.066	.335
CF6	-.111	**.787**	-.080	-.182	-.282	.077	-.187
APF1	.041	.092	.108	**.817**	.142	.050	.005
APF2	.022	.034	.156	**.818**	.068	.007	.021
APF3	.090	-.104	.124	**.867**	.011	.046	-.001
BI1	-.101	.070	**.860**	.096	.071	.018	-.261
BI2	.063	.368	**.807**	.218	.282	-.016	.127
BI3	.063	.378	**.809**	.218	.282	-.016	.127

It was also important to re-group the factors in order to ease the observation of their loadings, and subsequently aggregating them as one variable ready for regression. Table 7.10 shows the re-grouped factors according to how the indicators loaded within their specified constructs. The remaining poorly-loaded factors were deleted to avoid confusions.

Table 7.10 Regrouped-Exploratory Factor Analysis

	1	2	3	4	5	6	7
SOI1	.779						
SOI3	.634						
SOI4	.879						
SOI5	.777						
CF1		.806					
CF2		.856					
CF3		.806					
CF5		.726					
CF6		.787					
BI1			.860				
BI2			.807				
BI3			.809				
APF1				.817			
APF2				.818			
APF3				.867			
EE1					.773		
EE3					.679		
EE4					.746		
EE5					.681		
PE1						.814	
PE2						.725	
PE3						.718	
PE4						.585	
PE5						.826	
FC1							.843
FC2							.653
FC3							.718
FC4							.701
FC5							.874

Furthermore, Kaiser-Meyer-Olkin (KMO), a measure of sampling adequacy and Bartlett's Test of Sphericity (BTOS) were performed. The value score for KMO was found to be .727 whereas BTOS Approx. Chi-Square was 3249.305 with a significant value of .000 (Table 7.11). The results reflected that the sampling is deemed adequate for the study as it obtained the standard value of above 0.7 thresholds (Ishiyaku et al., 2016). The significance value of Bartlett's test suggested that at least one of the variances is different from the others (homogeneity of variance), allowing a rejection of a null hypothesis which states that 'all variances are equal' (Pallant, 2007). Equally, the results from the data were in line with the previous researches

conducted since the items used rhymed well with the constructs and exhibited the total variance explained at 77.6% (Appendix VII); hence, not over ruling the previous studies' findings (Ishiyaku et al., 2016).

Table 7.11 KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.727
Bartlett's Test of Sphericity	Approx. Chi-Square	3249.305
	Df	435
	Sig.	.000

7.4.4 Reliability of Measured Scales

Reliability as an essential issue in dimension scale, is defined as the degree to which the scores in a specific sample are free from random measurement error, and is estimated as one minus the percentage of the total observed variance due to random error (Kline, 2011). The most common measure of reliability is internal consistency which is defined as the degree to which items are inter-correlated or measure the same thing (Kline, 2011). The mostly reported measurement of internal consistency is the Cronbach's alpha. Alpha values of above .6 are adequate and they suggest internal consistency of the measurement scale. In contrast, coefficient alpha of less than .6 indicates low internal consistency of the measurement scale (Malhotra, 2009). The Cronbach's alpha was computed and the alpha coefficients of the seven constructs were found to be above the suggested threshold and ranged from 0.749 to 0.939 (Table 7.12). These results suggested that the dimension scales were consistent and further analysis could be carried out.

The study also sought it relevant to run KMO and BTOS for individual constructs to reconfirm the communality loadings and variance explained for each variable. According to Kaiser (1974) as cited in Field (2011), variance explained of .50 for a construct indicates that the data are adequate and further analysis can be carried out. The results revealed that all the

variables had a significant contribution with variance explained of above 50%, KMO values of more than .7 which was well above the suggested threshold and a p-value of .000. The details of the SPSS outputs of the computed variables are shown in Appendices VIIIA-G. Meanwhile, the summarised score values of the KMO, BTOS, p-values and variance explained of individual constructs are included in the reliability table below (Table 7.12).

Table 7.12 Reliability Test

Variable	No. of items	Cronbach Alpha	KMO	BTOS	p-value	%Variance Explained
Performance Expectancy (PE)	4	.750	.782	188.796	.000	59.516
Efforts Expectancy (EE)	5	.749	.729	166.424	.000	53.837
Social Influence (SOI)	5	.842	.799	435.046	.000	73.965
Facilitating Condition (FC)	5	.909	.790	480.941	.000	75.808
Clients Factor (CF)	4	.870	.746	370.534	.000	77.366
Audit Profession Factor (APF)	3	.915	.756	231.442	.000	85.922
Behavioural Intentions (BI)	3	.939	.770	371.361	.000	66.053

KMO =Kaiser-Meyer-Olkin; BTOS = Bartlett's Tests of Sphericity

7.4.5 Multi-Collinearity Test

Multicollinearity is the violation of one of the standard regression assumptions which advocates that the independent variables are not perfectly correlated. If the independent variables are highly correlated, it can affect the estimations of the co-efficient so that they are no longer stable in the unit of their arithmetic significance, magnitude and direction (Tabachnick and Fidell, 2013). As a result, the adjusted R^2 turns out to be excessively high and not statistically significant. In uncovering multi-collinearity, the study conducted statistical checks before running regression. Pearson Product correlation (r) was conducted on all the constructs in order to establish the inter-items relationship among the variables. If the variables show extreme correlations with other variables (i.e. $r > .90$), it is said to have multicollinearity problems (Tabachnick and Fidell, 2013). In other words, the variables are too closely related to each other, which would be difficult to determine the best predictors.

The results showed that the lowest correlation was 2% (r = 0.023) between CF and EE while the highest correlation was 84% (r = 0.838) between SOI and FC (Table 7.13). These results suggest that there was no multi-collinearity among the variables (Tabachnick and Fidell, 2013). Further still, a post diagnostic test was performed after running regression where the Variance Inflation Factor (VIF) was computed as indicated in Table 7.16. The threshold for cases of severe multi-collinearity is indicated by a VIF of 10 and above (Field, 2013; Hair et al., 2010). Consequently, the results indicated that all the items had VIF values of below 10, which meant multi-collinearity problem, did not exist.

Table 7.13 Correlations (r)

		PE	EE	FC	CF	APF	BI	SOI
PE	Pearson (r)	1	.149	.147	.161	.103	.188	.183
	Sig. (2-tailed)		.622	.134	.536	.298	.370	.062
	N	106	106	106	106	106	106	106
EE	Pearson (r)	.149	1	.325**	-.023	.402**	.404**	.523**
	Sig. (2-tailed)	.622		.001	.818	.000	.000	.000
	N	106	106	106	106	106	106	106
FC	Pearson (r)	.147	.325**	1	.082	.108	.070	.838**
	Sig. (2-tailed)	.134	.001		.822	.270	.473	.000
	N	106	106	106	106	106	106	106
CF	Pearson (r)	.161	-.023	.082	1	.188	.571**	.036
	Sig. (2-tailed)	.536	.818	.822		.054	.000	.710
	N	106	106	106	106	106	106	106
APF	Pearson (r)	.103	.402**	.108	.188	1	.327**	.105
	Sig. (2-tailed)	.298	.000	.270	.054		.001	.283
	N	106	106	106	106	106	106	106
BI	Pearson (r)	.188	.404**	.070	.571**	.327**	1	.186
	Sig. (2-tailed)	.370	.000	.473	.000	.001		.056
	N	106	106	106	106	106	106	106
SOI	Pearson (r)	.183	.523**	.838**	.036	.105	.186	1
	Sig. (2-tailed)	.062	.000	.000	.710	.283	.056	
	N	106	106	106	106	106	106	106

**. Correlation is significant at the 0.01 level (2-tailed).

7.4.6 Multiple Regression

To answer RQ2 and the underlining hypothesis, a multiple regression modelling was employed for this particular objective to predict the influence of combined constructs on the theoretical framework. The framework proposed that a relationship existed between the six

IVs (PE, EE, SOI, FC, CF & APF) on the DV (BI to increase the use of IS). Furthermore, hierarchical regressions were performed where ordinal and categorical variables were added to test any incremental influence on the DV as suggested by prior studies. Specifically, six demographic features of respondents were entered into the regression equation separately and changes of R^2 with their significance values were recorded. The SPSS output result of the hierarchical regression is attached in Appendices IXA-F. Meanwhile, the initial regression results are explained in the next sub-sections.

Generally, the regression command on SPSS produces three tables simultaneously, namely (1) the model summary, (2) ANOVA; and (3) beta coefficients. In this case, Tables 7.14, 7.15 and 7.16 are relevant in explaining the outcomes of the regression and in answering RQ2.

Table 7.14 Model Summary[b]

Model	R	R Square	AdjustedR Square	Std. Error of the Estimate	Durbin-Watson
1	.714[a]	.509	.479	.33156	1.514

a. Predictors: (Constant), PE, EE, SOI, FC, CF, APF

b. Dependent Variable: BI

Table 7.14 shows an initial summary of the model with six predictors (PE, EE, SOI, FC, CF and APF) against one DV (BI). The overall regression value (R) is .71 with a standardised error of estimate (SEE) of .33 which is quite below the R value. The most important values of the regression results are the R^2 and adjusted R^2 which explain the value of the model by combining the predictors. It can be seen that the model explains approximately 51% of the DV (BI) adjusted to 47.9%. According to Field (2013), R^2 values between 50% and 70% imply a moderate effect. Likewise, Durbin-Watson statistics, which is an autocorrelation test on the independence of residuals, revealed a value of 1.514. According to Durbin and Watson (1971) as cited in Field (2013), autocorrelation values should be between 0 and 4. Values close to zero imply a positive autocorrelation while values close to 4 suggest a negative

autocorrelation and between 1.5 and 2.5 imply no autocorrelation. In this study, the value of 1.514 suggests that residuals are normally distributed and autocorrelation problem does not exist. The regression results are further explained by the outcomes of 'ANOVA' in Table 7.15 below.

Table 7.15 ANOVA[a]

Model		Sum-of Squares	Df	Mean Square	F	Sig.
1	Regression	11.178	6	1.863	16.95	.000[b]
	Residual	10.773	98	.110		
	Total	21.951	104			

a. Dependent Variable: BI

b. Predictors: (Constant), PE, EE, SOI, FC, CF, APF

Table 7.15 is the second explanation of the regression results reported as ANOVA. ANOVA is used to identify interaction effects between variables, between and within the groups; hence, providing confirmations for further complex propositions (Field, 2013). Specifically, a one-way ANOVA (Table 7.15) was applied to relate the means on the perceptions of respondents regarding factors influencing the usage of IS. The results exhibited the 'explained sum of squares' (ESS) of 11.178 and 10.773 for regression and residuals respectively, making a total sum of squares of 21.951. ESS is a statistical estimate that is used to describe how well a model is after being confirmed by a significant F-value (Field, 2013). Hence, the overall F-test showed that a relationship existed between the IVs and DV, which was statistically significant at .000. A detailed interpretation of the regression results follow in sub-section 7.5.

Meanwhile, the value of each coefficient (beta), the degree of influence and their relationship with the DV is presented in a linear equation as follows:

$$\hat{Y} = \alpha + \beta_1 X_{PE} + \beta_2 X_{EE} + \beta_3 X_{SOI} + \beta_4 X_{FC} + \beta_5 X_{CF} + \beta_6 X_{APF} + \acute{\varepsilon}$$

Where:

$\hat{Y}$ = BI to increase the use of IS
β = Partial regression coefficients
PE = Performance Expectancy,
EE = Efforts Expectancy,
SOI = Social and Organisational Influence,
CF = Clients' Factor,
APF = Audit Professional Factor;
$\acute{\varepsilon}$ = Error term.
α = Constant

The regression equation explains the relationship between the DV and IVs with unstandardised beta values that explain the proportionate increase of 1 unit in each of the IV when other variables are held constant (ceteris paribus). For instance, if ceteris paribus when PE increases by 1, BI (DV) increases by .041. Similarly, a one increase in other remaining predictors leads to an increment in the DV as reflected in table 7.16. The final regression results are presented as:

Y = 2.378 + 0.041 PE + 0.343 EE + 0.0208 SOI +0.094FC + 0.353 CF + 0.035 APF+ ε.

The regression equation is a distinctive summary of the unstandardised beta coefficients that appear in Table 7.16 which reflect the final regression output.

Table 7.16 Coefficients[a]

Model	Unst Coefficients.	Stand Coefficients		Sig.	Collinearity Statistics	
	B		t			
		Error	Beta		Tolerance	VIF
1	(Constant)	2.378	.423	5.628	.000	
	PE	.041	.056	.053	.728	.468	.946	1.057
	EE	.343	.081	.407	4.230	.000	.841	1.189
	FC	.094	.014	.122	.906	.367	.926	1.079
	CF	.353	.046	.561	7.653	.000	.931	1.074
	APF	.035	.009	.072	.876	.383	.746	1.341
	SOI	.028	.017	.036	.238	.812	.776	1.287

a. Dependent Variable: BI

Table 7.16 reveals the six predictors with their beta coefficients, t values, Sig, and collinearity statistics. As a summary, the findings of the table exhibit that (1) all the variables are positively related to the DV (BI); and (2) there are two statistically significant variables.

Again, the detailed meaning and interpretation of each variable in the table is explained in sub-section 7.5.

7.5 Results and Interpretation

7.5.1 The Co-efficient of Determination (R^2) and F- Statistics

The end result of the regression (table 7.14) shows an overall model results (R^2) of approximately 51%, adjusted to 47.9%. Both R^2 and adjusted R^2 are used to define the explanatory power of the model. This end result shows that the identified predictors explained 51% of the variant in the BI to increase the use of IS. The adjusted R^2 is commonly lower than the R^2 as it corrects the inclusion of added variables into the model and which traditionally produces reliable conclusion on the model (Field, 2013). Similarly, the F-test (Table 7.15), which is a statistical model assessment, examined the significance of the overall model and produced results of 16.95 which were significant at 1%. These outcomes show that the model has a representative explanatory power of the relationship between the DV and IVs. It can therefore be concluded that the identified factors are acceptable predictors for BI to increase the use of IS by external auditors in Tanzania. The interpretation and contribution of each individual variable with its size of effect on the DV follow in the next sub-sections.

7.5.2 Performance Expectancy (PE)

PE measures the degree of acceptance that IS can facilitate various audit-related tasks, so as to influence external auditors to increase the use of IS. The results showed a positive sign between PE and BI, even though the relationship was not statistically significant. The regression formed a co-efficient value of .041 and a t-value of 0.728. This result means that an increase in expected performance level in conducting audit tasks may result in an increase in IS usage. In other words, the more auditors expect to improve their productivity levels and

other benefits from using technology, the more likely they will increase the use of IS. Nevertheless, this finding is statistically weak, which means PE construct is not the best predictor of the BI to increase the use of IS by external auditors in Tanzania.

7.5.3 Efforts Expectancy (EE)

The study exhibited a significant positive relationship between EE and BI to increase the use of IS. This finding supports the alternative hypothesis which states that when IS promises its usability with minimum learning curves, the higher is the possibility that auditors would increase its usage. This finding can also be interpreted to mean that external auditors consider learning, understanding and using technological features as the most important factors that can influence their BI to increase IS usage. EE had a co-efficient of 0.343 and a t-value of 4.23, which is much higher than the 1.96 critical region thresholds for a 95% confidence level, producing a p-value of .000. This permits the rejection of a null hypothesis (H0) which states that EE does not influence the usage of IS. This finding is essential as it settles the critical role of perceived usability of audit software surrounding the decisions to increase the use of IS. Comparable findings were documented by Razi and Madani (2013), when examining CAATTs acceptance by auditors in the US. They found that when technological features increase in difficulties, it affected the perceived benefits of using that particular technology. This shows that increasing the system's usability significantly improves the BI to increase its usage.

7.5.4 Social and Organisational Influence (SOI)

H3 tested the relationship between SOI and BI to increase the use of IS. The regression results produced an insignificant positive relationship between the influence of collegiality and management on the usage of IS by external auditors. The co-efficient value was .028 and

a t-test of .238. This finding presented a positive beta symbol which advocates that an increase in the usage of IS could be partly explained by an increase in co-workers' influence and that of the top management. The study was expected to be in line with the findings from the interviews that the audit firms' management encouraged the usage of IS and provided support to their subordinates to use IS. However, this finding was not statistically supported. Curtis and Payne (2014) reported similar results on a positive relationship between SOI and the use of CAATTs in the external audit environment although the results were not significant. In the original UTAUT, the factor was a strong predictor of technology usage but it seemed that when tested in the audit environment it could produce inconsistent results.

7.5.5 Facilitating Condition

H4 measured the relationship between BI to increase the use of IS and the available resources that the firm has to acquire and use IS. The study found that the variable was positive but not significant. The plausible explanation of this finding means that auditors are ready to increase the use of IS when they are well equipped with knowledge of IT through training. The finding could also mean that as audit firms increase training for auditors, the likelihood that the beneficiary of training would find the need to increase usage of IS for audit purposes. This finding also implies that an audit firm's infrastructure has an influence on auditor's usage of technology. However, this variable was not the best predictor of the BI on decisions for auditors to increase the use of IS. The regression result produced an insignificant positive relationship between FC and BI to increase the use of IS, with a co-efficient of .094 and a t-value of .906. This result is similar to that obtained by Wehner and Jessup (2005) and Mahzan and Lymer (2008) who failed to document any significant relationship between FC and technology usage. Likewise, Gonzalez et al. (2012) and Pedrosa et al. (2015) documented similar results.

7.5.6 Clients' Factor (CF)

Another construct used to assign for BI to increase the use of IS was clients' factors (CF). This construct exhibited a significant positive relationship with the BI to increase the use of IS. It formed a co-efficient of .353, which was significant at 1% with a t-statistic of 7.653. This result indicates that the usage of IS was influenced by the nature of the client's business, IT integration, complexity and the audit risk. This could also be interpreted to mean that external auditors are keen to observe their clients' usage of technology in relation to their own application. These findings are consistent with Ahmi and Kent (2013) who found that the usage of GAS by external auditors in the UK was positively influenced by client-related factors.

7.5.7 Audit Professional Factor (APF)

With respect to H6, the study postulated a relationship between BI to increase the use of IS and the aspects of the audit profession. It may be expected that the motivation for BI to use technology may be enhanced by pressure/support of the audit oversight, the available methodology to follow and accountability to the audit stakeholders. However, the outcomes of regression formed a positive relationship between the two constructs, but the relationship was not significant. The co-efficient was .035 with a t-value of .876. The t-statistic falls within the acceptance ratio for the null hypothesis, indicating that we cannot reject the alternative hypothesis which suggests that the BI to increase the use of IS can be influenced by the APF. This end result is similar to the findings from the exploratory study by Widuri et al. (2014) who failed to document the influence of audit authorities with the use of GAS by external auditors in Indonesia.

7.5.8 Hierarchical Regression on Demographic Factors

The literature suggested that the use of technology can be influenced by individual factors, some of which (i.e. age, gender and experience) are contained in the UTAUT. This study conducted hierarchical regressions to find the influence of the individual factors beyond the identified IVs. Six demographic variables were tested namely, age, gender, experience in computerised auditing, professional affiliation, type of auditor and IT skills. When 'gender' was included as an additional factor, the adjusted R^2 increased from 47.1% to 56%, with R^2 change of 8% and the model was significant ($p<0.000$). Unstandardised beta value for gender was .477 and t value of 4.346 which was significant at .000. Surprisingly, other two factors (SOI and FC) also became significant. This finding suggests that gender has a strong positive influence on the BI to increase the use of IS by external auditors. Similarly, 'IT skills' and 'professional certification' produced significant results but with small incremental effects on R^2 change. The remaining factors 'age' and 'auditor type' were not statistically significant. The SPSS output results are summarised in Appendices IXA-F. These end results suggest that the motivation to increase the use of technology can be influenced by the gender of auditors, experience in computerised auditing, IT skills of the users and professional certification. Further research can be conducted by including these variables in the regression equation on a larger sample size to explore more on these reported findings.

7.5.9 Moderating Variable: Voluntariness

The study did not consider relevant to test for any effect of the variable 'Voluntariness' as the majority of respondents (95.9%) mentioned that IS usage was not voluntarily used (see table 7.3). It should be remembered that this study defined IS as any computer software or application that is used by auditors to accomplish various audit-related activities. This definition includes the use of basic IS tools such as Microsoft office in preparation of audit

reports and engagement letters. It is understandable that the usage of these simple office-related applications cannot be left under 'voluntarily used tools' when the NBAA require all audit reports be prepared and stored in electronic copies (R5, R9, R12). Therefore, this study suggests for researchers to test for incremental effect of the variable 'Voluntariness' when a specific audit software such as ACL, IDEA, Pro-Audit, GAMX and so on are considered for use in the external audit environment rather than when they are combined with other simple IS tools.

7.6 Summary of the Chapter

The Chapter has presented the quantitative findings of the study from data that were gathered through a questionnaire. The main purpose of using a large sample was to test the factors for IS usage by external auditors to identify the best predictors so as to compare and contrast with qualitative findings. Similarly, the types of software that auditors used were compared with technologies that were mentioned in the qualitative part of the study. The findings revealed that Efforts Expectancy and Clients' factors were the significant drivers for auditors to increase the use of IS. Furthermore, hierarchical regression showed that gender, experience in computerised auditing, IT skills and professional certification were significant factors that contributed incrementally on the BI for IS usage but with a small increment in R^2 change. The next Chapter is the last Chapter which presents the conclusion, discussion, limitations and recommendations for further research.

CHAPTER 8

DISCUSSION, RECOMMENDATION AND CONCLUSION

8.1 Introduction

This Chapter presents the overall findings from the analysis on the IS usage and its impact on financial audit process and e-fraud detection. The central objective of the study was to explore the extent of IS usage by external auditors in Tanzania by understanding the current state of IS usage, the factors that influenced the usage of IS and its impact on financial audit process and on e-fraud detection. As discussed in the methodology Chapter, this study used qualitative data as the main source of enquiry and quantitative data as a secondary source which was nested on the qualitative method. The study had five (5) objectives as shown in Chapter one that seek to find answers through qualitative enquiry with one objective that aimed to test the adopted UTAUT theory, which was addressed through inferential statistics. Hence, an exploratory methodology was espoused by utilising a pragmatic approach to make the study extra communicative.

Since the study used a concurrent simple mixed method approach, it is essential to discuss the findings in light of any differences that emerged from the two data sources. Therefore, the summarised findings in relation to empirical results of prior scholars and theories, limitations of the study, recommendations and suggestions for further research are presented. Meanwhile, the implication of the study and conclusion are reported from the key outcomes.

8.2 Summary of the Key Findings

This sub-section highlights the key findings of the study to draw attention on the major conclusions in bullets form. Since qualitative approach was the main enquiry tool, no hypothesis was developed; rather, the study advanced five (5) research questions which formed the basis of the study. The five research questions were:

RQ1: What is the extent of IS usage by external auditors in Tanzania?

RQ2: What factors influence the usage of IS by external auditors in Tanzania?

RQ3: How does the usage of IS impact financial audit process?

RQ4: How do external auditors detect e-fraud in computerised business platforms?

RQ5: What is the impact of the IS usage on e-fraud detection?

1. The findings revealed that external auditors in Tanzania use IS tools and techniques ranging from basic office-related applications to audit software. OAT, and AAT were used by all the interviewed respondents while NADTT and ECT/intruders' detection technologies were used by the respondents in the large audit firms. Specifically, ACL was the common AAT used by the majority of the respondents followed by IDEA. Meanwhile, GAM-X, Pro-Audit, Auto-Audit, PCAS, SASoft, AS2, EMS and Teammate were used differently in audit engagements.

2. There was a positive perception regarding the use of IS amongst external auditors, as the use of these tools facilitated various audit tasks. While MS Excel was used in analysing data of less computerised clients, ACL, IDEA and other In-house developed software were used to audit more automated clients such as banks and telecoms due to their large volume of transactions, risky environment and products complexities. Electronic documentation and working papers were the common cited achievements from the use of IS tools.

3. The usage of IS by external auditors was mainly influenced by external factors, namely, the changing clients' environment and the audit professional factors. However, audit professional factors were found to affect the intention for auditors to increase the use of IS in the qualitative part, but when the factor was tested on the survey sample, it was found to be not statistically significant. Further, the hierarchical regression revealed that auditor type, professional affiliation and experience were significant moderators of the identified factors in influencing the BI to use IS by external auditors.

4. Furthermore, the interview results suggested that IS had an impact on the financial audit process. The interview findings revealed that audit firms were steadily converging from manual to IS-based audit processes. Large audit firms, were using software which had in-built audit procedures and guidelines in auditing each class of accounts. Electronic-based documentation systems and preparation of working papers were computerised which enhanced adherence to standards and transparency.

5. The interview findings further revealed that IS had an impact on e-fraud detection. Audit firms had installed ECT/intruders' detection systems. Specifically, ethical hacking tools and techniques were used to perform penetration testing in five (42%) of the interviewed respondents within their audit firms. Through the use of ethical hacking techniques, not only e-fraud was minimised, but the extent of hackers and other unauthorised access to the entity's system was detected. It was reported that through the use of IS tools and techniques, auditors could identify fraud that was not detected in the past. Various transactions fraud was detected such as illegal creation of fake accounts, stealing cash from customers' accounts, IT-related faults, stealing and misuse of passwords, illegal transfers of cash in small denominations from different

customers and mobile banking-sim swap fraud, among others. However, auditors did not use advanced IS tools such as CA or data mining techniques to detect e-fraud as was suggested by prior studies in audit technology.

6. The quantitative findings revealed that the theoretical framework that was proposed which incorporated the elements of UTAUT was valid in predicting BI to use IS by external auditors. The statistical computed R^2 value revealed that the factors predicted 51% of the motivation to use IS, adjusted to 47.8% which was significant at .000.

7. Last but not least, the overall findings revealed that the actual usage of IS tools by external auditors can be aimed to improve the audit process and to detect e-fraud. In other words, the proposed conceptual framework can be improved in future and be used to study adoption and post-adoption outcomes of using CAATTs/GAS in different settings, where improved audit process and e-fraud detection can be incorporated as outcomes.

Table 8.1 Summary of the Key Findings

Objectives	Findings	Comments
To explore the extent of IS usage by external auditors in Tanzania	External auditors used OAT (Office Applications, emails, electronic working papers), AAT (ACL, Teammate, GUMX, Caseware; SASoft), ECT/intruders detection technology (ethical hacking tools) and NADTT (EMS, Teammate, Email; Messengers).	IS tools were used to perform various audit tasks
To examine the factors for the use of IS by external auditors	External factors were more influential (changes in clients' computing environment and the audit oversight factors). Efforts expectancy factors related to the ease to use the audit software was statistically significant in the survey results.	Clients' related factors were the most influential factor in both the QUAL and Quant findings.
To assess the impact of IS on audit process	Audit firms are steadily converging from manual computerised processes to effect the audit life cycle. Documentation and preparation of working papers were computerised, audit planning has changed to include IT experts among the team. Audit testing includes testing of the systems as well as transactions.	New Contribution
How auditors detected e-fraud in computerised platforms	Auditors used ethical hacking tools to conduct penetration testing to detect the possibility of hackers to the clients' systems. ACL and IDEA were also used to detect abnormality and outliers as signals for fraud to have occurred.	New contribution
To assess the impact of IS on e-fraud detection	Various transactions-related frauds were discovered using IS tools and techniques. FSF had reduced as culprits were aware that auditors' detection mechanisms have increased.	New contribution

8.3 Discussion of the Findings

The motivation for conducting this study was the changing nature of the audit clients in embracing technology which has increased complexities, errors, frauds and other irregularities that calls for understanding on how auditors assessed risks in such an environment. Most prior studies in this area explored the usage of IS tools and techniques among internal auditors or in the developed countries, leaving emerging markets especially those in Africa to be unexplored. Furthermore, prior studies reported inconsistent results on factors for IS usage in auditing and also none of the studies validated UTAUT in the external audit environment for developing countries. This study will be the first to explore the use of IS among external auditors in Tanzania. Hence, thirteen (13) external auditors at management level were interviewed. At the same time, 106 questionnaires were received as appropriate for analysis. Through the review of literature, this study proposed a theoretical framework of IS usage which incorporated factors influencing IS usage and the post-adoption impact of IS on the audit process and e-fraud detection. This conceptual framework has not been proposed in any prior studies before this.

The remaining part of this Chapter discusses the outcomes of this study in relation to four aspects as mentioned below:

1. Restatement of the findings as reported in Chapters six (6) and seven (7).
2. Assessments of similarities and differences that arose from the use of qualitative and quantitative data sources.
3. Assessment of the results in relation to past scholars and to identify whether there are any consistent or inconsistent findings.
4. Evaluating the conclusions of this study in relation to its contributions to the present body of knowledge.

8.3.1 The extent of IS Usage by External Auditors in Tanzania

This study used both interviews and questionnaires to explore the extent of IS usage by external auditors in Tanzania. The findings from both the qualitative and quantitative data revealed that external auditors in Tanzania had adopted various IS tools and techniques to perform audit tasks. The type of IS tools used by external auditors were OAT, AAT, NADTT, and ECT/intruders' detection technologies. OAT are the general technologies that are used by auditors to perform office-related tasks to foster work efficiency. Notably, the use of MS Word and Excel were dominant and auditors used them in the preparation of working papers, documentation of audit evidence and report writing. Besides that, audit firms had installed work emails and messengers to ease communication in different engagement locations.

Furthermore, external auditors used AAT for tasks that are specifically related to audit such as computations, data analysis, re-confirming account balances, selection of samples for testing, obtaining evidence or identifying journal entries for testing and identifying unusual patterns in transactions. The interview findings revealed that the most common AAT was ACL, which was used by large firms. Other IS tools such as Teammate, IDEA (or Caseware), EMS, GAM-X, Pro-Audit, Auto-Audit, PCAS, and Excel were also used. The usage of ACL, IDEA, GAMX and other In-house developed software was necessary when auditing banks than in any other clients. This is because banks were considered most risky clients, highly automated with a large volume of transactions. Some audit firms used more than one audit software at the same time.

The reported findings form part of contribution to the literature because no prior study had documented a detailed analysis on the types of tools that were used by external auditors. Most studies reported ACL as the most used tool by external auditors (Curtis and Payne, 2014), while others reported external auditors (especially in small audit firms) were not even aware

of the presence of IS tools (GAS) for audit purposes (Ahmi and Kent, 2013). Similarly, a recent study from a developing country (Indonesia), found that 52% of external audit firms used commercially available IS tools, mainly ACL and IDEA (Widuri et al., 2016). Some internally developed software was also reported to be largely used by Big Four Audit firms. However, none of the studies mentioned the exactly names of additional software.

Consistent to Indonesian context (Widuri et al., 2016), this study found that 50% of the interviewed respondents used ACL while IDEA was the second most used audit software. Additionally, other internal software with their described names and functions were critically discussed (see Chapter 6). Furthermore, ethical hacking tools were used to check the possibility of hackers penetrating the entity's system, which the study finds to be a new practice in the external auditing context. In reporting the usage of ethical hacking techniques and the perceived importance in signalling e-fraud occurrence, it remains as the main contribution to the literature.

However, the use of varied IS tools by external auditors in Tanzania is contrary to some prior studies. For example, Ahmi and Kent (2013) found that 73% of external auditors in the UK did not make use of GAS. This difference is partly attributable to the nature of the surveyed firms by Ahmi and Kent (2013), which comprised mostly of auditors from small audit firms. The literature suggests that small firms mostly audit small clients whose integration of technology into their process is limited as compared to large clients. Another reason for the difference could be the selected case study of respondents for this study, who were mainly those that audited banks and financial institutions. It is understandable that the use of IS tools and techniques when auditing these type of clients is necessary.

8.3.2 Factors Influencing the Use of IS by External Auditors in Tanzania

This objective intended to derive the perception of auditors regarding the use of IS to establish whether it was due to the changing nature of technology among their clients or due to individual, organisational or other factors. Since this objective used interview and survey data, the study found some differences from qualitative and quantitative results. The qualitative findings revealed that IS usage by external auditors was mostly influenced by external factors that were related to the nature of the auditees' environment and the audit professional factors which were rated as 'highly influential' factors. These findings suggest that external auditors are aware of the possible risks that can happen on their clients' environment due to the increase use of technology. Likewise, the interview findings revealed that the NBAA was on a front line to speed up the adoption and usage of IS tools in auditing by ensuring that auditors comply with the requirements of ISAs such as documentation, transparency, stamping and audit effectiveness.

Interestingly, the NBAA had even recommended audit software (PCAS) to be used by local audit firms-those that could not afford the cost of installing audit software. The NBAA looked for an affordable software vendor and made agreements to supply the software to those audit firms and made its usage mandatory for local audit firms that had no proper methodical ways of documenting their audit evidence. The software has in-built procedures embedded in it to ensure adherence to the standards and best practices in auditing. These findings are contrary to Widuri et al. (2014), who found that a low usage of GAS in Indonesian audit firms was due to low support from the audit oversight bodies. The findings are also contrary to Curtis and Payne (2014) who found that the low usage of CAATTs was due to reluctance and voluntariness allowable by the audit oversight bodies.

The plausible explanation for some differed findings between Tanzania and other countries could be due to institutional pressures. It was mentioned in the interviews that the NBAA had put stringent measures for audit firms in Tanzania to adhere to the requirements of ISAs and the easiest way to comply is through the use technology. For instance, the Report on Observance of Standards and Codes which supervises accounting standards for most of the World Bank member states highlighted various weaknesses in audit practices in Tanzania and one of the main issues was "*audit firms in Tanzania were detaching from using technology*" (Worldbank, 2005 pp.11). The report further urged the NBAA to assume its full responsibility and to be strict on its supervisory role. These factors could partly explain why the external audit environment in Tanzania has moved forward in adoption of IS as compared to other developing countries partly to comply with the World Bank's requirements.

Meanwhile, other external factors were related to the nature of clients' complexity which motivated auditors to use IS tools. The use of the tools could ease the work of re-computations and data analysis to the clients with large volumes of transactions. Especially when auditing banks and other financial institutions, insurance companies and telecom companies, it was found to be impossible to audit without using IS tools and techniques. Other factors include attaining high levels of efficiency and effectiveness on the side of the audit firm, accountability, to ease the audit tasks such as communications and to increase the level of assurance on the audit report. Furthermore, IS auditors and IT experts considered the use of IS as part and parcel of their daily activities; hence, creating a new variable *'relevance to task'*. Other reasons include easing supervision and fostering compliance and adherence to ISA.

Prior studies found a relationship between technology usage and individual characteristics of users. However, through qualitative data collected in this study it could not establish the differences between the usage of IS tools among external auditors with the personal

characteristics such as gender, age, experience, education, or professional affiliation. Nonetheless, it was observed that respondents who had experience in computerised audit and those who were IT experts showed more confidence when clarifying the usage of IS tools and techniques as compared to non-IT experts. These findings were confirmed when the respondent (a partner) invited a fellow partner who was an IT expert in firm L into the conversation to respond to technical questions related to IT usage, especially with regards to e-fraud and the use of audit tools and techniques. Due to a small number of interviewed respondents, the study could not establish the link between age and the usage of IS in auditing. The same applied to gender and experience in auditing which are important moderators in the UTAUT.

Meanwhile, the quantitative findings proposed six factors as predictors for IS usage by external auditors. These factors were Performance Expectancy, Efforts Expectancy, Social and Organisational Influence, Facilitating Condition, Clients' factor and the audit profession factor. The findings revealed that the six identified factors were significant predictors of the BI for auditors to increase the use of IS. This was supported by the value of adjusted R^2 which showed that the predictors explained 47.9 % of the variance with F-value (16.94), which was significant at (.000). These factors are discussed in details in the next sub-headings.

(i) Statistically Significant Factors: Clients' Factor and Efforts Expectancy

The findings revealed that clients' factor and efforts expectancy were the significant predictors that motivated external auditors to increase the use of IS. In other words, auditors would increase the intentions to use IS if the clients' environment becomes more automated and complex with perceived large audit risk. These findings are consistent with those observed by prior scholars (Bierstaker et al., 2001; Vendrzyk and Bagranoff, 2003; Hunton et

al., 2004; Kotb and Roberts, 2011; Ahmi and Kent, 2013), who found that as clients' level of automation increases (in adopting e-business) external auditors would shift from manual-based to technology-based audit techniques.

The findings further showed that auditors perceived EE (the ease to use software), as a significant condition to influence the behaviour to use IS. This implies that external auditors would be motivated to increase the use of IS when it promises ease of use with low learning curves. This finding is consistent with Razi and Madani (2013) who found that when technology features increased, it affected negatively the 'PEOU' variable which eventually affected negatively the perceived benefits of using the system. This finding could further suggest that audit software should promise its usability, flexibility, and easy to learn, which is similar to the findings from other scholars (Kim et al., 2009; Diaz and Loraaz, 2010; Gonzalez et al., 2012). These scholars found that efforts expectancy was among the strongest significant predictors for auditors to use CAATTs. It was found that when the tools were easy to learn, it affected other factors such as perceived benefits, social influence and facilitating condition. The managerial implication of these findings suggest that software vendors should design software which suits the specific needs of the audit so as to speed IS adoption, acceptance and usage.

(ii) Inconsistent Findings between Qualitative and Quantitative Data

The study findings revealed some inconsistent outcomes between qualitative and quantitative data with respect to PE, FC, and APF. PE is the perceived benefits that are acknowledged by individuals from using innovation (Venkatesh et al., 2003). The interview findings revealed that IS usage was mostly appreciated when auditing banks and complex clients with multiple products while simple technological tools were used when auditing less computerised clients. Out of nine (9) items of the construct 'perceived benefits', two were rated as 'highly

influential' while seven (7) were rated as 'somewhat influential' (see table 6.2). In contrast, the variable PE was not statistically the best predictor for IS usage by external auditors in Tanzania. These combined qualitative and quantitative findings suggest that majority of external auditors in Tanzania still prefer to use manual techniques during auditing. The usage of simple accounting software by most of their clients (except banks), as reported in the interview data, might justify the preferences of using manual techniques in auditing. This can be confirmed by one of the items in the factors *'audit using IS fits well with the way I want to do my work'* which was rated the lowest and hence, loaded poorly in EFA. As a result, it was removed from further analysis.

Another plausible explanation for the inconsistent findings is that within the majority of auditors, there is some level of resistance to change, which means most respondents still believe in traditional manual techniques irrespective of their having the required knowledge and training in IT. These findings are consistent with those observed by Curtis and Payne (2014:104), who reported some of the auditors saying *'never will I use audit tools during auditing'*, due to their trust in auditing using manual techniques. This finding could further suggest that if audit management did not make it mandatory to use IS, most likely, many auditors would still prefer using traditional manual techniques to accomplish audit tasks.

Likewise, the factor 'FC' was found not to be statistically significant. This is due to a mixture of respondents who came from large as well as medium audit firms. The capacity of technology usage and general resource capabilities between the two can differ significantly and causing inconsistent results.

Similarly, the APF was found positive but not significant, which means the use of IS tools by external auditors was influenced by audit professional factors but the factor was not the best predictor. ISAs suggest for auditors to use IS tools and techniques when auditing complex

clients and in a situation where manual judgement cannot guarantee effective audit assurance. Nevertheless, the use of IS tools is still voluntary and is left under the decision of individual auditors. The differed results between qualitative and quantitative findings regarding the construct APF means that the influence of the oversight body (i.e. the NBAA) was more felt at the management level for compliance purposes and not to individual auditors who filled in the survey. These findings are consistent to prior studies (Widuri et al., 2016) who found that GAS usage in Indonesia was partly influenced by audit professional factors.

(iii) Demographic Factors: Ordinal and Categorical Variables

The study ran several hierarchical regressions to test the moderating effect of gender, age, experience in computerised auditing, IT skills, type of auditor, and professional affiliation on the 'factors for the use of IS'. The study found that gender, experience in computerised auditing, IT skills and professional affiliation were significant predictors beyond the identified factors. However, the effect size was small with change in R^2 ranging between .03 and .08.

8.3.3 The Impact of IS on Financial Audit Process

The qualitative findings revealed that external auditors used IS tools and techniques in the audit process. The audit process composes of five main procedures which are planning, execution, gathering evidence, testing and reporting the audit findings to stakeholders. The interview findings revealed that external auditors planned the audit differently when auditing a manual client, computerised client or complex clients such as banks and telecoms. It was found that when auditing manual clients, the audit team composed of only financial auditors who would test manual documents and report the findings. However, when auditing computerised clients, one or two IS auditors or IT experts were included as part of the audit

team. On the contrary, when auditing complex clients, the audit team was composed of more IT experts and the use of IS tools and techniques during the audit process was dependable on the level of computerisation of the audit client. The use of IS tools during the audit process was perceived more important when auditing banks and telecoms due to the volume of transactions and complexity of their products as compared to other clients. It was reported that the complexity in banks becomes intense when their products are embedded with telecom services in offering mobile banking transactions which commanded auditors to increase the use of IS tools.

8.3.4 The Impact of IS on E-fraud Detection

This study had an aim to understand how auditors detected e-fraud in e-business platforms, and the impact of IS on e-fraud detection. The qualitative findings found that external auditors relied mostly on penetration testing to detect the possibilities of intruders hacking the clients' systems especially when they audited bank clients. Penetration testing was conducted using IS tools and techniques known as ethical hacking tools. Apart from using ethical hacking tools to conduct penetration testing, external auditors used techniques recommended by the ISAs which require them to understand the client's computerised platform and to assess the integration of IT into the business processes. As such, the audit was planned accordingly to establish whether/when to use IS tools and techniques for a particular audit assignment. Besides that, in the case of suspicious grounds on the presence of e-fraud risk, the partner would consider reviewing the audit team, increasing the sample size and/or inclusion of fraud examiners among the team. Besides that, strengthening of internal control systems of the entity was considered as both a preventive and detective measure to e-fraud. Furthermore, respondents reported taking a risk-based audit approach at all times when auditing complex computerised clients. Furthermore, auditors practised constant scepticism

in the audit process, asking questions to management, verifying documents, signatures and authorisations.

In contrast, the interview findings further revealed that external auditors did not use CA methodologies. Largely, CA was regarded as expensive to use because it involves real time monitoring of the entity's data (Omoteso et al., 2010). It was reported that the nature of businesses (audit clients) in Tanzania may not afford the audit costs attached to CA. Furthermore, it was deemed not necessary to replace the current audit methodologies in favour of CA because auditors perceived the nature of reported e-fraud in Tanzania as low compared to other neighbouring countries. Hence, the e-fraud which is currently reported could be sufficiently addressed without replacing the available audit mechanisms and tools (R9, R10, R11 and R12a).

Furthermore, it was found that auditors managed to detect systems-related frauds such as the weaknesses of the electronic controls, the creation of fake accounts to steal cash from the entity, internal hacking of customers' accounts by IT experts, some of which were in collaboration with top management, and money laundering. The use of ethical hacking tools and techniques created a positive impact by reducing the number of e-frauds committed because auditors could provide recommendations on the systems' faults and vulnerability which helped clients to update their systems. Furthermore, the use of IS and techniques deterred new fraud from occurring and also reduced FSF because the culprits became aware that auditors were equipped with new audit tools and techniques that would discover any attempts to fraud the entity.

8.4 Limitations of the Study

This study utilised a simple mixed method approach which was conducted on a concurrent mode. A concurrent mixed method means that both qualitative and quantitative data were collected at the same time period. This approach has limitations to the findings because the best approach would be to adopt a longitudinal approach to a mixed method which would produce more robust findings for the reason that technology is dynamic. Similarly, the study used purposive sampling to select respondents for interviews. The lack of random selection of respondents may have limited the chances of other auditors to participate, which can be claimed to create bias in the findings.

Aside from purposive sampling, a case study approach that looked at e-fraud in mobile banking platforms to understand the move of IS usage amongst external auditors was also conducted. The study falls short by not considering other online related frauds which could be happening in other sectors. Therefore, the findings of this study in relation to e-fraud detection are mostly applicable to external auditors' use of tools and techniques to audit bank clients and other financial institutions in Tanzania.

Last but not least, a qualitative study of purposive selection of 13 respondents from only one city (Dar es Salaam), excluded external auditors from other regions in Tanzania. This could have limited the study from generalising the findings. A stratified sample selection of respondents would produce results that are unbiased of this limitation. Furthermore, the 106 quantitative findings could be perceived by most positivists' researchers as a too small a sample for generalisation. However, it should be noted that, as of 31 December 2017, the NBAA had a membership of only 2,038 fully certified accountants including those who hold certificates to perform audits (NBAA, 2017). Meanwhile, in 2015, there were only 553 registered active auditors in public practice from which the sample size of this study was

based on. This shows that the accounting profession in Tanzania is still very small and hence it was extremely difficult to access them in the process of data collection.

8.5 Recommendations for Future Research

This study explored the extent of IS usage in general from low application such as Office applications to advanced audit software. It may be difficult to generalise factors for the usage of a simple audit tool and factors for the usage of advanced systems. Future studies could explore factors for the usage of IS according to their functions such as OAT, AAT, or NADTT rather than combining them as audit tools in one group.

Furthermore, this study targeted auditors who audited banks and financial institutions which also happened to be from the large and medium audit firms. Future studies can target auditors from small audit firms because they are the majority in Tanzania as compared to large and medium audit firms. Besides that, small audit firms combined have employed more people as compared to large and medium audit firms and also they audit many small and even medium clients. It would be interesting to explore how auditors in small audit firms in Tanzania are advancing to embrace technology and their perception on technology usage.

Further, this study was conducted on external auditors to reflect on their usage of IS tools to audit their automated clients. Future studies might include internal auditors within the banking sectors and other large businesses registered on DSE in order to understand the types of tools and techniques used in the audit process including their IT competence levels. Likewise, the government of Tanzania has automated its accounting procedures since the year 2013. It could be relevant to study the level of IS usage by government auditors in various departments and to understand the challenges encountered by the CAG and its audit teams.

Furthermore, this study was based on the perception of external auditors regarding the impact of IS usage on e-fraud detection by focussing mostly on transaction frauds instead of FSF. Future studies can use the secondary data of registered companies in DSE to see how FSF has decreased over time before and after integration of IS into audit methodologies. For example, pre-IT adoption versus post IT adoption to determine a statistically difference in the overall frauds decrease which will produce a better assessments of fraud reduction rather than by relying only on experiences from the respondents.

Likewise, future studies could seek a better understanding on the impact of IS usage by external auditors on the audit quality from the stakeholders' perspective. Studies could be conducted by interviewing shareholders and other stock market participants. There is pragmatic evidence regarding audit quality and the use of technology in the audit process since auditors still use manual techniques to accomplish audit tasks. Therefore, by interviewing shareholders, a new understanding of the issue can be assessed rather than basing on auditors' self-evaluation, which this study focussed on.

Last but not least, external auditors (especially partners) expressed the need for universities to include IT into undergraduate curriculum in order to reduce the costs of training auditors as well as to simplify the understanding of audit software and the clients' computing platforms. Thus, future studies can explore the perception of accounting academics in Tanzania on their readiness to include IT and e-business into the accounting curriculum. Similarly, studies can also assess the extent of IT inclusion in the national accounting professional curriculum in Tanzania and in other countries.

8.6 Conclusion

This study explored the extent of IS adoption by external auditors in Tanzania following the increased e-business complexity among their clients where e-fraud was reported to be on the

rise. The study considered a case study of banks which are also the main audit clients and large contributors to GDP, to assess the usage of IS amongst external auditors when assessing risks in such an environment. Overall, the findings suggest that external auditors in Tanzania were using various IS tools when conducting audit tasks, ranging from low to high level of IS tools. Notably, auditors used ACL, IDEA, Teammate and EMS, GAMX, Pro-Audit, SASoft, AS2, MS Excel and other In-house software. The degree of IS usage was dependable on the nature of the clients they audited, the volume of the transactions of the clients' data, the complexity of the clients' technology and the perceived audit risk component.

The intention to increase the usage of IS tools among external auditors was statistically influenced by clients' factors and efforts expectancy. Although the qualitative findings suggested a strong influence from the audit oversight body (NBAA) for auditors to use IS tools, the quantitative results did not show a significant relationship with audit professional factors, which imply that the NBAA influence to use IS was more felt at the management level for compliance purposes and not to individual auditors who filled in the survey. The motivating factors for auditors to use IS tools from both qualitative and quantitative findings were found to mostly come from clients' factors, which included the level of audit risk component, business and IT complexity of their clients. Interestingly, some of the respondents mentioned that their audit firms had fully computerised their audit procedures and had adopted a paperless audit approach. Most of these audit firms were large international affiliated firms where the audit life cycle was embedded within the audit software. Meanwhile, other respondents stated that their audit firms had partly computerised their audit procedures involving at least documentation and electronic working papers.

The study did not find evidence in relation to the usage of advanced IS tools such as data mining, CA or forensic audits to identify e-fraud. Auditors perceived the level of e-fraud occurrences in Tanzania as 'less risky' compared to other neighboring countries. As a result,

they perceived the use of advanced tools such as CA as unnecessary for that environment. Besides that, the cost implication attached to CA methodologies may not be affordable by most clients in Tanzania. Irrespective of not using CA or forensic audit techniques, auditors used ethical hacking tools as intruders' detection mechanism to test for possibilities of unauthorised access to the clients' systems and to identify weaknesses in the systems.

To sum up, the extent of usage of IS amongst external auditors in Tanzania was examined and the factors motivating the use of IS were explored and statistically tested. It was found that auditors perceived the use of IS as important but the usage differed according to the needs of their clients. The study found that the most common IS technologies are OAT and AAT, while networking data transfer (NADTT) was used by large audit firms. External factors to technology usage had a strong impact, namely, the changing clients' e-business environment and oversight body, particularly the NBAA. The NBAA recommended some of the audit technologies for adoption such as PCAS software.

It was also noted from the interviewed auditors that technology usage was perceived as vital even under resources constraints and other challenges such as power shortages. All auditors were found to have a positive perception on technology usage with anticipation that their firms would increase IS usage in future. However, the study observed a difference in the use and understanding of audit technologies between financial auditors and IS auditors, suggesting a need for a careful organisational structure in order to maintain a balanced human resources capabilities to ensure quality audit is achieved.

In conclusion, this study finds evidence which suggest that external auditors in Tanzania are aware of the increased risk in computing business platforms. The fact that clients' factor was the most motivating factor for IS usage for both qualitative and quantitative findings; and the increased enrolment in the ISACA-Tanzania local Chapter, suggest that auditors are keen to

learn new technology so as to improve the audit performance levels. Furthermore, the use of ethical hacking tools and techniques suggest a step forward in detecting e-fraud and to ensure that the clients' IT platform is safe.

8.7 Contribution of the Study

This study exhibited theoretical aspects related to the usage of IS in the external audit environment and filling the gap in the literature by adding two constructs: the audit process and e-fraud detection that has been lacking. Thus, theoretically, the study extends the literature on the extent of use of IS by external auditors in a developing country's context (Tanzania) where the study was conducted for the first time by integrating factors for IS usage and post adoption impacts on the audit process and e-fraud detection. The findings can foster similar studies to other developing countries where e-business is gaining momentum. Furthermore, the study contributes to the theory of acceptance and use of technology (UTAUT) by including two new variables (clients' factor and the audit professional factor) which are relevant to the external audit environment. The modified model could be useful in conducting studies in other developing countries by including large sample sizes of auditors so as to yield better results.

Even though research on technology adoption, acceptance and usage in external auditing is still scarce, there are few studies that have been carried out. Most of them examined determinants for CAATTs/GAS adoption and usage or challenges involved in the adoption process (Janvrin et al., 2009; Ahmi and Kent, 2013; Curtis and Payne, 2014; Pedrosa et al., 2015; El-Sood et al., 2015; Widuri et al., 2016). However, none of them was able to integrate the post-adoption aspects of IS usage on the audit process and on e-fraud detection. Therefore, by integrating these two variables into the theoretical model of this study, it exhibits valuable contributions to the literature.

Specifically, the study delivers a highlight on the extent of usage of IS by external auditors in a developing country's perspective (Tanzania), where there was no similar study conducted in this particular setting of respondents (external auditors). Prior studies were conducted in developed countries such as UK, US, Germany, Portugal, Singapore and very recently, Middle East, Asia and three African countries (Egypt, Nigeria and Botswana). Hence, the findings of this study can contribute to the literature on Sub-Saharan African countries which is still unexplored.

Similarly, the study makes contributions in terms of the types of IS tools that are used by external auditors in other countries by comparing and contrasting with those that are used by auditors in Tanzania. For instance, the study has found new software and audit programmes that were used such as GAMX, AS2, teammate, EMS and ethical hacking tools and techniques which were not clarified by other researchers in audit technology. Furthermore, the study has proposed a conceptual framework that integrates aspects of UTAUT with external factors which can be used to study technology adoption by both external and internal auditors. There has not been any study that had come up with that model, hence these are also valuable contributions of this study.

Additionally, the study reasoned that technology usage in auditing should be tailored to have an impact on the audit process and e-fraud detection. Consequently, these items were incorporated into the conceptual framework where future studies can modify it to study IS usage in another setting. Besides that, the study has contributed to the audit literature by highlighting the types of e-fraud that can be a source of material misstatements in FSs, in addition to highlighting computer-based mechanisms to detect online frauds. Even if the study did not find evidence of usage of advanced tools and techniques in fraud detection such as data mining or CA, the available tools can be used by external auditors to reflect their own

usage and appreciate various advanced technologies that are available for auditing computerised clients and also for e-fraud detection.

Practically, the study postulates information to audit stakeholders such as the shareholders and the accounting oversight body. The study informs shareholders that there are available tools which auditors can use effectively to audit their financial information and to provide better audit services. Since 50% of the interviewed respondents mentioned that their audit firms had already invested in audit technologies aiming to improve audit testing, the audit firms can only recover their IT investments positively when the software is being used. Furthermore, the audit oversight body (NBAA) can use this study to gauge the extent of usage of IS among external auditors in Tanzania and to establish a re-evaluation of adherence to standards and best practices.

Likewise, the accounting academics can use this study to design curriculum at undergraduate level. It is important to recall that some respondents, especially owners of audit firms (partners), were dissatisfied by the quality of accounting graduates in Tanzanian universities as they are perceived as lacking important components of IT knowledge. Yet, businesses in Tanzania were advancing into computerised processes and storage of accounting information. Hence, the accounting academics in Tanzanian institutions can use this study to incorporate some elements of IT and e-business risks into the syllabus so as to prepare future accountants/auditors to have competence in auditing computerised clients. Besides that, it was revealed from the interviews that auditors who had sufficient knowledge of both IT and accounting, provided valuable contributions to the audit process. As a result, audit firms were ready to reward them higher remunerations.

REFERENCES

Abu-Musa, A. A., (2008), Information technology and its implications for internal auditing: An empirical study of Saudi organisations, *Managerial Auditing Journal*, Vol. 23 (5) pp. 438-466.

ACCA (2012), Assessing the risk of material misstatement ACCA Paper Series 01 March 2012. Available online at http://www.accaglobal.com/gb/en/member/discover/cpd-articles/audit-assurance/material-misstatement.htm. [Accessed on 20/08/2016].

ACFE (2006), Association of Certified Fraud Examiners (ACFE) Report to the nation on occupational fraud and abuse: Technical report, Texas. Association of Certified Fraud Examiners.

AFE, (2006), Report to the Nation on Occupational Fraud and Abuse, Technical Report, Association of Certified Fraud Examiners, Texas.

Ahed. L., and Lous. S. (2008), Information Systems and Performance: an analytical approach to understand IS value in business organisations. *Journal of Information Technology and Management*, Vol. 5, pp 9-22.

Ahmi, A. Saidin S.Z., and Abdullah, A. (2014), IT Adoption by Internal Auditors in Public Sector: A Conceptual Study, *Procedia-Social and Behavioural Sciences* Vol.164, pp 591-599

Ahmi, A., and Kent, S. (2013), The utilisation of generalized audit software (GAS) by external auditors, Managerial Auditing Journal, Vol. 28 (2), pp. 88 – 113.

AICPA, (2001), American Institute of Certified Public Accountants the Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit. *Statement of Auditing Standards* No. 94. New York.

AICPA, (2002), American Institute of Certified Public Accountants Statement on Auditing Standards (SAS) No.99: (superseded SAS 82) Consideration of Fraud in a Financial Statement Audit. New York: AICPA.

AICPA, (2006), American Institute of Certified Public Accountants Consideration of fraud in a financial statement audit, Responses involving the nature, timing, and extent of procedures to be performed to address the identified risk. AU-C Section 240; SAS No. 122; SAS No. 128, New York: AICPA.

Ajinkya, A. F., Kashikar, A. G., and Zunzunwala, A. (2010), Ethical Hacking ,*International journal of Computer Applications,* Vol. (10), pp. 14-20.

Ajzen I. (1991), The theory of planned behaviour. *Organisational Behaviour and Human Decision Processes,* Vol. 50, pp. 79-211

Al Omari, L., Barnes, P., and Pitman, G. (2013), A Delphi Study into the Audit Challenges of IT Governance in the Australian Public Sector. *Electronic Journal of Computer Science and Information Technology'*, Vol. 4 (1).

Al_Khasawneh, A., and Mohammad, S. B. (2014), An improved side view face authentication using wavelets and neural networks. *International Journal of Engineering Sciences and Management Research*, 1(5), 24–31.

Alam, S. H. (2009), Adoption of internet in Malaysian SMEs*, Journal of Small Business and Enterprise Development,* Vol. 16 (2), pp. 240-255. Al-Duwaila, N., and Al-Mutairi, A.

(2017), The Opinion of Auditors towards the Importance and Knowledge of Information Technology in Kuwait. *International Journal of Business and Management*, Vol.12(3), pp.170-182.

Alanezi, F., and Brooks, L. (2014) Combatting Online Fraud in Saudi Arabia Using General Deterrence Theory (GDT), Twentieth Americas Conference on Information Systems, Savannah, 2014.

Alexander, D. Britton, A., and Jorissen, A. (2011) International Financial Reporting and Analysis, Cengage Learning, Walworth, UK.

Al-Fehaid, M. (2003), An investigation of the influence of information technology on audit risk: an empirical study in Saudi Arabia, Un-published Doctoral Thesis Submitted in partial fulfilment of the requirements for the award of Doctor of Philosophy of Loughborough University.

Ali-Akbar, F., Abbaspour, A., and Ghassemi, R. A. (2013), The Effect of Information Technology on Organisational Structure and Firm Performance: An Analysis of Consultant Engineers Firms (CEF) in Iran, *Procedia - Social and Behavioral Sciences,* Vol. 81, pp. 644 – 649

Aliyu, A. A., and Tasmin, R. (2012), The Impact of Information and Communication Technology on Banks‟ Performance and Customer Service Delivery in the Banking Industry, International Journal of Latest Trends in Finance & Economic Sciences, Vol.2(1), pp. 80-91.

Alkebsi, M., Aziz, K. A., Mohammed, Z. M., and Dhaifallah, B. (2016), The Relationship Between Information Technology Usage , Top Management Suppport And Internal Audit Effectiveness, *International Management Accounting Conference.* (pp. 321–336).

Alles, M., Gerard, B., Kogan, A., and Vasarhelyi, M. (2006), Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens, *International Journal of Accounting Information Systems* Vol. 7, pp 137-161.

Alles, M.G., Kogan, A., and Vasarhelyi, M. A., (2004), Restoring auditor credibility: tertiary monitoring and logging of continuous assurance systems, *International Journal of Accounting Information Systems* Vol.5 pp. 183– 202.

Alles, M.G., Kogan, A., and Vasarhelyi, M. A., (2008), Putting Continuous Auditing Theory into Practice: Lessons from Two Pilot Implementations, *Journal of Information Systems* Vol. 22, (2), pp.123-136.

Alleyne, P., and Howard, M. (2005), Exploratory Study of Auditors' Responsibility for Fraud Detection in Barbados, *Managerial Auditing Journal,* Vol. 20 (3), pp. 284-303.

Amirinia, H., Kazemi, A., and Darvish, Z. A. (2015), Data Mining and Knowledge Extraction in the Risk Based Insurance Audit: A Case Study, *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 4 (8), pp.425-430.

APB, (2006), Auditing Practices Board. International Standard on Auditing (UK and Ireland) 240: The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements, Auditing Practices Board; London.

APB, (2010) Scope of an Audit of Financial Statements of Private Sector Entities arising from the requirement of ISAs (UK and Ireland). Retrieved April 4, 2016, from http://www.frc.org.uk/apb/scope/private.cfm

Appiah, K. O., and Nketiah, S. (2014), Computerised Accounting Information Systems : Lessons in State-Owned Enterprise in Developing Economies. Fianance and Management in Public Services, 12(1). Retrieved from koapiah.ksb@knust.edu.gh.

Ary, D., Jacobs, L. C., and Sorensen, C. (2010), Introduction to Research in Education (8th ed.). Wadsworth, Cengage Learning.

Bagozzi, R.P. (2007), The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. Journal of the Association for Information Systems, 8 (4), pp.244–254.

Bagranoff, A. N., Simkin, M.G., and Norman, C.S. (2007), Accounting Information Systems, 10th Edition, John Willey and Sons Ltd, LA.

Bagranoff, N. A., and Vendrzyk, V. P. (2000), The Changing Role of IS Audit Among The Big Five US-Based, *Accounting Firms. Information Systems Control Journal*, Vol.5, pp. 33–37.

Balasubramanian, V., Nagarajan, S. G., and Veerappagoundar, P. (2016), Mahalanobis distance-the ultimate measure for sentiment analysis. *International Journal of Information Technology*, Vol. 13 (2), pp. 252–257.

Banker R. D; Chang H., and Kao, Y. (2002), Impact of Information Technology on Public Accounting Firm Productivity *Journal of Information Systems* Vol. 16 (2), pp. 209-222).

Bardhan, R. I., and Thouin, M. F. (2013) Health information technology and its impact on the quality and cost of healthcare delivery, *Decision Support Systems,* Vol. 55(2), pp. 438-449.

Barua, A. C. Kriebel., and Mukhopadhyay, T. (1995), Information technologies and business value: An analytic and empirical investigation, Information Systems Research 6 (1), pp. 3-23.

Bazeley, P., and Jackson. K. (2013), Qualitative Data Analysis with NVivo Second Edition. Research Support Pty Limited, Australia, Query, Inc., Colorado and University of Colorado.

Berwick, D.M. (2003), Disseminate Innovations in Health Care, *Journal of the American Medical Association,* Vol. 289 (15), pp. 1969–1975.

Bharadwaj, A. S. (2000), A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation, *MIS Quarterly* Vol 24 (1), pp 169-196.

Bierstaker, J. P., Burnaby, P., and Thibodeau, J. (2001), The Impact of Information Technology on the Audit Process: An Assessment of the State of the Art and Implications for the Future, *Managerial Auditing Journal*, Vol. 16 (3), pp 159-164.

Bierstaker, J., Janvrin, D., and Lowe, D. J. (2014), What factors influence auditors' use of computer-assisted audit techniques? *Advances in Accounting*, Vol. *30*(1), 67–74.

Bierstaker, J.L., Brody, R.D., and Pacini, C. (2006), Accountants' perceptions regarding fraud detection and prevention methods. Managerial Auditing Journal, Vol. 21 (5), pp. 520-535.

Boczko, T. (2007), Corporate Accounting Information Systems. Harlow, Financial Times Prentice Hall.

Bologna, G., and Lindquist, R. (1995), Fraud Auditing and Forensic Accounting. John Wiley and Sons. New Jersey.

Bolton, R., and Hand, D. (2002), Statistical fraud detection: A review. (Unsupervised profiling methods for fraud detection), *Statistical Science,* Vol. 17 (3), pp. 235-255.

Bostron, N. (2015), Artificial intelligence is getting smarter by leaps and bounds. https://www.ted.com/talks/nick_bostrom_what_happens_when_our_computers_get_smarter_than_we_are? Accessed on 15/11/2017.

BOT, (2014), Banking Supervision Annual Report, Bank of Tanzania, Dar es Salaam, Tanzania

Boyle, D.M; DeZoort, T. F., and Hermanson, D. R. (2015), The effect of alternative fraud model use on auditors' fraud risk judgments, *Journal of Accounting and Public Policy,* Vol. 34 (6), pp 578-596.

Braton, D., and Van de, W. (2011), Neopatrimonial Regimes and Political Transitions in *Africa, World Politics,* Vol.46 (4), pp 453-489.

Braun, R. L., and Davis, E. (2003), Computer-Assisted Audit Tools and Techniques: Analysis and Perspectives, *Managerial Auditing Journal,* Vol. 18 (9), pp. 725 – 731.

Brazel, J. F (2008), How do Financial Statement Auditors and IT Auditors Work Together? *The American CPA Journal,* pp 38-43, Available at: http://www4.ncsu.edu/fbrazel/MyResearch/IT/auditorCPA/journalpub.pdf [Accessed on 9/05/ 2015].

Brazel, J.F. and Agoglia, C.P. (2007), An examination of Auditor Planning Judgements in a complex Accounting Information System Environment. *Contemporary Accounting Research*, 24 (4), pp.1059-1083.

Brian, S. (2018) Fraud increasing in both cost and complexity for UK organisations: states PwC Survey, http://www.risk-uk.com/fraud-increasing-cost-complexity-uk-organisations-states-pwc-survey/ [accessed on 3/3/2018].

Brockett, P.L., Xia, X., and Derrig, R.A. (1998), Using Kohonen's self-organising feature map to uncover automobile bodily injury claims fraud, *The Journal of Risk and Insurance*, Vol. 652, pp. 245-274.

Brown, A. D., Humphreys M., and Gurney P.M. (2005), 'Narrative, Identity and Change: A Case Study of Laskarina Holidays'; *Journal of Organisational Change Management* Vol. 18 (4), pp. 312-326.

Bryman, A., and Bell, E. (2011), Business Research Methods, Third Edition, Oxford: Oxford University Press.

Brynjolfsson, E., and Hitt, L. M. (1998), Beyond the Productivity Paradox. *Communications of the ACM*, 41(8), pp. 49-55.

Byrne, B. M. (2009), Structural Equation Modeling with AMOS. Uta.Fi. Retrieved from http://www15.uta.fi/arkisto/aktk/lectures/sem_en/pdf/sem_exercise_v2.5.pdf

Caglio, A. (2003). 'Enterprise resource planning systems and accountants: towards hybridisation?'*European Accounting Review*, Vol. 12, (1), pp. 123–53.

Carminati, M., Caron, R., Maggi, F., Epifani, I., and Zanero, S. (2015), Banksealer: A decision support system for online banking fraud analysis and investigation, *Computers and Security Journal,* Vol. 5 (3), pp. 1 7 5-1 8 6.

Cassell, C., and Symon, G. (2004), Essential guide to qualitative methods in organisational research, London: Sage.

Chan, D., and Vasarhelyi, M. (2011), Innovation and practice of continuous auditing. *Int J Account Inf System,* Vol.12, pp.152–60.

Cheng, S., and Cho, V. (2010), An integrated model of employees' behavioral intention toward innovative information and communication technologies in travel agents. *Journal of Hospitality and Tourism Research,* Vol.35 (4), pp. 488- 510.

Chiu, V., Liu. Q. and Vasarhelyi, M. A. (2014), The development and intellectual structure of continuous auditing research, *Journal of Accounting Literature* Vol. 33, pp. 37–57.

Cho (2007), The impact of information technology on economic growth in Korea, 2007 International Forum on Strategic Technology, 3-6 Oct. 2007https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4798543 [accessed on 27 August 2017)

Chou, S. Y., and Pearson, J. (2011), A Demographic Study of Information Technology Professionals' Organisational Citizenship Behavior. *Journal of Management Research*, *3* (2), 1–16.

Christini, G., Fetsko, M., and Hendrickson, C. (2004), Environmental management systems and ISO 14001 certification for construction firms. *Journal of Construction Engineering and Management,* 130(3), pp. 330–336.

CICA, (2003), Electronic Audit Evidence, Toronto: CICA.

CICA/AICPA, (1999), Continuous auditing Research Report, Toronto, Canada: The Canadian Institute of Chartered Accountants.

Cohen, J. (1998), Applied Multiple Regression/Correlation Analysis for Behavioural Sciences, 3rd Edition. Menwah, NJ: Lawrence Erlbaum Associates.

Collins, K. M. T., Onwuegbuzie, A. J., and Jiao, Q. G. (2006), Prevalence of mixed methods sampling designs in social science research. *Evaluation and Research in Education,* Vol. 19, pp. 83-101.

Companies Act, (2002), Dar es Salaam.

Conway, M.J and Huffcutt, I. (2003), Review and Evaluation of Exploratory Factor *Analysis Practice in Organisational Research,* Vol.6 (2), pp. 147–168.

Cook, R. D. (1977), Detection of Influential Observation in Linear Regression, *Technometrics,* Vol. 19(1) pp. 15-18.

Cosserat, G. (2004), Modern Auditing, Chichester: John Wiley and Sons.

Cramer, D. (1998), Fundamental statistics for social research, London; Routledge.

Cramer, D., and Howilt. D (2004), The SAGE dictionary of statistics, London; SAGE.

Cressey, D. R. (1973), Other People's Money, Montclair, Patterson Smith, p. 30

Creswell, J. W. (2002), Educational research: Planning, conducting, and evaluating quantitative and qualitative research. Upper Saddle River, NJ: Pearson Education.

Creswell, J. W. (2007), Qualitative Inquiry and Research Design: Choosing Among Five Approaches (2nd Ed., p. 416). Thousand Oaks: Sage.

Creswell, J. W. (2009), Qualitative, Quantitative and Mixed Methods Approach, Third Edition, Sage, LA.

Creswell, J. W., and Plano Clark, V. L. (2011), Designing and conducting mixed methods research (2nd ed.). Thousand Oaks, CA: Sage.

Crites, S. (2008), Best Practices in Accounting Online Cash Management Security, *Commercial Lending Review*, Vol. 23 (3) pp.21-25.

Crotty, M. (1996), Phenomenology and Nursing Research. South Melbourne: Churchill Livingstone.

Curtis, M. B., and Payne, E. A., (2014), Modelling voluntary CAAT utilization decisions in auditing, *Managerial Auditing Journal,* Vol. 29 (4) pp. 304 – 326.

Curtis, M.B., and Payne, E. A. (2008), An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing, *International Journal of Accounting Information Systems*, Vol. 9 (2), pp. 104.

Curtis, S., Gesler, W., Smith, G., and Washburn, S. (2002), Approaches to sampling and case selection in qualitative research: Examples in the geography of health, *Social Science and Medicine,* Vol.50, pp. 1001-1014.

Danish. J., and Muhammad, N.N. (2011), Is Ethical Hacking Ethical? *International journal of Engineering Science and Technology,* Vol 3 (5), pp. 3758-3763.

Davia, H.R.; Coggins, P.; Wideman, J., and Kastantin, J. (2000), Accountant's Guide to Fraud Detection and Control (2nd Edition). John Wiley and Sons: Chichester, UK.

Davis, F. D. (1989), Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly,* Vol. 13 (3), pp. 319–340,

Davis, F. D., Bagozzi, R. P. and Warshaw, P. R. (1989), "User acceptance of computer technology: A comparison of two theoretical models", *Management Science,* Vol.35, pp. 982–1003.

De Leon, A. R., and Carrière, K. C. (2005), A generalized Mahalanobis distance for mixed data. *Journal of Multivariate Analysis,* Vol.92 (1), 174–185.

De Vaus, D. A. (1993), Surveys in social research (3rd ed.) London: UCL Press.

Debreceny, R., Lee, S., Neo, W., and Toh, J.S. (2005), Employing generalized audit software in the financial services sector: challenges and opportunities, *Managerial Auditing Journal*, Vol. 20 (6), pp. 605-618.

Denzin, N.K., and Lincoln, Y.S. (2005), Sage handbook of qualitative research (3rd edition), Thousand Oaks: Sage.

Desimone, J. A., Harms, P. D., and Desimone, A. J. (2015), Best practice recommendations for data screening. *Journal of Organisational Behavior,* Vol. 36(2), pp. 171–181.

Dewa, M., and Zlotnikova, I. (2014), Current Status of e Government Services in Tanzania: A Security Perspective. *Advances in Computer Science: an International Journal,* Vol. 3, (3), pp. 114-122

Diaz, M. C., and Loraaz, T. (2010), Learning new uses of technology while on an audit engagement: Contextualizing general models to advance pragmatic understanding, *International Journal of Accounting Information Systems* Vol.11, pp. 61–77.

Doane, D. P., and Seward, L. E. (2011), 'Measuring Skewness', *Journal of statistics Education,* Vol. 19(2), pp. 1-18.

DSE, (2016), Dar es Salaam Stock Exchange - Listed Companies https://www.african-markets.com/en/stock-markets/dse/listed-companies. [Accessed on 20/12/2016].

Dunning, H., Williams, A., Abonyi, S., and Crooks, V. (2008), A mixed method approach to quality of life research: A case study approach. Social Indicators Research, Vol. 85, pp.145-158.

Durbin, J., and Watson, G. S. (1971), Testing for serial correlation in least squares regression III, *Biometrika,* Vol. 58 (1), pp. 1–19.

Dyck, A., Morse, A., and Zingales, L. (2010), 'Who blows the whistle on corporate fraud?' *Journal of Finance,* Vol.65 (6), pp. 2213–2253.

Ebimobowei, A. Ogbonna, G. N and Enebraye, Z. P. (2013)Auditors' Usage of Computer Assisted Audit Tools and Techniques: Empirical Evidence from Nigeria, Research Journal of Applied Sciences, Engineering and Technology 6(2): 187-195,

Elly, T., and Boter, H. (2011), Increasing the competitive strengths of Tanzanian tourism firms-the strategic role of information technology. http://www.icsb2011.org/download/18.62efe22412f41132d41800011474/739.pdf

El-Sood, H. A., Kotb, A., and Allam, A. (2015) Exploring Auditors' Perceptions of the Usage and Importance of Audit Information Technology, International Journal of Auditing, Vol. 19, pp.252–266.

Ernst and Young (2000), '5th Global Fraud Survey' Ernst and Young Publication.

Ernst and Young (2006), '9th Global Fraud Survey' Ernst and Young Publication.

Ernst and Young (2015), The future of assurance: How technology is transforming the audit. EY Publication. Published in the UK http://www.ey.com/Publication/vwLUAssets/EYemeia-fso-assurance-viewpoint-technolog.

Ernst and Young, (2010), 'Fraud the unmanaged Risk: An International Survey of the Effect of Fraud on Business'. London: Ernst and Young.

Ernst and Young, (2012), Business Manual and Company Returns, EY, Dar es Salaam.

Essellar, W., and Lishan, E. (2013), Understand what is happening in ICT in Tanzania: Evidence for ICT Policy Action, Policy Paper No. 11; available at http://www.researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Policy. [Accessed on 21/12/2015].

Estevez, P., Held, C., and Perez, C. (2006), Subscription Fraud Prevention in Telecommunications Using Fuzzy Rules and Neural Networks *Expert Systems with Applications* Vol.31, 337-344.

Estévez, P., Held, C., and Pérez, C. (2006), Subscription fraud prevention in telecommunications using fuzzy rules and neural networks", *Expert Systems with Applications,* Vol. 31, pp. 337-344.

Farrell, L., and Franco, P. (1999), The Role of the Auditor in the Prevention and Detection of Business Fraud, SAS No. 82, *Western Criminology Review,* Vol. 2 (1), pp. 1-11.

Field, A. (2013), Discovering Statistics Using IBM SPSS Statistics. London: Sage Publications.

Fischer, C.T. (2009), Bracketing in qualitative research: conceptual and practical matters: Psychotherapy research, Journal of the society for psychotherapy research, Vol. 19 (4-5), pp.583-590.

Fishbein, M., and Azjen, I. (1970), Understanding attitudes and predicting social behaviour. *The Theory of Reasoned Action*. The persuasion handbook: Developments in theory and practice.

Flint, D. (1998), Philosophy and principles of auditing. London: Macmillan.

Flowerday, S., Solms, R.V., Technology, I., Engineering, F., and Mandela, N. (2004), Continuous Auditing: Verifying Information Integrity and Providing Assurances for Financial Reports. *Computer Fraud and Security,* pp.12– 16.

Flowerday. S., Blundell, A. W. and Von-Solms, R. (2006), Continuous auditing technologies and models*: A discussion, computers and security* Vol.2 (5), pp. 3 2 5 – 3 3 1.

Friedman, A. L. and Miles, S (2002) Stakeholders: Theory and Practice, Oxfordshire, Oxford University Press,

Fuchs, M., Hopken, W., Foger, A., and Kunz, M. (2010), E-business readiness, intensity, and impact: an Austrian destination management organisation study. Journal of Travel Research, Vol 49 (2), pp. 165-178.

Galetsas, A. (2007), Statistical Information on Network Security. European Commission

Genuchten, R. V., Haring, W., Kassel, D. V., and Yakubi, K. (2012), Mobile phone use in Tanzania. Amsterdam: vrije universiteit amsterdam.

Ghasemi, A., and Zahediasl, S. (2012). Normality tests for statistical analysis: A guide for non-statisticians. *International Journal of Endocrinology and Metabolism,* Vol. 10 (2), pp. 486–489.

Ghasemi, A., Shafeiepour, V., and Elham-Barvaye. M. (2011), The impact of Information Technology (IT) on modern accounting systems. *Procedia-Social and behavioural sciences,* Vol. 28, pp. 112-116.

Gibbs, J. L., and Kraemer, K. L. (2010), A cross-country investigation of the determinants of scope of e-commerce use: an institutional approach. *Electronic Markets,* Vol.14 (2), pp. 124- 137.

Gonzalez, G.C., Sharma, P.N. and Galletta, D.F. (2012), The antecedents of the use of continuous auditing in the internal auditing context, *International Journal of Accounting Information Systems,* Vol. 13 (3), pp. 248-262.

Gonzalez, S. M., and Gidumal, J.B. (2016), A model that connects information technology and hotel performance, *Tourism Management,* Vol. 53, pp. 30-37.

Goodhue, D.L. and Thompson, R.L. (1995), Task-Technology Fit and Individual Performance. *MIS Quarterly,* Vol.19(2), pp.213-217.

Gopalakrishuna, M., Sabouri, M.S., Hong, T.S., and Zulkifli, N. (2008), Information Technology Adoption in Small and Medium-sized Enterprises: An Appraisal of Two Decades Literature. Interdisciplinary*, Journal of Research in Business,* Vol. 1(7), pp.53–80.

Grandón, E. E., Nasco, S. A., and Mykytyn, P. (2011), Comparing theories to explain e-commerce adoption, *Journal of Business Research*, Vol.64, pp.292–298.

Greenstein-Prosch, M., McKee, T. E and Quick, R. (2008), A Comparison of the Information Technology Knowledge of United States and German Auditors. *The International Journal of Digital Accounting Research*, Vol. 8 (14), pp. 45-79.

Guba, E. G., and Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin and Y.

Guest, G. Bunce. A., and Johnson. L (2005), Filed Methods; How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. SAGE online books available at http://www.sagepublications.com [Accessed on 30/05/ 2016].

Gullkvist, B., (2003), Adoption and Impact of e-Accounting, *Frontier of e-Business Research,* pp. 536-544.

Gunasekaran, A., and Ngai, E.W.T. (2005), E-commerce in Hong Kong: an empirical perspective and analysis, *Internet Research,* Vol. 15 (2), pp.141 – 159.

Hair, J.F. Black, W.C. Babin, B.J. and Anderson, R. E. (2010), Multivariate data Analysis (7th ed.). Upper Saddle River,: NJ: Pearson Prentice Hall Pearson Education.

Hassan, N. R. (2006), New Approaches to Studying Information Technology: Escaping the Organisational Straightjacket *Informing Science Journal* Vol. 9; pp.243-260.

Havelka, D., and Merhout, J. W. (2008), Information Technology Auditing: A Value Added IT Governance Partnership between IT Management and Audit; *Communication of the Association for Information Systems*; Vol.23 (26), pp. 463-482.

Helms, G. I., and Mancino, J. M. (1999), Information technology issues for the attest, audit, and assurance services functions, The CPA Journal, Vol. 69 (5), pp. 62-63.

Henn, M. (2009), A critical Introduction to Social Research, London: Sage.

Hofstede, G. (1984), Culture's Consequences: International Differences in Work-Related Values, Beverly Hills CA: SAGE Publications

Hopwood, W.S., Leiner J.J., and Young, G.R. (2008), Forensic Accounting Mc Graw-Hill/Irwin.

Hua, J. S., Huang, S. M., Yang, L. W., and Yen, D. C. (2008), An investigation of Zipf's Law for fraud detection*, Decision Support Systems,* Vol. 46, pp. 70-83.

Huang, S. M., Hung, Y. C and Tsao, H. H. (2008). Examining the determinants of computer-assisted audit techniques acceptance from internal auditors' viewpoints, *International Journal of Services and Standards* Vol.4 (4), pp. 377-392.

Hung, Y., Yang, Y., Yang, H., Chuang, Y. (2011) Factors affecting the adoption of e-commerce for the tourism industry in Taiwan. Asia Pacific Journal of Tourism, Vol. 16 (1), pp. 105-119

Hunton, J. E., Wright, A. M., and Wright, S. (2004). Are Financial Auditors Overconfident in Their Ability to Assess Risks Associated with Enterprise Resource Planning Systems? *Journal of Information Systems*, Vol. 18 (2), pp. 7-28.

Hurmerinta, P., L., and Nummela, N. (2006), Mixed methods in international business research: A value-added perspective. Management International Review, Vol.46, pp. 439-459.

Hyuha, M., and B.J. Ndulu. (1990). Inflation and economic recovery in Tanzania: Further empirical evidence. Mimeo. Dar es Salaam.

IFAC, (2002), Audit Risk: Proposed International Standards on Auditing and Proposed Amendment to ISA 200, Objective and Principles Governing an Audit of Financial Statements, International Federation of Accountants, New York, NY, International Auditing and Assurance Standards Board, Exposure Draft, October.

IFAC, (2006), International Education Practice Statement (IEPS) 2.1, Information Technology for Professional Accountants, International Federation of Accountants (IFAC), International Accounting Education Standards Board (IAESB).

IFAC, (2009a), ISA 240. International Standard on Auditing No.240. The Auditors' Responsibilities Relating to Fraud in an Audit of Financial Statements. The International Federation for Accountants (IFAC), International Auditing Standard Board (IASB).

IFAC, (2009b), ISA 315 International Standard on Auditing No. 315 Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment. The International Federation for Accountants (IFAC), International Auditing Standard Board (IASB).

IFAC, (2009c), ISA 200 International Standard on Auditing No.200- Overall Objectives of the Independent Auditor and the Conduct of an Audit In Accordance With International Standards on Auditing. The International Federation for Accountants (IFAC), International Auditing Standard Board (IASB).

IFAC, (2009d), ISA 300 planning an audit of financial statements, International Federation for Accountants (IFAC), International Auditing Standard Board (IASB).

IFAC, (2009e), ISA 450, Evaluation of misstatements identified during the audit. International Federation for Accountants (IFAC), International Auditing Standard Board (IASB).

Ihucha, A. (2014), Exim Bank (T) cyber fraud cases go to court, The East African, Saturday, March, 29 2014, available at http://www.theeastafrican.co.ke/business/2560-2262182-owx2l1z/index.html.

IIA, (2009), The Professional Practices Framework: Institute of Internal Auditors Altamonte Springs, FL.

IMF, (2005), Reports on the Observance of Standards and Codes (ROSCs), International Monetary Fund, IMF http://www.imf.org/external/NP/rosc/ [accessed on 05/01/2016].

IMF, (2009), Tanzania: the story of an African transition, Washington, D.C.: International Monetary Fund, IMF Multimedia Services Division; available at: https://www.imf.org/external/pubs/ft/books/2009/tanzania/tanzania.pdf. [Accessed on 30/12/2015]

IMF, (2016), Report on World Economic Growth March 2016; Available at https://www.imf.org/events/world-economic-growth-on-africa-2016/. [Accessed on 5th May 2016].

ISACA, (1999), IT Auditing Guideline: G3 Use of Computer-Assisted Audit Techniques (CAATs). Information systems audit and control association, at https://www.google.com/search?q=ISACA+(1999)+IT+Auditing+Guideline%3. [Accessed on 19/09/2015].

ISACA, (2009), IS Auditing Guideline, Use of Computer Assisted Audit Technique (CAATTs), Information Systems Audit and Control Association, Houston, TX.

Ishiyaku, B., Kasim, R., and Harir, A. I. (2016). Confirmatory Factoral Validity of Public Housing Performance Evaluation Constructs. *Journal of Building Performance,* Vol.7 (1), pp.9–22.

Jans, M., Lybaert, N., and Vanhoof, K. (2010), Internal Fraud Risk Reduction: Results of A Data Mining Case Study*, International Journal of Accounting Information Systems,* Vol. 11, pp 17–41.

Jans, M., Lybaert, N., and Vanhoof, K., (2009), A Framework for Internal Fraud Risk Reduction at IT Integrating Business Processes: The IFR2 Framework, *International Journal of |Digital Accounting Research* Vol. 9, pp.1-29.

Janvrin, D., Bierstaker, J., and Lowe, D. J., (2008), An Examination of Auditing Information Technology Use and Perceived Importance, *Accounting Horizons* Vol.22 (1) pp1-21.

Janvrin, D., Bierstaker, J., and Lowe, J.D. (2009), An Investigation of Factors Influencing the Use of Computer-Related Audit Procedures, *Journal of Information Systems* Vol. 23(1), pp. 1-22.

Jarvinen, T. (2012), Factors Influencing Auditors ' Information Usage : Experience , Risk , Task Structure and Information Reliability. Universitas wasaensis.

Juneja, G. (2013), Ethical Hacking: A Technique to Enhance Information Security. *International Journal of Innovative Research in Science, Engineering and Technology*. ISSN online (2319-8753) Available at https://www.rroij.com/open-access/ethical-hacking-a-technique. [Accessed on 25/12/2016].

Keila, P.S., and Skillicorn, D. B. (2005), Structure in the Enron email dataset. In Workshop on Link Analysis, Security and Counterterrorism, SIAM International Conference on Data Mining, pp. 55–64.

Kemper, E. A., Stringfield, S., and Teddlie, C. (2003), Mixed methods sampling strategies in social science research. In A. Tashakkori and C. Teddlie (Eds.), Handbook of mixed methods in social and behavioral research (pp. 273-296). Thousand Oaks, CA: Sage.

Khalifa, M., and Shen, K. N. (2008), Explaining the adoption of transactional B2C mobile commerce *Journal of Enterprise Information Management*, Vol. 21(2), pp.110–24.

Khan, R., Cox, P. (2017). Country Culture and National Innovation. Archives of Business Research, 5(2), pp 124-135.

Kiabel, D. (2012), Internal Auditing and Performance of Government Enterprises: A Nigerian Study. *Global Journal of Management and Business Research*, Vol. 12 (6), pp. 6-18.

Kigen, P., Kisutsa, C., Muchai, C., and Kimani, K (2014), Kenya Cyber Security Report: Rethinking Cyber Security-An Integrated Approach. Available at www.seriano.com [Accessed on 30/11/ 2015].

Kim, H. J., Mannino, M., and Nieschwietz, R. J. (2009), Information technology acceptance in the internal audit profession: Impact of technology features and complexity. *International Journal of Accounting Information Systems*, Vol. 10, pp 214–228.

Kim,H., Kotb, A., and Eldaly, M. K. (2016) "The use of generalized audit software by Egyptian external auditors: The effect of audit software features", Journal of Applied Accounting Research, Vol. 17 Issue: 4, pp.456-478.

Kirkos, E., Manolopoulos, Y., Spathis, C. (2007), Data Mining techniques for the detection of fraudulent financial statements, *Journal of Expert Systems Applications*. Vol 32, pp 995-1003.

Kisanga., D. and Ireson. G. (2015), Barriers and strategies on adoption of e-learning in Tanzanian higher learning institutions: Lessons for adopters; International *Journal of Education and Development using Information and Communication Technology*; Vol. 11 (2), pp. 126-137.

Kline, R. B. (2011), Principles and Practices of Structural Eqaution Modeling. (T. D.Little, Ed.) (3rd ed.). New York: The Guilford Press New York London.

Knapp, C. M. (2013), Contemporary Auditing, Cengage Learning, KL.

Knechel, W. (2001), Auditing: Assurance and Risk, Cincinnati, OH: South-Western College Publishing.

Knofczynski, G. T., and Mundfrom, D. (2007), Sample Sizes When Using Multiple Linear Regression for Prediction. Educational and Psychological Measurement, Vol. 68 (3), pp. 431–442.

Kohli, R., and Devaraj, S. (2003) Measuring Information Technology Payoff: A Meta-Analysis of Structural Variables in Firm-Level Empirical Research, *Information Systems Research,* Vol.14 (2), pp. 127-145.

Korpelainen, E. (2011), Theories of ICT System Implementation and Adoption – *A Critical Review Working Papers,* Department of Industrial Engineering and Management, Aalto University, Helsinki.

Kotb, A., and Roberts, C. (2011), The Impact of E-Business on the Audit Process: An Investigation of the Factors Leading to Change. *International Journal of Auditing,* Vol. 12 (3) pp. 150–175.

Kotb, A., Roberts, C., and Sian S. (2012), E-business audit: Advisory jurisdiction or occupational invasion? *Critical Perspectives on Accounting* Vol. 23, pp. 468– 482.

Kotb, A., Roberts, C., and Stoner, G. (2013), E-business in accounting education in the UK and Ireland: Influences on inclusion in the curriculum. *The International Journal of Management Education* Vol. 11, pp. 150–162.

Kotb. A., Sangster. A., and Hendersen. D. (2014), E-business internal audit: the elephant is still in the room! *Journal of Applied Accounting Research*. Vol 15 (1), pp. 43-63.

Kotsiantis, S., Koumanakos, E., Tampakas, V., and Tzelepis, D. (2006), Forecasting Fraudulent Financial Statements using Data Mining. *International Journal of Computational Intelligence*, Vol 3(2), pp. 104-110.

KPMG, (2005), African Fraud and Misconduct Survey 2005, at http://allafrica.com/fraudstories/200510270516.html[accessed on 09/09/2015].

KPMG, (2006), Fraud Risk Management; Developing a Strategy for Prevention, Detection and Response to Fraud; A Manual Guide for Auditors, available at: www.kpmg.com/CN/en/.../Fraud-Risk-Management-O-200610.pd.

Krejcie, R.V., and Morgan, D.W. (1970) Determining Sample Size for Research Activities. Educational and Psychological Measurement, 30, pp.607–610.

Kumar, M., Salim, A. T., and Ramayah, T. (2013), Business Research Methods, Kuala Lumpur Malaysia: Oxford University Press.

Kumar, R. (1999), Research Methodology: A step-by-step guide for beginners. Melbourne, Australia: Addison Wesley Longman Australia Pty Limited.

Lal, P. S., and Bharadwaj, S. (2016), Understanding the impact of cloud-based services adoption on organisational flexibility. *Journal of Enterprise Information Management,* Vol.29, pp. 566 – 588.

Lau, C. K., and Ooi, K. W. (2016), A case study on fraudulent financial reporting: evidence from Malaysia, *Accounting Research Journal*, Vol. 29(1), pp.4-19,

Lee, C. C., Cheng, H. K., and Cheng, H. H. (2007), An empirical study of mobile commerce in insurance industry: Task–technology fit and individual differences, *Decision Support Systems,* Vol.43 (1), pp. 95-110.

Lincoln, Y. S., and Guba, E. G. (1985), Naturalistic inquiry. Beverly Hills, CA: Sage.

Lotto, J. (2014), Examining the Impact of Information Technology on Internal Auditing Effectiveness in Tanzanian Organisations. *Time Journals of Social Sciences,* Vol. 2(3), pp 13-23.

Lubua, E., and Maharaj, M. (2012), ICT Policy and E-transparency in Tanzania. IST-Africa. Dar Es Salaam: IIMC International Information Management Corporation.

Lubua, W. (2014), Cyber Crimes Incidents in Financial Institutions of Tanzania. *International Journal of Computer Science and Business Informatics* Vol.14 (3), pp. 37-48.

Luke, D. (2018) Digital banking fraud in South Africa: Scams to watch out for: Business and Finance Magazine, available at https://www.thesouthafrican.com/banking-fraud-in-south-africa [accessed on 25th August 2018].

Mahzan, N., and Lymer, A. (2014), Examining the adoption of computer-assisted audit tools and techniques: Cases of generalized audit software use by internal auditors, *Managerial Auditing Journal*, Vol. 29 (4), pp. 327-349.

Maitlis, S. (2012), Narrative Analysis. In G. Symon and Cassell (Eds), Qualitative Organisational Research, pp.492-511.

Malhotra. N. K (2009), Marketing Research, 4th Edition, NJ, Pearson Publication.

Mandari, H., Koloseni, D., and Nguridada J. (2017), Electronic fiscal device (EFD) acceptance for tax compliance among trading business community in Tanzania: the role of awareness and trust, I*nternational Journal of Economics, Commerce and Management,* Vol. 5 (3), pp. 142-158.

Mansour E. M. (2016) Factors Affecting the Adoption of Computer Assisted Audit Techniques in Audit Process: Findings from Jordan, Business and Economic Research, Vol. 6, No. 1, pp.248-271.

Marcelle, A. (20090, Challenges Facing the Modern Day Auditing Profession: Will this lead to a Big Four audit market dominance? A discussion paper available at http://www.accountancysa.org.za/challenges-facing-the-modern-day-auditing-profession/ [accessed on 15/12/2017].

Masamila, B. (2014), State of Mobile Banking In Tanzania and Security Issues *International Journal of Network Security and Its Applications* (IJNSA), Vol.6 (4), pp53-64.

Maswera, T., Dawson, R., and Edwards, J. (2008), E-commerce adoption of travel and tourism organisations in South Africa, Kenya, Zimbabwe and Uganda. *Telematics and Informatics,* Vol. 25, pp. 187 – 200.

Maswera, T., Dawson, R., and Edwards, J. (2008), E-commerce adoption of travel and tourism organiations in South Africa, Kenya, Zimbwabwe and Uganda. *Telematics and Informatics,* Vol. 25, pp. 187 – 200.

Matthews, D. (2006), 'From ticking to clicking: changes in auditing techniques in Britain', The Accounting Historians Journal, Vol. 33 (2), pp. 63–101.

Maxwell, J. A. (2005), Qualitative research design. Newbury Park, CA: Sage Publication.

Mbelle, A.V.Y. (2004), 'The effectiveness of Tanzania's investment promotion institutions promoting indigenous capital. Dar es Salaam, Mimeo.

Mckee, T. E. (2000), Accounting/Auditing Technology in Norway: An Investigation of the Norwegian Accounting/Auditing Professions Knowledge and Views on Information Technologies. Norwegian Institute of Public Accountants (DnR), Oslo, Norway.

McKim, C. A. (2017), The Value of Mixed Methods Research: A Mixed Methods Study, Journal of Mixed Methods Research, Vol. 11(2), pp. 202–222.

Melville, N., Kraemer. K., and Gurbaxani. V. (2004), Review: Information Technology and Organisational Performance: An Integrative Model of IT Business Value. *MIS Quarterly*, Vol. 28 (2), pp 283-322.

Mercy, W. B., and Rafe, M., (2017), Fraud in mobile financial services: Protecting consumers, providers, and the system. Brief. Washington, D.C, CGAP,

Merriam, S. B. (2009), Qualitative Research: a guide to design and implementation. Revised and expanded from Qualitative research and case study applications in education. San Francisco: Jossey-Bass.

Messier, W. F., and Boh, M. (2012), Auditing and Assurance Services in Malaysia, Second Edition, OH, Mc Grow Hill.

Miah. M., and Omar, A. (2012), Technology Advancement in developing countries during Digital Age, *International Journal of Science and Applied Information Technology*, Vol.1 (1), pp.30-38.

Miiro, F., Othman, A., Sahari, M., and Burhan, M. (2016), A Measurement Model of Talent Management Practices Among University Staff in Central Uganda, *Journal of Positive Management*, Vol. *7*(3), 3–19.

Miles, M., and Huberman, A. M. (1994), Qualitative data analysis: An expanded sourcebook (2nd ed.). Thousand Oaks, CA: Sage Publication.

Minichiello, V., Aroni, R., & Hays, T. (2008). In-depth interviewing: Principles, techniques, analysis. Frenchs Forest, N.S.W: Pearson Education Australia.

Mohamed, D. M., and Habib, M. H. (2013), Auditor independence, audit quality and the mandatory auditor rotation in Egypt, *Education, Business and Society: Contemporary Middle Eastern Issues,* Vol. 6 (2), pp.116-144,

Molina-Azorin, J. F. (2011), The use and added value of mixed methods in management research. Journal of Mixed Methods Research, Vol. 5(1), pp.7-24.

Mooney, J.L., Harrell, H.W., and Ludwig, S.E. (2000), Audit Software that Help Your Company Stop Fraud, *Journal of Corporate Accounting and Finance*. Vol.11 (4) pp 17-23.

Moorthy, M., Seetharaman, A., Mohamed, Z., Gopalan, M., and San, L. (2011), The impact of information technology on internal auditing, *African Journal of Business Management,* Vol. 5(9), pp. 3523-3539.

Morawczynski, O. (2015), Fraud in Uganda: How million were lost to internal collusion. http://www.cgap.org/blog/fraud-uganda-how-millions-were-lost-internalcollusion [Accessed 30/06/ 2016]

Morse, J. M. (1991), Approaches to qualitative-quantitative methodological triangulation. Nursing Research, 40, 120-123.

Morse, J. M. (1995), The significance of saturation. Qualitative Health Research, Vol.5, pp. 147- 149.

Morse, J. M. (2003), Principles of mixed methods and multimethod research design. In A. Tashakkori and C. Teddlie (Eds.), Handbook of mixed methods in social and behavioral research, Thousand Oaks, CA: Sage.

Morse, J. M., & Field, P. A. (1995). Qualitative research methods for health professionals. Thousand Oaks, CA: Sage.

Moshi, H.P.B., and Kilindo. A.A.L. (1990), The impact of government policy on macroeconomic variables: A case study of private investment in Tanzania. AERC Research Paper 89. African Economic Research Consortium, Nairobi

Muchiri, D. (2016) Mobile money, loan, ATM fraud & crime, Annual Forensic Audit Conference, Institute of certified public accountants in Kenya https://www.icpak.com/wp-content/uploads/2016/08/DAY2-SESSION2-Mobile-Money-Dennis-Muchiri.pdf

Mugisha, I., (2014), Two men arrested for allegedly defrauding rwf495m from tigo; the new times, at http://www.newtimes.co.rw/section/read/183244/ [accessed on 15/03/2016].

Mwaikali, E. J. (2014), Assessment of Challenges Facing Customers in Automated Teller Machines in the Banking Industry in Tanzania: A Case of Some Selected Banks in Tanzania. *International Journal of Research in Business and Technology*, Vol.4 (3), 480-488.

Myers, M.D. (2009), Qualitative research in business & management, 1st ed, London. Sage publications Ltd.

Mzenzi, S., and Gaspar, A. F. (2015), External auditing and Accountability in the Tanzanian local government authorities, *Managerial Auditing Journal*, Vol. 30 (7) pp. 681 – 702.

Naibei, K. I., Oima, D., and Ojera, P. (2014), Moderating Effect of Business Risk on the Audit Fee Model Among Small Audit Firms : Case of Western Region Kenya. *European Scientific Journal*, Vol.10(10), pp.445–462.

NBAA (2006) Harmonisation of accounting standards in Tanzania: Process, stakeholders & opportunities http://www.nbaa-tz.org/home.htm/accounting/sallu/pdf

NBAA, (2015), Miscellaneous information for the national board of accountants and auditors regarding list of active members, audit firms and other information by NBAA in Tanzania, www.nbaa.gov.tz/news/pdf. [Accessed on 20/12/2015].

Ndulu, B. (2012), Mobile money transactions top TZS1.7tn. http://www.telegeography.com/products/commsupdate/articles/2012/12/13/mobile-money-transactions-top-tzs1-7tn-bank-of-tanzania-reports/. [accessed on 08/05/2015].

Newman, G. R. and Clarke, R.V.G (2003), Superhighway Robbery; Preventing E-Commerce Crime, NY, Willian Publishing.

Ngai, E. W.T., Hu, Y., Wong, Y. H., Chen, Y., and Sun, X. (2011) "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision. Support System*, Vol. 50 (3), pp. 559–569.

NICB, (2008), National Insurance Crime Bureau (US) https://www.nicb.org/ [Accessed on 25/09/2015].

Nicholaus, S.C. and Venkatakrishnan, V. (2013), Challenges of mobile-phone money transfer services' market penetration and expansion in Singida District, Tanzania. IRACST-*International Journal of Research in Management and Technology*, 3 (6), pp.205-215.

No, W. G., and Vasarhelyi, M.A. (2017), Cybersecurity and Continuous Assurance *Journal of emerging technologies in accounting*, American Accounting Association, Vol. 14 (1), pp. 1–12.

Nor K., and Pearson J.M. (2008), An exploratory study into the adoption of Internet banking in a developing country: Malaysia. *Journal of Internet Commerce*, Vol. 7 (1), pp.29–73.

Nugi N. (2011) State of Information Technology Auditing in Botswana, *Asian Journal of Finance & Accounting*, Vol. 3, No. 1: E8

Nyaga, J. K. (2014), Mobile banking services in the East African community (EAC): Challenges to the Existing Legislative and Regulatory Frameworks. *Article in Africa Economic Brief,* Vol. 1(8), pp 23-35.

Nyerere, J. (1967), Education for Self-Reliance. Dar Es Salaam: Government Press.

Nyman, C., Nilsson, F. and Rapp, B. (2005), Accountability in local government: principal-agent perspective, *Journal of Human Resource Costing and Accounting,* Vol. 9 (2), pp. 123-137.

O'Brien, D. P., and Scott, S. (2012), Correlation and regression in approaches to quantitative research: A guide for dissertation students' edition, Oxford, Oak Tree Press.

O'Cathain, A., Murphy, E., and Nicholl, J. (2010), Three techniques for integrating data in mixed methods studies. British Medical Journal, Vol. 314, pp.1147-1150.

O'Leary, A. (2004), The Essential Guide to Doing Research. London: Sage Publications.

Odom, L., and Henson, R. (2002), Data Screening: Essential techniques for data review and preparation. In Southwest Educational Research Association (pp. 1–37).

Öhman, P., Häckner, E., and Sörbom, D. (2012), Client satisfaction and usefulness to external stakeholders from an audit client perspective, *Managerial Auditing Journal,* Vol. 27 (5), pp.477-499.

Okoye A.E (2004), International Accounting: World Wide Accounting Diversities and Harmonisation, Nigeria Journal of Business Administration. Vol. 6(1), pp 165-178).

Omoteso K., Patel A., and Scott P. (2008), An Investigation into the Application of Continuous Online Auditing in the U.K*, the International Journal of Digital Accounting Research*, Vol.8, pp. 23-44.

Omoteso, K., Patel, A., and Scott, P. (2010), Information and Communications Technology and Auditing: Current Implications and Future Directions, *International Journal of Auditing,* Vol.14, pp 147–162.

Onwuegbuzie, A. J., and Collins, K. M. (2007), A Typology of Mixed Methods Sampling Designs in Social Science Research .*The Qualitative Reports,* Vol. 12 (2), 281-316.

Onwuegbuzie, A. J., and Leech, N. L. (2007), A call for qualitative power analyses. Quality and Quantity: *International Journal of Methodology*, Vol. 41, pp.105-121.

Onwuegbuzie, A. J., Jiao, Q. G., and Bostick, S. L. (2004), Library anxiety: Theory, research, and applications. Lanham, MD: Scarecrow Press.

Oreku, G. S., Li, J., Kimeli, K., and Mtenzi, F.J. (2009), State of Tanzania e-readiness and e-commerce: overview. *Information Technology for Development,* Vol.14 (4), pp.302 – 311.

Orlikowski, W. J. and Iacono, C.S. (2001), Research Commentary: Desperately Seeking the IT in IT Research—A Call to Theorizing the IT Artifact. *Information systems research,* Vol. 12 (2), pp. 121-134.

Osborne, J. W. (2015), What is Rotating in Exploratory Factor Analysis? Practical

Assessment, *Research and Evaluation,* Vol. 20(2), pp. 1–7.

Osborne, J. W., and Costello, A. B. (2004), Sample size and subject to item ratio in principal components analysis and exploratory factor analysis. Practical Assessment, Research and Evaluation, Vol. 9(11), pp. 1–13.

Pallant, J. (2007), SPSS Survival manual. *Journal of Advanced Nursing*, Vol. 36 (3), pp. 478–478.

Palmer, K. N; Douglas, E. Ziegenfuss, R., and Pinsker, E. (2004), International Knowledge, Skills, and Abilities of Auditors/Accountants, *Managerial Auditing Journal*, Vol. 19 (7) pp. 889 –896.

Paula, M.-K., Martin, E., Emmanuel, I., Beatrice, I., and Dadi, M. (2016), Africa cyber security report 2016-achieving cyber security resilience: enhancing visibility and increasing awareness. Technical report, Serianu Limited and United State International University (USIU).

PCAOB (2007), Public Company Accounting Oversight Board- an Audit of Internal Control over Financial reporting that is integrated with an Audit of Financial Statements. Auditing Standard No. 5. Washington, D.C.: Government Printing Office.

Pedrosa, I., Costa, C. J., and Laureano, R. (2015), Financial Auditors and Models for Individual Technology Acceptance: collecting data using expert interviews. *Selected papers on IRIS Information Systems Research Seminar in Scandinavia*, the IRIS Association Nr. 3. Available at www.akademickaforlag.no/pdf. [Accessed on 30/12/2015].

Ponemon Institute, (2013), Cost of Cyber Crime Study: United States. Available at: https://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.

Popoola, O; Ahmad, C.A., and Samsudin, A.S. (2014), Forensic Accounting Knowledge and Skills on Task Performance Fraud Risk Assessment: Nigerian Public Sector Experience. Accepted for publication in the Conference Proceedings of The Global Symposium on Social Sciences (IBSSS) 2013 Okinawa, Japan.

Popp, K. M. and Meyer. R. (2014), Profit from Software Ecosystems: Business Models, Ecosystems and Partnerships in the Software Industry. Norderstedt, Germany: BOD.

Porter, B., Simon, J., and Hatherly, D. (2008), Principles of External Auditing, Third Edition, Willey, LA.

Power, M. (2000), The Audit Society: Second Thoughts. *International Journal of Auditing.* Vol. 4 (1) pp. 111–119.

Pratt, C. (1999), Julius Nyerere: Reflections on the Legacy of his Socialism. Canadian Journal of African Studies, Vol. 33 (1), pp. 137–52.

PwC, (2007), Economic crime: people, culture and controls. the 4th bi-annual global economic crime survey. Technical report, PriceWaterhouse&Coopers, NY.

PwC, (2014), Threats to the Financial Services sector, Financial Services sector analysis of Global Economic Crime Survey. Available at www.pwc.com/crimesurvey/pfd. [Accessed on 20/10/ 2015).

PwC, (2018), Global Economic Crime Survey 2018: UK findings-Pulling fraud out of the shadows, https://www.pwc.co.uk/forensic-services/assets/gecs/global-economic-crime-survey-2018-uk-findings.pdf [accessed on 03/03/2018].

Qorro, E. (2017), Tanzania among most peaceful countries globally: Global Peace Index. The Guardian, IPP Media, 27th July, 2017, available at https://www.ippmedia.com/en/news/tanzania-among-most-peaceful-countries-globally.

Quaddus, M., and Achjari, D. (2005), A model for electronic commerce success. *Telecommunication Policy,* Vol. 29, pp. 127-152.

Ramachandran, J., Subramanian R, and Kisoka, I. J. (2012), Effectiveness of Internal Audit in Tanzanian Commercial Banks, *British Journal of Arts and Social Sciences* Vol.8 (I), pp 32-43.

Ramamoorti, S., and Weidenmier, M.L. (2004), Research Opportunities in Information Technology and Internal Auditing *Journal of Information Systems* Vol.20, (1) pp. 205-219.

Razali, M. M., and Wah. Y. B. (2011), Power comparisons of Shapiro-Wilk, Kolmogorov-Sminov, Lilliefors and Anderson-Darling Tests, *Journal of Statistics Modelling analysis* Vol. 2 (1), pp.21-33.

Razi, M. A., and Madani, H. H. (2013), An analysis of attributes that impact adoption of audit software: An empirical study in Saudi Arabia. *International Journal of Accounting and Information Management,* Vol. 21(2), pp. 170-188.

Rezaee, Z. (2002), Financial Statement Fraud: Prevention and Detection, NJ: John Wiley & Sons.

Rezaee, Z., and Reinstein, A. (1998), The impact of emerging information technology on auditing, *Managerial Auditing Journal,* Vol. 13(8) pp. 465 – 471.

Rezaee, Z., Elam, R., and Sharbatoghlie, A. (2001), Continuous auditing: the audit of the future, *Managerial Auditing Journal,* Vol. 16 (3), pp.150-158,

Rogers, E. (2003), Diffusion of Innovations, 5th Edition. NY: Simon and Schuster.

Rosli, K., Yeow, H. P., and Siew, E. G. (2013), Factors Influencing Audit Technology Acceptance by Audit Firms: A New I-TOE Adoption Framework, *Journal of Accounting and Auditing: Research and Practice* Vol. 2; pp 1-11.

Ross, A. S; Westerfield. R. W., and Jaffe. J (2009), Modern Financial Management. McGraw Hill Higher Education, NYC.

Rumanyika, J. D. (2015), Obstacles towards Adoption of Mobile Banking in Tanzania: A Review *International Journal of Information Technology and Business Management,* Vol.35 (1), pp.1-17.

Sacks, S.E. (2014). Fraud risk: Are you prepared? *Journal of Accountancy*, Vol. 198 (3), pp 57-63.

Salehi, M., and Alipour, M. (2010), E-banking in Emerging Economy: Empirical Evidence of Iran, Int. *J. Econ. Finance* Vol. 2(1), pp. 201-209.

Salwani, M. I., Marthandan, G., Norzaidi, M. D., and Chong, S. C. (2009), E-commerce usage and business performance in the Malaysian tourism sector: empirical analysis. *Information Management and Computer Security*, Vol. 17(2), pp. 166-185.

Sánchez, D., Vila, M., Cerda, L. and Serrano, J. (2009): "Association rules applied to credit card fraud detection", *Expert Systems with Application,* Vol. 36, pp.3630-3640.

Sandelowski, M. (1995), Focus on qualitative methods: Sample sizes in qualitative research. Research in Nursing and Health, Vol. 18, pp. 179-183.

Saunders, M, Lewis, P., and Thornhill, A. (2007), Research methods for business student, 4th edn, Harlow: Pearson Education.

Saunders, M, Lewis, P., and Thornhill, A. (2012), Research methods for business student, 6th edn, Harlow: Pearson Education.

Seeburn, K. (2013), Information Systems Auditor: What are the Key Knowledge requirements? *International Journal of Auditing Technology,* Vol.1 (1), pp 34-44.

Sekaran, U., and Bougie, R. (2010), Research Method for Business. London, UK: John Wiley and Sons Ltd.

Senft, S., and Gallegos, F. (2008), Information technology control and audit, CRC Press.

Shaikh, J.M., (2005), E-commerce Impact: Emerging Technology – Electronic Auditing *Managerial Auditing Journal;* Vo. 20 (4) pp.408 – 421.

Shapiro, S. S., and Wilk. M. B. (1965). Analysis of Variance Test for Normality (Complete Samples) *Biometrica,* Vol. 52 (3) pp. 591-611

Sharma, A., and Panigrahi, P.K (2012), A Review of Financial Accounting Fraud Detection based on Data Mining Techniques. *International Journal of Computer Applications,* Vol. 39 (1), pp. 1-11.

Siddiqui, K. (2013), Heuristics for sample size determination in multivariate statistical techniques. *World Applied Sciences Journal,* Vol.27(2), pp.285–287.

Silverman, D. (2007), A very short, fairly interesting and reasonably cheap book about qualitative research. London: Sage Publication.

Silverman, D. (2010), Doing Qualitative Research (3rd ed.). London: Sage Publications.

Silverman, D. (2013), Doing Qualitative Research, Fourth Edition, Sage Publications.

Simkin, M. G, Rose, J. M. and Norman, S. C. (2015), Core Concepts of Accounting Information Systems, 13th Edition. LA: Willey.

Singleton, T. (2006), Generalised Audit Software: Effective and Efficient Tool for Today's IT Audits. Information Systems, pp.1–3.

Skillicorn, D.B., Vats, N. (2007) Novel information discovery for intelligence and counterterrorism. *Decision Support Systems*. Vol. 43, pp.1375-1382.

Smith, B., Yurcik, W., and Doss, D. (2002), Ethical Hacking: the security justification redux, *IEEE Transactions*, pp. 375-379.

Soltani, B (2013), Auditing: An International Approach, Third Edition, Pearson Education Ltd.

Stanton, G. (2012), Detecting fraud: Utilizing new technology to advance the audit profession. Best thesis award: University of New Hampshire http://scholars.unh.edu/honors/18.

Stoel, D., Havelka, D., and Merhout, J.W., (2012), Analysis of Attributes that Impact Information Technology Audit Quality: A study of IT and Financial Audit Practitioners, *International Journal of Accounting Information Systems* Vol.13 pp. 60-79.

Stone, Diane (January 2004). Transfer agents and global networks in the 'trans-nationalisation' of policy, *Taylor and Francis,* Vol. 11 (3), pp. 545–566.

Strauss, A., and Corbin, J. (1998), Basics of qualitative research: Techniques and procedures or developing grounded theory. Thousand Oaks, CA: Sage.

Subaryani, S., Zainol, B., Suhaily, A., Samsuri, B., Rahimah, T., Tunku, B., and Jie, S. J. (2017), Determinants of Computer Assisted Audit Techniques (CAATTs). *European Journal of Business and Social Sciences,* Vol. 6(2), pp. 135–150.

Sun, C. (2012), From CAATTs Adoption to Continuous Auditing Systems Implementation: An Analysis Based on Organisational Routines Theories, *MIS Review* Vol. 17 (2), pp. 59-85.

Sun, Y. and Davidson, I. (2015), Influential factors of online fraud occurrence in retailing banking sectors from a global prospective, *Information and Computer Security*, Vol. 23 (1), pp. 3 – 19.

Symon, G. and Cassell, C. (2012), Qualitative Organisational Research. Core Methods and Current Challenges. London: Sage.

Tabachnick, B.G., and Fidell, L.S. (2013), Using Multivariate Statistics, 6th Edition, London, Pearson.

Taherdoost, H., Sahibuddin, S., and Jalaliyoon, N. (2004), Exploratory Factor Analysis ; Concepts and Theory 2 Factor Analysis 3 Types of Factor Analysis 4 Exploratory Factor Analyses. *Advances in Applied and Pure Mathematics,* 375–382.

Tan, K. S., Chong, S. C., Uchenna, B. L., and Eze, C. (2010), Internet-Based ICT Adoption among SMEs: Demographic Versus Benefits, Barriers, and Adoption Intention, *Journal of Enterprise Information Management*, Vol. 23 (1), pp. 27-55.

Tanzania e-government strategy (2013), United Republic of Tanzania President's Office – Public Service management.

Tanzania Investments Centre (2015), How to Invest in Tanzania. Available at: http://www.tanzania-gov.de/investment/investing-in-tz/.[accessedon [20/12/2015]

Tanzania National Bureau of Statistics (2014), Ministry of Finance, June, (2014), Accessed at http://www.nbs.go.tz/takwimu/references/Tanzania_in_figures2012.pdf. [Accessed on 15/12/2016].

Tanzania Revenue Authority, (2014), VAT Tax Act, Laws of Tanzania, Dar es Salaam, Government of Tanzania.

Tanzanian National ICT Policy. (2003), National ICT Policy. Dar Es Salaam: The Government of Tanzania.

Tashakkori, A., and Creswell, J. W. (2007). Developing publishable mixed methods manuscripts. *Journal of Mixed Methods,Research,* Vol. 1, pp. 107-111.

Tashakkori, A., and Teddlie, C. (1998), Mixed methodology: Combining qualitative and quantitative approaches, Thousand Oaks, CA: Sage.

Tatiana M, Azzali S, and Fornaciary L (2014). Audit Quality of Outsources Information Technology Controls. *Managerial Auditing Journal* Vol.29 (9), pp. 837-862.

Taylor, S. & Todd, P. A. (1995), 'Understanding information technology usage: A test of competing models', Information Systems Research, Vol. 6,(2), pp. 144–176.

TCRA (2015), Tanzania Communication and Regulatory Authority Quarterly Telecom Statistics,.http://www.tcra.go.tz/images/documents/telecommunication/telecomStats [Accessed on 30/03/ 2016].

Teddlie, C., and Yu, F. (2007), Mixed methods sampling: A typology with examples. *Journal of Mixed Methods Research,* Vo. 1, pp. 77-100.

Thorpe, R., and Holt, R. (2008), The Sage Dictionary of Qualitative Management Research. Sage.

Tornatzky, L.G., and Fleischer, M (1990), The Processes of Technological Innovation. Lexington Books, Lexington, Massachusetts.

TPSF (2014), Tanzania Private Sector Foundation Chairman's Progress Report for the Year 2013/14report; Available on http://tpsftz.org/. [Accessed on 20/12/2015].

Tracy. S. J. (2010), Qualitative Quality: Big Tent. Criteria for Excellent Qualitative Research. *Sage Journals.* Vol. 16 (10) pp. 837-851.

Tum, K. (2013), Continuous Audit: From the concept towards the implementation, *International Journal of Business and Social Research (IJBSR),* Vol.3 (7), pp.1-7.

Tumi, A. (2013), An Investigative Study into the Perceived Factors Precluding Auditors Form Using CAATS and CA. International Conference for Advanced Research In Business Dubai, 1st December 2013, pp. 1–87.

Van-Raaij, E.M and Schepers., J.J.L. (2008), The Acceptance and Use of a Virtual Learning Environment in China, *Computers and Education*, Vol. 50 (3), pp. 838-852.

Van-Vlasselaer, V., Bravo, C., Caelen, O.C., Eliassi-Radd, T., and Akoglue, L. (2015), APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions, Decision Support Systems, Vol. 75, pp. 38–48.

Vasarhelyi, M. A., Alles, M., Kuenkaikaew, S., and Littley, J., (2012), The acceptance and adoption of continuous auditing by internal auditors: A micro analysis, *International Journal of Accounting Information Systems* Vol. 13, pp. 267–281.

Vasarhelyi, M. A., and Halper, F. B. (1991). "The continuous audit of online systems," *Auditing: A Journal of Practice and Theory*, Vol. 10(1), pp. 110–125.

Vasarhelyi, M. A., and Romero, S. (2014), Technology in audit engagements: a case study, *Managerial Auditing Journal,* Vol. 29 (4) pp. 350 – 365.

Vasarhelyi, M. A., Teeter, R. A., and Krahel, J. P. (2010), Audit education and the real-time economy. *Issues in Accounting Education*, Vol.*25*(3), pp.405–423.

Vasarhelyi, M.A., Alles, M., Kuenkaikaew, S., and Littley, J. (2012), The acceptance and adoption of continuous auditing by internal auditors: A micro analysis, *International Journal of Accounting Information Systems*, Vol.13, pp.267–281.

Velte, P. (2017). What do we know about empirical joint audit research ? A literature review, *Accounting and Finacial Control,* Vol. 1(1) pp. 1-12.

Vendrzyk, V. P and Bagranoff, N. A., (2003), The Evolving Role of Information System Audit: A Field Study Comparing the Perceptions of Information System and Financial Auditors. *Advances in Accounting*, Vol. 20, pp.141–163.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003), User acceptance of information technology: toward a unified view, *MIS Quarterly,* Vol. 27 (3), pp. 425-478.

Venkatesh, V., Thong, J.Y.L. and Xu, X. (2012), Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology, *MIS Quarterly,* Vol. 36 (1), pp. 157-178.

Vicente, M.R., and López, A. J. (2009), To what extent firms are using e-commerce? some evidence for the EU-27. ftp://ftp.zew.de/pub/zewdocs/veranstaltungen/ICT2009/papers/Vicente.pdf.

Vîlsănoiu, D. and Şerban, M., (2010), Changing Methodologies in Financial Audit and Their Impact on Information Systems Audit, *Journal of Information Systems,* Vol. 4 (1), pp. 57-65.

Wan, N. S. Wan, I., and Ali, A. (2013), Conceptual Model for Examining the Factors That Influence the Likelihood of Computerised Accounting Information System (CAIS) Adoption among Malaysian SMEs. *International Journal of Information Technology and Business Management* Vol.15 (1), pp.235-247.

Wehner, D., M. H. and Jessup, C.M. (2005), Factors Affecting Generalized Audit Software Usage. In: AAA Midwest Accounting Meeting. St. Louis Missouri.

Welsh, E. (2000), Dealing with Data: Using NVivo in the Qualitative Data Analysis Process./www.qualitative-research.net/index.php/fqs/article/view/865 [Accessed on 15/05/ 2015].

Whitten, J. L., Bentley, L. D. and Dittman, K. C (2008), Systems Analysis and Design Method. 5th Edition, New York, Mcgraw-Hill Higher Education.

Widuri, R., O'Connell, B., and Yapa, P W.S. (2016), Adopting generalized audit software: an Indonesian perspective, *Managerial Auditing Journal*, Vol. 31 (8/9), pp.821-847.

Widuri, R., O'Connell, B., and Yapa, P. W.S. (2014), Adoption and use of generalized audit software by Indonesian audit firms: some preliminary findings, Paper presented at the 4th Annual International Conference on Accounting and Finance, Singapore.

Willborn, W.W. (1989), Quality audits and technological excellence, *International Journal of Quality and Reliability Management,* Vol. 6 (4), pp. 19-26.

Wolf, E. J., Harrington, K. M., Clark, S. L., and Miller, M. W. (2013), Sample Size Requirements for Structural Equation Models: An Evaluation of Power, Bias, and Solution Propriety, *Journal of Educational and Psychological Measurement,* Vol. 73(6), pp. 913–934

World Bank (2005) Tanzania : Accounting and Auditing. Washington, DC. © World Bank. https://openknowledge.worldbank.org/handle/10986/8442 License: CC BY 3.0 IGO."

Wyden, R. (1995), "Requiring Auditors Who Really Audit: A Decade After the Darkest Days of the S&L Collapse, the Financial Fraud Detection and Disclosure Act will Answer the Questions: Where Were the Accountants and Why Didn't They Speak Up? It will Also Put Well Armed Auditors Back Where They Belong." Roll Call (March 27).

Yin, R. K. (2009), Case Study Research: Design and Methods (4th ed., p. 240). California: Sage Publications.

Yirrell, S. (2007), Fraud explodes in 2006, The Accountancy Age, www.accountacyage.com/2173741. [Accessed on31/01/2016].

Yong, A. G., and Pearce, S. (2013), A Beginner's Guide to Factor Analysis : Focusing on Exploratory Factor Analysis. *Tutorials in Quantitative Methods for Psychology,* Vol.9(2), pp. 79–94.

Yuan, Y., Gretzel, U., and Fesenmaier, D. R. (2003), Internet technology use by American convention and visitors bureaus. Journal of Travel Research, Vol. 41, pp. 240-255.

Zainudin, A. (2012), Research Methodology and Data Analysia (2nd Ed.). Shah Alam, Selangor Malaysia: Universiti Teknologi MARA Press.

Zamalia, M. (2008), Handbook of Research Methodology: A Simplified Version. Shah Alam, Selangor Malaysia: University Publication Centre (UPENA) UiTM.

Zareapoor, M., Seeja, K. and Alam, M.A. (2012), Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria., *International Journal of Computer Applications* Vol. 52 (3), pp.34-41.

Zhu, K., and Kraemer, K.L. (2005), Post-adoption variations in usage and value of e-business by organisations: cross-country evidence from the retail industry. *Information Systems Research,* Vol. 16, (1), pp. 61-84.

Zhu, K., Kraemer, K.L., and Xu, S. (2006), The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business, Journal of *Management Science,* Vol.52 (10), pp. 1557-1576.

Zhuang, Y., and Lederer, A.L. (2006), A resource-based view of electronic commerce. J*ournal of Information and Management,* Vol. 43, pp. 251-261.

APPENDICES

Appendix I: Summary of Theoretical Review of Literature

Appendix 1A: Theoretical literature from the developed world

Year	Author	Model used	Nature of the study	Methodology	Target Audience	Findings
2015	Pedrosa, Costa and Laureano	Factors motivating the use of CAATTs by statutory auditors in Portugal	UTAUT	Survey	External Auditors	Performance expectancy was the main motivation to use CAATTs while IT skills and training on software were the main barriers to CAATTs adoption
2014	Mahzan and Lymer	Factors influencing CAATTs adoption	UTAUT	Interview-qualitative-study-UK andMalaysia	Internal Auditors (executives)10 organisations	Performance expectancy and Facilitating condition were supportive predictors of information systems But Effort expectancy and Social influence were not strongly supported. Furthermore, experience and voluntariness did not moderate effort expectancy and Social Influence.
2014	Curtis and Payne	The auditor decision of utilizing CAATTs in auditing	UTAUT	Survey +case study for the last factor (budgetary pressure)	75 External auditors (Big4)	Firms with long term budget strategies are more likely to adopt CAATTs in auditing as compared to firms with short term strategies.
2014	Ahmi et al.,	The adoption of CAATTs by internal auditors in government departments in Malaysia	TOE	Survey	Not 460	A proposed model ready for use
2013	Razi and Madani	Factors influencing the adoption of information systems auditing	TAM	Survey	227 Internal auditors	Perceived benefits and organisational readiness were the strongest predictors. External influence had no influence on the use of audit software in auditing
2012	Stoel et al.,	Attributes that impact the quality of IT audit	ITAQ Model	Survey	Internal Auditors	IT audit quality is a function of: audit organisation, client organisation, target process, process methodology, audit personnel and audit organisation (from ITAQ model) in addition to auditor independence and audit process methodology.
2013	Ahmi and Kent	Factors influencing adoption of GAS by external auditors in the UK	Information Technology Audit Quality (ITAQ) factors	Survey	205 External Auditors	GAS adoption was influences by job relevance, cost and resources, technology infrastructure, auditor's knowledge and

						experience and support from the management. Client factors related to IT and e-business complexity also influenced significantly.
2012	Varsahely et al.	Investigating the status of CA acceptance by internal auditors	TAM	Interview: Case study	10 Internal audit mangers in 10 organisations	Management support and employees knowledge of information systems highly influencing the use of CA by internal auditors. There was a big difference in the installation of information systems among companies Four stages of CA adopters: traditional stage, emerging CA, maturity and full CA. Most companies were in traditional and emerging stages.
2012	Gonzalez, Sharma and Galletta	The antecedents of the use of continuous auditing	UTAUT	Survey	210 Internal Auditors	EE (easy to use) and social influence (organisational related factors) were the strongest predictors for auditors to use CA. Voluntariness and annual sales were significant moderators of social influence and performance expectancy respectively.
2012	Sun	From CAATTs Adoption to Continuous Auditing Systems Implementation	Organisational Routine Theory	Interview-Case study to one organisation that adopted CAATTs for three years	12-personel executives, auditors, IT staff and Managers	Collaborative learning highly influence the use of CAATTAs by auditors Specialised knowledge skills was the main barrier for auditors effective use of CAATTs
2010	Diaz and Loraaz	Investigating the post adoption behaviour of technology by internal auditors	UTAUT	Interview	Auditor Interns	Efforts expectancy (easy to use) strongly affected the learning process of the audit interns. As features became more complex, it in turn affected other factors such as budgetary pressure, social influence and efforts expectancy.
2009	Janvrin et al.,	Factors influencing acceptance of CAATTs by auditors	UTAUT	Survey	External auditors-Big4 +small and medium firms combined	Performance expectancy (perceived usefulness) and facilitating condition strongly impacted external auditors use of technology in auditing Auditor training in the use of CAATTs could results into effective future adoption
2009	Kim, Mannino	Impact of technology	TAM	Survey	185 Internal auditors	The results found that technology complexity

	and Nieschwietz	features and complexity on auditors acceptance of information systems				features strongly influence on adoption decisions. The basic features like database queries, ratio analysis, and audit sampling were more accepted by internal auditors while the advanced features like digital analysis, regression/ANOVA, are less accepted by internal auditors
2008	Havelka and Merhout	Attributes that constitutes information technology audit quality	Technology Task Fit	Survey	Internal Auditors	IT audit quality is a function of: audit organisation, client organisation, target process, process methodology, audit personnel and audit organisation
2008	Curtis and Payne	Examining contextual and individual Factors Affecting Technology Implementation Decisions in Auditing	UTAUT	Survey	181 internal auditors	Firms have the ability to influence the implementation of new technology through longer-term budget plans. individual perception in risk aversion and budgetary pressure significantly influence decisions to implement technology
2008	Mahzan and Lymer	Factors influencing the Adoption of CAATTs by Internal Auditors in the UK	UTAUT	Survey	95 Internal Auditors	Internal auditors' use of CAATTs is very high, particularly GAS. Employees' training and compatibility of software within the department highly influenced the adoption of software. Absence of motivation to use CAATTs, enactment of best practices, performance measurement criteria and IT challenges are the barriers to successful CAATTs adoption
2005	Wehner and Jessup	Factors Affecting the usage of GAS software by auditors	UTAUT	Survey	Both Internal +external auditors (71 in total sample)	Auditor Training in software positively impact GAS usage. Female auditors used GAS software often than males. Experience is positively related to GAS usage, Senior auditors used GAS more than audit managers.

Appendix I-B: Theoretical literature from developing countries

Year	Author	Country	Topic	Model	Findings
2016	Widuri, O'Connel & Yapa	Indonesia	Adopting generalized audit software: an Indonesian perspective",	TOE (EA)	Environmental factors highly influenced GAS usage such as availability of IT-skills, clients' related factors, support from professional regulatory authority and availability of GAS in many languages.
2016	Mansour,	Jordan	Factors Affecting the Adoption of CAATTs	UTAUT (EA)	Performance expectancy and firm's facilitating conditions influenced CAATTs adoption decision
2016	Kim, Kotb & Eldaly	Egypt	The use of GAS by Egyptian external auditors	TAM (EA)	-Perceived ease of use has a stronger effect on GAS use -Use of GAS is more affected by co-worker, supervisor, or organization through perceived usefulness, but not by job relevance, output quality, and result demonstration
2016	Lal &Bharadwaj	India	Understanding the impact of cloud-based services adoption on organizational flexibility	Company Executives	-The data revealed that cloud-based services provide relative advantage in terms of scalability, accessibility, and on-demand deployment of services within no time. -Easy to use interface, experience, and expertise of the cloud service provider as well as support from top management plays important role in the cloud adoption decision.
2015	El-Sood, Kotb &Allam	Egypt	Exploring auditors' Perceptions of the Usage and importance of IT audit tools	EA	-The findings reflect the highly perceived importance of using audit technology in technical and administrative procedures, specifically to assess risk -The importance of audit technology is relatively higher for those in Big 4 firms, with less years of auditor experience and higher auditor technology expertise
2014	Ahmi , Saidin & Abdullah	Malaysia	IT adoption by internal auditors in public sector: A conceptual study	TOE (IA)	Proposed a combination of external factors, organisational factors and technology factors to influence CAATTs adoption.
2014	Lotto	Tanzania	Examining the impact of IT on internal auditing effectiveness in Tanzanian organizations	Nil (IA)	The finding reveal that the internal audit profession lags behind in effective use of IT to support their duties factors, which contributed to the hindrance in IT usage include lack of top management support as a critical problem , inadequate training programs, lack of involvement in IT development, poor budgetary to the internal audit department
2013	Rosli et al.	Malaysia	Factors Influencing Audit Technology Acceptance by Audit Firms	I-TOE (EA)	The study predicts a potential influence to come from organisational, individual, environmental and technological related factors.
2013	Razi & Madani	Saudi Arabia	An analysis of attributes that impact adoption of audit software	Nil (IA)	External pressure has no impact on the adoption decision Organisational Readiness and Perceived Benefits are reasonably good predictors of Adoption Intention of audit software.

2013	Ebimobowei et al	Nigeria	Auditors' Usage of Computer Assisted Audit Tools and Techniques	UTAUT (EA)	The result revealed that performance expectancy, effort expectancy, facilitating conditions and social influence were positively associated to CAATTs usage
2013	Nugi	Botswana	State of IT Auditing in Botswana	Nil (Companies +Government)	-e-government is increasing faster compared to business sector -e-learning is increasing -IT auditing is still low -IT auditing is facing challenges such as human capital, policy &education
2011	Moorthy et al.,	Malaysia	The impact of IT on internal Auditing	NiI (IA)	-IT affects internal control (control environment, risk assessment, control activities, information and comm and monitoring) -Auditor has responsibility to assure the governance level of management understand IT risks and the liabilities potentially transferred to board members.
2011	Lin & Wang	Taiwan	A selection model for auditing software	Nil (IA)	Most influential factors for systems usage were system functions, data processing, and technical support from vendors. The most important factor for selection of auditing software is cost and system stability, data processing accuracy, technical support and purchase cost
2008	Huang	Taiwan	Determinants of CAATTs adoption by internal auditors	TAM (IA)	Reasons related to high cost of implementation and long-learning curves, highly affected a low usage of GAS among internal auditors.
2003	Al-Fehaid	Saudi Arabia	An investigation of the influence of information technology on audit risk	Nil (IA + EA)	The findings revealed that the adoption of IT-based accounting systems by clients of audit firms in SA has contributed to a possible increase in audit risk due to insufficient training among clients staff and incompetence in IT audit in some of the audit firms.

Note EA = External Auditors, IA = Internal Auditors.

Appendix II: Relevant Technology in Auditing

Technology	Definition
1. Word Processing	Computer program that facilitates entry and preparation of documents such as letters or reports.
2. Electronic Spreadsheets	Software which allows the auditor to enter either alphanumeric or numeric data and manipulate it either via standard functions or auditor programmed functions
3. E-Mail	Exchange of mail messages via Intranets and/or the Internet.
4. Electronic Working Papers	Software which generates a trial balance, lead schedules, and other schedules useful for the recording of evidence in an audit or assurance engagement
5. Internet Search and Retrieval	Permits user to search text that is in electronic format and retrieve, view, and print desired text.
6. Image Processing	Conversion of paper documents into electronic form through scanning and the subsequent storage and retrieval of the electronic image

7. Electronic Presentations	Software that facilitates the organisation and use of text, voice, and/or images to communicate concepts
8. Generalized Audit Software	Computer program which helps the auditor access client computer data files, extract relevant data, and perform some audit function such as addition or comparison.
9. Expert Systems	Computer software that provides relevant information and/or decision models to assist a human in making a decision or accomplishing some task.
10. Embedded Audit Modules	Programmed routines incorporated into an application program which are designed to perform an audit function
11. Real-time Audit Modules	Programmed routines incorporated into an application program which are designed to perform an audit function
12. Database Search and Retrieval	Software that uses relational structures between data files and facilitates varying data retrieval and use.
13. Simulation Software	Abstraction of some aspect of real system via software. Auditor may use model to evaluate the reliability of information from real world sources. This may be thought of as a very high level analytical review of a company's data.
14. Flowcharting/Data Modelling	Software using the source code version of programs to produce flowcharts of program logic
15. Computer Aided Systems Engineering Tools	Integrated package of computer tools that automate important aspects of the software development process to increase software development effectiveness in terms of productivity of systems development and quality of developed systems.

16. Encryption Software	Changing data using some type of encoding/decoding algorithm so that unauthorized persons who can access the encrypted data will not be able to read it or use it.
17. Groupware	Software that permits auditors to categorize, store, and share data among themselves as well as communicate with each other about that data, preferably in a real-time mode.
18. Cooperative Client/Server Environment	Distribution of processing functions between two or more computers as in a local area network. This also includes end-user computing where users on the network also process and store data on their personal computers.
19. Workflow Technology	Software and hardware that facilitates the capture of data in the work place to improve management of the business. For example, using an electronic scanner to record the movement of materials in a warehouse based on the barcodes on the materials.
20. Database Design and Installation	Software that permits the creation and use of relational structures between data files
21. Time Management and Billing Systems	Computer program, which assists in capturing, managing, billing, and reporting time, spent on professional activities.
22. Test Data	A set of transactions processed by the auditor to test the programmed or procedural operations of a computer application
23. Small Business Accounting Software	Accounting software package used to record transactions, maintain general and subsidiary ledgers, and generate financial statements.
24. Digital Communications	Bandwidth – telecommunications devices used to facilitate the rapid and unfettered transfer of data.
25. Tax Return Preparation Software	Software, perhaps incorporating expert knowledge, which assists the accountant/auditor in identifying relevant information, capturing and recording it in a manner that can be filed with tax authorities.
26. Firewall Software/Hardware	Part of "security technology" that enforces an access control policy between two networks.
27. User Authentication Systems	Devices used to verify that a system user is who he/she claims to be.

28. EDI-Traditional	Transfer of data or payments electronically between computers using software that may, or may not, require human intervention to affect the transfer.
29. EDI-Web Based	The extension to XML-based EDI
30. Wireless Communications	The ability to transfer digital data without the use of cables, twisted- pair, or fibre optics.
31. Agent Technologies	Programmed modules that are given certain levels of authority and autonomy to act on behalf of their "supervisor", such as to decide whether to order more inventory and from which supplier
32. Intrusion Detection and Monitoring	Part of "security technology" that identifies unauthorized requests for services
33. Internal Network Configurations	Linkage of individuals and data through hardware and software systems that permit the exchange of various types of data.
34. External Network Configurations	Intranet, extranet, and Internet access devices than enable users physically separated from the server to access it.
35. Enterprise Resource Planning	Business-wide information systems that cross boundaries
36. Application Service Providers	Companies which host (provide hardware, software and connectivity) for specific business applications

Source: Greenstein-Prosch et al. (2008)

Appendix III: Various E-fraud Detected through Data Mining Techniques

Author	Technique Used	Application Area	Detection	Prevention
Bermudez et al. (2008)	Skewed Logic Link Bayesian Analyses	Automobile Insurance Fraud	Detection and	
Brockett et al. (1998)	Kohonen's Self-Organizing Map Fraud	Automobile Insurance	Detection	
Brockett et al., (2002)	Principal Component Analysis	Automobile Insurance Fraud	Detection	
Derrig and Ostaszewski, (1995) Fraud	Fuzzy set theory	Automobile Insurance	Detection	
Kim and Kwon, (2006)	Insurance Fraud Recognition System (Korea)	Insurance Fraud	Detection	
Major and Riedinger (2002)	Electronic Fraud Detection (EFD) Fraud	Health Care Insurance	Detection	
Phua et al. (2005)	Meta-classifiers	Automobile Insurance Fraud	Detection	
Viaene et al. (2005)	Bayesian Neural Network Fraud	Automobile Insurance	Detection	
Viaene et al.(2007)	Logistics Regression	Automobile Insurance Fraud	Detection	
Yang and Hwang (2006)	Frequent Pattern Mining Fraud	Health Care Insurance	Detection	
Pathak et al. (2003)	Fuzzy Logic based expert system	Insurance Fraud	Detection	
He et al. (1997)	Neural Network	Health care insurance fraud	Detection	
He et al. (1997)	Kohonen's Self-Organizing Map Fraud	Health Care Insurance	Detection	
Bolton and Hand (2002)	Peer Group Analysis and Break point Analysis	Credit Card Fraud	Detection	
Juszczak et al. (2008)	Many different classification techniques	Credit Card Fraud	Detection	
Maes et al. (2002)	Bayesian Belief network	Credit Card Fraud	Detection	
Sanchez et al. (2008)	Fuzzy rules	Credit Card Fraud	Detection	Prevention

Stolfo et al. (2000)	Meta-classifiers	Credit Card Fraud and Intrusion	Detection	
Brause et al.,(1999)	Rules and Neural Network	Credit Card Fraud	Detection	
Dorronsoro et al. (1997)	Neural Network	Credit Card Fraud	Detection	
Fan(2004)	Decision Tree	Credit Card Fraud	Detection	
Bonchi et al. (1999)	Decision Tree	Fiscal Fraud	Detection	
Deshmukh and Talluru (1998)	Rule-based Fuzzy Reasoning System	Financial Statement Fraud	Detection	
Fanning and Cogger (1998)	Neural Network	Financial Statement Fraud	Detection	
Hoogs et al. (2007)	A Genetic Algorithm Approach	Credit Card Fraud	Detection	
Kirkos et al. (2007)	Neural Network and Bayesian Belief Network	Financial Statement fraud	Detection	
Lin et al. (2003)	Fuzzy Neural Network	Financial Statement Fraud	Detection	
Green and Choi (1997)	Neural Networks	Financial Statement Fraud	Detection	
Estevez et al. (2006)	Fuzzy Rules and Neural Network Fraud	Telecommunications	Detection	Prevention

Source: Jans et al. (2009)

Appendix IV Questionnaire

Nottingham University Business School

Dear Prof./Dr./Mr./Mrs/Ms,
Habari za kazi/Greetings!

Thank you for accepting to participate in the research project. Your participation in this research is voluntary, and you may change your mind about being involved in the research at any time, and without giving a reason.

My name is Asha Baleche Katamba, a PhD student at the Nottingham University of Nottingham Malaysia campus. This is a self-funded research which may attract interest to a varied group of people including auditors, audit firms and audit stakeholders such as clients and the regulatory authorities.

In general, the research is about the increasing complexities on electronic business platforms among audit clients in using technologies to effect business transactions. In such platforms of processing and storing information, there have been reported increased risk of electronic fraud where internal or external system experts are likely to be involved. In order to understand the mechanisms to detect, prevent and curb such fraud, the study investigates the current extent use of technology by external auditors and their perceived benefits of technology for risk assessment purposes. The responses obtained, will help the study to develop a theoretical model that will address opportunities and challenges in technology adoption in the external audit environment.

Kindly complete the attached field survey which may take about 10-15 minutes of your time. Your response will be anonymous and treated in the strictest confidence. The input collected is very important in getting the accurate findings which will reflect the actual scenario of your organisation. There is no right or wrong answer and information derived from this questionnaire will be used for research purposes only and will not be shared with any other parties or organisation. The aim of this research is to produce a PhD thesis in which some part of it could be submitted for publication in academic journals.

In case of any questions or complaints related to this survey, please do not hesitate to contact me on my details below; or my supervisors: Associate Prof Dr. Angelina Yee Seow Voon at Angelina.yee@nottingham.edy.my or Dr. How Shi Min at shi.min@nottingham.edu.my

Alternatively, you may wish to contact the Nottingham University Business School directly on the email: nubs-rec@nottingham.edu.my

Thank you for your participation.

Yours Sincerely,

Asha Baleche Katamba
PhD Student
Nottingham University Business School
University of Nottingham Malaysia Campus
Email: ksyx4ait@nottigham.edu.my
Phone: +255-713-377883

SECTION A: PERSONAL PROFILE

[1] What is your gender?

- ☐ Female
- ☐ Male

[2] Please specify your age group:

- ☐ 18-24 years
- ☐ 25-34 years
- ☐ 35-44 years
- ☐ 45-54 years
- ☐ 55 years and above

[3] What is your current position in the firm?

- ☐ Partner/director
- ☐ Audit Manager
- ☐ Senior Auditor
- ☐ Junior Auditor

[4] How many years have you been in the firm?

- ☐ 0-5 years
- ☐ 6-10 years
- ☐ 11-15 years
- ☐ 16-20 years
- ☐ 21 years and above

[5] How many years of experience do you have in auditing?

- ☐ 0-5 years
- ☐ 6-10 years
- ☐ 11-15 years
- ☐ 16-20 years
- ☐ 21 years and above

[6] How many years of experience do you have in computerised auditing?

- ☐ None
- ☐ 0-5 years
- ☐ 6-10 years
- ☐ 11-15 years
- ☐ Above 15 years

[7] How do you rate your overall Information Technology (IT) skills?

- ☐ Very Good
- ☐ Good
- ☐ Adequate
- ☐ Basic
- ☐ Very basic

[8] I consider myself more as

- ☐ IT Auditor
- ☐ Financial Auditor
- ☐ Other……

[9] College education level

- ☐ Diploma
- ☐ Degree
- ☐ Master
- ☐ PhD
- ☐ Other.....

[10] Professional Certification(s) (Tick as many boxes as are applicable)

- ☐ Certified Internal Auditor (CIA)
- ☐ Certified Public Accountant (CPA)
- ☐ Certified Information System Auditor (CISA)
- ☐ Chartered Certified Accountant (ACCA)
- ☐ Certified Management Accountant (CIMA)
- ☐ Certified Financial Examiner (CFE)
- ☐ Certified Financial Planner (CFP)
- ☐ Other:…….

SECTION B: ORGANISATION PROFILE

[11] When was your firm established? Please specify the year……

[12] Category of Firm: Please choose only one of the following:

- ☐ Large
- ☐ Medium
- ☐ Small

SECTION C: USE OF INFORMATION SYSTEMS

[13] Do you use Information Systems (any computer application) in your audit tasks?

- ☐ Yes
- ☐ No

(If your answer is 'Yes' please continue to question 14; *but if your answer is 'No' please continue to question 17)*

[14] For how many years has your organisation implemented Information Systems?

- ☐ I don't know
- ☐ Less than 2 years
- ☐ 2 to 5 years
- ☐ More than 5 years

[15] Is the use of information systems in your organisation mandatory?

- ☐ Yes
- ☐ No

[15] If you use Information Systems, which of the following products do you currently use?

(Please tick all that apply-multiple choices are allowed)

- ☐ Microsoft Excel
- ☐ Audit Command Language (ACL)
- ☐ Case ware
- ☐ Pro-Audit
- ☐ IDEA
- ☐ Active Data
- ☐ Top CAATTs
- ☐ SAS
- ☐ In-house software
- ☐ Any other……

[16] In general terms, how can you rate the benefits of using information systems? Please choose the appropriate response for each item

Benefits	**Strongly Disagree[1)**	**Disagree [2]**	**Don't Know [3]**	**Agree [4]**	Strongly Agree[5]
To reduce errors					
Reduced manual computations					
Saving in efforts and time					
Simplified retrieval of clients records					
Simplified preparation of working papers					
Improved data monitoring					
Enhanced information sharing					
Easy to identify fraud					
Improved responses to risk					

[17] Please indicate the degree to which you agree with the following factors in influencing you to use Information Systems.

17A	**Performance Expectancy: Is the expected increased efficiency from using technology**	**Strongly Disagree[1]**	**Disagree[2]**	**Neutral[3]**	**Agree[4]**	**Strongly Agree[5]**
PE1	I would find information system useful in my job					
PE2	Using information systems would enable me to accomplish task more quickly					
PE3	Using information systems would increase my productivity					
PE4	If I use information systems I would increase my chances of getting a raised pay					
PE5	Using information systems would reduce the time I spend on unproductive activities					
PE6	I think using information systems fits well with the way I like to work					

17B	**Effort Expectancy: Is the expected degree of ease in using technology**	**Strongly Disagree[1]**	**Disagree[2]**	**Neutral[3]**	**Agree[4]**	**Strongly Agree[5]**
EE1	My interaction with the system would be clear and understandable					
EE2	It would be easy for me to become skilful at using information systems					
EE3	I would find information systems easy to use					
EE4	Learning to operate the system would be easy for me					
EE5	Auditing using the systems would require a lot of					

	my mental efforts					

17C	Social and organisational influence: Is the influence from co-workers and management in using technology	Strongly Disagree[1]	Disagree[2]	Neutral[3]	Agree[4]	Strongly Agree[5]
SOI1	People who influence my evaluation think that I should use information systems					
SOI2	People who are important to my career think that I should use information systems					
SOI3	The senior management of my firm will be helpful in the use of information systems					
SIO4	In general, the organisation will likely support using information systems					
SOI5	People in my organisation who use information systems have more prestige than those who do not					

17D	Facilitating Condition: How you believe there is availability of resources to use technology	Strongly Disagree[1]	Disagree[2]	Neutral[3]	Agree[4]	Strongly Agree[5]
FC1	There are available budget resources necessary to use information systems					
FC2	There is availability of up to date IT infrastructure within the organisation					
FC3	Information systems may be compatible with clients' systems					
FC4	A specific IT person (or group) would be available for assistance with system difficulties					
FC5	Sufficient training in information systems auditing has been provided regularly.					

17E	Client Factors: factors related to the client's context that would influence you to use technology	Strongly Disagree[1]	Disagree[2]	Neutral[3]	Agree[4]	Strongly Agree[5]
CF1	The average clients' IT environment is complex					
CF2	The average clients' business environment is complex					
CF3	The average size of clients' business is large					
CF4	Most of our clients are not concerned about data security					
CF5	The average clients do not have strong internal control systems in place.					
CF6	The average level of audit risk is high					

17F	Audit Professional Factors: Factors related to the audit authority and professionalism	Strongly Disagree[1]	Disagree[2]	Neutral[3]	Agree[4]	Strongly Agree[5]
AP1	The National Board of Accountants and Auditors encourages me to use of information systems					
AP2	I use information system as an act of accountability					
AP3	I use information systems as there is available audit methodology to follow					

17G	BI – Behavioural intentions to increase the use of information systems.	Strongly Disagree[1]	Disagree[2]	Neutral[3]	Agree[4]	Strongly Agree[5]
BI1	I intend to increase the use of information					

	systems in the next 5 years					
BI2	I would recommend the firm to increase the use of information systems in future					
BI3	I predict the organisation will increase the use information systems in the future					

Appendix V: Interview Guide

(A) Auditor Demographic questions

1. Please tell me about yourself, your position, qualification, work experience and nature of audit tasks that you do? How long have you been working with this organisation?

(B) Information Systems usage by External Auditors

2. What are the main computer software do you use for audit purposes?

3. What are the benefits and limitation derived from the use of information systems in auditing?

4. What decisions necessitated you to use one audit software over the other? Are there some audit tasks that are left to be done manually?

(C) Information Systems and risk assessment of e-fraud

5. How do you currently assess risk of electronic fraud to your computerised clients?

6. What potential impacts does the use of information systems have in risk assessment of e-fraud? Do you think fraud has reduced after using technology in auditing?

7. What types of frauds have you detected through the use technologies, would you mind if I ask?

8. Have you been using continuous auditing or/forensic audits/ investigative auditing? What impact does it have on e-fraud detection?

9. What do you think should be done in order to improve risk assessment and detection of electronic fraud?

(D) Impact of Information systems on Audit Process

10. Apart from using IS tools and techniques for control purposes, what other impact(s) does the usage have on the audit process?

Factors influencing the use of information systems

11. What propelled your audit firm to start using technology in auditing? How many years ago?

12. Do you (or your organisation) intend to increase the use of information systems in future, let say in the next five years? Please explain why you think so.

Other: Clients' business complexity and technology usage

13. How do you view the current level of technology usage by your clients' (such as e-business integration) in relation to a change in external audit procedures in your organisation?

Appendix VI: Normality Tests

	N	Mean	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
PE1	106	1.54	-2.129	.025	1.677	.046
PE2	106	1.35	-1.687	.025	1.230	.046
PE3	106	2.08	-1.374	.025	1.886	.046
PE4	106	2.34	-1.802	.025	1.308	.046
PE5	106	1.62	-2.149	.025	2.118	.046
PE6	106	1.39	-1.830	.025	2.491	.046
EE1	106	1.43	.270	.025	-1.961	.046
EE2	106	1.82	-.694	.025	-1.210	.046
EE3	106	1.48	-1.240	.025	2.105	.046
EE4	106	1.56	-.231	.025	-1.984	.046
EE5	106	1.49	-1.712	.025	1.906	.046
SI1	106	1.26	-.868	.025	1.269	.046
SI2	106	1.40	-.365	.025	-1.471	.046
SI3	106	0.51	-.038	.025	-2.037	.046
SI4	106	1.37	-.130	.025	-1.199	.046
SI5	106	1.37	-1.593	.025	2.412	.046
FC1	106	1.35	-1.490	.025	2.033	.046
FC2	106	1.40	-.111	.025	-1.961	.046
FC3	106	1.32	-1.254	.025	2.209	.046
FC4	106	1.36	.599	.025	1.674	.046
FC5	106	1.38	1.420	.025	2.183	.046
CF1	106	1.80	.344	.025	1.342	.046
CF2	106	2.35	.306	.025	1.320	.046
CF3	106	2.46	-.048	.025	1.634	.046
CF4	106	2.38	-.312	.025	1.092	.046
CF5	106	2.40	2.608	.025	1.173	.046
CF6	106	2.08	1.357	.025	2.058	.046
APF1	106	1.04	-1.867	.025	1.730	.046
APF2	106	1.02	-1.589	.025	2.023	.046
APF3	106	1.78	-1.374	.025	1.168	.046
Valid N (listwise)	106					

Appendix VII: Total Variance Explained

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	8.467	29.196	29.196	8.467	29.196	29.196	6.301	21.727	21.727
2	4.170	14.381	43.576	4.170	14.381	43.576	3.646	12.572	34.299
3	3.341	11.519	55.096	3.341	11.519	55.096	3.636	12.537	46.835
4	2.470	8.517	63.613	2.470	8.517	63.613	2.942	10.145	56.980
5	1.699	5.857	69.470	1.699	5.857	69.470	2.323	8.010	64.990
6	1.235	4.257	73.727	1.235	4.257	73.727	1.903	6.561	71.551
7	1.126	3.884	77.612	1.126	3.884	77.612	1.757	6.060	77.612
8	.869	2.996	80.608						
9	.862	2.971	83.579						
10	.771	2.660	86.238						
11	.697	2.404	88.642						
12	.545	1.880	90.522						
13	.466	1.606	92.128						
14	.429	1.479	93.608						
15	.330	1.138	94.745						
16	.286	.985	95.731						
17	.213	.734	96.464						
18	.181	.624	97.088						
19	.170	.587	97.676						
20	.147	.509	98.184						
21	.119	.410	98.594						
22	.089	.306	98.901						
23	.078	.270	99.171						
24	.072	.249	99.420						
25	.063	.219	99.639						
26	.049	.168	99.806						
27	.027	.093	99.900						
28	.017	.058	99.958						
29	.012	.042	100.000						

Appendix VIII KMO, Bartletts Test and Total Variance Explained for Individual Variables

Appendix VIII-A

Performance Expectancy (PE)-KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.715
Bartlett's Test of Sphericity	Approx. Chi-Square	121.627
	df	6
	Sig.	.000

Performance Expectancy (PE)-Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.381	59.516	59.516	2.381	59.516	59.516
2	.823	20.578	80.093			
3	.444	11.106	91.199			
4	.352	8.801	100.000			

Appendix VIII-B

Efforts Expectancy (EE)-KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.729
Bartlett's Test of Sphericity	Approx. Chi-Square	166.424
	df	10
	Sig.	.000

Efforts Expectancy (EE)-Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.692	53.837	53.837	2.692	53.837	53.837
2	.801	16.014	69.851			
3	.725	14.492	84.343			
4	.556	11.113	95.456			
5	.227	4.544	100.000			

Appendix VIII-C

Social & Orgn Influence (SOI)- KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.799
Bartlett's Test of Sphericity	Approx. Chi-Square	435.046
	df	10
	Sig.	.000

Social & Organ Influence (SOI)-Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.698	73.965	73.965	3.698	73.965	73.965
2	.665	13.290	87.255			
3	.376	7.515	94.770			
4	.170	3.405	98.175			
5	.091	1.825	100.000			

Extraction Method: Principal Component Analysis.

Appendix VIII-D

Facilitating Condition (FC)-KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.790
Bartlett's Test of Sphericity	Approx. Chi-Square	480.941
	df	10
	Sig.	.000

Facilitating Condition (FC)-Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.793	75.858	75.858	3.793	75.858	75.858
2	.713	14.252	90.110			
3	.239	4.784	94.894			
4	.174	3.473	98.367			
5	.082	1.633	100.000			

Appendix VIII-E

Client Factor (CF)-KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.746
Bartlett's Test of Sphericity	Approx. Chi-Square	370.534
	df	6
	Sig.	.000

Client Factor(CF)-Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.095	77.366	77.366	3.095	77.366	77.366
2	.653	16.315	93.681			
3	.176	4.406	98.087			
4	.077	1.913	100.000			

Extraction Method: Principal Component Analysis.

Appendix VIII-F

Audit Professional Factor (APF)-KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.746
Bartlett's Test of Sphericity	Approx. Chi-Square	231.442
	df	3
	Sig.	.000

Audit Professional Factor (APF)-Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.578	85.922	85.922	2.578	85.922	85.922
2	.270	8.992	94.914			
3	.153	5.086	100.000			

Extraction Method: Principal Component Analysis.

Appendix VIII-G

BI- KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.742
Bartlett's Test of Sphericity	Approx. Chi-Square	71.361
	df	3
	Sig.	.000

BI-Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.982	66.056	66.056	1.982	66.056	66.056
2	.590	19.673	85.729			
3	.428	14.271	100.000			

Extraction Method: Principal Component Analysis.

Appendix IX Hierarchical Regression

Appendix IX-A Hierarchical Regression for Gender

Model SummaryIVs & Gender

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.714[a]	.509	.479	.33156	.509	16.947	6	98	.000
2	.768[b]	.589	.560	.30489	.080	18.891	1	97	.000

a. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC

b. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC, Gender

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.178	6	1.863	16.947	.000[b]
	Residual	10.773	98	.110		
	Total	21.951	104			
2	Regression	12.934	7	1.848	19.877	.000[c]
	Residual	9.017	97	.093		
	Total	21.951	104			

a. Dependent Variable: BI

b. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF

c. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF, Gender

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
2	(Constant)	3.032	.417		7.277	.000
	PE	.050	.051	.065	.973	.333
	EE	.291	.076	.346	3.857	.000
	FC	.325	.109	.422	2.978	.004
	SOIF	.323	.128	.419	2.535	.013
	CF	.302	.044	.481	6.879	.000
	APF	.075	.037	.050	.332	.895
	Gender	.477	.110	.365	4.346	.000

a. Dependent Variable: BI

Appendix IX -B Hierarchical Regression for Age

Model SummaryIVs & Age

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics: R Square Change	F Change	df1	df2	Sig. F Change
1	.714[a]	.509	.479	.33156	.509	16.947	6	98	.000
2	.725[b]	.525	.491	.32773	.016	3.303	1	97	.072

a. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC

b. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC, Age of Participants

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.178	6	1.863	16.947	.000[b]
	Residual	10.773	98	.110		
	Total	21.951	104			
2	Regression	11.533	7	1.648	15.339	.000[c]
	Residual	10.418	97	.107		
	Total	21.951	104			

a. Dependent Variable: BI

b. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF

c. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF, Age of Participants

Coefficients[a]

Model		Unstandardized Coefficients: B	Unstandardized Coefficients: Std. Error	Standardized Coefficients: Beta	t	Sig.
2	(Constant)	2.270	.422		5.383	.000
	PE	.059	.056	.078	1.059	.292
	EE	.340	.080	.403	4.242	.000
	FC	.113	.103	.146	1.094	.277
	SOIF	.042	.116	.055	.363	.718
	CF	.347	.046	.553	7.608	.000
	APF	.037	.039	.076	.943	.348
	Age of Participants	.097	.053	.130	1.817	.072

a. Dependent Variable: BI

Appendix IX -C Hierarchical Regression for experience in computerised auditing

Model SummaryIVs and Experience in computerised Auditing

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics: R Square Change	F Change	df1	df2	Sig. F Change
1	.714[a]	.509	.479	.33156	.509	16.947	6	98	.000
2	.721[b]	.519	.484	.32988	.010	1.999	1	97	.002

a. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC

b. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC, Experience in computerised Auditing

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.178	6	1.863	16.947	.000[b]
	Residual	10.773	98	.110		
	Total	21.951	104			
2	Regression	11.396	7	1.628	14.960	.000[c]
	Residual	10.556	97	.109		
	Total	21.951	104			

a. Dependent Variable: BI

b. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF

c. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF, Experience in computerised Auditing

Coefficients[a]

Model		Unstandardized Coefficients: B	Unstandardized Coefficients: Std. Error	Standardized Coefficients: Beta	t	Sig.
2	(Constant)	2.154	.449		4.795	.000
	PE	.030	.056	.039	.532	.596
	EE	.329	.081	.390	4.050	.000
	FC	.086	.103	.112	.831	.408
	SOIF	.040	.117	.052	.344	.732
	CF	.356	.046	.566	7.749	.000
	APF	.042	.040	.088	1.067	.289
	Experience in computerised Auditing	.551	.036	.104	1.414	.001

a. Dependent Variable: BI

I

Appendix IX -D Hierarchical Regression for IT skills

Model SummaryIVs and IT Skill

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.714[a]	.509	.479	.33156	.509	16.947	6	98	.000
2	.718[b]	.515	.489	.33131	.010	1.148	1	97	.004

a. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC

b. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC, IT Skills

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.178	6	1.863	16.947	.000[b]
	Residual	10.773	98	.110		
	Total	21.951	104			
2	Regression	11.304	7	1.615	14.712	.000[c]
	Residual	10.647	97	.110		
	Total	21.951	104			

a. Dependent Variable: BI

b. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF

c. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF, IT Skills

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
2	(Constant)	2.115	.489		4.328	.000
	PE	.033	.056	.043	.592	.555
	EE	.374	.086	.443	4.348	.000
	FC	.284	.104	.109	.809	.002
	SOIF	.006	.119	.007	.048	.962
	CF	.369	.049	.588	7.599	.000
	APF	.034	.039	.070	.860	.392
	IT Skills	.274	.069	.185	1.072	.007

a. Dependent Variable: BI

Appendix IX -E Hierarchical Regression for Auditor type

Model SummaryIVs & Auditor Type

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.714[a]	.509	.479	.33156	.509	16.947	6	98	.000
2	.743[b]	.553	.520	.31823	.043	9.383	1	97	.003

a. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC

b. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC, Auditor type

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.178	6	1.863	16.947	.000[b]
	Residual	10.773	98	.110		
	Total	21.951	104			
2	Regression	12.128	7	1.733	17.109	.000[c]
	Residual	9.823	97	.101		
	Total	21.951	104			

a. Dependent Variable: BI

b. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF

c. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF, Auditor type

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
2	(Constant)	2.688	.418		6.431	.000
	PE	.052	.054	.068	.977	.331
	EE	.357	.078	.424	4.581	.000
	FC	.056	.100	.073	.559	.577
	SOIF	.011	.113	.014	.094	.926
	CF	.397	.047	.632	8.531	.000
	APF	.027	.038	.056	.709	.480
	Auditor type	.231	.075	.223	3.063	.103

a. Dependent Variable: BI

Appendix IX -F-Hierarchical Regression for Professional Certification

Model SummaryIVs & Professional Certification

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics: R Square Change	F Change	df1	df2	Sig. F Change
1	.714[a]	.509	.479	.33156	.509	16.947	6	98	.000
2	.741[b]	.549	.516	.31953	.040	8.514	1	97	.004

a. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC

b. Predictors: (Constant), SOIF, CF, PE, APF, EE, FC, Professional Certifications

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.178	6	1.863	16.947	.000[b]
	Residual	10.773	98	.110		
	Total	21.951	104			
2	Regression	12.047	7	1.721	16.856	.000[c]
	Residual	9.904	97	.102		
	Total	21.951	104			

a. Dependent Variable: BI

b. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF

c. Predictors: (Constant), APF, PE, FC, CF, EE, SOIF, Professional Certifications

Coefficients[a]

Model		Unstandardized Coefficients: B	Unstandardized Coefficients: Std. Error	Standardized Coefficients: Beta	t	Sig.
2	(Constant)	3.006	.461		6.527	.000
	PE	.065	.054	.085	1.195	.235
	EE	.272	.082	.322	3.313	.001
	FC	.108	.100	.140	1.080	.283
	SOIF	.030	.113	.038	.262	.794
	CF	.362	.045	.576	8.131	.000
	APF	.031	.038	.064	.804	.424
	Professional Certifications	.153	.018	.222	2.918	.004

a. Dependent Variable: BI

Appendix X A Summary of Nodes Generated by Nvivo Software (Thematic Coding)

Coded themes	Sources	References	Created On	Created By
Categories of IS tools	0	0	22/7/2017 3:58:33 PM	ABK
Office automation technology	6	10	22/7/2017 4:02:01 PM	ABK
Audit automation technology	12	48	22/7/2017 4:22:13 PM	ABK
Ecommerce technology	4	4	22/7/2017 4:04:15 PM	ABK
Networking and data transfer	12	26	22/7/2017 4:03:42 PM	ABK
Impact of IS on e-fraud detection	0	0	22/7/2017 4:11:52 PM	ABK
Types of frauds detected	10	31	22/7/2017 4:13:26 PM	ABK
Solution to reduce e-fraud	2	9	22/7/2017 4:24:43 AM	ABK
Internal frauds detection	6	18	22/7/2017 4:32:38 PM	ABK
How e-fraud is detected	12	75	22/7/2017 4:33:44 PM	ABK
External frauds detection	6	7	22/7/2017 4:42:23 PM	ABK
Ethical hacking	6	14	22/7/2017 4:50:29 PM	ABK
Impact of IS on audit process	0	0	22/7/2017 4:57:44 PM	ABK
The conduct of the audits	10	43	22/7/2017 4:59:48 PM	ABK
Teams and Skills composition	9	35	22/7/2017 5:08:23 PM	ABK
Security of data	8	26	22/7/2017 5:10:08 PM	ABK
Planning the audit	3	5	22/7/2017 5:09:12 PM	ABK
Level of Audit risk	2	9	23/7/2017 3:56:27 AM	ABK
How the process has changed	1	7	23/7/2017 3:57:35 AM	ABK
Documentation	1	2	23/7/2017 3:59:32 AM	ABK
Factors influencing IS usage	0	0	24/7/2017 8:05:52 PM	ABK
Internal factors	8	25	24/7/2017 8:06:25 PM	ABK
Simplified tasks	3	21	24/7/2017 8:10:08 PM	ABK
Eased supervision	4	8	24/7/2017 8:22:12 PM	ABK
Monetary gain	5	9	24/7/2017 8:36:27 AM	ABK
Flexibility	6	11	24/7/2017 8:44:35 AM	ABK
Relevance to task	5	12	24/7/2017 9:24:37 AM	ABK
Audit effectiveness	7	13	24/7/2017 9:55:55 PM	ABK
Organisational efficiency	6	14	24/7/2017 9:56:25 PM	ABK
Availability of resources	8	12	24/7/2017 9:59:52 PM	ABK
Management pressure	9	7	25/7/2017 9:27:25 PM	ABK

External factors	12	50	25/7/2017 4:35:39 PM	ABK
Clients' IT intensity	9	11	25/7/2017 4:22:12 PM	ABK
Clients' products complexity	9	12	25/7/2017 2:36:27 AM	ABK
Audit risk	10	25	25/7/2017 2:04:35 AM	ABK
Client's e-business integration	7	12	25/7/2017 2:24:33 AM	ABK
Size of client's business	5	9	25/7/2017 4:05:53 PM	ABK
Pressure from regulators	6	15	25/7/2017 4:06:25 PM	ABK
Audit compliance	6	12	25/7/2017 4:20:57 PM	ABK
Ready available methodology	6	8	25/7/2017 4:27:25 PM	ABK
Accountability	3	8	25/7/2017 4:35:37 PM	ABK
Competitive advantage	2	9	25/7/2017 4:35:38 PM	ABK
Emerging themes	0	0	26/7/2017 4:43:30 PM	ABK
Recruitments of auditors	5	38	26/7/2017 4:45:08 PM	ABK
Skills change	4	7	26/7/2017 4:47:09 PM	ABK
Competence of accountants	4	8	26/7/2017 4:48:08 PM	ABK
What audit firms needs	5	11	26/7/2017 4:50:07 PM	ABK
E-government and IT audit	2	7	26/7/2017 9:13:01 PM	ABK
E-procurement	3	5	26/7/2017 9:23:03 PM	ABK
BMIF	2	4	26/7/2017 9:24:06 PM	ABK
The role of CAG	2	4	26/7/2017 9:27:07 PM	ABK
Support to the CAG	2	5	26/7/2017 9:33:08 PM	ABK
Continuous auditing	11	17	26/7/2017 4:47:17 PM	ABK
Understanding CA	6	8	26/7/2017 4:49:18 PM	ABK
The need for CA in Tanzania?	6	8	26/7/2017 4:50:19 PM	ABK
Cloud computing	2	12	26/7/2017 4:53:10 PM	ABK
Outsourcing for data storage	1	3	26/7/2017 4:55:16 PM	ABK
Users of clouds technology	4	5	26/7/2017 4:57:15 PM	ABK
Challenges of using clouds	2	4	26/7/2017 4:57:18 PM	ABK
Clients' complexity	12	42	26/7/2017 5:03:23 PM	ABK
Risk in banks' clients	12	28	26/7/2017 5:45:09 PM	ABK
Risk in Insurance Companies	5	9	26/7/2017 5:03:09 PM	ABK
Risk in Telecoms	8	10	26/7/2017 6:47:16 PM	ABK
Hotel industry	4	7	26/7/2017 6:39:39 AM	ABK
Air ticketing etc	4	6	26/7/2017 6:44:21 PM	ABK
Challenges in the audit profession	9	33	27/7/2017 4:44:08 PM	ABK
Individual challenges	4	10	27/7/2017 2:39:31 AM	ABK
Skills gap	4	7	27/7/2017 6:44:21 PM	ABK
Complexity in ISAs	5	7	27/7/2017 4:44:08 PM	ABK
Dynamic e-business audit	8	12	27/7/2017 2:39:31 AM	ABK
Organisational challenges	5	13	27/7/2017 2:39:32 AM	ABK
High staff turnover	4	6	27/7/2017 4:44:08 PM	ABK
High cost of training	4	7	27/7/2017 2:39:31 AM	ABK
Cost of retention	3	7	27/7/2017 2:39:32 AM	ABK
Clients' related challenges	4	11	27/7/2017 4:44:08 PM	ABK
Low IT savvy	6	15	27/7/2017 2:39:31 AM	ABK
Confidentiality of data	3	5	27/7/2017 2:39:32 AM	ABK
Accounting syllabus	6	8	27/7/2017 2:39:32 AM	ABK
Big data and auditor relevance	2	3	27/7/2017 2:48:05 AM	ABK

Appendix XI Research Ethics Approval Issued by REC at NUBS, the University of Nottingham Malaysia Campus

Nottingham University Business School

NOTTINGHAM UNIVERSITY BUSINESS SCHOOL

RESEARCH ETHICS COMMITTEE REVIEW FORM – STAFF AND DOCTORAL RESEARCH

Please complete and return this form electronically from your university email account to Nottingham University Business School's Research Ethics Committee (NUBS REC) (nubs-rec@nottingham.edu.my).

Project title: The Impact of Information Systems on Financial Audit: Analysis of External Auditors Role of Risk Assessment of Electronic Fraud	
PI: Asha Issa Baleche Katamba	***Date:*** 12 February 2016

1. In your professional judgement, is the proposed research project of minimal risk or more than minimal risk as defined by the ESRC Framework for Research Ethics? Please enter (X) in the appropriate box.

Minimal Risk	x	More than minimal risk		More info needed	

A project is regarded as "minimal risk" if:

- the applicant has answered 'no' to all of the questions on the checklist; and
- that you are satisfied that these answers are correct; and
- that you are satisfied that the proposal is complete and raises no other ethical issues

Projects judged to be minimal risk require independent review by two members of the committee. Many projects judged to be more than minimal risk will still be approved, but they will require greater scrutiny and may be reviewed by more than two members of the committee at the REC chair's discretion.

2. Regardless of the risk status of the project, please indicate your view (X) below:

Approve (unconditional)		Revise and Resubmit	
Approve (unconditional, non-binding suggestions)		Further information required	
Approve (conditional on minor changes)	x	Reject	

- Conditional approval is for minor amendments (e.g., changes to participant information sheets) which are straightforward enough not to require a full resubmission.
- Recommendations for minor amendments/revise and resubmit will be shared with the second reviewer so that a consensus may be reached where possible.
- If you request further information, this will be requested from the applicant and then forwarded to both/all the project reviewers.
- The REC chair may invite other committee members to review an application in the event of disagreement

3. Please complete below full details of the changes you recommend, details of the further information you require, or your reasons for rejecting the application.

Please mention that the data collected will be stored safely and will not be shared with other parties.

Appendix XII: An Approval Letter to Conduct the Research Issued by NUBS, the University of Nottingham Malaysia Campus



The University of Nottingham

UNITED KINGDOM · CHINA · MALAYSIA

Nottingham University Business School
Jalan Broga
43500 Semenyih
Selangor Darul Ehsan
Malaysia
Tel +6(03) 8924 8000
Fax +6(03) 8924 8019
www.nottingham.edu.my

February 24, 2016

To Whom It May Concern,

This serves to confirm that Ms Asha Issa Baleche Katamba, student ID: UNIMKL-016463 and Passport Number AB142416, is a registered student for PhD in Business and Management course in the Nottingham University Business School with The University of Nottingham Malaysia Campus.

She is currently collecting data for her PhD thesis. The title of her PhD thesis is "The impact of information systems on financial audit: Analysis of external auditor's task on risk assessment of electronic fraud".

We would be grateful if you could provide the relevant information and render her the assistance, she requires in order for her to complete her management project.

Information collected will be used for the purposes of the assessment of her management project.

Thank you.

Yours faithfully,
Dr Tang Kin Boon
Director of PhD Programme
Nottingham University Business School Malaysia

The University of Nottingham
in Malaysia Sdn Bhd (977210-K)

MSC-Status Company