

The Impact of Information and
Communication Technology on
Internal Control's Prevention and
Detection of Fraud

James Olusola Abiola
Doctor of Philosophy

April, 2013

The Impact of Information and Communication
Technology on Internal Control's Prevention and
Detection of Fraud

James Olusola Abiola

Thesis submitted to the Faculty of Business & Law at De
Montfort University in partial fulfilment of the
requirements for the Degree of Doctor of Philosophy

Department of Accounting & Finance

2013

Abstract

This study explores the Impact of Information and Communication Technology (ICT) on internal control effectiveness in preventing and detecting fraud within the financial sector of a developing economy – Nigeria. Using a triangulation of questionnaire and interview techniques to investigate the internal control activities of Nigerian Internal Auditors in relation to their use of ICT in fraud prevention and detection, the study made use of cross-tabulations, correlation coefficients and one-way ANOVAs for the analysis of quantitative data, while thematic analysis was adopted for the qualitative aspects. The Technology Acceptance Model (TAM) and Omoteso et al.'s Three-Layered Model (TLM) were used to underpin the study in order to provide theoretical considerations of the issues involved. The study's findings show that Nigerian Internal Auditors are increasingly adopting IT-based tools and techniques in their internal control activities. Secondly, the use of ICT-based tools and techniques in internal control positively impacts on Internal Auditors' independence and objectivity. Also, the study's findings indicate that Internal Auditors' use of ICT-based tools and techniques has the potential of preventing electronic fraud, and such ICT-based tools and techniques are effective in detecting electronic fraud. However, continuous online auditing was found to be effective in preventing fraud, but not suited for fraud detection in financial businesses.

This exploratory study sheds light on the impact of ICT usage on internal control's effectiveness and on internal auditors' independence. The study contributes to the debate on the significance of ICT adoption in accounting disciplines by identifying perceived benefits, organisational readiness, trust and external pressure as variables that could affect Internal Auditors' use of ICT. Above all, this research was able to produce a new model: the Technology Effectiveness Planning and Evaluation Model (TEPEM), for the study of ICT adoption in internal control effectiveness for prevention and detection of fraud. As a result of its planning capability for external contingencies, the model is useful for the explanation of studies involving ICT in a unique macro environment of developing economies such as Nigeria, where electricity generation is in short supply and regulatory activities unpredictable. The model proposes that technology effectiveness (in the prevention and the detection of fraud) is a function of TAM variables (such as perceived benefits, organisational readiness, trust, external pressures), contingent factors (size of organisation, set-up and maintenance cost, staff training and infrastructural readiness), and an optimal mix of human and technological capabilities.

Acknowledgements

“Generosity is not giving me that which I need more than you do, but it is giving me that which you need more than I do.” (Khalil Gibran)

I am an unrepentant believer in what Paul Valery said *“The best way to make your dreams come true is to wake up”* I have woken up to various challenges in the course of this programme and I thank God it has yielded results. Of course, I need to bear in mind what Martins Luther also said some years back *“All progress is precarious, and solution to one problem brings us face to face with another problem”*. I therefore regard the completion of this programme as a beginning of fresh challenges. Despite initial challenges experienced with my health, the almighty God has been faithful all through. I am sincerely indebted to my supervisory team: Ashok Patel and Dr. Kamil Omoteso who contributed in no small measure to make the PhD programme a success. They have been very generous indeed in sharing knowledge, thoughts and materials. To both of you I say a big thank-you.

I appreciate Professors David Crowther and Martyns Denscombe, Dr Ismail Adelopo, Dr. Kumba Jallo, Dr Peter Scott, Dr Yulia Rodionova and a host of other academics in Accounting and Finance department who have contributed in one way or the other to the success of this programme.

My very special thanks go to Dr David Russell, the HOD, Accounting and Finance department for his encouragement and support. The department gave me the opportunity to teach on part-time basis for two years during my PhD programme. It was quite a useful and exciting experience for me.

On the home front, I want to say a big thank-you to my wife, Lady Bola, for her unflinching support all these years and to my children Bisola, Temmy, Ope and Ife. Together they have been wonderful during my constant absence from their mist. I appreciate your love, patience and understanding. I say thank-you for believing in me.

May I also express my gratitude to my childhood friend and his wife Mr. and Mrs Segun Ojo. They have become a dependable extension of Abiola’s family

over the years. He made my contacts with Nigeria quite easy and successful each time I had cause to visit Nigeria in the course of my programme.

Finally, my gratitude will not be complete without mentioning the support I received from my colleagues: Dr Kemi Yekini; Dr Tokunbo Adenowo; Dr Onafowokan Oluyombo; Dr Musa Obalola and Pastor Thomas Olushola. A lot of times we shared experiences, compared notes and exchanged materials. I am indeed very grateful to you all.

James Abiola

De Montfort University

Leicester, UK

April, 2013

Table of Contents

Abstract.....	iii
Acknowledgements.....	iv
Table of Contents.....	vi
List of Figures	xiv
List of Tables	xv
List of Acronyms and Abbreviations	xviii
CHAPTER ONE	1
INTRODUCTION.....	1
1.0: Introduction to the Study	1
1.1.0: Problem Definition and the Aim of the Study.....	5
1.2.0: Main Objectives of this Study	8
1.3.0: Research Questions	8
1.4.0: Research Propositions	8
1.5.0: The Scope of the Study	10
1.6.0: Methodology.....	11
1.7.0: Significance, Originality and Key Outcomes of the Study.....	12
1.8.0: The Structure of the Thesis.....	14
1.9.0: Summary of Chapter	15
CHAPTER TWO	17
BACKGROUND TO THE STUDY	17
2.0: Introduction	17
2.1: Recent Economic and Financial Reforms in Nigeria	17
2.2: The Growth of Information Technology in Nigeria	21
2.3: Incidents of Fraud in the Financial Sector of the Nigeria Economy.....	23

2.4: Internal Audit Practice in Nigeria	26
2.5: Internal Auditing and Internal Control in the Nigerian Financial Sector	27
2.6: Summary of Chapter	30
CHAPTER THREE	31
A REVIEW OF LITERATURE	31
3.0: Introduction	31
3.1 Internal Controls – Towards a Working Definition	33
3.2: Internal Control Models.....	34
3.2.1: Committee of the Sponsoring Organisation (COSO).....	34
3.2.2: The Criteria of Control (CoCo).....	36
3.2.3: Control Objectives for Information and Related Technology (CobIT)	37
3.2.4: The Basel Committee on Banking Supervision’s Framework for IC System	37
3.3: Internal Audit	37
3.3.1: Developments in Internal Auditing.....	38
3.3.2: Internal Control and Internal Auditing.....	46
3.3.3: Internal Audit Effectiveness.....	47
3.3.4: Internal Auditors’ Effectiveness and Demographic Characteristics	49
3.3.5: Governance Activities of Internal Auditors.....	50
3.4.0: Internal Control and Computer-Assisted Auditing Tools and Techniques Literature...	54
3.5.0: Summary of Chapter	71
CHAPTER FOUR	72
LITERATURE REVIEW ON PREVENTION AND DETECTION OF ELECTRONIC FRAUD.....	72
4.0: Introduction	72
4.1.0: Internal Audit, E-business, and E-fraud	73
4.2.0: Application of Continuous Online Auditing	80
4.3.0: Electronic Fraud Literature	91
4.4.0: Summary of Literature	100

4.5.0: Gaps in the Literature	101
4.6.0: Emergence of Research Propositions from the Literature	103
4.6.1: Effectiveness of Internal Control	103
4.6.2: Proposition 1: Nigerian Internal Auditors are increasingly adopting IT-based tools and techniques.....	104
4.6.3: Proposition 2: The use of ICT-based tools and techniques in Internal Control impacts positively on Internal Auditors' independence.....	105
4.6.4: Proposition 3: Internal Auditors' use of ICT-based tools and techniques has the potential of preventing electronic fraud.	107
4.6.5: Proposition 4: Internal Auditors' use of ICT-based tools and techniques is effective in detecting electronic fraud.	109
4.7.0: Summary of Section	111
CHAPTER FIVE	112
THEORETICAL FRAMEWORK	112
5.0: Introduction	112
5.1.0: Commonly Used Theories in Information System Research	116
5.1.1: Theory of Reasoned Actions (TRA)	116
5.1.2: Theory of Planned Behaviour (TPB).....	116
5.1.3: Diffusion of Innovations (DOI)	116
5.1.4: Unified Theory of Acceptance and Use of Technology (UTAUT)	117
5.1.5: Model of the IT Implementation Process (MIIP)	117
5.2.0: Technology Acceptance Model (TAM).....	118
5.3.0: The Three-Layered Model from a Meta-Level Perspective	122
5.4.0: TAM and TLM: Competing or Complementary?.....	125
5.5: Summary of Chapter	129
CHAPTER SIX.....	130
RESEARCH METHODOLOGY	130
6.0: Introduction	130
6.1.0: Philosophical Foundation.....	131

6.1.1: Philosophical Basis of the Methodology	132
6.1.2: Summary of Research Methods from the Literature.....	137
6.1.3: Mixed methods Sequencing	139
6.2.0: Research Instruments and Validation.....	140
6.2.1: Sampling and Response Rate.....	141
6.2.2: Construct Measures	142
6.2.3: Drafting the Questionnaire	143
6.2.4: Internal Validity Testing	143
6.2.5: Reliability Check.....	144
6.3.0: Research Propositions	144
6.3.1: Current and Potential Implications of ICT Tools and Techniques for Internal Control.....	145
6.4.0: Research Design	146
6.4.1: Pilot Study	146
6.4.2: Outcome of Pilot Study.....	146
6.4.0: Collection of Data.....	Error! Bookmark not defined.
6.4.1: Interview	150
6.5.0: Data Analysis	155
6.5.1: Data Generated From Questionnaire	155
6.5.2: Secondary Data	158
6.6: The Body of Evidence Used in this Study.....	159
6.7: Limitations of the Methodology	159
6.8: Summary of Chapter	161
CHAPTER SEVEN	162
DATA ANALYSIS 1	162
7.0: Introduction	162
7.1 Detailed Analysis of Responses.....	163

7.2.0: Proposition 1: Nigerian Internal Auditors are increasingly Adopting IT-Based Tools and Techniques.....	163
7.2.1: Proposition 1.1: Internal Auditors’ Current Level of use of ICT Tools and Techniques for Internal Control Purposes is increasing.....	164
7.2.2 Interview Result on ICT Usage	173
7.2.3: Interview Questions on ICT Usage and Staffing Requirement.....	175
7.2.4: Discussion	177
7.2.5: The Use of ICT Tools and Techniques and the Size of Organisation.....	178
7.2.6: Interview Responses on the Use of ICT Tools and Techniques and Size of Organisations	180
7.2.7: Discussion	181
7.3: Proposition 1.2: Financial Institutions Current Level of Provision of ICT Tools and Techniques for internal control purposes is increasing.....	182
7.3.1: Discussion	186
7.4: Proposition 1.3: ICT Tools and Techniques are Useful to Internal Audit’s Task, Efficiency and Effectiveness	187
7.4.1: Interview Results on Usefulness of ICT Tools and Techniques.....	190
7.4.2: Discussion.....	194
7.5: Proposition 2: The Use of ICT-based Tools and Techniques Impacts on Internal Auditor’s Independence.....	195
7.5.1: Discussion	197
7.6: Summary of Chapter	198
CHAPTER EIGHT.....	199
DATA ANALYSIS 11	199
8.0: Introduction	199
8.1.0: Proposition 3: Internal auditors’ use of ICT–based tools and techniques has the potential of preventing electronic fraud.	199
8.1.1: Proposition 3.1: Internal auditor’s use of ICT has had positive impact on prevention of fraud.....	200
7.1.2: Proposition 8.2: COA has fraud preventive control.....	204

8.1.1: Interview Analyses on Continuous Online Auditing (COA) effectiveness for Prevention of Fraud.	206
8.1.3: Proposition 3.3: The extent of ICT utilisation for prevention of fraud is affected by auditor’s demographic characteristics (experience, training, gender and qualification).....	209
8.1.2: Discussion	211
8.2.0: Proposition 4: Internal Auditors’ Use of ICT-based Tools and Techniques are Effective in Detecting Electronic Fraud.....	213
8.2.1: Proposition 4.1 Use of ICT in internal control has had positive impact on detection of fraud.....	213
Proposition 4.2: COA has effective fraud detection control.....	218
Proposition 4.3: The extent of ICT utilisation for detection of fraud is affected by auditors’ demographic characteristics (experience, gender, training and qualification)	221
8.2.1: Discussion	225
8.3.0: Key Findings from the Study	227
8.3.1: Nigerian Internal Auditors are increasingly adopting IT-based tools and techniques (Proposition 1)	227
8.3.2: Internal auditors’ current level of use of ICT tools and techniques for internal control purposes are increasing (Proposition 1.1)	227
8.3.3: Financial Institutions’ Current Level of Provision of ICT Tools and Techniques for Audit Purposes is increasing (Proposition 1.2).....	230
8.3.4: The Usefulness of ICT Tools and Techniques for Internal Audit’s Task Efficiency and Effectiveness (Proposition 1.3).	231
8.4: The Use of ICT-based Tools and Techniques Impact on Internal Auditors’ Independence and Objectivity (Proposition 2)	232
8.5: Internal Auditors’ use of ICT-based Tools and Techniques has the Potential of Preventing Electronic Fraud (Proposition 3)	234
8.5.1: Proposition3.1: Internal auditors’ use of ICT has had positive impact on prevention of fraud.....	234
8.5.2: Proposition 3.2: Continuous Online Auditing’s (COA) has Effective Fraud Preventive Control	235
8.5.3: Proposition 3.3: The extent of ICT utilisation for prevention of fraud is affected by auditors’ demographic characteristics (experience, qualification, training and gender).....	236

8.6: Internal auditors’ use of ICT-based tools and techniques are effective in detecting electronic fraud (Proposition 4).....	236
8.6.1: Proposition 4.1: Use of ICT in internal control has had positive impact on detection of fraud.....	236
8.6.2: Proposition 4.2: COA has effective fraud detection control.....	237
8.6.3: Proposition 4.3: The extent of ICT utilisation for detection of fraud is affected by auditors’ demographic characteristics (experience, qualification and training)	237
8.7.0: Summary of Chapter	238
CHAPTER NINE	239
CONCLUSION AND RECOMMENDATION	239
9.0: Introduction	239
9.1.0: An Overview of the Thesis	239
9.1.1: A Self-Appraisal on Research Objectives	241
9.2.0: Placing the Findings within the Context of Applicable Theories	242
9.2.1: Technology Acceptance Model (TAM) and Adoption of ICT Tools and Techniques by Internal Auditors.....	243
9.2.2: The Three Layered Model (TLM) and Effectiveness of ICT Tools and Techniques for Prevention and Detection of Fraud	246
9.3.0: Technology Effectiveness Planning Evaluation Model in Internal Control.....	249
9.3.1: Relevance of Technology Effectiveness Planning and Evaluation Model to Previous Studies.....	252
9.4.0: Summary of Research Contributions	253
9.4.1: Contribution to Professional Practice.....	253
9.4.2: Contribution to Academic and Theoretical Debates	254
9.5: Possible Implications for the Policy Makers	256
9.6.0: Limitations of the Study.....	259
9.7.0: Recommended Areas for Future Research.....	260
REFERENCES.....	262
APPENDICES	317

Sample Cases from EFCC websites..... 345

List of Figures

Figure 1.1: Functions Affected by ICT Tools and Techniques Usage for Internal Control.....	7
Figure 1.2: The context of ICT tools and techniques usage for internal control within the scope of this study.....	10
Figure 1.3: Structure of the Research Process.....	14
Figure 3.1: A Summary of Literature Part 1.....	33
Figure 3.3: Internal Control.....	36
Figure 3.4: Traditional users of internal audit outputs.....	48
Figure 3.5: Governance Activities of Internal Auditors.....	51
Figure 4.1: A Summary of Literature Part 11.....	74
Figure 4.2: Major Modes of Electronic Fraud.....	80
Figure 4.3: COA Coverage.....	83
Figure 4.4: Framework of Internal control techniques combining fraud prevention and detection using data mining techniques.....	100
Figure 5.1: Summary of Theoretical Framework for the Study.....	116
Figure 5.2: TAM and Research Model.....	122
Figure 5.3: TAM Model for Adoption of ICT in Internal Control by Internal Auditors.....	123
Figure 5.4: A Three-Layered Model.....	127
Figure 6.1: The Three-World Framework.....	133
Figure 6.2: The Different Sources of Evidence Used in the Study.....	160
Figure 9.1: The Technology Effectiveness Planning and Evaluation Model.....	252

List of Tables

Table 2.1 Penetration of Information Technology in Nigeria.....	22
Table 2.2: Returns of Insured Banks on Fraud and Forgeries.....	26
Table 3.1: Software that can assist auditors.....	56
Table 3.2: PricewaterhouseCoopers (2007) survey.....	60
Table 3.3: Internal Audit Functions and its Effects on Internal Audit Control Components.....	70
Table 4.1: Frauds in the computing environment.....	78
Table 4.2: Summary of Previous Studies on Fraud Prevention and Detection Techniques...102	
Table 5.1: Theories Adopted by the Most Cited Articles and Books on ICT System Implementation and Adoption.....	117
Table5.2: Summary of Criticism of Contingency, Socio-Technical and Structuration Theories.....	125
Table 5.3: Summary of Propositions and Models Used for Explanations.....	130
Table 6.1 Summary of research methods from literatures.....	139
Table 6.2: Reliability Statistics: Cronbach Alpha.....	146
Table 6.3: Structure of Pilot Questionnaire.....	148
Table 6.4: Analysis of Returned Questionnaire by Business Type.....	149
Table 6.5: Structure of Final Questionnaire.....	150
Table 6.6: Analysis of Organisations Contacted for the Study.....	151
Table 6.7: Relevance of the Questionnaire and Interview Questions to the Study.....	154
Table 6.8: Common Tasks of Analysis and Applicable Techniques.....	156
Table 5.9: Statistical Methods Used for Analysis.....	157
Table 6.10: Criteria Used for Interpreting Correlation Coefficients.....	158
Table 7.1: A Combined Analysis of Questions 12, 13, 14 and 15 to Answer Research Proposition 1.1.....	165
Table 7.2 Gender * COA Cross-tabulation.....	167
Table 7.3 Age Audit Software Cross-tabulation.....	168

Table 7.4 Comparing Internal Auditors' ICT skills in different business types.....	169
Table 7.5 ANOVA.....	170
Table 7.6 Comparing Internal Auditors' ICT skills with their years of experience.....	171
Table 7.7: Specific ICT tools in Use.....	174
Table 7.8: Interview Result on ICT Usage.....	176
Table 7.9: Interview result on ICT usage and Staffing Requirement.....	178
Table 7.10: Packages/ICT Equipments Use by Participants' institutions.....	180
Table 7.11: Packages/tools use by Internal Auditors in Nigeria.....	184
Table 7.12: Calculated WAS for questions B26 and B30.....	185
Table 7.13: Interview Result on Usage of ICT tools and Techniques by Financial Institutions.....	186
Table 7.14: Summary of frequency tables for questions B1 to B16.....	189
Table 7.15: Spearman's rank Correlation Table.....	191
Table 7.16: Interview question C3.....	192
Table 7.17: Interview Question C1.....	193
Table 7.18 Questionnaires' Response on Internal Auditors' Independence.....	196
Table 8.1: Calculated WAS for Questions B14, B16, B19 and B20.....	202
Table 8.2: Types of fraud ICT tools and techniques have prevented.....	203
Table 8.3: ICT Fraud Prevention by Business Type.....	204
Table 8.4: ANOVA on ICT Fraud Prevention.....	205
Table 8.5: COA Preventive Control.....	206
Table 8.6: Spearman's rank correlation Table.....	207
Table 8.7: Interview on Continuous Online Auditing.....	210
Table 8.8: Internal Auditors' Qualification and Experience and Relationship with	

Prevention of Electronic Fraud.....	211
Table 8.8a: Internal auditors' experience and relationship with the use of ICT.....	212
Table 8.9: Use of ICT-based tools and techniques to detect electronic fraud.....	216
Table 8.10: Audit IT Skill * Fraud detection Cross-tabulation (A13* B18).....	217
Table 8.11 Correlation co-efficient on ICT skills and Fraud Detection.....	218
Table 8.12: Types of fraud ICT-based tools and techniques have detected.....	219
Table 8.12a: One-Way ANOVA Result for Groups of Financial Institutions.....	220
Table 8.13: Internal auditors' perception on COA capability to detect fraud.....	221
Table 8.14: Internal Auditors' Experience and the use of ICT Tools and Techniques to Detect Electronic Fraud.....	224
Table 8.14a Auditors' Experience and ICT Fraud detection.....	226
Table 8.15 Internal Auditors' Qualification and the use of ICT Tools and Techniques to Detect Electronic Fraud.....	227

List of Acronyms and Abbreviations

ACCA	Association of Chartered Certified Accountants
ACFE	Association of Fraud Examiners
AML	Anti Money-Laundering
APB	Auditing Practice Board
ATM	Automated Teller Machine
CAAT	Computer Assisted Audit Techniques
CAATTs	Computer Assisted Audit Tools and Techniques
CBN	Central Bank of Nigeria
CG	Corporate Governance
COA	Continuous Online Auditing
COBIT	Control Objectives for Information Technology
CoCo	Criteria of Control
COSO	Committee of Sponsoring Organisation
DOL	Diffusion of Innovations
EDI	Electronic Data Interchange
EFCC	Economic and Financial Crime Commission
FASB	Financial Accounting Standards Board
FATL	Financial Action Task Force
FITC	Financial Institution Training Centre
FRC	Financial Reporting Council
IA	Internal Auditor
IAF	Internal Audit Function
IC	Internal Control
ICAEW	Institute of Chartered Accounting England and Wales
ICAN	Institute of Chartered Accountants of Nigeria
ICT	Information and Communication Technology

IIA	Chartered Institute of Internal Auditors
IT	Information Technology
MIIP	Model of the IT Implementation Process
NDIC	Nigeria Deposit Insurance Corporation
NEPD	Nigeria Enterprises Promotion Decree
NICOM	National Insurance Commission
NICTP	Nation Information Communication Technology Policy
NIPCD	Nigeria Investment Promotion Commission Decree
OECD	Organisation for Economic Co-operation and Development
POB	Public Oversight Board
PWC	PricewaterhouseCoopers
SEC	Security Exchange Commission
TEPEM	Technology Effectiveness Planning and Evaluation Model
TAM	Technology Acceptance Model
TLM	Three-Layered Model
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
UTAUT	Unified Theory of Acceptance and Use of Technology

CHAPTER ONE

INTRODUCTION

1.0: Introduction to the Study

There is a dearth of research effort in developing countries, including Nigeria, especially in the area of internal control/auditing and electronic fraud, which is the primary focus of this study. The focus on electronic fraud is important, in the words of Sieber (1986:15):

“.....The problems caused by computer crime are bound to intensify in the future. Increasing computerisation, particularly in the administration of deposit money, in the balancing of accounts and stock-keeping, in the field of electronic funds transfer systems, and in the private sector, as well as new computer applications such as electronic home banking, electronic mail systems, and other interactive videotext systems will lead to increase in the number of offences and losses.....”

The observation made by Sieber (1986) has been proven quite accurate in more than two decades since it was made. For instance, Rusch (2001) discussed the growing rate of internet fraud in electronic business enterprises. The upward increase in the level of electronic fraud appears to be proportional with the increased expansion of legitimate internet use, which points to the fact that electronic fraud is becoming worldwide in scope and impact as it is now visible for fraudsters to plan and execute fraudulent schemes from anywhere in the world irrespective of their physical residence.

The evolution of the digital economy at a global level has changed in no small measure how business enterprises operate, generate, and display financial data; and much more importantly, how they are audited (Razaee et al. 2002, p.1). Most financial reports are now generated online and in real time, and the overwhelmingly rapid adoption and implementation of e-business technology has led to new challenges for Internal Auditors, specifically in the area of internal control effectiveness.

It is important to explain the concept of internal control in order to develop an understanding of the impact of Information and Communication Technology (ICT)

tools and techniques on internal control effectiveness in the prevention and detection of electronic fraud. The internal control system of an organisation is a structure laid down by executive managers for effective control of the entity's activities. It is closely linked with corporate governance. The Public Company Accounting Reform and Investor Protection Act (2002), otherwise generally referred to as the Sarbanes-Oxley Act, (2002), introduced in the United States, made it mandatory for management to initiate good internal control and provide assessment of its effectiveness. Most regulatory authorities worldwide are adopting the Sarbanes-Oxley Act control concept to prevent a repeat of the scandals which reverberated across the world as experienced with the likes of WorldCom or Enron (Weiddenmier and Ramamoorti, 2006)

The concept of internal control (IC) is very important for proper management of an organisations' risk, which may constitute barriers to the attainment of its set objectives if neglected. Budgeted profitability and achievement of set objectives may be impossible without a properly laid down control. This view is supported by Pickett (2005: 86) thus:

“Poor controls lead to losses, scandals; failures and damage to the reputation of organisations in whatever sector they are from. Where risks are allowed to run wild and new ventures are undertaken without a means of controlling risk, there are likely to be problems”

A number of control models have influenced the practice of internal control worldwide, models such as that of The Committee of Sponsoring Organisations (COSO), which was a product of professional endeavour of the Committee of Sponsoring Organisations developed after literature review on internal control as well as the Criteria of Control (CoCo), which is a contribution of the Canadian Institute of Chartered Accountants to international standards on internal control, and the Control Objectives for Information and Related Technology (CobiT), a framework for control of information technology (IT). Internal auditors are the most conversant with organisations' internal control systems. The Internal Auditor is regarded as the “custodian” of internal control - internal audit is part of the internal control system put in place by the management of an organisation. It is an aid to management; it ensures that the financial operations are correctly carried out according to the law and also in accordance with the wishes of the board or shareholders. IIA (1999:

Implementation Standard 2110.A2) explains the scope of internal auditing thus: “The internal audit activity should evaluate risk exposures relating to the organisation’s governance, operations and information systems regarding the: reliability and integrity of financial and operational information effectiveness and efficiency of operations safeguarding of assets and compliance with laws, regulations, and contracts”

The Internal Audit Function (IAF) is regarded as a significant aspect of corporate governance structure in organisational settings in order to complement the oversight activities undertaken by the board of directors and audit committee to ensure the integrity of the financial reporting process (Public Oversight Board, 1993). Similarly, Anderson, et al. (1993) and the Blue Ribbon Committee (1999) identified external auditing, internal auditing, and board of directors as monitoring mechanisms for business organisations, while the Institute of Internal Auditors (IIA), (2003) identified the fourth mechanism as the audit committee.

In response to corporate failure experienced worldwide in the last two decades, the internal audit function has enjoyed considerable focus both in practice and academic research (Levitt, 1998; 1999; Brown, 1999; Beasley et al., 1999; Cohen et al., 2002) However, the link between IAF and IC issues, especially within developing economies, has enjoyed very little patronage in the literatures.

The audit committee and the directors at the board level have direct responsibility for the formulation of the internal control framework. This governance responsibility is discharged through the assistance of Internal Auditors. The reporting line of IAF has remained one of the most controversial issues in academic literature and practice. For example, in a survey carried out in 2003 on IAF, it was found that about 50 per cent of the respondents in Belgium, Greece, Ireland, the United Kingdom and Spain report directly to an Audit Committee, whereas other countries have a far smaller percentage (Paape et al., 2003). A number of commentators have recommended that IAF should report directly to the audit committee in recognition of the importance of business

risk assessment and control to Corporate Governance (IIA, 2003; Hopwood et al., 2008; CBN, 2009; SEC, 2009). The main purpose for this arrangement as suggested by Hopwood et al. (2008: 274) “*is for the audit committee to serve as an independent check on top management and to independently ensure quality internal control processes and compliance.*”

A further major governance activity performed by Internal Auditors is control assessment. Reliance is placed on the experienced judgement of Internal Auditors by the audit committee to ensure that sufficient threat responses are implemented, and to identify if internal controls’ structures are adequate to proficiently support strategic, operational; reporting and compliance objectives (Gendron et al., 2004). This process is significant because an effective internal control system is a *sine qua non* for a reliable Enterprise Risk Management (COSO, 2004). The IAF is considered central to effective performance of management and the board of directors’ duties. The board of directors have a critical role to play in showcasing good internal control. The satisfactory discharge of the board's and its audit committee’s responsibilities rested squarely on effective internal audit function, which also relies on internal control that is capable of prevention and detection of errors and fraud. IIA (1999) defines internal audit thus: “Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation’s operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes”. From the definition of Internal Audit by the IIA, it is clear that independence and objectivity are central for effective performance of those functions. The use of ICT does not change the internal control objective and the obligation of Internal Auditors to assess risks. The independence and objectivity of those who are trusted with the usage of ICT in internal control are important in evaluating the effectiveness of such ICT tools and equipment. It is the motivation of this study to explore the impact of ICT on Internal Auditors’ independence and objectivity. Assessing the impact of ICT on Internal Auditors’ (users of ICT) independence validated the result of the impact of ICT on internal controls’ prevention and detection of fraud.

1.1.0: Problem Definition and the Aim of the Study

The expansion in business activities and the limitless opportunities provided by the internet usage have direct implication on the internal control function. This is more visible in the financial sector, as there is a noticeable transformation in traditional banking services (Awad, 1988). The Nigerian stock trading market is the second largest in sub-Saharan Africa with only South Africa larger in terms of volume. The financial sector accounts for more than 65 per cent of the stock on the Lagos exchange market (Security and Exchange Commission, 2010). There are mixed results from prior studies on levels of fraud and the apparent corporate governance problems in the financial sector of the Nigerian economy. For instance, Adewumi (1986) suggested poor internal control as the main reason for increased level of fraud. Oghojafor et al, (2010) identified a mismatch between supervisory skills of employees and the explosion in the numbers of banks and acquisitions of information technology. In order to have effective fraud prevention and detection, ensure accountability and good corporate governance practices, the instrument of internal control must be effective to identify and isolate illegal and fraudulent transactions.

Developments in ICT have made business transactions and marketing much more accessible than envisaged throughout the world. Nonetheless, it has also brought with it problems of control associated with the use of the internet. A number of studies have so far been carried out on the impact of ICT on auditing or accounting in developed countries but research work on the impact of ICT on the effectiveness of internal control systems in prevention and detection of electronic fraud in developing countries is scarce. One of such developing countries is Nigeria, where the financial sector appears to have a compelling need to examine the impact of ICT on internal control systems. This is necessary in view of recent government desires to attract more foreign direct investments to invigorate the economy through improved financial operations, which in turn necessitated benchmarking the effectiveness (COSO, 1994) of internal control against best practices. The development of ICT and its adoption by internet-based businesses is growing rapidly in developing countries such as Nigeria. Equally, internet-based fraudulent activities are growing across all business segments in Nigeria but much more in the financial sector (CBN, 2009). It is

therefore pertinent to examine the efficacy of the use of ICT in IC for prevention and detection of electronic fraud.

ICT tools and procedures are becoming increasingly inseparable in daily running and control of business enterprises' activities worldwide. For instance, in a survey conducted by PricewaterhouseCoopers, (2007), it was found that Internal Auditors are increasingly using ICT tools and techniques for control of their functions. This is as a result of increasing use of ICT for conducting and recording transactions in the financial sector, while at the same time opening up opportunities for fraud. Hence it is imperative to examine the effectiveness of ICT-based tools and techniques as being used by Internal Auditors in internal control. The functions of key stakeholders in internal control are now known to be affected by ICT tools and techniques usage as shown in Figure 1.1 on page 7. ICT tools and techniques usage in internal control has some level of direct impact on Internal Auditors (in terms of performance of their function and role), top management (in terms of reports and decision making), audit committee (in terms of reports and decision making), regulatory authorities (in terms of monitoring and ensuring public trust), accountants (in terms of their job functions and performance), and External Auditors (in terms of scope, quality and audit fees).

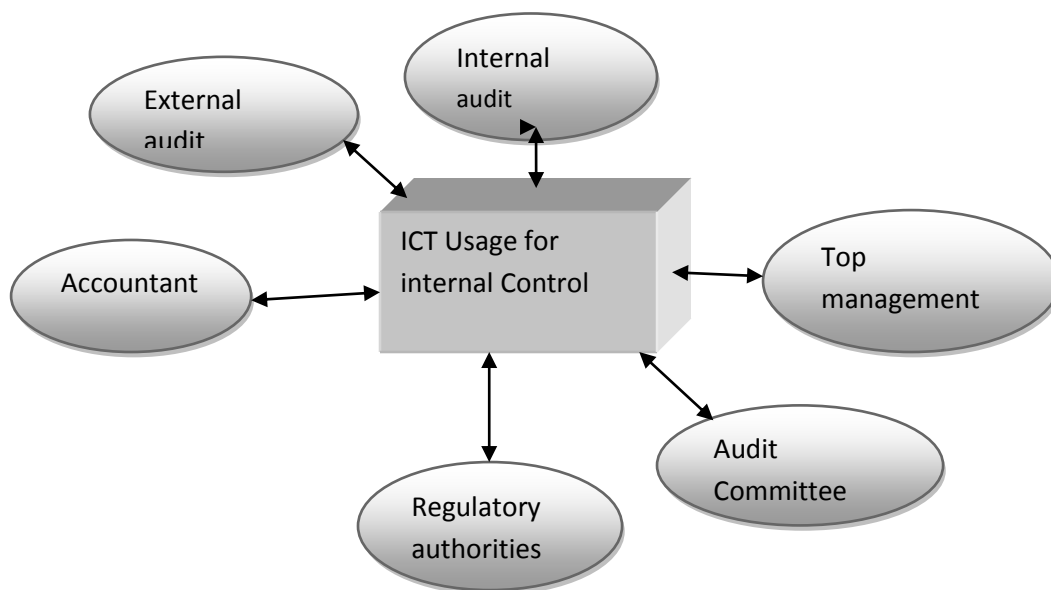


Figure 1.1: Functions Affected by ICT Tools and Techniques Usage for Internal Control

The six main functions affected by the usage of ICT tools and techniques are shown in Figure 1.1 above. Out of the six functions, Internal Audit is most directly involved in internal control activities. For instance, The IIA Performance Standard 2130 states that “Internal Auditors are involved in making appropriate recommendations for improving governance process in achieving the following objectives: promoting appropriate ethics and values within the organisation, ensuring effective organisational performance management and accountability, effectively communicating risk and control information to appropriate areas of the organisation and coordinating the activities of and communicating information among the board, external and Internal Auditors and management.”

The aim of this study is to examine the impact of ICT on the effectiveness of internal control in prevention and detection of electronic fraud in the Nigerian financial sector. This is done through the mirror of the Internal Audit Function. Internal Auditors are chosen because apart from being part of the Internal Control process they “evaluate and improve” the system of Internal Control in a “professional and impartial” manner (IIA, 1999).

1.2.0: Main Objectives of this Study

Based on the study's aim identified in section 1.1.0 above, the study sets out to achieve the following objectives:

To assess the level of ICT usage by Internal Auditors in internal control systems in Nigeria.

To examine the role ICT plays in Internal Auditors' independence and objectivity.

To assess the potential impact of ICT tools and techniques on electronic fraud prevention, and

To assess the effectiveness of ICT tools and techniques on electronic fraud detection.

1.3.0: Research Questions

In order to show a clear understanding and accomplish the aims and objectives of this study, the under-listed research questions are explored.

- i. What is the Internal Auditors' current level of ICT tools and techniques usage?
- ii. Does the use of ICT for internal control impact on Internal Auditors' independence?
- iii. How effectively does the use of ICT-based tools and techniques prevent electronic fraud?
- iv. How effectively does the use of ICT-based tools and techniques detect electronic fraud?

1.4.0: Research Propositions

Research propositions were developed from research objectives and subsequent questions. The propositions are evaluated by analysing data collected from questionnaire and interview.

1.0 Nigerian Internal Auditors are increasingly adopting IT-based tools and techniques for internal control. This is divided into three themes as follows:

1.1 Internal auditors' current level of use of ICT tools and techniques for internal control purposes is increasing.

1.2 Financial institutions' current level of provision of ICT tools and techniques for internal control purpose is increasing.

1.3 ICT tools and techniques are useful for internal control's task, efficiency and effectiveness.

2.0 The use of ICT-based tools and techniques in Internal Control impacts positively on Internal Auditor's independence and objectivity.

3.0 Internal auditors' use of ICT-based tools and techniques has the potential of preventing electronic fraud. This is divided into three themes as follows:

3.1 Internal Auditors' use of ICT has had positive impact on prevention of fraud

3.2 COA has effective fraud prevention control

3.3 The extent of ICT utilisation for prevention of fraud is affected by auditors' demographic characteristics (experience, gender, training and qualification)

4.0 Internal auditors' use of ICT-based tools and techniques are effective in detecting electronic fraud. This proposition is further split into three as follows:

4.1. Use of ICT in internal control has had positive impact on detection of fraud

4.2. COA has effective fraud detection control

4.3. The extent of ICT utilisation for detection of fraud is affected by auditors' demographic characteristics (experience, gender, training and qualification)

1.5.0: The Scope of the Study

This study focused on the financial sector of the Nigerian economy and the research questions are directed at identifying the effectiveness of the use of ICT for Internal Control in the prevention and detection of electronic fraud. Contextualising the scope of the study within the broader body of literature, Figure 1.2 below shows the research objectives in the context of ICT tools and techniques usage for internal control within the scope of this study.

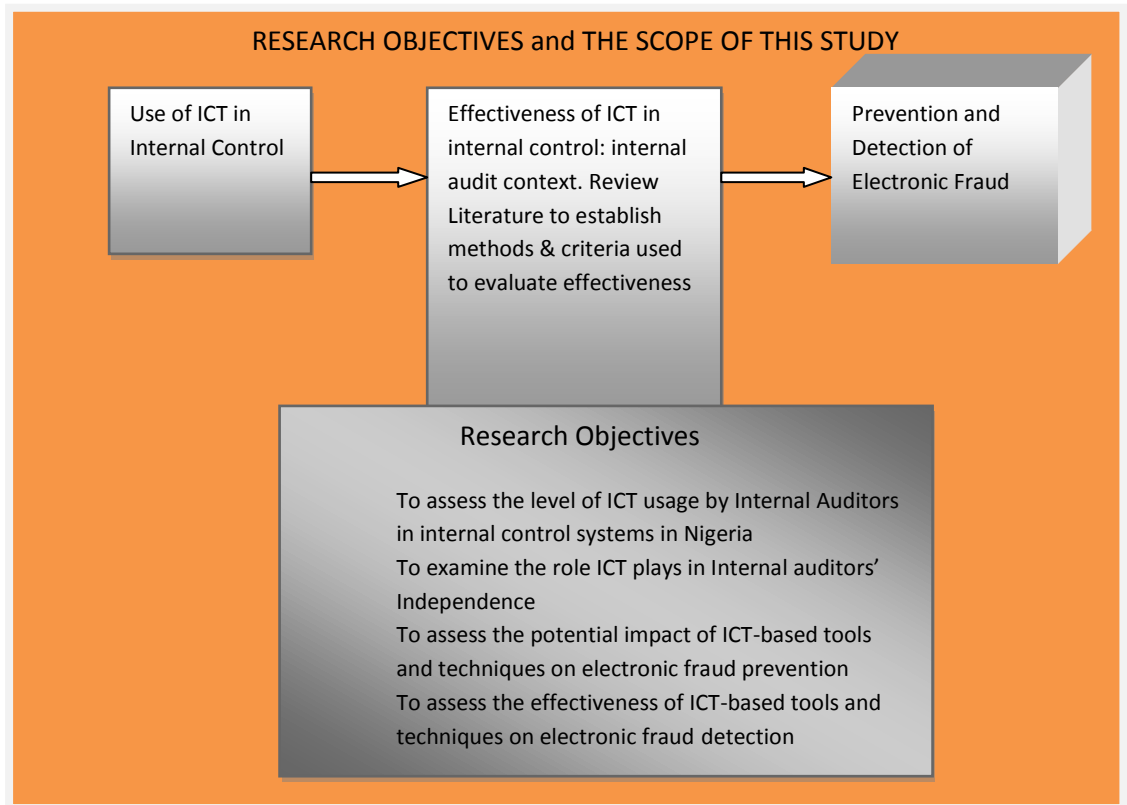


Figure 1.2: The context of ICT tools and techniques usage for internal control within the scope of this study.

Figure 1.2 shows that the scope of the research objectives locates the study in a post-implementation and business operational perspectives (a perspective that assesses system status, level of user satisfaction and further actions required to achieve set objectives). This study covers the activities of Internal Auditors working in the financial sector of the Nigerian economy since the main function of Internal Auditors is to ensure an effective internal control system whether ICT is being used or not.

Data were collected from Internal Auditors working in banking, insurance, stockbroking and investment firms through questionnaires and face-to-face

interviews. The choice of this diverse range of organisations is to enable the study to cover those organisations with common characteristics within the financial sector of the Nigerian economy. This study has carried out a detailed evaluation of the earlier listed phenomena to enable the researcher to provide appropriate answers to the fundamental questions raised in this section, which subsequently form the basis of the research objectives itemised in section 1.2.

1.6.0: Methodology

This study adopted both the quantitative and the qualitative research methodologies. The sample frame of 510 consisted of all Internal Auditors working in financial institutions in Nigeria that are using ICT tools and techniques for their basic operations. In the quantitative section, the researcher distributed 510 questionnaires (representing 100 per cent of the sample frame) that consist of a mixture of both open-ended and fixed-alternative questions. The open-ended questions were designed to give respondents the opportunity to supply their responses as they thought suitable, while the fixed-alternative questions adopted a five-option Likert scale. The study was piloted by testing the questionnaire on a set of people that were not too divergent from the target respondents, in order to detect possible deficiencies in its design and administration. This ensured the validity and reliability of the questionnaires used. The data obtained through administered questionnaires were analysed through the use of the Statistical Package for the Social Sciences (SPSS, version 18.0, employing both univariate and bivariate analyses. The latter is further strengthened, where necessary, by the use of Spearman's-rank correlation, a non-parametric technique used for measuring linear association between two variables based on ordinal datasets and one-way ANOVA (Cohen, 1998; Mitchell and Jolley, 2006).

The qualitative section concentrated on semi-structured face-to-face interviews with 21 prime executives in the internal audit function of financial organisations selected within the metropolis of Lagos (since more than 90 per cent of Internal Auditors operate in Lagos). The primary data collected from the questionnaire was helpful in setting up the interview questions in the second phase of the investigation.

Convenience sampling is adopted because investigating the impact of ICT tools and techniques on internal control in prevention and detection of electronic fraud incidence and improving security of internal control cannot be based on a random sampling either across industries or within a particular chosen organisation as it is subject to peculiar target research (targeting Internal Auditors as the main operators of internal control). Thematic analysis was adopted to analyse the results and observations from face-to-face interviews.

In addition, the study made use of Omoteso et al.'s Three Layered Model (TLM) to underpin the internal control effectiveness in prevention and detection of fraud. The TLM is a meta-level model comprising contingency, socio-technical and structuration theories. This is the first time the TLM will have been used by an independent researcher after it was proposed by Omoteso et al. (2007). TLM is combined in this study with the Technology Acceptance Model (TAM) which has remained popular with studies involving ICT adoption and usage.

1.7.0: Significance, Originality and Key Outcomes of the Study

There are limited studies on the impact of ICT on accounting or auditing in developed economies (Omoteso, 2006), whereas similar studies in developing countries are scarce. This study is privileged to be the first to explore the impact of ICT on the effectiveness of internal control systems in prevention and detection of fraud in a developing economy.

This study assessed the role, effectiveness and impact of ICT-based tools and techniques on internal control in preventing, detecting and controlling incidences of digital fraud, using a mixed methods approach. Its findings are of interest to policy makers within the executive and legislative arms of the Nigerian government and professional accounting bodies. Also, corporate financial organisations are able to design better control systems to curb fraudulent practices within their operations. The country's economic development could be enhanced as the financial sector constitutes the backbone of the nation's economic activities.

Past studies have investigated how consulting practice impacts independence of internal audit functions (Meredith and Akers, 2003). However, this study empirically

investigated how the use of ICT has affected the independence and objectivity of the internal auditor to perform his duties under management and board of directors. This is the first study that empirically carries out investigation of the impact of ICT on Internal Auditors' independence in a developing economy context such as Nigeria. The question of independence is important to the internal auditor as it is to the External Auditor. The effectiveness of ICT tools and techniques ultimately depends on impartial usage by Internal Auditors. This is reflected in the definition given by the IIA:

“Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve organisation’s operations.....”.

(IIA, 2004)

Without the independence and objectivity of IA the whole functions of assurance, consulting and adding values break down and it becomes difficult to see through the mirror of internal audit if ICT is having a positive or negative impact on internal control. The study found evidence which shows that the use of ICT for internal control has a positive impact on the reporting and operational independence of Internal Auditors.

In addition, this study has recommended new ways of operationalising the internal audit function by developing a new model: Technology Effectiveness Planning and Evaluation Model (TEPEM), to add to the understanding of prevention and detection of fraud in order to match the growing e-business activities and resultant control problems. Finally, the study identified ICT as a strong factor impacting internal control for effective prevention and detection of electronic fraud. Continuous online auditing is found to be effective for fraud prevention, however, not suited for fraud detection.

The next section provided the necessary background for the study in order to bring to light the peculiarity of the Nigerian financial and socio-political environment that may impact on financial internal control and accountability.

1.8.0: The Structure of the Thesis

Figure.1.3 below illustrates the structure of the research process followed. The research aim is used as a basis for a review of relevant literatures in order to identify knowledge gaps, deficiencies or limitations which possibly exist in current literature.

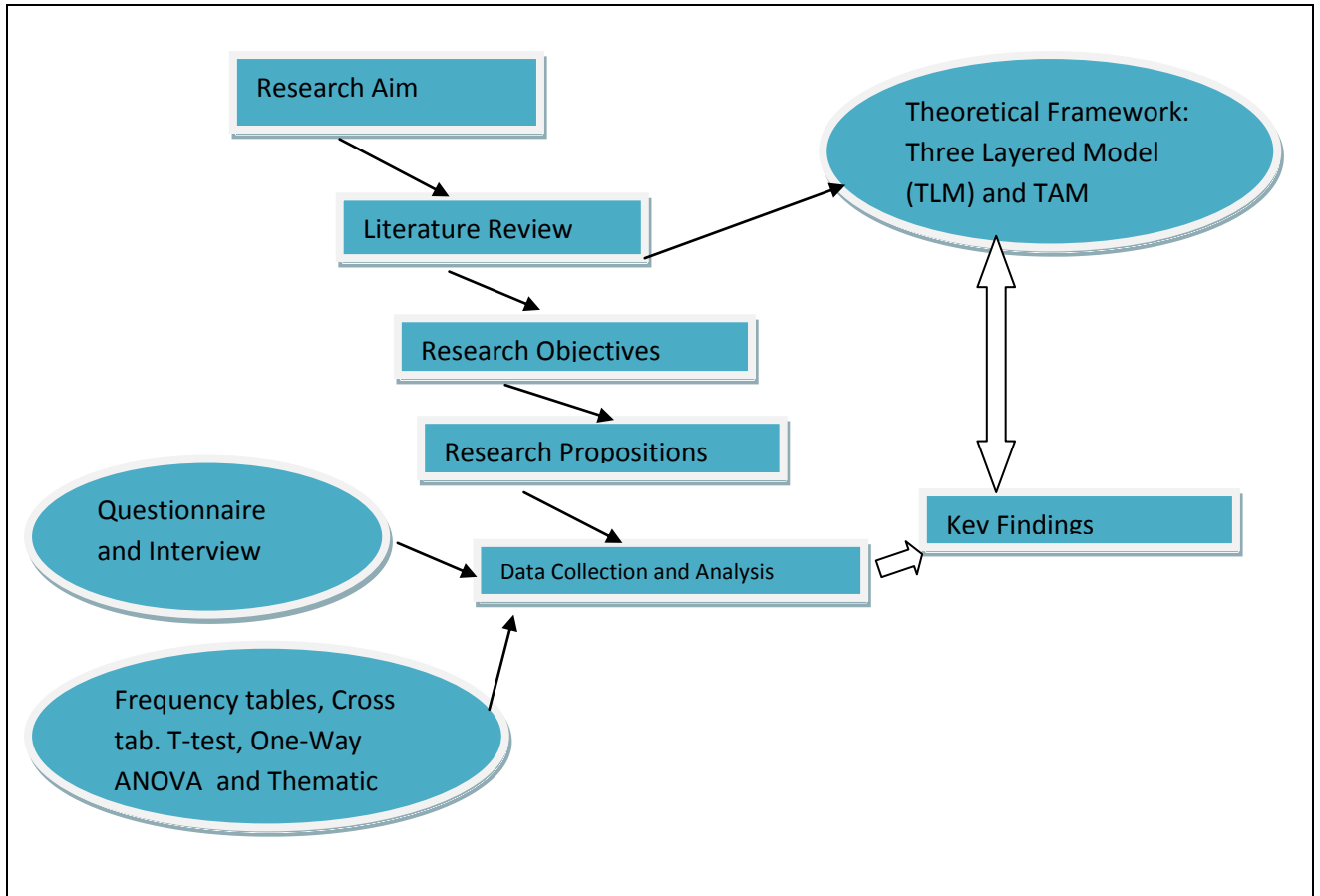


Figure 1.3: Structure of the Research Process

The researcher was able to formulate appropriate research objectives based on the hindsight gained from the review of literature. The objectives were further reviewed and expressed as research propositions. Research instruments were designed also based on knowledge gained from the literature. A mixed methods approach was adopted (questionnaire and interview) to collect data which was analysed using frequency tables, cross-tabulation, t-test, one-way ANOVA and thematic analysis to bring out key findings. Two theoretical models were used (Three Layered Model and Technology Acceptance Model) to underpin the study.

The remainder of the thesis is structured as follows:

In chapter 2, the researcher provided a historical perspective of the Nigerian commercial environment in order to provide necessary background for the central themes of the thesis. The chapter discussed internal control, internal auditing, and electronic fraud and ICT adoption efforts in the Nigeria environment. In chapters 3 and 4, the researcher produced a review of the literatures relevant to the main themes of the thesis. This involved a review of definitions and prior studies carried out in the area of internal control, internal audit, electronic fraud and ICT. In chapter 5 a review of the leading theoretical constructs that have prominence in the thesis were carried out to find appropriate theories that best explain the issues under investigation.

Chapter 6 sets out the research methodology issues and provided justifications for the chosen research strategy. The epistemological framework adopted in the study was provided and a consideration of alternative methods that could have been used was also undertaken.

Chapter 7 consists of initial data analysis and analysis of data concerning proposition 1 (Nigerian Internal Auditors are increasingly adopting IT-based tools and techniques), and proposition 2 (the use of ICT-based tools and techniques in internal control impact on Internal Auditors' independence and objectivity). Chapter 7 continues with data analysis for propositions 3 and 4: Internal Auditors' use of ICT-based tools and techniques has the potential of preventing and detecting electronic fraud. The two chapters present the empirical analyses and results of the study.

Finally, in chapter 9 the main findings of the research are discussed and summarised, while relating the applicability of the findings to the explanatory power of the TEPPEM model. The main contributions of the thesis to knowledge are highlighted along with limitations of the study. Future directions for research are identified and recommendations made.

1.9.0: Summary of Chapter

This chapter introduced the theme of the thesis: the impact of ICT on the effectiveness of internal control systems in prevention and detection of fraud in the

Nigeria financial sector. The chapter provided a general synopsis of the detailed research work carried out. The chapter started by providing a befitting overview of the thesis in the form of background details. A detailed outline of the aim, research problem, objectives and significance of the study, the methodology and research outcome were also provided.

The next chapter sheds light on the background to the study. It provides useful information on the political, economic and technological environment in which the study is situated. A review of the banking system before the colonial administration to date was carried out, since the banking system of any country reflects its economic viability. The professional and regulatory environment which may have an impact on internal control and internal auditing as a profession are also discussed. The chapter further sheds light on corporate governance challenges experienced in the financial sector and what measures regulatory authorities have taken to counter it. To show the importance of the war against e-fraud to the Nigerian government, samples of five cases initiated by EFCC are included in the Appendix.

CHAPTER TWO

BACKGROUND TO THE STUDY

2.0: Introduction

This section provides an historical perspective of the Nigerian commercial environment in order to provide necessary background for the central themes of the thesis. The section also considers the development of electronic transactions and the level of electronic fraud in the Nigerian financial environment. An attempt is also made to discuss the issue of corporate governance breakdown in relation to internal audit functions and existing institutional framework of internal auditing in Nigeria.

2.1: Recent Economic and Financial Reforms in Nigeria

Nigeria has an estimated population of 165 million (National office of statistics Abuja, 2010), 250 ethnic groups and a large landmass of 923,768 square kilometres (356,669 square miles). The country experienced a three-year long civil war that ended in 1970. In the same vein, incessant military coups d'état and a lack of accountability on the part of leadership as observed by Okike (2004, p. 707) "Accountability in all facets of the economy is an essential ingredient to the economic development of any nation. But achieving adequate accountability in Nigeria has become a major problem, which various governments have had to contend with, because of widespread corruption in almost all spheres of public and private endeavours and huge internal and external debts made the polity unstable and unattractive for direct foreign investment" (Iyayi, 2006). This is clearly stated by Okike (1994: 83) "Nigeria has had its own transformation (political, economic, and sociological) since independence. These changes include experimentation with different styles of government and different economic experiences (from a poor agrarian, cash-crop economy to an oil-based economy) and changing fortunes of the people – from poverty, through civil war, affluence, to crippling depression, and many ethnic tensions. This transformation within the Nigerian economy has significantly influenced the accounting profession in many respects". Nigeria for the first time in her political history had a successful civilian-to-civilian transition in 2008 notwithstanding the magnitude of protests that followed the announcement of

results. A number of meaningful developments in the polity, economy and technology have been recorded by the successive democratically-elected civilian governments. A number of reforms that targeted improving the economy and the polity in general were also embarked upon. Notable reforms included the setting up of an Economic and Financial Crime Commission (EFCC) to combat fraud and corruption; the bank recapitalisation reform that led to a reduction from 89 weak banks in the country to 24 strong banks, with about 12 being listed among the leading 1,000 banks in the world, an achievement that is quite unique (Soludo, 2007). Another important reform for the purpose of this study is the telecoms reform/deregulation among others that has made the country the fastest growing telecommunication nation in Africa and third in the world (NICTP, 2012). Furthermore, Nigeria is the most populous country in Africa with the latest estimated population of 165 million people (NPC, 2007). The Nigerian economy is growing, and with her abundant human resources has real potential to be a major economic force and beneficiary in the cyber space or e-commerce. For instance, Adekunle and Tella (2008:3) found that:

“...the vast Internet economy potential of Nigeria has not been fully utilised. For instance, in a 2000 export promotion conference in Geneva, Switzerland, it was observed that e-commerce is virtually non-existent. The few businesses that have an idea of what e-commerce is all about are having their hands full trying to cope with one infrastructural deficiency or another”.

The situation is however rapidly changing for the better. For instance, in another study Oyeyinka and Adeya (2002) found that only six per cent of the study population in Nigeria used the Internet to conduct electronic businesses. Extrapolating this to the whole adult population will give about eight million users. This is consistent with the observation of Adekunle and Tella (2008 : 3) that:

“.....despite this grim picture and the seeming monumental challenges.....as they attempt to engage in the Internet economy, an optimistic wave of improvement is blowing across the entire business community in Nigeria”.

Banking and allied services are the most prominent sector to benefit from this vast emerging Internet economy market. The rapid transformation in traditional banking services is quite noticeable. Electronic banking services in the form of e-transfer and withdrawal of large sums of money are encouraged. This facilitates the use of Automated Teller Machines on a wider scale. Other electronic banking products such

as Credit Cards, Smart Cards and Internet lending e-banking are also becoming popular (Awad, 1988).

The Information and Telecommunication sector has proved to be an important driver of the Nigerian economy in a bid to transform into Internet economy. The widespread adoption of sophisticated Internet-ready mobile telephone handsets within the last few years played an important role in facilitating the Internet economy in Nigeria. For instance, Adekunle and Tella (2008) observed that GSM technology is designed to function well with existing infrastructural facilities, especially the World Wide Web. To facilitate business transactions over 60 per cent of the population (about 84 million) have adopted the use of GSM technology. Adekunle and Tella (2008) further identified one other factor that propelled the digital economy in Nigeria as the commitments of most tertiary academic institutions into the Internet economy in the form of competitive online degrees and Internet advertisements. Consequently, most students and prospective students are encouraged to make use of Internet facilities.

To further encourage the use of electronic banking, the Central Bank of Nigeria (CBN, 2009) issued a circular to direct all banks in Nigeria from January 2009 to adhere to N10 million as the maximum amount for payment by cheque through the bank clearing system starting from January 1, 2010, while higher values are required to be effected only via the electronic payment system. According to the report, the rule appears to have been encouraged by the seeming success of the adoption of e-payment systems by Federal Ministries, Departments and Agencies (MDAs). The limit placed on amounts payable to bank customers has markedly changed the volume and value of transactions in favour of the electronic system. The UK has also recently given a nine-year-long notice to commercial banks to phase out the use of cheques in favour of electronic payments.

With the increased use of electronic payments, one may expect a jump in electronic fraud without a corresponding effort to strengthen internal control mechanisms. For instance, the CBN (2009:2) notes that:

“...the case of compliance with payment of large sums in an all-MDA test run of the electronic payment mode was quite expected. However, the implicit suggestion that the operation of the e-payment system so far has been graft-free is unproven just as

the apex bank's apparent expectation that spreading the e-payment net to cover an expanded segment of all bank users would reduce risks if the payment system overlooks the exposure of affected (public and private sector) financial transactions to the high risk of financial information interception and abuse".

It is in realisation of the potential risk that the CBN came up with another measure to put extra security on all ATM machines to secure the user and his/her money while they are using ATM cards for withdrawals. The measure included an email/SMS verification code which is sent to the user's mobile number or email addresses any time the ATM card is slotted into any ATM machine. The Nigerian economy is currently experiencing positive growth due to increased activities in the capital market. According to Ashamu and Abiola (2012: 256) "The fundamentals of the Nigerian economy are strong. This is evidenced by the fact that as of October 1, 2008, the quantum of Nigerian foreign reserve stood at about 63 billion US Dollars, while the foreign direct investments (FDI) remained strong at 8.5 billion. These statistics prove that Nigerians' vulnerability to the credit-induced crisis through currency depreciation is reduced".

Consolidations of commercial banks into 24 mega-banks with substantial paid-up capital also make funds available to other industries. With substantial investment in ICT, it is expected that electronic fraud will proportionately increase.

The banking system, which formally started in 1892 (Nwankwo, 1975) pre-dated Nigeria independence and has remained a central pillar of the Nigerian economy. According to Chiejine (2010), the financial system has undergone noticeable transformations in character, organisation and structure since 1892.

An array of scholars agreed that a country's financial system, as represented by the banking system, is a direct mirror of her economic development (Goldsmith, 1955; Shaw, 1973; Adewumi, 2009). It is because of this important role that the financial sector of the Nigerian economy is being repositioned at constant intervals particularly under the various reform agendas. Nigeria has experienced various financial reforms since 1929. The most significant reforms took place between 2004 and the present day. This period experienced a phenomenal increase in the share capital of banks and also led to mergers and acquisitions among those that survived the reforms. The

reform made more funds available to banks to invest in modern ICT tools and equipment in order to upgrade their services to meet international requirements.

2.2: The Growth of Information Technology in Nigeria

The National Information Communication Technology policy (NICTP) draft (2012) put together by the ministerial committee on ICT policy harmonisation noted:

“.....these policy and regulatory developments along with other government and private sector initiatives have resulted in significant improvement of the ICT sector. For instance, Nigeria has moved from approximately 400,000 available fixed telephone lines pre-1999 to over 90.5 million available mobile telephone lines by the first quarter of 2011, thereby making Nigeria’s telecommunications market the fastest growing in Africa. There are now modest ICT deployments in the functioning of government organisations, as well as in the private sector. In addition, ICT now drives some activities in the financial and oil and gas sectors while various e-government initiatives are ongoing in various departments at the three tiers of government.” (NICTP, 2012: 9)

NICTP (2012) further gave a breakdown of mobile and internet penetration as follows:

Table 2.1 Penetration of Information Technology in Nigeria

i.	Mobile Penetration (per 100 people)	55.76
ii.	Fixed Telephone Penetration (per 100 people)	0.48
iii.	Internet Penetration (per 100 people)	23.48 (2010)
iv.	Internet Users (000)	43,270 (2010)
v.	Broadband Penetration	6.1% (2010)
vi.	PC Penetration (Number of PCs per 100)	4.7 (2010)
vii.	Computers Assembled in Nigeria	<500,000
viii.	Number of Registered ICT Companies	350
ix.	Broadcasting Stations Nationwide	308
x.	Post Offices (inc. Postal agencies and shops)	3000 +

Source: (NICTP, 2012:10)

Table 2.1 above shows that the numbers of those who have access to internet in Nigeria as at 2010 are 43,270,000 people. This is about 24 per cent of the Nigerian population. This is expected to increase as the broadband penetration increases from the 6.1 per cent level.

In a study carried out in Nigeria, Adesina, and Ayo, (2010) empirically investigated the level of users' acceptance of e-banking in Nigeria. Extended Technology Acceptance Model (ETAM) was employed as a conceptual model to investigate factors that influence users' acceptance and intention to use electronic banking. The study employed 600 survey questionnaires administered to bank customers (users) within the Lagos metropolis. Data were collected from 292 respondents. Correlation and regression analysis were used to measure the impact of perceived credibility, computer self-efficacy, perceived usefulness and perceived ease of use on customers' attitude.

Adesina and Ayo (2010) found that "44.6% of the respondent always use ATMs; 22.3% almost always use ATMs and 12.2% use ATMs". The least used is the mobile banking system. 44.3 per cent of respondents claimed not to have ever used the mobile banking system. Respondents also identified network security and system privacy problems as a major hindrance for the use of internet banking. The study was able to identify perceived credibility as an additional factor to the TAM model.

The study provided an empirical basis for testing the TAM model in the Nigeria environment. However the data were collected only restrictively from bank customers in Lagos only. This may make generalisation of the result difficult. Adesina and Ayo's (2010) study provided a good reference point for the current study as the study is conducted in the same environment and making use of the TAM model. Unlike Adesina and Ayo's (2010) study, however, the target respondents are not bank customers but IAs of financial institutions.

In another study, Achimugu et al. (2009) conducted an impact analysis of adoption of ICT in developing countries. The study was designed to determine the level of ICT diffusion in the Nigeria economy, the impact on organisations as well as the factors responsible for the diffusion.

Achimugu et al. (2009) used the literature review approach to highlight the current trend in ICT usage in Nigeria. The paper further succeeded in shedding light on the areas of challenges. Achimugu's et al. (2009) appeared not to have achieved the goals set for themselves, as the study lacked empirical and theoretical inclinations to be able to determine the level of diffusion of ICT in the Nigeria economy. The study was purely descriptive in nature and lacked detailed analysis. However the study provided a good framework for further studies as it identifies major challenges facing ICT adoption.

2.3: Incidents of Fraud in the Financial Sector of the Nigeria Economy

Internet usage presents impressive statistics as computers and Internet penetrations are expected to increase phenomenally over the coming years. But there is a paradox, according to Seetharaman et al. (2006) the development of computer technologies in organisations has greatly enhanced the ability of people to defraud. Many commentators (for example, the Audit commission, 1987) observed that opportunities for misuse of ICT continue to increase in consonance with technological advancement. Many fraud cases go unreported for different reasons, therefore the amount of losses caused can only be estimated. The formats, causes and effects of fraud on banks and other financial institutions have been well documented by many authors, including Nwankwo (1991), Financial Institutions Training Centre (FITC) (1992) and various publications of the Nigeria Deposit Insurance Corporation (NDIC). With regard to the effects on banks and banking industries, Nwankwo (1991) said that fraud is the biggest single cause of bank failure, while Adewumi (2004) suggested that fraud is capable of damaging the banking habit of any economy. Fraud is therefore feared by all the banking stakeholders except the fraudsters themselves.

Efforts to control fraud in the Nigerian financial sector have been constant concerns both for the operators and regulators alike. The common control strategies adopted by banks focus on prevention, detection and investigation. The way banks exhibited the use of these strategies were discussed in the literature (Sydney, 1986; FITC, 1992; Nwankwo, 1991) Among other things, the installation and implementation of internal

control systems, use of bank inspectors, internal and External Auditors are identified as important.

Management often takes the blame for not doing enough to manage fraud. For instance, FITC (1992) asserted that poor management in terms of inadequate supervision; inadequate control and under-staffing are the most significant causes of fraud. Umoh (2004) also noted that bank fraud arises principally from weak internal controls and retention of staff with a fraudulent propensity. Sanusi (1986) drew similar conclusion by pointing to the weakness of internal control systems. Adewumi (1986) held management responsible stating that inadequate control is indicative of poor management.

To remedy the rising cases of bank frauds, FITC (1992) suggested the need to measure the efficiency of control systems and further observed that *“although some authors have suggested the causes of ineffectiveness of fraud control measures, past studies had failed to assess empirically the effectiveness of fraud control”* (FITC, 1992 : 19). This is what the present study is focusing on. Furthermore, Sanusi (1986) suggests that the answer is in efficient and well-monitored internal control systems, while FITC (1992) suggests adequate management supervision and regular balancing of accounts, training and retraining of staff as well as adequate internal controls. KPMG (2005), in its African Fraud and Misconduct survey says that the majority of respondents indicated that controls require review and improvement in order to reduce fraud. This view is more relevant now as most transactions are now conducted online. For instance, the number of reported cases of frauds and forgeries in insured banks rose during 2007 compared with previous years (NDIC, 2007) Table 2.3 below confirms this.

Table 2.2: Returns of Insured Banks on Fraud and Forgeries

Quarter	Year	Total No. of fraud cases	Total Amount Involved (N'M)	Total Expected Loss (N'M)	Proportion of Expected Loss to Amount Involved (%)
1st	2007	397	4,128.00	858.00	20.78
	2006	268	740.12	422.94	57.14
2nd	2007	335	1,083.94	562.53	51.89
	2006	284	1,429.06	824.17	57.67
3rd	2007	398	2,196.00	615.60	28.03
	2006	334	843.82	547.86	64.94
4th	2007	423	2,597.87	834.72	32.13
	2006	307	1,819.35	973.69	53.52
Average/	2007	1553	10,005.81	2,870.85	28.69
Total	2006	1193	4,832.17	2,768.67	57.29

Source: NDIC 2007 Annual Report and Statement of Accounts

As shown in Table 2.2, there was a total of 1,553 reported cases of attempted frauds and forgeries involving over N10.0 billion (Nigerian Naira) made up of (N8.8 billion, US\$591,487.8, GB£12,410 and 35,390 euro) occurred in 2007 compared with reported cases of fraud involving N4.8 billion made up of (N4.6 billion, US\$1.8 million and GB£14399.74) in 2006. Further analysis of the methods involved in fraud perpetration confirms that about 36 per cent (2006) and 43.5 per cent (2007) of the total fraud are accounted for by computer online fraud manifested in the form of posting of fictitious credit and fraudulent transfers. The jump in the level of fraud has been attributed to two sources, namely: the consolidation of banks and the resultant

availability of a large pool of cash and large investment on ICT and the resultant increase dependency on electronic banking.

Most of the regulatory authorities (Central Bank of Nigeria (CBN), Nigeria Deposit Insurance Corporation (NDIC); Nigeria Security and Exchange Commission (SEC) and The National Insurance Commission (NICOM)) strongly recommend a strong internal control system and well trained Internal Auditors for all financial institutions because of perceived vulnerability to computer fraud.

2.4: Internal Audit Practice in Nigeria

The importance of internal audit practice in relation to accountability cannot be overemphasised. According to Okike (2004:707) *“The success of the government’s anti-corruption campaign hinges on effective cooperation with various corporate governance mechanisms, prime amongst which is the role of accountants and auditors in financial reporting”*. The Institute of Chartered Accountants of Nigeria (ICAN) is the first professional institute regulating and controlling accountancy and auditing practice in Nigeria. The Institute became chartered by Act of parliament in 1965 (ICAN Act, 1965). “Prior to 1990, there was no regulation for the market of audit services in Nigeria and no professional code and standard of auditing practice. Most audit firms had to (and still) depend on the generally accepted auditing practices contained in various manuals of the international auditing firms to which they are affiliated, including guidelines of the International Federation of Accountants (IFAC), of which ICAN is a member” (Okike, 2004:712). With all the founding members drawn from ICMA, ACCA and ICAEW, The Institute of Chartered Accountants of Nigeria is an important regional member with about 35,000 members and 120,000 students of the International Federation of Accountants (IFAC) having pioneered the development of accountancy profession in West Africa sub-region. The majority of Internal Auditors in big companies in Nigeria are members of ICAN and have to abide by professional ethics and rules of the institute. The second accounting body in Nigeria recognised by Act of parliament is the Association of National Accountants of Nigeria (ANAN) whose members operate mainly in the civil service as public auditors and accountants. ANAN and the Chartered Institute of Taxation of Nigeria

(CITN) obtained Nigeria government recognition and compete with ICAN members to do both auditing and taxation practice respectively. Recently, the Institute of Certified Public Accountants of Nigeria (ICPAN) also became recognised as a ‘new entrant into the accounting professional bodies in Nigeria in spite of strong representation from ICAN the House of Representative unanimously passed the ICPAN Bill in October 2005 (ICAEW, 2007). All the members of these professional bodies can be employed as IAs in Nigeria. The majority of banks and insurance companies visited employed only ICAN members.

The Companies and Allied Matters Act of 1990 is also an important legislation for Internal Auditors. It imposes responsibility on audit committee to report on internal control effectiveness during the year (CAMA, 1990 section 359 (6)). The audit committee relies on the Internal Auditors to help them in this important task.

The SEC, CBN, NDIC, and NICOM exert institutional pressure on businesses especially financial institutions in the course of their oversight function through regular issuance of circular letters and off- and on-site inspections.

Commenting on the challenges to accounting and auditing practices in Nigeria, Okike (2009: 137) quoting R.S.O. Wallace, 1992 emphasised the cultural dimensions thus:

“Additionally, cultural factors often influence auditors’ relationships. Cultural demands – such as displaying respect for elders and loyalty to family, village or tribe – have and will continue to have telling effects on auditors’ independence and professionalism. The obligation to respect elders probably makes it difficult for a young Nigerian accountant to seek an explanation from an elderly person for a statement that the younger person knows is questionable”.

The effects of the cultural influence is even more pronounced with Internal Auditors since most of their internal clients are more often than not various line managers within their organisations who are mostly elderly persons who probably have spent more years in the same organisation than the internal auditor.

2.5: Internal Auditing and Internal Control in the Nigerian Financial Sector

There have been a number of recent developments within the Nigerian business environment that may have direct or indirect impact on internal control and internal audit functions. Most of the reforms carried out by various governments were aimed

at opening up the Nigerian economy to the outside world in order to provide an enabling environment for Nigeria to compete in the global economy.

For instance, in 1995 the Nigeria Enterprises Promotion Decree (NEPD), which hitherto restricted foreign ownership of shares in certain businesses was repealed and replaced with the Nigerian Investment Promotion Commission Decree (NIPCD) which is far friendlier to foreign investors. The resultant effect of this was an increase in foreign investment flow and the expansion of existing businesses including banks.

Furthermore 1995 witnessed massive deregulations of foreign exchange control in Nigeria. The strongly restricted exchange control regime was replaced with a very flexible exchange regulation. Private individuals alongside corporate bodies are now permitted to operate bureaux de change for exchanging foreign currencies to local Naira and vice versa. This is contained in Foreign Exchange (Monitoring and Miscellaneous Provision) Decree of 1995. Domiciliary accounts which were hitherto forbidden for individuals in Nigerian banks are now allowed for savings and withdrawals of foreign currencies. In spite of efforts directed at curbing money laundering activities, Nigeria is still listed among countries that have not made significant progress in addressing critical issues in their Anti Money Laundering (AML) campaign. According to the Financial Action Task Force (FATF), which was established in 1989 by the G-7 countries, the group-two countries include: Cuba, Bolivia, Ethiopia, Ghana, Indonesia, Kenya, Myanmar, Nigeria, Pakistan, Sao Tome and Principe, Sri Lanka, Syria, Tanzania, Thailand and Turkey. Ghana is the second country named with Nigeria in West Africa. One of the critical standards of FATF is anchored on a strict internal control framework aimed at applying preventive measures to safeguard the institutions involved in financial intermediation and other designated sectors which is part of the focus of this study.

The most important reform that impacted corporate internal control is privatisation which commenced in 1988. Most government controlled corporations were sold out to core investors. Ownership of fifty-seven (57) government corporations changed hands from being government controlled to individual investors through the privatisation programme by 1999 (Ahunwan, 2002)

Privatisation encouraged reforms in the capital market. The activities in the Lagos stock exchange were more than doubled. Most individuals and companies including banks have unrestricted access to finance from the capital market. Unexpectedly, most Chief Executive Officers struggled with a funds management problem which they were not prepared for, while maintaining the old internal control structures that were no longer relevant to the operational size and volume of transactions of their various institutions.

The bank consolidation reform initiated by the Central Bank of Nigeria has recorded some visible success. The number of banks reduced to 24 from 95 before consolidation. With the minimum capital raised to 25 billion Naira, Nigerian banks have enough liquidity to compete globally.

All these reforms brought with them obvious problems of internal control and corporate governance in the sense that most of the banks still operate the same management structure before the capitalisation with the Chief Executive Officer holding substantial equity and power even at board level and consequently overriding internal control with impunity.

In a recent study on poor corporate governance and its consequences on the Nigerian banking sector, Oghojafor, et al. (2010) found that the central bank regulatory officials lacked integrity and boldness to carry out effective oversight functions. Oghojafor et al. (2010) also noted that most examiners lack appropriate technological skills to match the technologically-driven banking operations. The study (Oghojafor et al., 2010: 249) observed that:

“...the explosion in the numbers of banks and information technology has not been matched with CBN supervisory employees’ skills improvement. Thus, there is the need to urgently intensify the training and retraining of these officials”.

The study further blamed the banking crises on poor governance culture on the part of management and the board. The study failed to blame the banking crises on inability of internal control and internal audit to checkmate fraudulent transactions and raise appropriate concerns to shareholders/audit committee. It is doubtful if Internal Auditors can be said to be objective or conduct their assignment without undue interference from management in a situation where the Chief Executive Officer can

override board decisions with possible impairment of Internal Auditors' independence and objectivity.

Evidence that all is not well with the Nigerian banking sector's internal control process can be found in the recently concluded EFCC cases against some bank executives. A good example is Oceanic bank where the former CEO Cecilia Ibru pleaded guilty to three of 25 counts of fraud and mismanagement in 2009. She was sentenced to six months in prison for fraud and ordered to hand over \$1.2bn or (£786m) in cash and assets (Punch newspaper paper, 2009).

Also, the former CEO of bank PHB was accused of fraud involving £320 million of depositors' funds. Other examples are Executive Chairman of Afribank fraud involving £220 million and CEO of Intercontinental bank of £108 million. (EFCC, 2012) These are all huge losses which would not have been possible without lapses in internal control and corporate governance. As a matter of expediency, the CBN sacked the management and board of five banks replacing them with selected new officials to protect the depositors' funds.

2.6: Summary of Chapter

This chapter has considered the detailed economic, financial and technological background of Nigeria in the last few years to the present. In particular the progress made in the banking sector, ICT sector and professional accounting services were explained. In the same vein the challenges being experienced in the financial sectors in terms of control lapses and subsequent level of frauds experienced within the Nigeria economy were also considered.

The next chapter provides a detailed review of literature on internal control, internal auditing functions, ICT tools and techniques, and recent development in internal auditing. This is done with a view to identifying gaps in the literature, a portion of which this study is designed to fill.

CHAPTER THREE

A REVIEW OF LITERATURE

3.0: Introduction

This chapter is devoted to the review of existing bodies of knowledge on related studies that have been carried out in areas of internal control, internal auditing, and effectiveness of ICT tools in the prevention and detection of electronic fraud in different nations cutting across different continent of the world in order to have a good understanding of what has been carried out and to highlight gaps that are available in the literature. This study intends to fill a portion of such identified gaps from the literature. In order to do this, the next session commences with definition of internal control and internal auditing and progressed to examine different internal control models including developments in internal auditing. A session is devoted to explanation on internal control effectiveness for fraud prevention and detection. A detailed critical review is carried out on internal control and internal auditing

Figures 3.1 on the next page summarises the key literatures reviewed in this chapter.

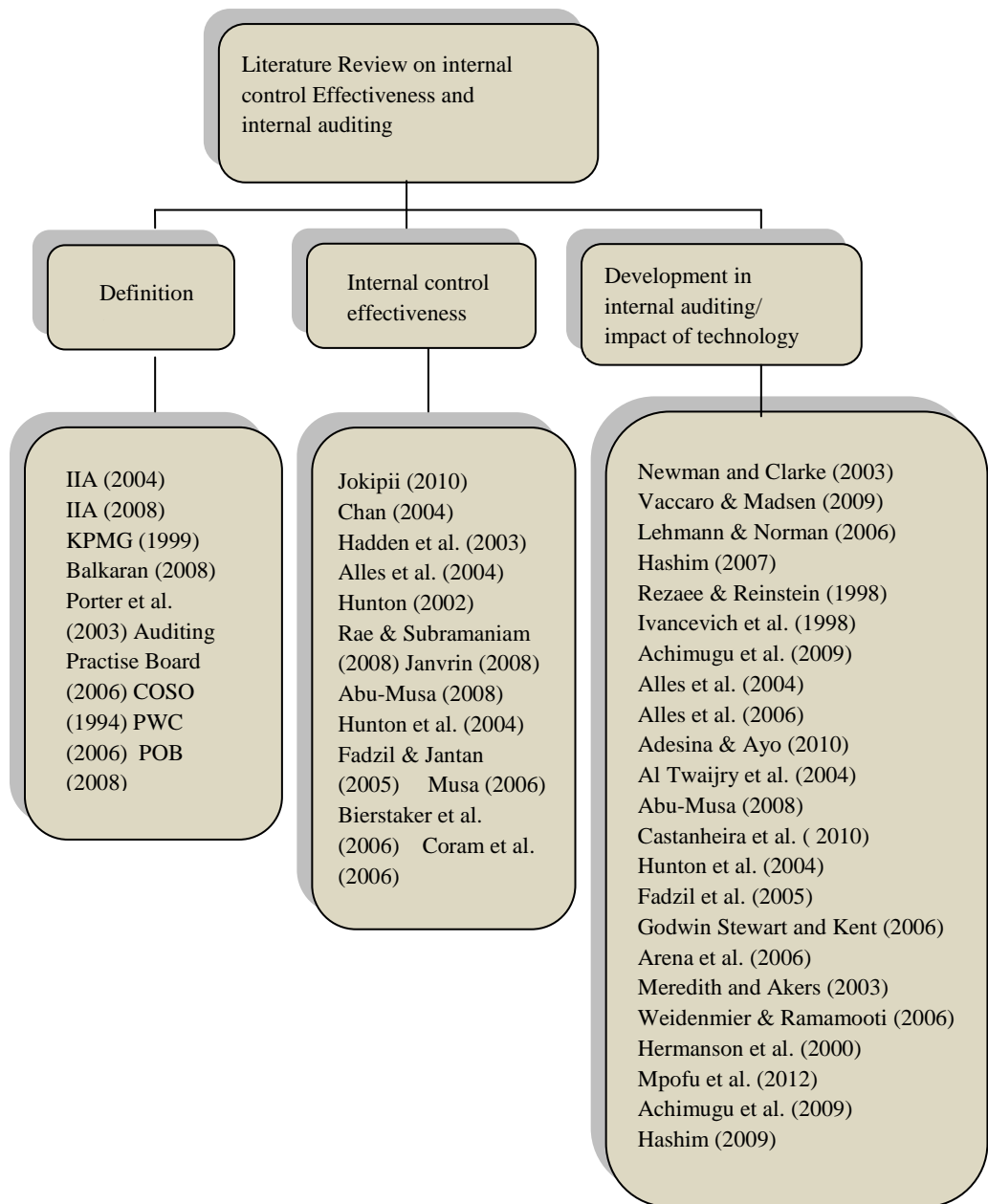


Figure 3.1: A Summary of Literature (Part 1)

3.1 Internal Controls – Towards a Working Definition

The difficulty in attempting a universally acceptable definition of internal control was noted by the Financial Markets Authority (AMF, 2004):

“unlike corporate governance, which now benchmarks standards against which issuers can compare themselves, the absence of a unanimously accepted reference framework for internal control makes the task of describing it much more difficult and can be an obstacle if one eventually wishes to assess the adequacy and effectiveness of the systems”.

The difficulty in attempting a universally acceptable definition notwithstanding, KPMG (1999:19) quoting the Turnbull Committee, made an attempt to describe internal control thus:

“An internal control system encompasses the policies, processes, tasks, behaviours and other aspects of a company that, taken together: facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company’s objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed, help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organisation; help ensure compliance with applicable laws and regulations, and also internal policies with respect to the conduct of business.”

The definition given by The Committee of Sponsoring Organisations (COSO, 1994) is still widely regarded as representing the dynamics of controls:

“Internal controls are put in place to keep the company on course toward profitability goals and achievement of its mission, and to minimise surprises along the way. They enable management to deal with rapidly changing economic and competitive environments, shifting customer demands and priorities, and restructuring for future growth. Internal controls promote efficiency, reduce risk of asset loss, and help ensure the reliability of financial statements and compliance with laws and regulations”.

Taking its cue from the above definition, the present study views internal control as effective when it “promotes efficiency, reduces risk of asset loss, and helps ensure the reliability of financial statements and compliance with laws and regulations”.

Establishment of control is inevitable where risks can be identified if achievement of objectives must be attained. In a highly risky environment like financial institutions, establishment of a reliable system of internal control is desirable. Pickett (2005) posits that setting a clear objective is the first step and the second step is scanning the environment to identify inherent risks that are intended to be controlled. It must be noted, however, that internal control is normally installed to manage or reduce and not to eliminate risk.

3.2: Internal Control Models

This section discussed different existing internal control models; (the Committee of the Sponsoring Organisations (COSO); the Criteria of Control (CoCo); the Control Objectives for Information and Related Technology (CobiT) and Basle Committee on Banking Supervisor) that are internationally recognised.

COSO (1992) introduced a framework for the consideration of control risks, which expanded the focus of the traditional view of controls at the detailed account and assertion level to include a global business perspective. The Information Systems Audit and Control Foundation (1998) issued the CobiT framework. CobiT follows a business orientation that begins with business objectives, which drives IS strategy (e.g. planning and organisation of IT) and the subsequent evaluation of risks and controls over information and data processing. According to Chan (2004), some auditors have found that the IT Governance Institute's CobiT aligns well with their Sarbanes-Oxley Act (SOA) compliance efforts. The Institute's IT control objectives for SOA further clarifies CobiT's relevance to SOA projects and reveals a high concentration of IT processes around COSO's "Control activities" and "Information and communication" components.

3.2.1: Committee of the Sponsoring Organisation (COSO)

The COSO model has been accorded international recognition as an acceptable standard for internal control. The model recognised the fact that all big organisations require a formal internal control procedure and recommends that adequate criteria be used in evaluating whether objectives are met or not. The COSO model provided a

useful platform that different control frameworks can be developed to reflect diversity in control environments.

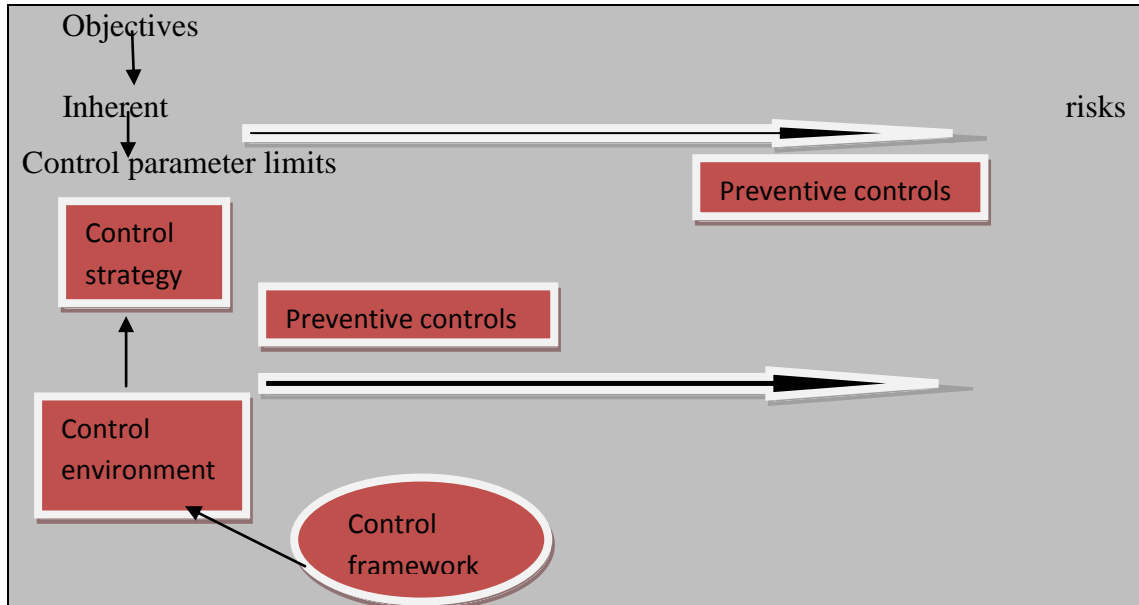


Figure 3.3: Internal Control

Source: Pickett (2005: 90)

In Figure 3.3 above the COSO framework recognises the control environment as a separate component. In essence the framework itself drives the environment and encourages organisations to develop a control strategy to respond to assessed risk. The COSO model recommends four components to define the responsibility of management for effective internal control: control environment; risk assessment; control activities and information and communication. COSO is regarded by many users to be powerful and dynamic. It has a wide coverage of structures and processes for control purposes. Internal control structure, internal control system, and internal control are used interchangeably to refer to the same constructs by different researchers. This study adopts Jokipii's (2010:120) approach by using internal control as the "broadest term that encompasses the other terms. Internal control system refers to the systematic use of an internal control structure The COSO framework has different descriptions for internal control structure. The following five components are distinguishable (Jokipii, 2010: 118):

"The control environment component defines the ethos of an organisation and the way it operates. This component refers to the creation of an atmosphere in

which people can conduct their activities and carry out their control responsibilities. It creates the overall control culture in the firm.

The risk assessment component refers to the processes of dealing with the risks that pose a threat to achieving the firm's objectives. It involves the identification, analysis and assessment of relevant risks.

The control activities component refers to policies, procedures and practices that assure management that the objectives are achieved and the risk mitigation strategies are carried out effectively.

The information and communication component ensures that relevant information is identified, captured and communicated in a form and time frame that allows personnel to carry out their duties and responsibilities effectively.

The monitoring component refers to a process of assessing the quality of control. It covers ongoing and periodical evaluations of the external supervision of internal controls by management or other parties outside the process."

SOX sec.404 recommends that a control framework be used but fails to identify which framework. The 1992 Internal Control-Integrated Framework by COSO is perhaps the only natural choice. The COSO framework was not popular with many users until SOX's passage (Alles et al., 2004; Colbert and Bowen, 2005).

According to Weidenmier and Ramamoorti (2006) obtaining better internal control effectiveness requires solutions to the following questions:

"...which (COSO) control components are the strongest and weakest in organisations? How does the selected framework affect the (IT) audit? Are internal controls more effective when the organisation has a well-developed ERM process"?

More empirical studies are required to determine the long-term effects and effectiveness of SOX and level of compliance by organisations.

3.2.2: The Criteria of Control (CoCo)

The criteria of control (CoCo) are a model developed by the Canadian Institute of Chartered Accountants (CICA) in 1992. CoCo has been accepted as a good international standard for internal control structures. The CoCo model has 20 criteria segmented into four areas thus: "purpose (direction), commitment (identity and values), capability (competence), and monitoring and learning (evolution)". CoCo is considered as an improvement on COSO as it is more flexible and improves decision

making and controls. The model is also divided into four groups thus: purpose; commitment; capability and learning monitoring (IIA, 2008).

3.2.3: Control Objectives for Information and Related Technology (CobiT)

Control Objectives for Information and Related Technology (CobiT) was developed in 1996 as a controls-based framework for IT governance. CobiT is also segmented into four domains thus: planning and organisation; acquisition and implementation, delivery and support; monitoring and evaluation. The CobiT model provides guidance to organisations on the use of IT resources and how to manage IT processes and organisation legal requirements.

3.2.4: The Basel Committee on Banking Supervision's Framework for IC System

The Basel Committee on banking supervision introduced the framework in 1998. Members of the committee include banking supervisory authorities from Sweden, Switzerland, Netherlands, the United Kingdom, and the United States. The framework incorporates elements of regulatory compliance. The Basel Committee has five elements of internal control which are: "Management oversight and control culture, risk recognition and assessment, control activities and segregation of duties; information and communication, and monitoring activities and correcting deficiencies" (IIA, 2008).

3.3: Internal Audit

The Institute of Internal Auditors (IIA) defines internal auditing as follows:

"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improve the effectiveness of the risk management, control, and governance process" (IIA, 2004).

The main target of Internal Auditors is on ensuring risk management, internal controls efficiency, and governance to ensure that stake holders' values are protected

and to reduce unintended surprises by improving business process and preventing fraud (Hermanson et al., 2010).

The Internal Auditors focus is on future events as a result of their continuous review and evaluation of internal controls and processes. In contrast, external auditing provides an independent opinion of a company's financial statements and fair presentation. The external auditing approach is mainly historical in nature, although some improvements that may have substantial impact on the future may be suggested in the auditor's recommendations to management based on the analysis of controls during a financial statement audit (Balkaran, 2008). An audit can be described as an independent investigation or a search for evidence to enable an opinion to be formed on the truth and fairness of financial statements prepared by another person or persons without undue influence in order to increase its usefulness and credibility.

These definitions alone pinpoint precisely the key distinctions that separate the two audit approaches. O'Regan, (2008) submitted that "internal audit goes beyond these assertions" and looked at sales operations in a much broader context by asking questions regarding the target market, sales plan, measurement of sales performance, and compliance with sales policies. Porter et al. (2003) and Balkaran, (2008) agreed that although there are differences between internal audits and external audits, they both have the same characteristics and the respective services they provide are essential to maintaining an effective governance structure. The scope of internal auditing within an entity is extensive and usually involves topics such as the efficiency of operations, safeguarding assets, compliance with regulations, measuring reliability of financial reporting and ensuring compliance with the organisation's policies and procedures.

3.3.1: Developments in Internal Auditing

In recent times, development in internal auditing has been of keen interest to various stakeholders and in particular the practitioners. This is indicated in the following reflections by Simone (2012: 1)

"To deliver what stakeholders want, the standard for an effective internal audit function has been raised and internal audit needs to elevate its performance to meet the always increasing stakeholder expectations. Businesses must evaluate total

enterprise risk, coordinate with the internal audit functions and break down organisational barriers to provide a holistic approach to risk management” (Simone, 2012, 1)

One common thread that runs through most of the internal auditing repositioning efforts is a clear attempt to re-examine performance expectations, while at the same time paying deserving attention to improving the potential for Internal Auditors’ career development. The Sarbanes-Oxley Act of 2002 legislation has profoundly influenced and redefined the practice of internal auditing in the last decade everywhere across the world (Sarbanes Oxley Act of 2002 is a Public Law 107-204 enacted by 107th congress in the United States of America to protect investors by improving the accuracy and reliability of corporate disclosures. It was enacted as a response to high profile financial frauds discovered in Enron and Worldcom). The Security and Exchange Commission (SEC) has the mandate for the administration of The Act. In this regard the SEC has power to publish rules and requirements.

The Act profoundly impacted how financial reporting can attain its expected objective of accuracy and transparency. In an attempt to make the chief executive officers more accountable for their actions, the SOX proposed that “*CEOs and CFOs should now personally sign and certify the correctness of financial reports*”. Most Security and Exchange Commissions in different countries across the world were motivated to issue more strict corporate governance procedures for listed companies to follow. This new pressure from the legislation and industry has triggered the need for improving internal auditing systems with ripple effects being felt all over the world. Internal auditors have no choice in the circumstance but to urgently seek new ways to enhance auditing effectiveness and efficiency even with the advent of ICT.

The question of using new auditing techniques such as Systems Control and ICT to assist auditors to improve the effectiveness of audit and hence corporate governance have been fully discussed in previous studies (Shaikh 2005, Debrecey et al., 2005).

Generalised Audit Software has proved extremely useful in the present dispensation and some auditors rely on it to obtain specific auditing information, but such software is generally not compatible with the complex file structures of database systems. As noted in the literature, auditors often have some degree of difficulty in preparing the

data for the first time (Braun and Davis, 2003). For auditors to be effective and efficient with the use of software they should be able to understand the technical language, such as data structure, database schema, and business process, and also be capable of creating required embedded auditing rules by themselves.

This study looked at the impact of ICT tools and techniques on internal control in prevention and detection of electronic fraud in the financial sectors of the Nigerian economy. The internal auditing function (IAF) is one of the pillars of corporate governance along with the External Auditor, executive management and audit committee of the Board of Directors (Gramling et al., 2004; Abiola, 2012). The Board of Directors has the overall responsibility to determine the governance process, which senior management implements and internal and External Auditors evaluate, under the control of audit committee (Treadway Commission, 1987; Blue Ribbon Committee, 1999).

The pivotal role of ICT in corporate governance and regulatory compliance is no longer in doubt. ICT both enables and drives effective governance structures, risk management, and control processes because it: (1) shapes an organisation by impacting on governance structure selection and the organisation's level of risk (Parker, 2001; Boritz, 2002); (2) helps establish the maintenance and enforcement of new governance process throughout the organisation (Hamaker, 2004; Fox and Zonneveld, 2004); and (3) helps implement and improve the risk management and compliance processes; employee retention, and reducing cost of capital and insurance premiums (PricewaterhouseCoopers, 2004).

The recently experienced changes in ICT have direct impact on the Internal Audit Function (Gorman and Hargadon, 2005). Consequently, the IIA requires Internal Auditors to understand how ICT is used and should be used in an organisation, as well as key ICT risks, controls, and ICT based audit techniques (Implementation Standard 1210.A3 (IIA), 2004). Thus given the new requirements of the Security and Exchange Commission (SEC) and IIA, both the Internal Audit Function and ICT have been prominently brought into the limelight within organisations. In this period of governance reform across the globe, according to Boritz: "ICT – Internal Auditing

research” has become a critical imperative. Surprisingly, however, Boritz (2002) states that:

“while the role of assurance practitioners, from an external perspective, has often been publicly discussed and debated, the role of the internal auditor and the resulting changes have not been quite so publicized” (Boritz, 2002, : 232).

In the same vein, Cannon and Crowe, (2004) emphasised the importance of ICT to the work of an auditor in the new dispensation thus:

“The ICT function is responsible for designing, implementing and maintaining many of controls over an organisation’s business processes. ICT has a critical role in collecting, processing and storing data that is summarized and reported in financial statements” (Cannon and Crowe, 2004: 31).

Many organisations are becoming increasingly dependent on the efficacy of ICT to increase the accuracy and speed of transaction processing and gain competitive advantages in terms of operational efficiency, cost savings and reduction of human errors. On the other hand, many types of risk have been associated with ICT, including loss of computer assets, erroneous record keeping, increased risk of fraud, competitive disadvantages, anytime the wrong IT is selected, loss or theft of data, privacy violations and business disruption (Warren et al., 1998; Gelinias et al., 1999; Hadden et al., 2003; Hermanson et al., 2006; Abu-Musa 2006).

Cannon and Crowe (2004) stated that many internal controls over financial data are integrated into computer programs and procedures that are written, implemented and maintained by the ICT function. By implication, assets and liabilities in an organisation are increased or reduced automatically by computerised process with little or no human interference. Securities parameters are properly predefined while transactions such as purchases of materials transfers of money and materials are routinely initiated and consummated *in-situ* within external entities. In most cases, the degree of automation can be such that human activity is limited to promulgating policies and rules and reviewing results.

Cannon and Crowe (2004) also argued that Internal Auditors (IA) merely struggle to maintain identity as the organisations they audit undergo radical changes as a direct consequence of rapid changes in ICT. Command and control structures are changing and being directly influenced by changes in Total Quality Management;, globalisation

and restructuring processes. The rapid changes in IT continuously render control procedures obsolete, and the relevance of traditional internal audit has become seriously questioned. Cannon and Crowe's (2004) study made use of case study approach to collect quantitative data through structured questionnaire. The study was able to meet its stated objectives of producing an empirical understanding of the impact of changing technology and business process on auditing. The study did not make use of any theory for its underpinnings. Perhaps making use of relevant theory would have helped better understanding of the changing role of auditors.

As technology changes occur more quickly, Internal Auditors must keep pace with emerging technological changes and be able to assess the impact on organisations' data processing system, as well as the chosen audit procedures (Razaei and Reinstein, 1998, : 465). Abu-Musa (2008) noted that in designing audit procedures, the internal auditor should consider the importance of the risk, the magnitude of any misstatement, the nature and class of transactions, the materiality of accounts balance or disclosure involved and, the characteristics of the specific controls used by the organisation.

The International Standard on Auditing 401 – Auditing in a computer Information Systems environment – states that:

“Auditing processes for both Internal Auditors and External Auditors have been rapidly changing. Factors prompting these changes include: the globalization of business, advances in technology, demands for value-added audits, the organisational structure of the client's Computerized Information System (CIS) activities, the extent of concentration or distribution of computer processing throughout the organisation, particularly as they may affect segregation of duties, and the availability of data source documents”.

Some computer files and other evidential matter (audit trail) that may be required by the Internal Auditor may exist for only a short period or only in machine-readable form. Accordingly, the Internal Auditor should have sufficient knowledge of computer skills to plan, and review the work performed. The auditor should also consider when specialised computer skills are necessary in an audit.

Rishel and Ivancervich (2003) stated that Internal Auditors serve a key role in addressing controls, risks and other important factors throughout the ICT implementation process. However, in an effort to improve the effectiveness of ICT facilities, Internal Auditors should also provide value-added services in areas that are often overlooked. An auditor's involvement in evaluating and improving the quality of the processes used to validate and document systems and train personnel could contribute to achieving a successful IT Implementation and reliable internal control system. During the validation and testing phase of implementation, Internal Auditors could also provide valuable input about configuring the systems in a way that incorporates appropriate controls in their organisations.

Meredith and Akers (2003) examined internal audit involvement in system development by conducting a questionnaire survey of 241 Chief Executive Officers (CEO). The aim of the study was to investigate whether it is better for Internal Auditors to act as consultants for system development to avoid compromising their independence.

The findings revealed that CEOs are not bothered about Internal Auditors getting involved at the planning and designing stages of system development but they do not want them involved at the implementation stage. The opinion of chief audit executives (CAEs) is varied and divergent on the question of Internal Auditors doubling up as consultants. Meredith and Akers (2003) study highlighted changing management expectations of internal audit functions in relation to the use and development of ICT. The traditional scope of internal audit has been extended from measuring and evaluating effectiveness of internal controls to providing consulting services.

Pathak et al. (2003) were of the opinion that the overall quality of various internal control facilities is determined to a great extent, by the internal auditing functions and the supporting business systems applications. In a small-sized system, reliance may be placed on the effectiveness of internal control to perform an IT audit by auditing

the end products. Whereas in large and complex systems, auditors may need to collect further evidence to ensure the quality of the internal control systems before placing reliance on their operational and application effectiveness. The reliability of the internal control system is important for the efficacy of the system audit.

Increasing knowledge of ICT has revolutionised the way modern organisations are run. Consequently the Internal Auditor has to adapt to the new organisation environment. The Internal Auditor no doubt receives considerably more exposure to IT systems nowadays than the past (Silltow, 2003), IT is no longer considered the exclusive domain of the IT specialist or even IT auditors as every auditor is expected to have a fair knowledge of ICT and be confident in leveraging technology to perform audit functions. Pathak et al. (2003) also suggested that:

“..the integration of applications and enterprise-wide IS will be a key trend for the future and will surely have a great impact on the entire set of knowledge, skills, methods, algorithms, and strategies of Internal Auditor. Accordingly, the audit practitioners and educators need to expand their skill set and knowledge bases to cope not only with current changes but also with future challenges.” (Pathak et al., 2003 in Abu-Musa 2008 : 441).

The speed at which changes in IT and managerial practices are being experienced force many organisations to rethink the rigid, documented control they have hitherto practised and find solutions where responsibility for control is being pushed down the organisation hierarchy and where oversight by management could not be achieved through traditional, compliance-based internal audit (Spiral and Page, 2003; Fadzil and Jantan, 2005). This has confirmed that internal auditing has undergone a paradigm shift from its traditional function which expanded its scope in a way that allows it to make greater contributions to all the stakeholders. The debate on whether internal auditing profession should serve both as a management consultant and an independent professional has not been concluded.

Previous studies have looked at audit independence and objectivity from the External Auditors' perspective. Only very few studies investigated factors affecting internal audit independence and objectivity (Christopher et al., 2009; Turley and Zaman, 2007; O'Lear and Stewart, 2007) despite the fact that it forms the bedrock of internal

audit definition as given by (IIA 1999). The Glossary to the IIA standards made a further distinction between independence and objectivity thus:

“Independence: The freedom from conditions that threaten objectivity or the appearance of objectivity. Such threats to objectivity must be managed at the individual auditor, engagement, functional and organisational levels”.

“Objectivity: An unbiased mental attitude that allows Internal Auditors to perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made. Objectivity requires Internal Auditors not to subordinate their judgment on audit matters to that of others”.

It appears that ‘independence’ of Internal Auditors here refers to the complete state of affairs that allows Internal Auditors to perform their primary functions with an objective attitude. Objectivity relates to the state of individual mind which may be subject to culture and environment (IIA, 1999)

Godwin and Yeo (2001) examined two factors that may influence the independence and objectivity of internal audit in Singapore. The study made use of questionnaire survey to collect data from chief Internal Auditors who are members of the Institute of Internal Auditors in Singapore. The research instrument and questions were adapted from the Scarbrough et al.’s, (1998) study. The study mainly investigated two factors considered probable that can affect the independence and objectivity of the internal audit function, the first being the ‘relationship between internal audit and the audit committee while the second is the extent to which the internal audit function is staffed by employees who are likely to be promoted up to line management positions’.

The result found that independent audit committee can provide support to the Internal Audit Function and this may offset problems with objectivity that may arise with Internal Auditor’s reports on line managers. One major limitation of the study is that all respondents were members of IIA. There is high likelihood of bias in an attempt to project their professional members as being objective in every situation and circumstances.

In a related study Stewart and Subramaniam (2010) examined emerging research literatures on internal audit independence and objectivity. The purpose of the study was to provide a review of the most recent literature on internal audit independence and objectivity. The literature review covers a period of ten years from 2001 to 2010.

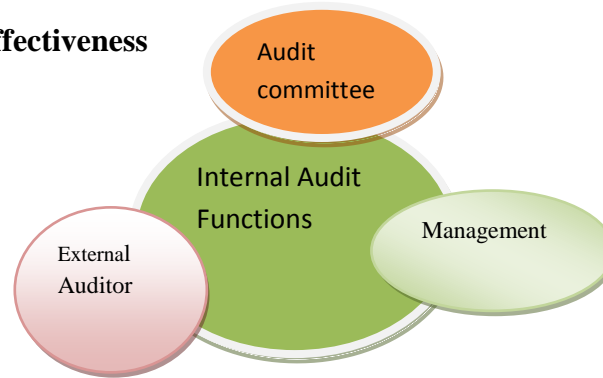
Out of 12 studies reviewed, seven studies used survey methods; three used case studies, one used interview and one used archival method to collect data. All the studies examined Internal Auditors' independence in relationship to the audit committee. Most of the studies reviewed provided empirical support that audit committee composition can impact on oversight activities and that Internal Auditors' close relationship with management can place their independence from management at risk. Prior studies on internal audit independence and objectivity suffer from a lack of theoretical guidance. In addition, none of the studies reviewed examined the impact of ICT on Internal Auditors' independence and objectivity.

3.3.2: Internal Control and Internal Auditing

The system of internal control can be extended to include specific procedures and acts, including but not limited to control in accounting, processes, purchasing, distinction of duties, and financial reporting. Efficient and reliable communication supported by good procedures of internal check within an organisation is a good driver of internal control systems. Management rather than the External Auditor has the responsibility to form and supervise the system of internal control. However External Auditor's sole responsibility is to give judgment on the defects and functioning of such systems.

Pickett (2005) considered internal auditing as an important aspect of the entire auditing process. Essentially internal auditing is part of internal control system. It is the branch within an organisation that implements and applies a programme of internal auditing as a complete test of the effectiveness of all aspect of the internal control system. Risk assessment, control assessment and assessment of security and control have become key elements of modern internal auditing governance activity.

3.3.3: Internal Audit Effectiveness



Source: Author

Figure 3.4: Traditional users of internal audit outputs

The traditional users of internal audit output include management for control and decision making, audit committee to ensure the integrity of financial reports and External Auditors to assure reliance on clients' control systems. Internal audit has undergone a paradigm shift from an emphasis on accountability about the past to improving future outcomes to help auditees operate more effectively and efficiently both in the private and the public sectors (Nagy and Cenker, 2002; Stern, 2002; Godwin, 2004). Internal audit is effective if it meets the intended outcome it is supposed to bring about. Sawyer (1995) states an, "...Internal Auditor's job is not done until defects are corrected and remain corrected." Van Gansberghe (2005) explains that internal audit effectiveness in the public sector should be evaluated by the extent to which it contributes to the demonstration of effective and efficient service delivery, as this drives the demand for improved internal audit services.

Factors influencing internal audit effectiveness, according to Van Gansberghe (2005) include: perceptions of stakeholders and ownership; legislations affecting internal audit functions; organisation and governance set-up; conceptual framework and improved professionalism. Van Gansberghe (2005) based his opinion on the results of a consultative meeting that concentrated on improving public sector internal audit. Effective internal audit undertakes an independent evaluation of financial and operating information systems and procedures, to provide useful recommendations for improvements as necessary.

Using agency theory, Xiangdong (1997) explained the important role that internal audit plays in an economy and concluded that internal audit has an advantage over external audit in obtaining information quickly and discovering problems at an earlier stage; and Spraakman (1997), applying the theory of transaction cost economics, demonstrated how internal audit recommendations are important to the management of government organisations.

Prior literature relating to internal audit effectiveness has either focused on internal audit's ability to plan, execute and objectively communicate useful findings (Xiangdong, 1997; Spraakman, 1997; Dittenhofer, 2001); or taken a broader view and included factors that transcend the boundary of a single organisation (Van Gansberge, 2005). A model, which assumes that there is a common interest to achieve organisational goals for auditee management, top management and internal audit, is used for the purpose of analysis. Since, audit effectiveness fosters the achievement of a common goal; there would be a natural incentive in an organisation to improve it. The model considers four potential factors – internal audit quality, management support, organisational setting, and auditees' attributes to explain audit effectiveness, and shows how the interacting factors improve audit effectiveness.

Internal audit quality is determined by the internal department's capability to provide value added recommendations, and is germane to audit effectiveness. Internal audit has to appraise its performance and continually evaluates its service (Ziegenfus, 2000). Audit quality is associated with the level of staff expertise, the extent of services provided and the level to which audits are properly planned, executed and communicated. Audit findings and recommendations is not useful unless management shows interest in implementing them. Adams (1994) used agency theory to explain that it is in the interest of management to ensure existence of a strong internal audit department. To the customer receiving internal audit services implementation of audit recommendation is important and relevant to audit effectiveness (Sawyer, 1995; Van Gansberghe, 2005)

3.3.4: Internal Auditors' Effectiveness and Demographic Characteristics

Auditors' demographic characteristics such as knowledge (as measured by level of professional education), experience, training, age and gender are assumed to be important for audit effectiveness. An experienced auditor is presumed to be knowledgeable. The knowledge base needed by an expert auditor may be presumably acquired through experience (Abdolmohammadi and Shanteau, 1991). The question of auditors' demographic characteristics and how it affects his work and decision making in audit have not been fully resolved by prior studies in spite of increasing interest in this area. For example, while Abdolmohammadi and Wright (1987) observed that task complexity acts as a moderating variable, Choo (1989) and Colbert (1989) reported mixed results from literature on auditors' experience separately reviewed. David and Solomon (1989) suggested that experience may not be the appropriate characteristics but instead proposed performance as defined by efficiency and effectiveness of an audit.

Extending prior research, Estes and Reames (1990) studied effects of demographic characteristics on materiality decisions using multivariate analysis. The study was administered on 596 CPAs. The demographic characteristics tested were experience, education, and place of work, frequency of materiality decision, gender and age. The results of multivariate analysis indicated that age and place of employment may affect materiality decisions and the confidence in materiality decisions may be affected by years of external auditing experience, place of employment, frequency of materiality decisions and gender. The study is significant as the choice of subject was restricted to expert group unlike most prior studies that made use of novice group to test the difference in problem representation.

In a more recent study, Lehmann and Norman (2006) conducted experimental investigation on the effects of experience on complex problem representation and judgement in auditing. Their study was situated within the context of a going concern task. Lehmann and Norman (2006) study made use of 116 graduate auditing students and professionals. Out of 51 professionals, 26 worked with large regional or local firms. The experiments were conducted in the classroom for students or places of employment for professionals. The result of the study was that more experienced auditors have more concise problem representations than novices, and that some

types of concepts featured in problem representation are associated with judgement notwithstanding the level of experience (Lehmann and Norman, 2006). One major limitation of the study is the use of mixed subject (novice and experts) in the experiment. This may make generalisation of the result difficult. However, the study contributed to the body of literature on auditors' demographic characteristics by extending the results of prior study (e.g. Christ, 1993).

3.3.5: Governance Activities of Internal Auditors

Weiddenmier and Ramamoorti, (2006) developed research questions for each governance activity performed by the IAF in relationship with IT. Three main areas were identified by Weiddenmier and Ramamooti (2006): Risk Assessment, Control Assessment, and Security and Privacy Compliance Assessment. These main areas are now examined in details.

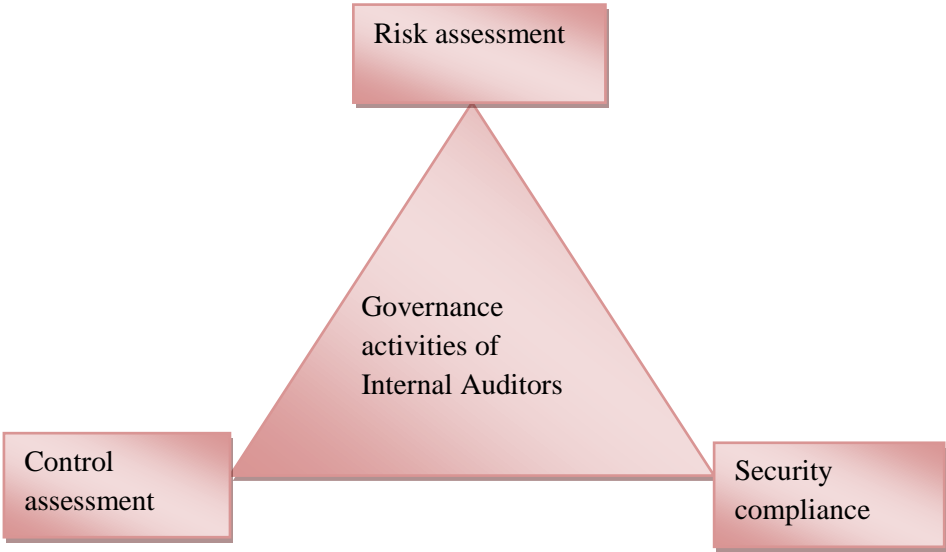


Figure 3.5: Governance Activities of Internal Auditors.

Source: Author

Risk Assessment and Internal Audit

The statement issued by the Public Oversight Board – POB (2008) highlighted its concerns regarding the ability of auditors to properly assess risks arising from rapidly evolving information processing systems. The POB encouraged auditors to expand their knowledge of new business-oriented IS, as such knowledge would facilitate the development of more effective audit approaches. The POB also recognised the need to attract and retain qualified IT specialists for audit support. The POB also confirmed that increasingly, auditors would find it necessary to understand fully the risk associated with new and advanced business IS, and the controls that are needed and respond to those risks. The totality of this is known as Enterprise Risk Management (ERM) which is defined as:

“...the discipline by which an organisation in any industry assesses, controls, finances, and monitors risks from all sources for the purpose of increasing the organisations short and long-term value to its stakeholders” (The Casualty Actuarial Society, 2003, 3).

Conceptually, internal auditing is associated with the control-based approach for its activities. In the recent times, corporate governance centred on risk management, providing the impetus for the IAF to move to a risk-based approach (McNamee and Selim, 1998). In order to plan its engagement and define the audit universe IA must identify and assess risks in the organisational context (IIA Performance Standard 2008, A1).

Allen, et al. (2006) conducted a review of a number of auditing literature around topics such as business risk, inherent risk, control risk, fraud risk. Allen et al.’s (2006) work contributed to project on risk assessment initiated by the Public Company Accounting Oversight (PCAOB). The following items of conclusions are listed by Allen et. al., (2006, 158):

“Using a business process focus in assessing client risks appears to offer a number of advantages in the audit, especially if supported with appropriate decision aids and analytical procedures. Firms apply the business process approach differently, so guidance for using this approach may be helpful. This approach may result in auditors being less sensitive to micro-level risks, and decision aids must be carefully designed, as their orientation (i.e., a negative focus emphasizing risks and their consequences versus a positive focus) can influence auditor judgments. Industry expertise and specialization are critical to effective risk assessment. Fraud risk assessments are enhanced by considering fraud risks separately from misstatements due to error,

brainstorming about fraud risks, and thinking strategically about client management's possible efforts to commit and conceal fraud."

Business process approach is an innovative process of promoting effectiveness and efficiency by aligning with the needs of customers with utmost flexibility while deploying technology to improve overall output. Allen et al. (2006) concluded that there are similarities between the literature and recommendations of PCAOB's (2005) briefing paper and highlighted a number of supportive research topics for further study.

In a related study, Castanheira, Rodrigues, and Craig, (2010) examined factors associated with the adoption of risk-based internal auditing. The purpose of their study was to analyse company-specific factors associated with adoption of risk-based auditing and explore the role of internal auditing in enterprise risk management (ERM). 96 mailed questionnaire surveys were sent to chief Internal Auditors in Portuguese organisations. The questionnaire was designed to contain closed questions in order to avoid ambiguous interpretations. 59 (61 per cent) usable responses were received. Descriptive statistics (x square test) and Principal Component Analysis (PCA) were used to test 20 hypotheses formulated for the study.

Castanheira et al. (2010) found that 75, 89, and 100 per cent of respondents support the proposition that the larger the size of entities, the more likely they are to apply risk-based approaches. Furthermore the study also found that the internal audit functions of almost half of the organisations in the finance industry were involved in risk management. The number is more significant than organisations which engage in non-finance. This is consistent with (Gramling and Myers (2006) cited in Castanheira et al. (2010).

The study achieved the objective for which it was initiated although it suffered from a number of obvious defects. For instance, the amount of data collected was very small (only 96 questionnaires were mailed out). This made multivariate analysis of the data impossible. The distribution of the questionnaire was also not based on a clear

statistical basis: it was impossible to find out for instance how many questionnaires went to small, medium and large firms respectively. All these combined made generalisation of findings difficult. In addition, the questionnaire survey was carried out in 2006 whereas the result of the study was published in 2010. The time lag is long enough to make the result irrelevant given the trend of development in enterprise risk management and adoption of risk-based auditing.

Control Assessment and Internal Audit

Control assessment is the second important governance function of Internal Auditors. To ensure adequate implementation of risk responses, audit committee places reliance on the Internal Audit Function in order to determine if internal controls effectively support strategic, operational; reporting and compliance objectives (Gendron et al., 2004). Manual controls are still being used for compliance processes thereby increasing the likelihood of compliance failures considerably, even by the large organisations despite the increased demand for IT Controls (PricewaterhouseCoopers, 2004).

Internal auditors need to be adequately trained to understand and mitigate security hazard any time they occur as a result of good ICT security controls. Surprisingly, Ivancevich et al. (1998) found that the existence and size of the Internal Audit Function is not associated with (perceived) disaster recovery plan strength.

In another study, Caglio (2003) examined the effects integrated information systems (Enterprise Resource Planning) had on modern accountants. The study made use of a case study approach and Giddens' structuration theory as underpinning theory. The study conceptualised the change in accountants' practices and position as a structuration process. The study further recommended a form of hybridisation concerning the roles of the Information System and accountant. Caglio (2003) was able to break new ground in accounting literature by using a dynamic framework to describe the impact of ERP on accounting as a profession.

3.4.0: Internal Control and Computer-Assisted Auditing Tools and Techniques Literature

With the ever-increasing system complexity, especially computer-based accounting information systems, including enterprise resource planning (ERP), and the vast amount of transactions, it is impractical for auditors to conduct the overall audit manually. It is even more impossible in an e-commerce intensive environment because all accounting data auditors need to check are computerised.

In the past three decades auditors most commonly outsource technical assistance in some auditing area from an information system auditor sometimes referred to as an electronic data processing (EDP) auditor. Information system practices within the big audit firms (known as “the Big Five”) were estimated to have grown at the rate of between 40 to 100 per cent during 1990 and 2005 (Bagrahoff and Vendrzyk, 2000: 35).

The term “auditing with the computer” is commonly used to illustrate the employment of computer technologies by auditors to perform some audit work that otherwise would be done manually or outsourced. Such technologies are extensively referred to as computer assisted auditing tools (CAATs) and have been a key player in the way modern audits are conducted.

In auditing with the computer, auditors employ CAATs with other auditing techniques to perform their work. As its names suggests, CAAT is a tool to assist auditors in performing their work faster, better, and at lower cost. CAATs are as important to the auditing profession as auditing knowledge, experience and professional judgement.

There is a variety of software available to assist auditors. Some are general-purpose software and some are especially designed and customised to be used to support the entire audit engagement processes. Many auditors consider simple general ledger, automated working paper software or even spreadsheet as audit software. In this thesis, however, the term audit software refers to software that allows the auditors to perform the overall auditing process generally known as generalised audit software.

Generalised audit software (GAS) is an automated packaged originally developed in-house by professional auditing firms. It facilitates the auditor in performing necessary tasks during most audit procedures but mostly in the execution and documentation phase.

Basic features of a GAS are data manipulation (including importing, querying and sorting), mathematical computation, cross-footing, stratifying, summarising and file merging. It also involves extracting data according to specification, statistical sampling for detailed tests, generating confirmations, identifying exceptions and unusual transactions and generating reports. In short, they provide auditors with the ability to access, manipulate, manage, analyze and report in a variety of formats.

CAATs could help the auditor to identify symptoms early in the life of a fraud with the aid of the digital analysis, which involves the examination of patterns in data. Mooney et al. (2000) noted that “computers can and do assist employees in perpetrating fraud”. However, computers can also be used to detect improper activities. A number of software packages are available to internal audit departments that can be utilised to aid in the detection of fraud. Table 3.2 contains a list of software that can assist internal audit staff in detecting fraud or in managing their fraud investigation, and reporting. This list does not include proprietary packages that have been developed by the Big five firms.

Table 3.2: Software that can assist auditors

Software that supports fraud detention, management, and prevention	Software that supports automation and audit functions
ACL; IDEA; Financial Crime Investigator; WIZ Rule; DATAS for IDEA; The Analyst’s Notebook; Veris Social Security; Number Validation Services; SSNDTECT; Auto Fraud Investigation	ADM Plus; Audit Leverage; Audit Master Plan Auditor Assistant; Auditor’s Software Toolset; Auto Audit SE; Auto Audit 2000; Expert choice; Management Audit Ltd; Pentana Tracker; Pinpoint; WorkForce 2.0
	PANEL B (Data and system security)
	i. Active Security

	<ul style="list-style-type: none"> 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)

In the words of Mooney et al. (2000: 21)

“Surprisingly, a recent survey indicated that nearly 40 percent of the internal audit departments surveyed do not utilize fraud-detection software. This suggests a real need to educate and inform organisations of the availabilities of capabilities of this special-purpose software”.

The researcher now summarises relevant literatures on internal control and usage of ICT for internal control effectiveness.

Janvrin (2008) carried out experimental research to examine to what extent internal control effectiveness increases the value of internal evidence. This is done by looking at two relevant characteristics, source objectivity and internal control effectiveness, and how auditors evaluate evidence items supporting accounting estimates. The study extends prior studies which are increasingly examining internal control effectiveness vis-à-vis the demand for generating faster financial reports with minimum guarantee for audit quality (Botosan and Harris, 2000; Searcy et al., 2003).

Janvrin (2008) adopted a controlled experiment approach. A sample of 24 auditors who participated in the experiment were selected from one international audit firm. The study made use of one way ANOVA for the analysis of data sets obtained.

The result of the study suggests that auditors are more likely to place reliance on internal control effectiveness only when they evaluate external evidence items and

that internal control effectiveness reduces the impact of relying on internal as opposed to external evidence.

The strong point of the study is that positivist methodology was made use of by developing experimental procedures. However the use of limited sample frame of 24 auditors in one firm surrogate casts doubts on the outcome and possibility of generalisation. Furthermore, Janvrin's (2008) study focused on External Auditor for the assessment of internal control as against internal auditor which is the primary focus of this study.

In a related study, Rae and Subramaniam (2008) examined quality of internal control procedures (ICP) in a study that brought together theoretical concepts from organisational justice, internal control and fraud literature. The study led to the development of two separate models relating to employee fraud and the quality of internal control procedures.

Data collected from 64 Australian firms through survey were used for the development of the two models. Logistic regression analysis was used to test the first model while multiple regression analysis was used for the second model. Rae and Subramaniam (2008) posited that risk management procedures must be formulated with respect to employee's fraud by paying attention to perceptions of justice in the workplace and Internal control policy quality. The study expands the frontier of knowledge by extending prior literatures on internal control (Holtfreter, 2004; Meiners, 2005; Leinicke et al., 2005) and most importantly providing empirical evidence that linked fraud triangle framework (Albrecht et al., 1984) with organisational justice and internal control framework (Moorman, 1991; COSO, 2004).

The observed limitation of the study stems from data collected from financial controllers or chief accountants who interpreted ICP quality in the light of their own position in the organisation. Furthermore the ICP quality construct can be improved by using holistic interpretation from the view point of internal and External Auditors, financial controllers and the audit committee of the board.

Jokipii (2010) carried out a study on determinants and consequences of internal control in firms using a contingency theory based analysis. The study makes use of the contingency approach to examine the design of the internal control structure and its observed effectiveness in different contexts. Jokipii's (2010) study employed structural equation model (SEM) to examine relationships among firms. Data were collected online survey from 741 firms in Finland.

The result of the study expanded the boundary of knowledge on many fronts. For instance, the study was able to present empirical findings using measurement models for internal control and its effectiveness in practice. Unlike earlier studies which have concentrated on particular control variables (Hooks et al., 1994; Mills, 1997) the internal control concept is considered in its totality employing different methods. Furthermore this study is able to examine the action of contingency theory on internal control sufficiently more than prior literature in order to bring out the importance of the relationship in understanding internal control within organisations. The study also examines important contingency characteristics that should be put in perspective when considering internal control in organisations.

Internal control effectiveness was operationised by considering how well three objectives of internal control frameworks are met by the organisation: efficiency and effectiveness of activities; reliability, completeness and timeliness of financial and management information, and compliance with applicable laws and regulations. Four-item questions were used to measure the indicators before an average score was obtained.

The study found among other things that a "prospector strategy (aggressiveness strategy) and high perceived environmental uncertainty do matter more in internal control than the other contingency characteristics examined".

However one of the observed limitations of the study is that Internal Auditors who are directly involved with the internal control process are not involved in data collection even though a cross-sectional approach was used. A longitudinal study involving internal control is more likely to present a different result.

In a recent study, PricewaterhouseCoopers (2007) surveyed the chief audit executives (CAEs) of Fortune 250 companies to gain insight about trends likely to affect Internal Auditors over the next five years and what they expect internal audit to look like in 2012. The questionnaire survey was combined with interview to achieve a mixed methods approach to the investigation. PricewaterhouseCoopers was able to obtain required responses from nearly a third of the Fortune 250. A total of 82 survey responses and 19 in-depth interviews were conducted across the survey population. The findings of the PricewaterhouseCoopers (2007) survey showed the following trends as impacting internal audit roles, responsibilities, and functions.

Table 3.3: PricewaterhouseCoopers (2007) survey

Trend	Impact on Role & responsibility very strong (%)	Impact on function moderate (%)	Combined Total Impact & responsibility + Impact on function.(%)
Technology	60	35	95
New Regulations	51	37	88
Risk Management	58	29	87
Corporate governance	58	26	84
Ethics and Compliance	56	21	77

The survey showed that between 2007 and 2012 technology, risk management, fraud prevention and globalisation are expected to significantly impact internal audit roles, responsibility and functions in that order. The survey also attempted to find what factors drive the greatest projected increases in responsibility ten identified factor : continuous auditing or monitoring; auditing the ERM process; auditing outsourced or offshore operations; fraud detection; fraud risk assessments; auditing executive compensation and disclosures; auditing operational efficiency and effectiveness; auditing IT security; auditing or evaluating compliance with laws and regulations; fraud investigations. Continuous auditing or monitoring is identified as having the greatest impact in driving projected increase in responsibility of Internal Auditors with a combined totals of 90 per cent. It was also found that fraud detection and fraud risk assessments are expected to produce significant increases in responsibility for internal audit functions.

The PricewaterhouseCoopers (2007) survey has been very useful for academics and policy makers in that it sheds light on possible future outcomes of internal audit functions in a technologically changing global environment. However the choice of Fortune 250 for data collection restricts the generalisation of results to developing countries. Besides, the methods used to analyse the data collected were doubtful as they were not clearly stated.

In an earlier study on adoption and impact of e-Accounting, Gullkvist (2003) carried out an exploratory study in order to extend the frontier of knowledge in understanding factors influencing small and medium businesses to adopt e-Accounting. The study built on the earlier adoption model Iacovou et al. (1995) developed. Gullkvist extended Iacovou's (1995) model by including 'trust' as one of the four factors determinants of e-Accounting adoption and adapting it to Technology Adoption Model (TAM) pioneered by Davis (1989).

Gullkvist (2003) study is based on limited literature review and did not test the hypothesis with any data. However the study is important to ICT adoption literature as it has proposed both questionnaire and interview research methods for data collections. The study also suggested extension of Iacovou's earlier model by inclusion of trust as one of the important determinant of e-Accounting. This is yet to be tested; however it has presented a good opportunity for further research.

In a related study Hashim (2007) examined the extent of ICT skills, use, and adoption among owners of small and medium enterprises (SMEs) in Malaysia. The main objective of the investigation is to examine ICT skills and innovation characteristics of SME owners in Malaysia and to examine if there is any relationship between ICT skills, use, adoption patterns, and adoption categories as constructs.

Hashim, (2007) surveyed 383 SME owners in Malaysia. The benchmark use for SME is an annual sales turnover not more than RM25 million and not more than 150 full-time employees. The study is unique in the sense that its unit of analysis is the SME owners themselves rather than the firm as is usual with many previous studies (Ndubusi and Jantan, 2003; Shiels et al., 2003; Lai and Hsieh, 2007).

Hashim, (2007) made use of two appropriate theories to underpin the study (the diffusion of innovation theory and the theory of perceived attributes). The theories have helped to further illuminate the results obtained from this investigation. The data gathered from the respondents were analysed using factor analysis.

The finding of the study clearly shows that SME owners in Malaysia as in most developing countries possess below-average ICT skills and many do not have access to computers. The majority find IT difficult to use and understand and therefore find its adoption difficult. The study further shows the level of ICT adoption among SME owners in Malaysia is low.

Hashim, (2007) contributed to literature by providing useful insights into the knowledge gap in understanding IT adoption in a developing economy. However the design of the questionnaire in English may be a problem to many prospective small business owners who do not read in English. The research is likely to have discriminated against such people whose number may be significant by inadvertently omitting them in the survey. Furthermore the dependence on factor analysis as the main analytical statistical tools is questionable. While it may be a useful tool for categorising and summarising data, it may not be useful to draw definitive conclusive results on the study.

The issue of 'corporate transparency' has engaged the attention of corporate social responsibility and business ethics scholars for a long time. Vaccaro and Madsen (2009) examined corporate dynamic transparency as the new ICT-driven ethics. The study proposed that dynamic information sharing, conducted by means of ICT, drives organisations to exhibit greater openness, transparency and accountability to the benefit of all stakeholders within and outside the organisation. The study further presented three ethical arguments to justify the implementation of dynamic transparency by business firms in order to augment and complement communication flows to stakeholders.

Vaccaro and Madsen (2009) made use of a literature review approach for their investigation. They identified the most frequently used definitions of corporate transparency in the area of business ethics, computer ethics and public policy.

Theoretical analysis was drawn from empirically-grounded scholarly studies such as (Weil et al., 2006; Fung et al., 2007; Vaccaro and Madsen, 2009)

The study is able to break new ground in the area of ICT-driven ethics and transparency as a new perspective in business and computer ethics. The study was able to predict that ICT will impact on transparency and ethical standard of Internal Auditors in near future. Future studies are needed to demonstrate the effects and impact of ICT-driven ethics on the independence and objectivity of Internal Auditors.

Mpofu, Milne and Walkins-Mathys (2012) conducted a multiple case study in South Africa on ICT adoption and development of e-business among SMEs in South Africa. The paper identified key ICT adoption attributes and examined how these influence ICT adoption and development of e-business among small hotel businesses in South Africa. Mpofus' et al. (2012) was a response to most previous studies on ICT adoption in small firms (Beckinsale and Ram, 2006; Zappala and Gray, 2006; Gibbs et al., 2007; and Manuelli et al., 2007). Semi-structured interviews, observation and document analysis were used to collect data from three case studies sampled from different locations. These data were analysed qualitatively. The study makes use of TAM as underpinning theory to shed more light on findings.

The study identified personal skills as one of those attributes that are important for adoption of ICT besides organisation attributes, adoption attributes and social networks. The study used only three hotels in South Africa for the case studies, so it may be difficult to generalise the findings of ICT adoption framework to all SMEs in South Africa. Hotel businesses have their own peculiarities and are different from other businesses. However the output of this study will be beneficial for policy-makers in terms of effective policy formulation.

Rezaee and Reinstein (1998) studied the impact of emerging IT on auditing functions. The study discussed the main issues of SAS No 80, which offers auditors guidance to accumulate sufficient evidence to audit the CIS of their clients. Rezaee and Reinstein (1998) observed that IT has made inputting information for transactions and events simpler and led to evaluating the related controls and results more critically. Accordingly, accumulating sufficient evidence needed to construct an informed decision means understanding where to look for that evidence, what control

procedures to consider, and how to evaluate such procedures. Rezaee and Reinstein's (1998) study is an important contribution towards understanding the impact of ICT on auditing. Even though the study achieved what it was designed to do, it failed to examine the implications of ICT on detection of accounting mistakes and fraud in the course of auditing.

Hermanson et al. (2000) conducted an exploratory study to examine the IT-related activities of Internal Auditors in US organisations. Information gathered from over 100 Internal Audit directors indicated that Internal Auditors focus primarily on traditional IT risks and controls, such as IT asset safeguarding, application processing, data integrity, privacy and security. However, other areas such as risks related to systems development and acquisition received little attention from Internal Auditors. The results also revealed that several factors have been associated with Internal Audit performance of IT evaluations, including the nature of the audit objective, the prevalence of computer audit specialists on the Internal Audit staff and existence of new CIS. Even though the study suffered from lack of theoretical underpinnings, the study met its stated objective and contributed to knowledge in understanding the focus of Internal Audit activities. The study was however carried out in a developed economy, i.e. the United States. This makes generalisation of results to a developing economy unrealistic. The current study is carried out in response to the call of Hermanson et al. (2000) to investigate the role of other groups beyond Internal Auditors that might be potentially involved in IT risk assessment and management, particularly for areas receiving little attention from Internal Audit, and to examine the efforts of other groups in addressing such risks.

Rishel and Ivancevich (2003) discussed some important responsibilities for Internal Audit in the IT implementation process. They argued that Internal Audit responsibilities traditionally have been centred on risk management issues and control testing, particularly in the pre-implementation and monitoring phases of IT projects, rather than playing an integral role in enhancing the viability of IT implementations. The study suggested that Internal Auditor can and should provide input with regard to system configuration in order to ensure that the proper integral controls are in place. Internal Auditors should also communicate with the IT team to ensure that new systems and modifications to existing systems are adequately documented. As proper

documentation can be so vital to internal audit in its evaluation of controls and risks, Rishel and Ivancevich (2003) study is a step ahead of Hermanson et al.'s (2000) work. However, they made use of the case study approach incorporating unstructured questionnaires. Perhaps the study could have benefited more from the use of interviews to strengthen the data collection method.

The debate about whether consulting impacts the independence of the internal audit function has been documented in the auditing literature. Meredith and Akers (2003) surveyed 241 chief executive officers (CEOs) to investigate their opinions on Internal Auditors' involvement in systems development, including whether Internal Auditors' independence is compromised by such involvement and whether auditors should act as consultants for system development projects. The results of the study revealed that CEOs are more concerned with the internal audit function remaining independent than with auditors acting as consultants to an organisation. The respondents were essentially indifferent regarding Internal Auditors' involvement in the planning and design phases and did not support Internal Auditor involvement in the development, implementation, and maintenance phases. The results of the comparison of the perceptions between CEOs and chief audit executives (CAEs) show that there are significant differences between the groups regarding their expectations. CEOs placed more importance on independence while CAEs emphasized the need for Internal Auditor acting as consultants.

Hadden et al. (2003) examined the perceived IT qualifications and IT activities of audit committees, Internal Auditors and External Auditors regarding IT risk management. The results of the study revealed that some organisations were able to achieve more effective IT oversight by tapping into the resources of the audit committee and External Auditors to a greater extent. The audit committee members indicated that their IT oversight role should be greater than what it presently is. The results suggested that although audit committees appear to provide limited oversight of IT-related risks, they generally believe that their committees should take a more active role in overseeing this area. The results also revealed no significant differences in Internal Auditor-perceived IT qualifications or activities between the in-house versus outsourced groups. The results suggested that the Internal Auditors' commitment to IT oversight was rated "above moderate", while the External

Auditor's involvement in IT oversight was rated moderate, significantly lower than Internal Auditor mean rating. Hadden et al., study meets its stated objective. However, drawback noticed from the study is that it failed to consider the ability of Internal Auditor to meet the stated commitment to IT oversight which has been rated above average.

Chan (2004) studied the IT dimension of SOA in order to determine the manner and extent to which IT systems meet the Act's requirements. Chan (2004) mentioned that the connection between IT and SOA could be found in several recent documents, including an auditing standard proposed in October 2003 by the Public Company Accounting Oversight Board (Release No 2003-017). The document stated that "the nature and characteristics of a company's use of IT in its IS affect the company's internal control over financial reporting". The Information Systems Audit and Control Association's IT Governance Institute has also addressed their issue in its recent discussion document, IT control objectives for SOA, and in written response to the PCAOB's proposal in November 2003, Chan argued that even now, relatively little formal attention has been devoted to the IT aspect of the SOA.

Cannon and Crowe (2004) discussed the importance of IT to the internal control environment and described many aspects of IT professional culture that might affect IT's perception of its role with respect of financial controls and compliance with SOA. The paper highlighted the importance of the IT function to the control environment and the success of any SOA initiative, Cannon and Crowe (2004) argued that the IT area does not necessarily view effectiveness of financial controls as their own responsibility. However, SOA imposed new responsibilities on organisations, some of which should necessary be delegated by the IT function. Accordingly, the IT function and Internal Auditor need to understand and accept these responsibilities. The study suggested that only a few individuals in the IT area have a background in internal controls or business processes. Cannon and Crowe's (2004) work contributed to the knowledge of dynamics of internal control and the need for Internal Auditors to retrain to meet up with the new challenges posed by technology and regulations. However, an observed drawback of the study is that it lacked theoretical underpinnings.

Al Twaijry et al. (2004) examined the relationship between internal and external audit in Saudi organisations using a questionnaire survey. The results of the study revealed that External Auditors expressed much concern about the independence, scope of work and small size of many internal audit departments in Saudi organisations. Internal Auditors considered co-operation between internal and External Auditors to be limited although External Auditors were more positive regarding the same issue. The findings also revealed that the extent of reliance by the External Auditors on the work of the Internal Auditor varied with the quality of the internal audit department. External auditors believe that the Internal Auditor function in many Saudi organisations lacked professionalism and independence from management, which adversely affected their work and the potential for reliance on it. They recommended devoting more resources to establish independent and competent Internal Auditor departments in order to enhance the reliability of Internal Auditor in Saudi organisations. The study at best contributed to understanding the perception of professionalism and independence of Internal Auditor by External Auditors as only the opinions of the External Auditors were surveyed. The question of independence can only be verified from the participants involved and not the observer like External Auditor as is the case in this study.

In a related study, Lehmann and Norman (2006) conducted experimental investigation on the effects of experience on complex problem representation and judgment in auditing. Their study was situated within the context of a going concern task. Lehmann and Norman's (2006) study made use of 116 graduate auditing students and professionals. Out of 51 professionals only 26 worked with large regional or local firms. The experiments were conducted in the classroom for students or places of employment for professionals. The result of the study was that more experienced auditors have more concise problem representations than novice auditors. (Lehmann and Norman, 2006).

Lehmann and Norman (2006) is a good reference point on the impact of experience on the efficiency of auditors. However the result obtained are inconclusive probably because the experiment did not use homogenous respondents. The present study is designed to extend Lehmann and Norman's (2006) study by empirically investigating

the effects of personal characteristics such as experience and qualification of Internal Auditors.

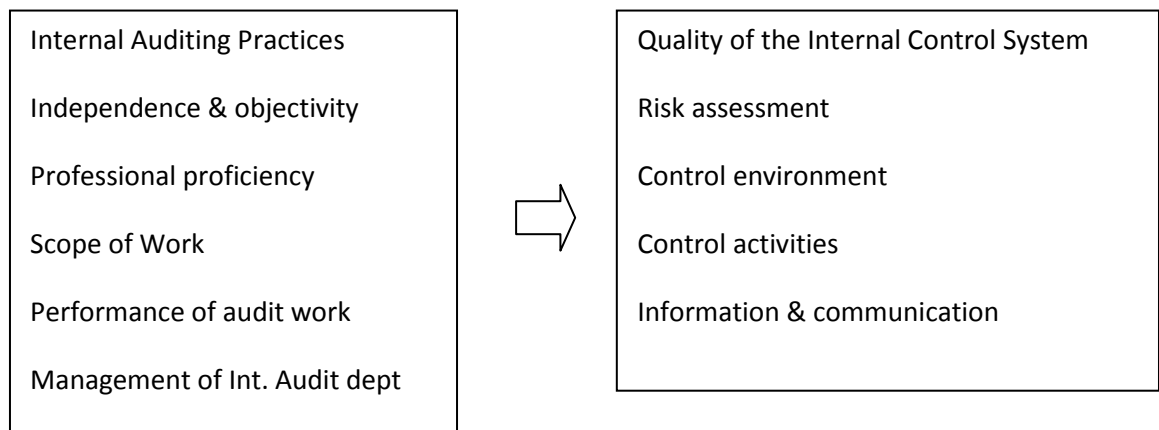
Abu-Musa (2008) carried out an empirical study on information technology and its implications for internal auditing. The study investigates the impact of emerging IT on Internal Auditors' activities and examines whether the IT evaluations performed in Saudi organisations vary, based on evaluation objectives and organisational characteristics. The study adopted a survey approach using a self-administered questionnaire. About 700 questionnaires were randomly distributed to a sample of organisations in five cities. A total of 218 valid and usable questionnaires were collected and analysed. The results of the study reveal that Internal Auditors need to enhance their knowledge and skills of Computer Information System for the purpose of planning, directing, supervising and reviewing the work performed. The results of the study are consistent with Hermanson et al., in that Internal Audit focus primarily on traditional IT risks and controls, such as IT data integrity, privacy and security, asset safeguarding and application processing. The findings of this study have important implications for managers and Internal Auditors, enabling them to better understand and evaluate their computerised accounting systems. Abu-Musa's (2008) study is important to the present study because it is the only study done so far in a developing economy focusing on Internal Auditors and ICT. The study however failed to measure the effectiveness of Internal Auditors using ICT in detecting and preventing fraud even though that was not its primary focus. Another drawback of the study is that it lacked theoretical underpinnings. To a large extent the study meets its stated objective of investigating the impact of IT on Internal Auditors' activities.

Fadzil and Jantan (2005) examined internal auditing practices and internal control systems. The two main objectives of their study were to investigate whether the internal audit departments of companies in Malaysia complied with the Standards for the Professional Practice of Internal Auditors (SPPIA) IIA, (2000) and secondly to investigate whether compliance with SPPIA will affect the quality of the internal control system of the company. Fadzil and Jantan (2005) adopted two sets of questionnaires in the study. The study measured internal audit practices with the items listed in the SPPIA while internal control was measured by means of the

statement on internal control designed for the guidance of directors of public listed companies. The study made use of descriptive and inferential approaches.

The results of the study revealed that management of the Internal Audit department, professional proficiency, objectivity, and review significantly influenced the monitoring and risk assessment aspect of the internal control system. The performance of audit work, the objectivity/independence of Internal Auditor and audit reporting significantly influence the control activities aspect of the internal control system. Fadzil and Jantan (2005) was the first empirical study that was able to link the compliance of the Internal Audit function to the SPPIA components and its effect on the internal control system. This is depicted in the Table 3.4 below:

Table 3.4 Internal Audit Function and Its Effects on Internal Control Components



Source: Fadzil and Jantan (2005)

Furthermore the study also linked the independence and objectivity of Internal Auditor to the quality of the internal control system for the first time.

The observed setback for the study is that only Chief Audit Executives were examined to the neglect of other key internal audit staff. Data collected across different categories of audit staff could have enriched the result since Internal Auditors typically work as a team.

In a related study Abdolmohammadi and Boss (2010) investigated explanatory and control variables that are associated with proportion of time spent by the internal audit functions on information technology (IT) audits. The study made use of large

samples of 1,029 chief audit executives selected from Australia, New Zealand, Canada, the UK and the United States. The results showed increase of approximately 1 per cent yearly for time spent on IT audits. For instance IAF spent 7.9 per cent in 2003, 10.61 per cent in 2006 and the projection for 2009 was put at 13.40 per cent.

The study made use of multivariate regression to show that four variables are positively and significantly associated with IT audits: “the certified information system auditors (CISA) certification, Internal Audit Function age, training, and the number of organisational employees”. Abdolmohammadi and Boss’s (2010) study is important in predicting how Internal Auditors are adopting the use of IT. As the Internal Audit Function are increasingly engaging IT audit the importance of traditional central data processing department is being reduced.

The study was able to meet the stated objectives however there are some observed limitations. For instance the study concentrated on the Chief Audit Executives (CAEs) alone for responses. CAEs may not be true representatives of internal audit staff. Secondly the data base used was adapted from the Common Body of Knowledge in Internal Auditing. Some of the variables used for the collection of initial data may not be appropriate: for example IAF age was used as proxy for organisational knowledge. It is possible for organisational knowledge to be affected by other variables.

Godwin-Stewart and Kent (2006) investigated the voluntary use of Internal Auditor by Australian publicly listed companies to identify the main factors leading listed companies to have an Internal Audit function. The study made use of questionnaire survey to generate the data. The results of the study showed that a large proportion of Australian listed companies do not use Internal Auditors and many of those organisations that do, have only one or two Internal Audit staff. The results also revealed an association between the use of Internal Auditors and a commitment to strong risk management. A strong association between Internal Audit and the size of the organisation has been found, suggesting that smaller organisations do not regard Internal Audit as cost effective. The results also revealed a significant relationship between Internal Audit and the complexity of the organisation’s business structures. However, the study found only weak support for an association between the use of

Internal Audit and strong corporate governance. The study is important for the understanding of contingency and socio-technical theories to explain the impact of ICT on Internal Auditors. The study drawback is that it concentrated its survey only on large corporations in Australia and New Zealand. Small and medium sized organisations are excluded.

Arena, Arnaboldi, and Azzone (2006) carried out a multiple case study to describe and compare the main characteristics of IA departments in six Italian companies and investigated the influence of enacted regulations on their development. The results of the study revealed a wide range of the diversity in IA department characteristics, confirming the relevance of institutional pressures, and also providing evidence of the influence of additional elements in their development. The study demonstrated that there was a significant influence of regulations on the development of IA, and this influence was stronger with regulation-imposed sanctions.

Sarens and de Beelde (2006) interviewed CAEs in ten different large manufacturing and service companies located in Belgium and Belgian subsidiaries in US companies. The results of the study suggested that in the Belgian cases, Internal audit focus on severe shortcomings in the risk management system which creates opportunities to demonstrate their value. Internal Audit is playing a pioneering role in the creation of a higher level of risk and control awareness and a more formalised risk management system. However, in the US cases, Internal Auditors' objective evaluations and opinions are a valuable input for the new internal control review and disclosure requirements maintained in the SOA. The study introduced some recommendations for improving internal control system as an integral valuable part of the assurance role. It also underlines the importance of regulations on Internal Audit work. Again, the study is limited to large organisations in Belgium; the result may not be true for all firms irrespective of their size.

Ololube, (2006) conducted a detailed analysis of a research survey on the impact and uses of ICT and the issues that underlie the integration of ICT in teacher education programmes in Nigeria. The study is a follow up to an earlier study (Yusuf, 2005) which investigated teachers' self-efficacy in implementing computer education in

Nigerian secondary schools. The study made use of a two-paged structured questionnaire with a four- point Likert scale (survey design). The questionnaires were administered to 180 respondents out of which 154 questionnaires (86 per cent) were retrieved. The respondents consisted of staff of three Nigerian higher institutions conducting teacher training. Questionnaires were analysed using SPSS version 13.5 the main statistical tools used are Pearson Correlation Coefficient and One-way-analysis of variance (ANOVA).

Ololube, (2006) found that there is a significant relationship between the poor provision and uses of ICT instructional materials during pre-service teacher training and performances after graduation. However the relationships between variables and respondents' demographic profile show that there is no significant difference in the overall ANOVA analysis. This result has direct implication on the IT skills in Nigeria as lack of necessary skills on the part of the teachers will impact directly on the pupils and ultimately the public since you cannot give what you do not have.

Ololubes' (2006) research is a valuable contribution to ICT adoption in a developing country like Nigeria where there is noticeably wide research lacuna. However the sample size of three teachers training institutions appears to be too small in a country like Nigeria where there is a wide geographical spread and over ninety universities with virtually all of them having a faculty of education where teachers are being trained. The research also suffered from lack of theoretical underpinning.

3.5.0: Summary of Chapter

This chapter reviewed relevant literature on internal control effectiveness and internal auditing. Attempt was made to review the various definitions of internal control and internal auditing. Attention was also directed at the review of recent developments in internal auditing and the impact of technology. The review so far constitutes the first part of literature intended for this study. The second part in chapter four consists of literature on continuous online auditing, prevention and detection of electronic fraud.

CHAPTER FOUR

LITERATURE REVIEW ON PREVENTION AND DETECTION OF ELECTRONIC FRAUD

4.0: Introduction

The last chapter concentrated discussion on internal control effectiveness and internal auditing. The chapter elaborated on basic definitions, internal control effectiveness and development in internal auditing/impact of technology. Figure 4.1 below gives a summary of work done in this chapter.

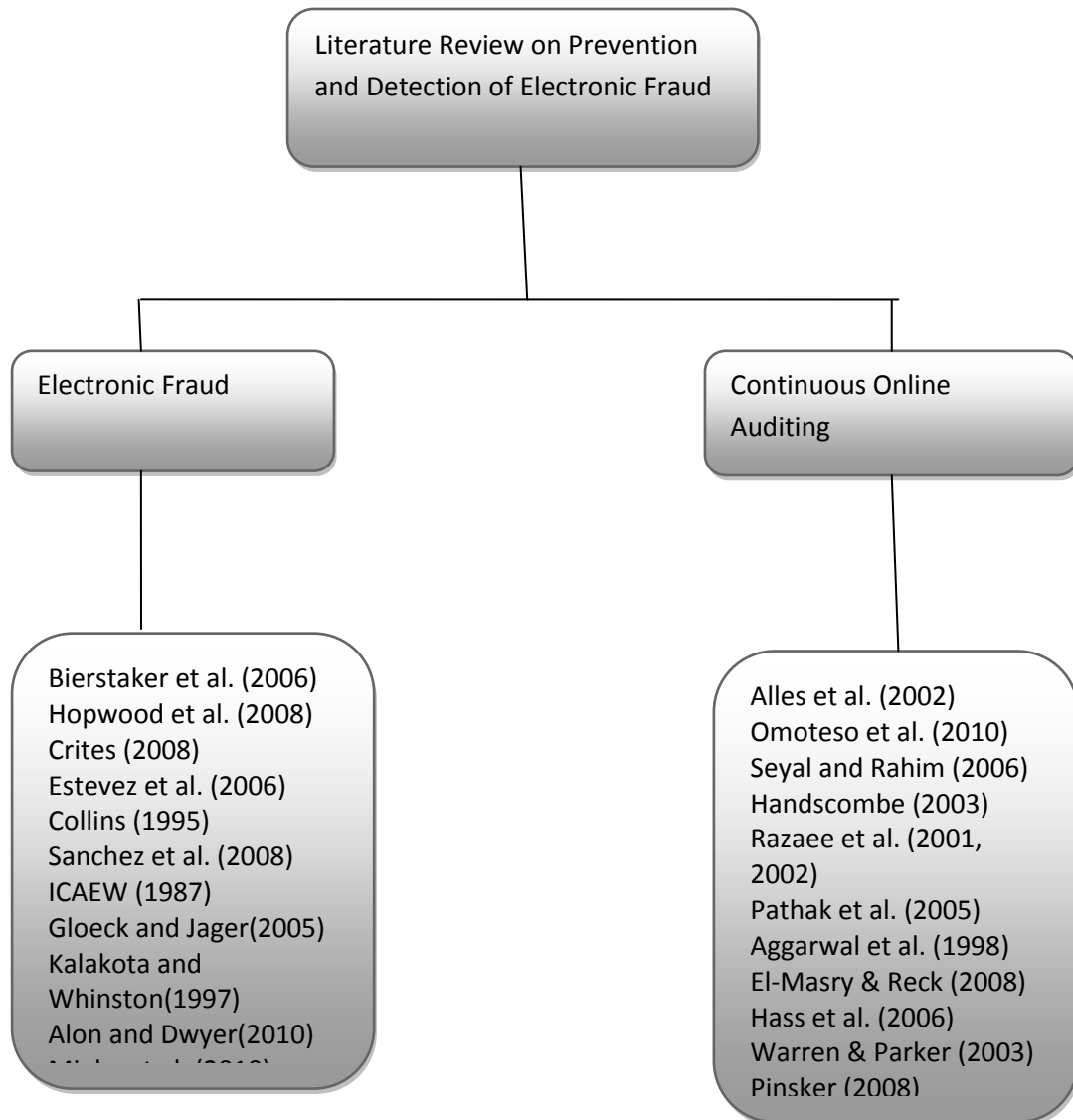


Figure 4.1: Summary of Literature part 11

4.1.0: Internal Audit, E-business, and E-fraud

The constant increase in the web user base has had beneficial effects on e-commerce. Kalakota and Whinston (1997) explained e-commerce attributes with a couple of essential characteristics. Communications technological innovation enhances the delivery, accessibility and storage of data regarding product, services and customers, and makes the process of payments by telephone or computer networks possible. Technological innovation boosts the proficiency of the business process by automating firms' transactions and workflows, which include monitoring inventory and customers, streamlining business-to-business ordering and receiving, allowing cost control by management while ensuring quality of the product and service delivery. On the Web storefronts offer you the potential of shopping and marketing products and services on the Web. Despite the fact that the motivation driving e-commerce is not really different from that of conventional commerce, the new circumstances thrown up by the electronic ways of doing business should provide new prospects for crime (Newman and Clarke, 2003).

The globalised storefront along with transfer of financial activity into an internet site rather than private transactions between seller and buyer (even if they are strangers), as in conventional commerce, obviously impinge on the question of whether each participant in the transaction can trust one another (Newman and Clarke, 2003). Trust could be the significant issue that concerns internet business. A study conducted by Commerce net (Lombardi, 1998) disclosed that the leading explanations for shoppers not purchasing on the internet were insufficient trust and also regarding the payment mechanism. E-business merchants have invested considerably in demonstrating good reasons to be trusted on the internet (encrypted on the web payment certificates) as well as in facilitating the fee settlement mechanism as easily as possible (one-click buy by using debit/credit card or electronic cash). The main aim in the web design of e-business continues to be to make marketing a lot quicker, to reach buyers more speedily and effectively, to make purchasing more economical and simple, and to reassure customers' fears on security (Newman and Clarke, 2003).

The commercialisation of the Internet two decades ago has transformed the utilisation of ICT in the business world. Since then billions of funds have been committed to expansion and improvements of e-business (Sarner, 2004). The 'collapse' of many

big businesses that are well known on the Web (dot-coms) in the last decade has not affected the steady growth of e-commerce (Ames, 2001). E-business has proved to be an important enterprise endeavour with impressive successes. Examples are Tesco, Asda, Dell, Amazon, etc. (Lee, 2001; Barnes and Hilton, 2004). Prior studies support the view that if carried out properly; an e-business technique can lead to considerable business profits (Chan et al; 2001; Stansfield and Grant, 2003; Sarner, 2004).

This perspective is likewise supported by the Forrester Research Survey (Bartels et al., 2006). In the study, the executives and decision-makers in business from around the globe were asked to arrange their important technology themes for 2006 according to their priority. The respondents rated “the initiation of Internet and e-commerce activities” as one of their prime priorities (Bartels et. al. 2006). As a result, essentially the most critical concerns relating to security and the way to guarantee the productive utilisation of ICT have been given a deserving prime priority in internet business worldwide.

Newman and Clarke (2003) stated that there are attributes about the computing environment – ‘the ICT that makes e-commerce feasible – that makes certain types of crimes attainable, and which criminals cannot resist’. Clarke (1999) expanded this view point to an idea of “hot products” by distinguishing attributes of product patterns or models that made their theft feasible, more desirable, and more enticing. He came up with the acronym CRAVED to sum up these attributes. The attributes merely illustrate the vulnerability to theft which may be evidenced in the layout or display of the merchandise. The attributes include the following: Concealable, Removable, Available, Enjoyable, and Disposable.

Newman and Clarke (2003: 61) used this point of view to illuminate the knowledge of the internet environment that makes e-business feasible. They discovered the elements in ICT that make commission of crime feasible. This is given the acronym SCAREM: Stealth, Challenge, Anonymity, Reconnaissance, Escape, and Multiplicity. “Stealth: Stealth is undoubtedly a ‘Convenience’ offered to all who utilize the Web. It tends to make commission of crimes considerably less difficult. Fraudsters make use of or imitate the motion of a system operator, fraudulently get hold of passwords and make use of distant storage on an harmless party’s computer system to discover just a couple of procedures. These intruders are practically invisible (Klelnigi, 2000).

Challenge: the Internet fraudster's literatures are full of essential inspiration to 'beat' the internet procedures. They operate incredibly extended hours, and turn out to be obsessed with fulfilling their nefarious undertaking (Clough and Mungo, 1992). The obsession is nonetheless to the disadvantage of being discovered. However the actual circumstances may present a situation where there is no risk of getting caught at all. This may be the case where fraudsters can possibly intercept the transmission of data and divert it into an anonymous third party account. In the Internet business, timing is of the utmost relevance. Communications involving important messages such as electronic-funds transfer are effected practically at the speed of light. Virtually all key break-ins of computing procedures are products of continuous activity by the hacker over extensive periods of time, covering several weeks or months (Ahuja, 1997).

Anonymity: extended duration of intrusion is feasible because of the anonymity features provided to users of the computer. Newman and Clarke, (2003) attempted to differentiate anonymity from stealth, which is 'sneaky and secretive'. Innovative hackers might also 'mimic the IP addresses of others ('Spoofing') making their e-mail extremely difficult, to track' (Ahuja, 1997: 12).

Reconnaissance: probably the most crucial ingredient in the rational options that fraudsters select in carrying out their illegal activity is the preference for appropriate targets. The cyber space tends to make it feasible to scan a huge number of web servers and personal computers that are connected to the web trying to find possible gaps in security. The scanning can be achieved automatically without much effort using computer software available for sale on the Internet.

Escape: no-one will venture to carry out a crime if the risk of being caught is very high or if a visible trail of evidence will be left behind that might eventually lead to detection. Exceptionally some hardened criminal may not be bothered about the consequence of their actions before the crime is actually carried out (Katz, 1998). According to Newman and Clarke (2003 : 61)

"It is however, obvious that crime-inducing aspects of the information system environment of anonymity, deception and stealth all combine to make it extremely difficult for law enforcement to track down the crime to the individual perpetrator, especially when the fraud itself may never be detected, even by its victims".

Multiplicity: when a physical theft occurs, a determinate amount of asset may be lost. This is what might be referred to as a finite act. However if a fraudster hacks into a bank's computer file he is presented with infinite opportunities to 'multiply' his act. Indiscriminate access into a precious database would make additional crimes enticing. Newman and Clarke (2003 : 63) argued further that:

"...not only do the information systems of e-commerce provide special opportunities for crime, but also information itself contains attributes that make it an attractive target of crime. And since information is the stuff of e-commerce, it's targeting threatens the entire fabric of e-commerce".

The different fraud types and examples with possible estimate of cost of what has been experienced before are summarised in the Table 4.1 below:

Table 4.1: Frauds in the computing environment

Fraud type or Incident	Examples
Electronic funds transfer fraud	Convertible 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	Prime target: Specific Information System or intelligence. This is the most well known computer crime. Hackers have broken into banks in Los Angeles, the Los Alamos National Research Centre, the LA Police Department, Scotland Yard, Pacific.
Cross-border crime	Prime-target: trusting customer. 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.
Extortion and blackmail	Transitional target: bulletin board used to convey threat to kill Microsoft President Bill Gates. Offender used encrypted messages and images posted on AOL Netgil Bulletin Board, demanding transfer of \$5,246,827.62 to a Luxembourg bank account. Offender caught, tracked to Long Grove, Illinois.
Credit card fraud	Convertible target: In an example of cross-border crime, two British men in Wales hacked into e-commerce website in the USA, UK, Canada, Thailand and Japan and stole credit card information for 26,000 accounts. Stolen numbers sold in cyber markets of former Soviet Union Richtel and Matt(2002).
Accounting fraud	Convertible targets: these include intervening in the information systems underlying the automation of buying and selling; Purchasing and Payment fraud, circumvention of payment authorisation controls, and many other techniques that utilise opportunities afforded by lack of paper trails in computerised record-keeping. The scandals of Enron and WorldCom Accounting are recent hi-tech examples of these essentially old crimes(Staff, 2002).
Money laundering	Prime and Convertible target: Infiltration of banking system by organised crime, use of electronic non-bank transfer and cyber-banking, and many other sophisticated techniques (Financial Action Task Force, 2001)
Investment fraud	Prime target: customers duped by bogus banks that use the web as a transitional target to set up fraudulent websites. Bogus company that promises

	to turn iron-ore rocks into gold, and many more. Wyatts and Edward (1999).
Telemarketing fraud	Prime target: customer and groups of customers. The top ten telemarketing frauds of 2000 were (in order of incidence); prizes/sweepstakes, magazine sales; credit card sales, work-at-home, advance fee loans, telephone slamming, credit card loss protection, buyers clubs, telephone cramming, travel/vacations transitional targets: fraudulent websites and e-mail used to promote scams.
Identity theft	Convertible target: a husband/wife team (the modern Bonnie and Clyde) stole the identities and emptied the bank accounts of their victims in over six US States (Kristin and Davis, 1998).
Criminal conspiracy	International networks to trade in pornography, the Wonderland club; organised crime in smuggling, drugs, gambling and prostitution all enhanced by convertible target of the computing environment (Grant et al., 1997).
Aiding and abetting crime	Convertible target: Intelligence provided by how-to new groups; bomb-making, lock picking, counterfeiting, encryption fixes, smart card cloning (Mann and Sutton, 1998).

Source: Newman and Clark, 2003:54

In digital accounting systems, personnel frauds have a tendency to include attacks on computer hardware and software including databases. These attacks can be classified in into five categories: input manipulation, direct file alteration, program alteration, data theft, and sabotage as illustrated by Figure 4.2 below. According to Hopwood et al.,(2008), the most significant of digital fraud are input manipulation, direct file alteration and program alteration in order of magnitude.

The Association for Fraud Examiners (ACFE) observed that the typical business organisation loses more than five per cent of its annual revenue to occupational fraud (ACFE, 2006). Most occupational fraud schemes involved either the accounting department or upper management within the company.

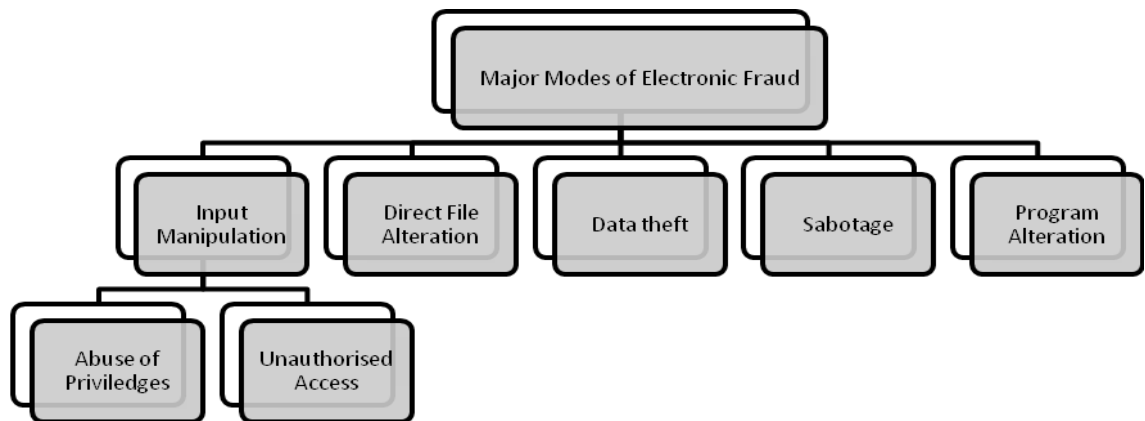


Figure 4.2: Major Modes of Electronic Fraud.

Source: Hopwood, Leiner and Young, (2008: 306)

Input manipulation – this is regarded as the most common means of computer fraud. It is common with fraudulent employees who normally take undue advantage of their vantage position. Input manipulation may take the form of data alteration or deliberate typing of incorrect data into the computer system. Input manipulation may take two different forms. It can be committed through abuse of privileges or unauthorised access. Abuse of access privileges occurs when an employee who is legitimately provided with access privileges to a portion of the system relevant to his job schedule enters into the system a new entry without documentation. The system may be manipulated further to reflect approval details in the electronic audit trail. The second aspect of input manipulation concerns unauthorised access. This may involve an employee gaining access to sensitive programs that he is not authorised to access using another employees’ identity or password. It may be difficult to track down the perpetrator through audit trail except in cases where the accounting system logs provide the IP address where the fraudulent transaction was entered. Investigation may become more difficult where a computer administrator is involved who has overriding privileges. In some situations ‘false’ audit trail may be created to divert attention to an innocent employee.

Direct file alteration – When an employee logs into a system, an audit trail is left because log in details such as log in name, password, time and system location must

be put in place. Some employees however, have enough technical knowledge to manipulate system-type tools to directly modify accounting files. It is difficult to rely on audit trail in this case as no trail is left in the accounting system except in some cases general computer system logs trails.

Data theft – valuable data may be stolen by employees and outsiders. It is easier for employees to steal data they regard as ‘high value information’ and sell it to competitors. A good system will normally allocate different levels of authority according to their official level and function. Restrictive access and printing permission may be necessary for sensitive information files.

Sabotage – computer sabotage may be very destructive as it is usually carried out by former employees or programmers who are disgruntled with the organisation but who have good knowledge of the system. It can take the form of file erasure, file alteration, or outright physical damage.

Program alteration – unauthorised changes to programs by a programmer or an employee constitute program alteration. Usually it is done in order for the perpetrator to benefit unduly. An example is the alteration involving a programmer that rounds off every cent from the payroll of a large organisation and accumulate it in an account controlled by him. Program alteration is difficult to detect in a normal audit trail.

In the past few years, more emphasis is being placed on electronic fraud involving identity theft and payment fraud. While many treasury and accounting departments do put in place basic fraud-oriented policies, procedures put in place by internal control department of organisations are not able to adequately address required controls necessary to protect liquid assets. According to Crites (2008), internet-related online access recorded more than eight per cent of the fraudulent access cases. The rate of growth of this new approach of means of access is a cause of concern for organisations and financial establishments. Many financial establishments are deploying their resources in creating awareness among their customers and business associates on how to discover web frauds and scams that may be in form of spyware and phishing.

Quite a few financial establishments as well as their customers have incurred incidents of fraud electronically that far exceeds the average loss seen with traditional cheque fraud. Using scams such as phishing, criminals steal access credentials transfer funds via internet. Often, the fraudster recruits an unsuspecting “mule” seeking easy money using advertisements via e-mail or posting easy-money jobs on online jobs boards. The mule facilitates getting the money out of the country and helps make it more difficult to trace the real criminal.

The ACFE, quoted in Crites 2008 notes in a 2006 Report to the Nation on Occupational Fraud and Abuse “that most of the fraud committed was initiated by individuals in the accounting department or senior-level management. Approximately 30 per cent of such fraud was committed by accounting employees, while about 20 per cent was committed by upper management or executive-level employees. The next highest group within a company to commit fraud was individuals in the sales department, which represented approximately 17 per cent” (Crites, 2008: 2).

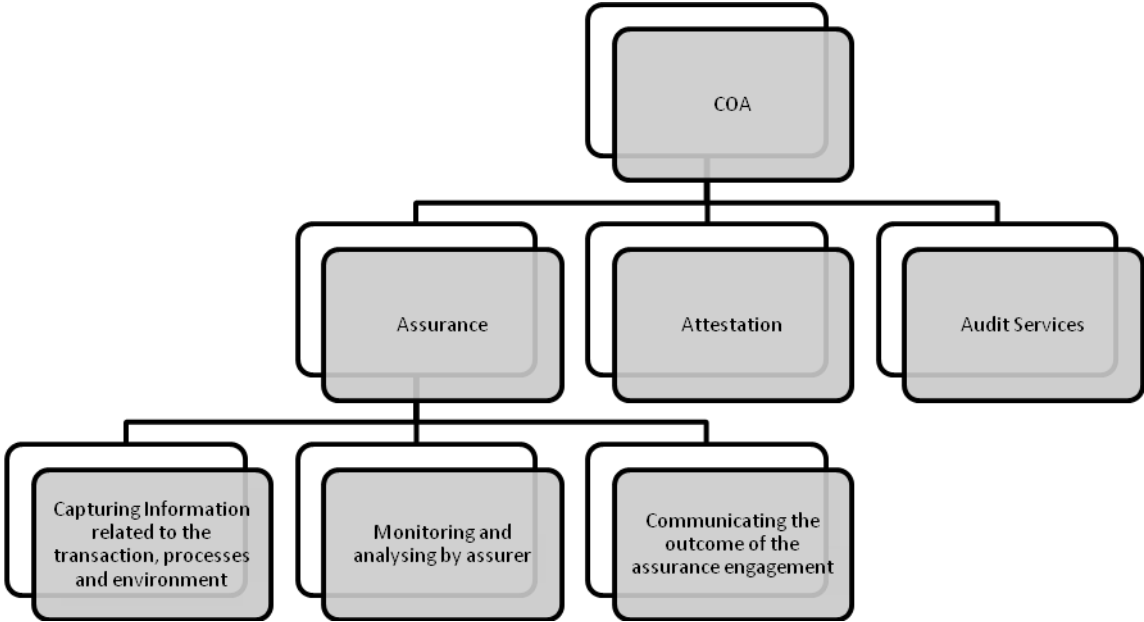
Staff training should be used to emphasise to employees that fraud must not be tolerated in the work place as it does a lot of damages to the company existence. Fraud decimates the entity’s assets and threatens its very existence therefore it must be promptly reported by all employees.

Apart from staff training, organisations must establish effective staff-management lines of communication and written down internal controls procedures that may be helpful in fraud prevention and detection. Anti-fraud specialists have suggested the establishment of anonymous mail boxes, hotline or special forum for reporting negative activities that may lead to fraud (ACFE, 2006).

4.2.0: Application of Continuous Online Auditing

The rapidly changing information flows and increasing availability of online real-time processing prompted accounting profession to reconsider the audit process. As auditors (Internal and External) are now adopting online technology in carrying out their audit tasks, there were very few empirical investigations on effectiveness of Continuous Online Auditing (COA) especially for Internal Auditors in providing continuous assurance (Alles, et al., 2002).

COA is variously described as real-time, concurrent or “lights-out” auditing. “It is a comprehensive electronic process that enables auditors to provide some degree of assurance on continuous information simultaneously with or very shortly after, the disclosure of the information” (Omoteso et al., 2008 : 76). Indeed COA coverage may be represented as in Figure 4.3 below:



Source: Author

Figure 4.3: COA Coverage

As the Internal Auditor is the focus of this study, the researcher probed the assurance component of COA further. The issue of assurance is so fundamental to the concept of COA that often the terms continuous assurance and continuous auditing are used interchangeably. However, some researchers identified a key distinction between continuous assurance and the concept of continuous auditing (Vasarhelyi 1998; Vasarhelyi and Halper 1991; Razaee et al., 2002). Continuous auditing is described as the application of modern information technologies to the standard audit products i.e, internal control or annual audit opinion. It is a step in financial audit that has evolved over time from manual to systems-based methods. Continuous assurance on the other hand has been argued to be value adding in any transaction. The Elliot

Committee (1997) gives a clear opinion about the need for assurance in any generic exchange of goods or services.

“.....the audit tradition is a professional asset of incalculable value. It derives from the market place need for high-quality, decision-making information. The financial statement audit provides assurance that an information set presented to investors and creditors is reliable. But the marketplace need for high-quality information is far greater than the need for reliable historical-cost-basis financial statements. Thus, assurance services not only respond to the growth problems of the audit tradition to the wider marketplace...” (Elliot, 1997: 61)

This view is reinforced by the modern stakeholder view of auditing as a value laden process whose end product should be relied upon. In achieving the objectives of COA auditors make use of continuous audit of database applications, data capture procedures, systems audit and real time analytical procedures and communicating the outcome (Kogan et al., 1996). Apart from accuracy, which is traditionally generally acknowledged, an important element for value laden financial information assurance is timeliness.

Shaikh, (2005) examined the impact of e-commerce and emerging technology in electronic auditing. The purpose of the study is to further assist auditors to improve the quality of their audit work by demonstrating how to effectively use emerging information technologies (computer–assisted auditing techniques (CAATs)).

Shaikh (2005) used emerging information technology to construct infrastructure and came up with the electronic auditing (EA) framework which is simply auditing with form of object-oriented distributed middleware, internet security technologies and intelligent agents. The study is a demonstration of how auditors can effectively make use of existing and emerging CAATs with the support of IT.

The research work made use of case study approach to demonstrate how accountants may conveniently audit the loan account of a bank with EA framework. The study made original contribution to knowledge by developing the EA framework. The set back of EA is that auditors may need to design specialised audit software for each client if different operating system are involved.

Yu, Yu, and Chou (2000) carried out an exploratory study on the impact of electronic commerce on auditing practices, an auditing process model for evidence collection and validation. The main purpose of their study was twofold. The study x-rayed potential impacts of electronic commerce on auditing practice in the ever changing paperless environment. Secondly, Yu et al. (2000) proposed a periodical auditing process model (PAPM) to facilitate auditors' evidence and a continuous auditing process model (CAPM) to extend the functions of PAPM. This is a response to prior studies related to the implementation of electronic commerce (EC) to various business domains and the obvious gaps noted about business overall internal control procedures and how audits can be conducted effectively (Panurach, 1996; Pyle, 1996; Camp and Sirbu, 1997; Kalakota and Whiston, 1997; Tenenbaum et al., 1997).

Furthermore the study found that CAPM is a more effective model suitable for continuous online auditing than PAPM. According to (Yu et al., 2000: 1) "...the CAPM approach intends not only to ensure integrity and effectiveness of the entire accounting system but also to guarantee the correctness and usefulness of the public dissemination".

The study appears to meet its set objective and contribute to literature on COA by illustrating a conceptual framework which shows the feasibility of continuously auditing electronic transactions in the electronic commerce environment.

Yu et al. (2000) used a practical approach using specific transaction flow to illustrate how PAPM and CAPM might work. The study would have benefited more if a longitudinal approach was adopted using real practical transaction flow over a specified period. Although it would have cost more time and other resources to complete, a more reliable result would have been achieved.

In a related study, El-Masry and Reck, (2008) conducted a 2x2x2x2 between participants laboratory experiment in their research paper titled "Continuous online auditing as a response to the Sarbanes-Oxley Act. The main purpose of their work is "to examine investors' perceptions of the usefulness of continuous online auditing (COA) prior to and after the Sarbanes-Oxley ((SOX) Act and assesses the current value relevance of continuous auditing" (El-Masry and Reck, 2008: 1). The study looks at COA as a new assurance service and considers whether it is of value

relevance to investors (whether COA has the ability to reduce investors' risk perceptions and increase investors' EPS estimates).

The study is a follow up to earlier studies calling for more research in the area of economic feasibility of COA and its possible impacts on the firm (Vasarhelyi, 1998; Kogan et al, 1999; Razaee et al, 2002; Wright, 2002; Li et al., 2007).

El-Masry and Reck, (2008) made use of two main hypotheses to test investors risk perception when COA is being used and the value of the firm. A laboratory experiment was conducted in the form of 2x2x2x2 between participants. A number of variables were computed for better understanding and samples were tested for 2002 before the introduction of SOX and 2005 after the introduction of SOX. A mail questionnaire survey was used to elicit responses from investors. MANOVA statistics were used to test the statistical significance of variables. One of the noticeable drawbacks of the study is the choice of a single proxy for financial leverage (traditional business risk). It is possible for SOA to mitigate other types of traditional business risks. Besides, the study suffers from lack of statistical power since many univariate differences between group means followed the expected directions.

El-Masry and Reck's, (2008) study is of high significance and value for establishing the current economic feasibility of continuous online audits. The study also shows the investors' perceptions of COA as a factor that mitigates firm risk thereby increasing in value relevance after the introduction of SOX. The study is useful in explaining the presence of a significant demand on COA by investors and firms.

In an earlier study, Aggarwal, Rezaee, and Soni (1998) carried out a literature review on internal control considerations for global electronic data interchange (EDI). The central theme of their paper focused on three dimensions of global EDI: (1) internal control in global EDI, (2) control measures to mitigate potential risks of using global EDI, and (3) identified characteristics and advantages of global EDI.

Aggarwal et al. (1998) used an exploratory approach to address the gaps identified from previous literature on EDI by properly identifying and documenting risks assessments and effective internal control structures to mitigate risks associated with

global EDI systems (Aggarwal et al., 1998; Paulson, 1993). They identified six critical advantages EDI provided to organisations as follows:

- i. Shorter response time and, tight inventory controls, improved cash management, and improved income as a result of elimination of unnecessary paper work.
- ii. Reduction in lead time improves inventories and cash management.
- iii. Fast and efficient communication improves business relationships with customers and suppliers.
- iv. EDI makes for better coordination and effective world-wide economies of scale.
- v. EDI improves decision making through instant availability of data from all subsidiaries wherever they are located and
- vi. Coordination and flexibility of operations are improved with subsidiaries, internal and external partners (Dearing, 1990; and Cahn, 1992, cited in Aggarwal et al., 1998).

Furthermore Aggarwal et al. (1998) made use of five integrated components that provide the structure and shape the process of internal control as identified in Committee of Sponsoring Organisation's report to assess inherent risks in global EDI. They identified six risks associated with global EDI.

- i. "Inability to transmit transactions because of failure to translate from one format to another.
- ii. Lack of integrated hardware and software;
- iii. Failure of software, hardware, or equipment;
- iv. Existence of cultural and language barriers;
- v. Lack of adequate laws governing EDI transactions; and

- vi. Loss of data integrity due to erroneous inputs, poor communication line, deliberate modification, or malfunction of hardware or software”.
- (Aggarwal et al., 1998: 75)

Aggarwal et al.’s, (1998) study achieved its objective; however EDI issues can be better addressed by conducting either field studies or surveys of the leading organisations that are currently using EDI technology. Such studies can result in development of suitable models that will be of benefit to the international business community.

Cheung and Lam (1995) carried out a survey in Hong Kong to evaluate the trend of EDI developments in Hong Kong in comparison with some neighbouring countries. The motivation for this work was the noticeable gap between development and popularity of EDI in North America, Europe, Australia, and Singapore. The pilot survey was limited to Hong Kong accountants in order to elicit their opinion on reasons for using and not using EDI and what they considered as the advantages and disadvantages of EDI.

Cheung and Lam issued 78 questionnaires out of which 76 were returned as fully completed and usable representing a response rate of 97.4 per cent. Data analysis was done using SPSS. A one-way ANOVA was conducted to test the significance of the differences in means of subpopulation. The open-ended questions were subsequently eliminated from the analysis because respondents failed to provide any responses to them.

The result of the survey showed that at the time the survey was carried out only 33 per cent of the respondents replied that their companies were using EDI. The obstacle to EDI penetration was agreed to be the slow pace of computerisation. The survey results further indicated that more cost-benefit analysis was required for proper EDI implementation and that the government of Hong Kong must show interest in the development of EDI.

A number of drawbacks are noticeable in Cheung and Lam’s (1995) study. The first being the sample frame of 78 accountants. The reasons for not using EDI in Hong Kong could have been captured more appropriately if other professionals (IT

specialists, auditors, lawyers and Chief Executive Officers) involved with EDI were included in the survey.

In a related study Seyal and Rahim (2006) investigated EDI adoption in Bruneian small businesses. The choice of small organisation is a novel idea and a clear departure from the trend of earlier research studies which concentrated on large organisations.

Seyal and Rahim (2006) successfully divided different factors addressed by past empirical studies (1992-2002) on EDI adoption into four: Innovation; Compatibility; Environmental and Organisational. The study went on to examine three of these four factors. For example, the Organisational factor was broken down into IT knowledge and top management support; external factors consisted of government support and trading partner influences while the economic factor consisted of perceived direct benefits, perceived indirect benefits and perceived cost.

Seyal and Rahim (2006) used questionnaire survey to collect data from 130 SMEs based on a stratified random sampling plan. 87 organisations responded but responses from three of them were not usable. A 65 per cent response rate was achieved.

Data collected was analysed with Pearson Correlation and Step-Wise Regression Analysis. The findings suggested that organisation factors and external factors were not significant for the adoption of EDI in Brunei's small organisations. However, economic factors such as perceived cost and perceived benefits are found to be important predictors.

However the criteria used for determining what small and medium organisations were was not clear.

In response to a joint Canadian Institute of Chartered Accountants (CICA) and Accounting Standards Board (ASB) of the AICPA study group (Wood Committee) report in 1999 calling for more studies on Continuous Auditing, Rezaee, Sharbatoghlie, Elam, and McMickle, (2002) based their paper titled "Continuous Auditing: Building Automated Auditing Capability" on a review of related literature, the experiences of the authors and innovative continuous auditing applications. Razaee et al. (2002) highlighted the important changes HTML format has introduced

into production of financial statement. Most companies provide financial disclosures through the internet by using HTML format which simply does not allow analysis, searching and manipulation of information without downloading and transferring into spreadsheet or any other suitable software application with manipulating ability (Razaee et al., 2002).

Rezaees' et al.,(2002) is an exploratory study which seek to examine conditions that must be met for continuous audits to be viable, in order to enhance further understanding and implementation of continuous auditing.

The study identified three important conditions that make COA different from the traditional audit process. The first one is that the auditor's knowledge of the client's business and industry should increase to assure reliability and relevance of electronic documents and better understand related risks associated with internal control activities. Secondly, it is important that the auditor understands the flow of transactions and types of control activities that ensure validity and reliability in the real-time accounting environment. The third requirement according to Rezaee et al. (2002) is that the auditor needs to make use of a control-risk-oriented audit plan that must focus on adequacy and effectiveness of internal control. This is achieved through the use of internal control templates that are capable of performing sophisticated controls such as authentications, firewalls, encryption of sensitive information and passwords. In addition, COA requires auditors to develop their own software audit tools (CATTs) capable of performing the audit procedure electronically and evaluate possible risks associated with internal control.

Rezaee et al.,(2002: 151) further identified a number of benefits of COA:

- i. “reducing the cost of the audit assignment “by enabling auditors to test a larger sample (up to 100 per cent) of the client's transactions and examine data faster and more efficiently than the manual testing required when auditing around the computer;
- ii. Reducing the amount of time and costs auditors traditionally spend on manual examination of transactions and accounts balance;

- iii. Increasing the quality of financial audits by allowing auditors to focus more on understanding a client's business and industry and its internal control structures; and
- iv. Specifying transactions selection criteria to choose transactions and perform both tests of controls and substantive tests throughout the year on an ongoing basis.”

Rezaee et al.'s study (2002) achieved its set goals and succeeded in presenting an approach for building COA capacity, audit data warehouses and data marts. It has contributed tremendously to the literature and provided a pathway on which subsequent research on COA is conceived. The authors used pragmatic approach by relying on related literature, personal experience and an innovative continuous applications approach for their work. A case study approach could have been more relevant to test the efficiency and drawbacks of an emerging concept such as COA as it would afford the researcher more opportunity of practical investigation.

In a recent study Omoteso et al. (2008) conducted an investigation into the application of continuous online auditing in the UK. This study appears to be the first empirical study emanating from the UK in this area. The study adopted a mixed methods of questionnaire and in-depth semi-structured interview on a one-to one basis. A total of 96 organisations were contacted while only 31 questionnaires were returned and five interviews conducted. The open-ended parts of the questionnaire were analysed with the use of Microsoft Excel and Access. The findings indicate that the readiness of audit professionals and their clients to adopt COA is still a contentious issue. The paper concludes with some reflections on what the expansion of COA might mean for the auditing profession.

The first drawback noticed from this study is the time lag between when the data collection (2004) and the time analysis was done (2008). A period of four years may be a long time for the views and perceptions expressed to have changed due to rapidly changing technological initiatives. Apart from this, the sample frame used appears to be small and it is doubtful if the triangulation used can compensate for the problems associated with generalisation of results across the wider geographical and industrial spectrum. However, Omoteso et al.'s (2008) study provides a watershed for future

empirical studies to determine how the profession's views on the use of COA are developing and how they will be expected to develop over time in view of changing technology and working environment.

Pinsker (2008) conducted a survey using MBA students and business professionals in the US to empirically examine competing theories to explain continuous disclosure technology adoption intentions using XBRL as the example technology. The purpose of this study was to test competing theories from Pinsker's earlier new research framework so as to provide necessary insight of XBRL as an example of technology adoption for managers in firms intending to adopt but who have a low level of XBRL knowledge.

Pinsker (2008) made use of survey methodology using experienced business professionals and MBA students who proxy for middle level managers. The results were analysed using T-test. Two theoretical models, Fichman's (1992) model and Li et al.'s (2004) theory of corporate governance were used in the study.

The survey results indicated that both the TAM and absorptive capacity theories were able to predict XBRL adoption intentions. The regression result was useful in explaining the observed variations as it explained the users' intentions in adoption of XBRL. T-tests showed that participants believe XBRL technology would be easy to learn and understand and that it would be useful for their job. But there are conflicting signals when the research proposition for perceived usefulness was supported and that of attitudes towards technology was not supported despite the fact that they are mutually inclusive.

Pinsker's (2008) study achieved its aim by providing a theoretical framework for studying continuous disclosure (CD) technology adoption using XBRL. The findings extended the frontiers of knowledge in understanding perceived benefits of XBRL adoption for firms. The study also made use of more statistical test than previous studies (Link and Siegel, 2002 quoted in Pinsker, 2008). The study supports the fact that both the TAM and absorptive capacity represent appropriate theories for studying technology adoption. This study will also make use of TAM to further empirically test technology adoption by Internal Auditors.

The major drawback of the study is that the MBA students were used to proxy for middle level managers. The researcher is one of their instructors. There is a tendency for the participants to give responses that are pleasing to the researcher and not necessarily what they consider appropriate. This is what is referred to as ‘evaluation apprehension effects’.

Kim et al. (2009), examined information technology acceptance in the Internal Auditor profession and the impact of technology features and complexity. Kim et al.’s 2009 study is an attempt to bridge knowledge gaps by addressing specific technology features for professional groups such as Internal Auditors.

Building on prior studies on TAM (Davies et al., 1989; Taylor and Todd, 1995; Igbaria et al., 1997; Thompson et al., 1991) the study made use of a sample of 185 Internal Auditors of the IIA by identifying technology features of General Audit Standard considered important for Internal Auditor assignment. TAM variables of system usage, perceived usefulness; perceived ease of use, technology features and complexity were tested. Structural equation techniques and T-test statistics were employed for the analysis.

The study found that technology features have enormous influence on technology acceptance and this may be extended to other professional groups apart from Internal Auditors. The study further found that the relationship of TAM variables is changed by technology features, for instance perceived usefulness has more impact on the usage of basic features than perceived ease of use. The main contribution of the study is the extension of TAM by inclusion of technology features into the model.

However one noticeable weakness of the study is the neglect of external variables of TAM in the study. The study assumes that external variables will not affect the overall result since the objective was to measure technology usage by examining the technology features. This may not be completely true.

4.3.0: Electronic Fraud Literature

Globalisation, coupled with the increasing use of computer network and internet to initiate and process financial transactions has led to increasing fraudulent activities. The fraudsters are improving on their tactics and sophistication as improved methods

of electronic transaction are being discovered. Research is on going to increase the level of technology sophistication ahead of the fraudsters. This section considers research in the area of ICT and fraud prevention and detection.

Abu-Musa (2006a) investigated the perceived threats of Computerised Accounting Information Systems (CAIS) in Saudi organisations. The results of the study revealed that almost half of the responding Saudi organisations suffered financial losses due to internal and external CAIS security breaches. The results also revealed that accidental and intentional entry of bad data, accidental destruction of data by employees, employees sharing passwords, introduction of computer viruses to CAIS, suppression and destruction of output, unauthorized document visibility, and directing prints and distributed information to people who are not entitled to receive them are the most significant perceived security threats to CAIS in Saudi organisations. The study introduced some suggestions and recommendations to strengthen the IT security controls and to enhance the awareness of CAIS security issues in Saudi organisations in order to manage the IT risks and to achieve a better protection of CAIS and IT internal controls. The study made use of survey questionnaire to collect data and analysed it using the SPSS package.

In another study, Abu-Musa (2006b) empirically examined the existence and adequacy of CAIS security controls to prevent, detect and correct security breaches in Saudi organisations. The results of the study highlighted a number of inadequately implemented CAIS security controls and introduced some suggestions and recommendations to strengthen the weak points and to close the loopholes in the CAIS security controls in Saudi organisations. The data used in this study is suspect as most companies would rather not disclose grievous computer security breaches for obvious reasons. Also the association between security breaches and fraud was not established.

Bierstaker et al. (2006) surveyed 86 accountants, Internal Auditors and certified fraud examiners to examine the extent to which they use fraud prevention and detention methods, and their perceptions of the effectiveness of these methods. The results indicated that firewalls, virus and password protection, and internal control review and improvement are quite commonly used to combat fraud. However, continuous

auditing, discovery sampling, data mining, forensic accounting techniques, and digital analysis software are less often used, despite receiving high ratings of effectiveness due to lack of resources and their reluctance to invest in fraud prevention and detection control systems. This study is important for fraud prevention and detection methods especially as the digital age is changing the face of auditing.

However, because the study was conducted in the United States, a developed economy, it is doubtful if the result can be generalised to a developing economy like Nigeria where poverty and struggles for personal survival are endemic.

Coram et al. (2006) carried out a study to assess the value of the internal audit function in detecting fraud within organisations. The study also evaluated differences in the effectiveness of fraud detection between organisations that choose between different internal audit approaches such as: internal audit function within the organisation (in-sourcing); out-sourcing; and a combination of both. The study found a significant positive relation between an organisation having an Internal Audit function and the number and value of self-reported frauds. The likelihood of fraud detection increases with organisation with Internal Audit function. The findings of this study are particularly interesting as they put outsourcing in a different perspective from prior studies, which found that financial statement users do not perceive a difference between internal audit in-sourcing and out-sourcing (James 2003; Lowe, Geiger and Pany 1999) and the belief that an external provider (outsourcing) is technically more competent.(Carey, Subramaniam and Ching, 2006). The measure of fraud used in this study is from the 2004 KPMG Fraud Survey administered on large organisations in New Zealand and Australia. In the original data KPMG sent the research instrument to 2164 of Australia's and New Zealand's largest organisations. Only 491 organisations responded (22.6 per cent). The amount of fraud reported was for a period of two years before the survey was conducted. This study suffers from many flaws. For instance, the study concentrated on large organisations with an established history of internal audit. The fact is that internal audit may be associated with organisations with good governance and internal controls may in turn prove to be the factors that increase the propensity to detect fraud rather than internal audit per se. The study was conducted in developed economy (New Zealand and Australia). So the result may not be easily generalisable to developing economies. The secondary

data used were collected more than two years before the study was conducted. The time lag is enough to invalidate the result as new technology is now increasingly involved in fraud perpetration. The effectiveness and value of internal audit in detecting fraud within organisations are not considered in this study. Most of the prior research has just focused on perceptions from External Auditors in this area (Coram et al., 2006). It is the intention of the current study to examine the effectiveness of ICT tools and techniques as used by IAs in detecting and preventing fraud in a developing economy using Nigeria as a case study.

Alon and Dwyer (2010) extended the studies on decision aids for fraud risk assessment by incorporating the impact of group interaction on decision aid reliance. Alon and Dwyer (2010) carried out fraud risk assessment in a 2 x 2 between-subjects experimental design. The experiment made use of 27 participants. 15 of the participants used decision aid and 12 are without decision aid. Another control group of 35 individual participants was set up. Participants were asked to list and rate the likelihood of risk occurring and complete the reliance scale.

Alon and Dwyer's (2010) study succeeded in integrating the fraud risk assessment and decision aid literature by evaluating decision quality and effectiveness of group fraud risk assessment. The findings provide a useful insight on how auditors' brainstorming impacts fraud risk assessment, decision aid support system and its reliance. The findings supported the hypothesis that decision quality of groups with decision aid will exceed the decision quality of groups without a decision aid.

The observed limitations of the study are the use of small sample size which is drawn mainly from graduating and Master level students. A study of this nature would have benefited more from a larger sample size drawn from different categories of practicing auditors. It is yet to be seen if IAs in Nigeria complement the use of IT with group brainstorming in order to be effective in fraud prevention and detection.

In an earlier study Payne and Ramsay (2005) investigated fraud risk assessments and auditors' professional scepticism. Payne and Ramsay's (2005) study made use of 3 x 2 between-subject design with 294 staff and senior auditors of three of the (formally) Big five accounting firms. The study made use of a two-way analysis of variance (ANOVA) for data analysis. The findings show that junior auditors are more sceptical than seniors. The level of scepticism is noticed to have reduced with experience.

The study substituted the measurement of auditors' assessment of client truthfulness for the measure of professional scepticism. This is largely due to the interpretation given to professional scepticism which in turn affects the outcome of the study.

Gloeck and Jager (2005) examined the phenomenon of fraud in South Africa's public sector. The results of numerous other studies were used to identify factors which are conducive to the occurrence of fraud. In other words, factors which, if they exist, create a positive environment for fraud. Respondents were asked to rank these factors according to their perceived order of influence. Gloeck and Jager (2005) use the following scale.

- 10 = Most likely reason for fraud to increase
- 1 = Least likely reason for fraud to increase

The results are (in order of importance): Weak internal controls (factor 7.0); bad management (6.63); lenient penalties (6.43); low social values (5.68); socio economic imbalances (4.80); inadequate legislation (4.76); high workload (4.64); and other factors (3.37). This result shows that weak (or inadequate) internal controls are seen as the most influential factor in creating a fraudulent environment. Two other factors contributing significantly towards frauds are weak (bad) management and lenient penalties.

Gloeck and Jager's (2005) focused their survey solely on Government or public institutions in South Africa. A replication of this survey in a financial environment, which is the primary focus of this research, may not necessarily indicate the same result. One major criticism of this study is that the researchers make use of the result of the work of others (secondary data) whose primary motives were not focused on investigating factors that contributed to increase in electronic frauds. Besides, the study failed to examine the impact of ICT tools and techniques on fraud prevention and detection which is of interest to this study.

Many authors believe that fraud prevention should take precedence over fraud detection. This is because prevention may be effected before actual damage is done (Bologna and Linqvist, 1995). Fraud prevention actually starts by creating a work

environment that ensures honesty which includes hiring honest people, remunerating them adequately and competitively and creating a conducive, safe and secure work environment (Mieke Jans et al., 2009). Establishment of fraud, specific internal controls and proactive fraud-specific examinations which are the direct responsibility of management reinforces fraud prevention. Recent studies have not agreed on the effectiveness of internal control in prevention and detection of fraud.

Some studies rate detection of fraud by means of tip-offs or by accident higher than by internal control mechanism (ACFE, 2006; PWC, 2007). Others identify internal controls as the key factor to prevent and detect fraud (Ernst and Young, 2006).

The research literature concentrates more on fraud detection than prevention. Few studies concentrate on internal fraud risk, which consists of fraud prevention and detection (Mieke Jans et al., 2010).

In a recent study, Mieke Jans et al.,(2010) built on the application of data mining in mitigating external fraud, to propose a framework that strengthens internal control framework for external fraud. Mieke Jans et al.'s (2010) IFR (internal fraud risk) framework was able to combine mitigation of both fraud prevention and detection. They also extended the data mining approach to both external fraud and internal fraud. However, it is yet to be seen if this framework will be effective where the current framework of internal control does not apply to data mining techniques risk (IFR). The framework is as shown in Figure 4.4 below. Mieke et al.'s (2010) study contributed to existing literature in two significant ways. Firstly their study focused on internal fraud which typically involves unsupervised data and more importantly also focused on risk reduction instead of fraud detection which were common in the literature. The study did not focus only on predicting the fraud class but on carefully observing all extreme values and grouping them into four categories (step v in the diagram): those that are of extreme value but logical on closer examination, those that are outright fraudulent; those that are merely circumventing procedures and those that are errors or mistakes. The last two categories fall under fraud prevention and may be analysed further by means of the fraud triangle.

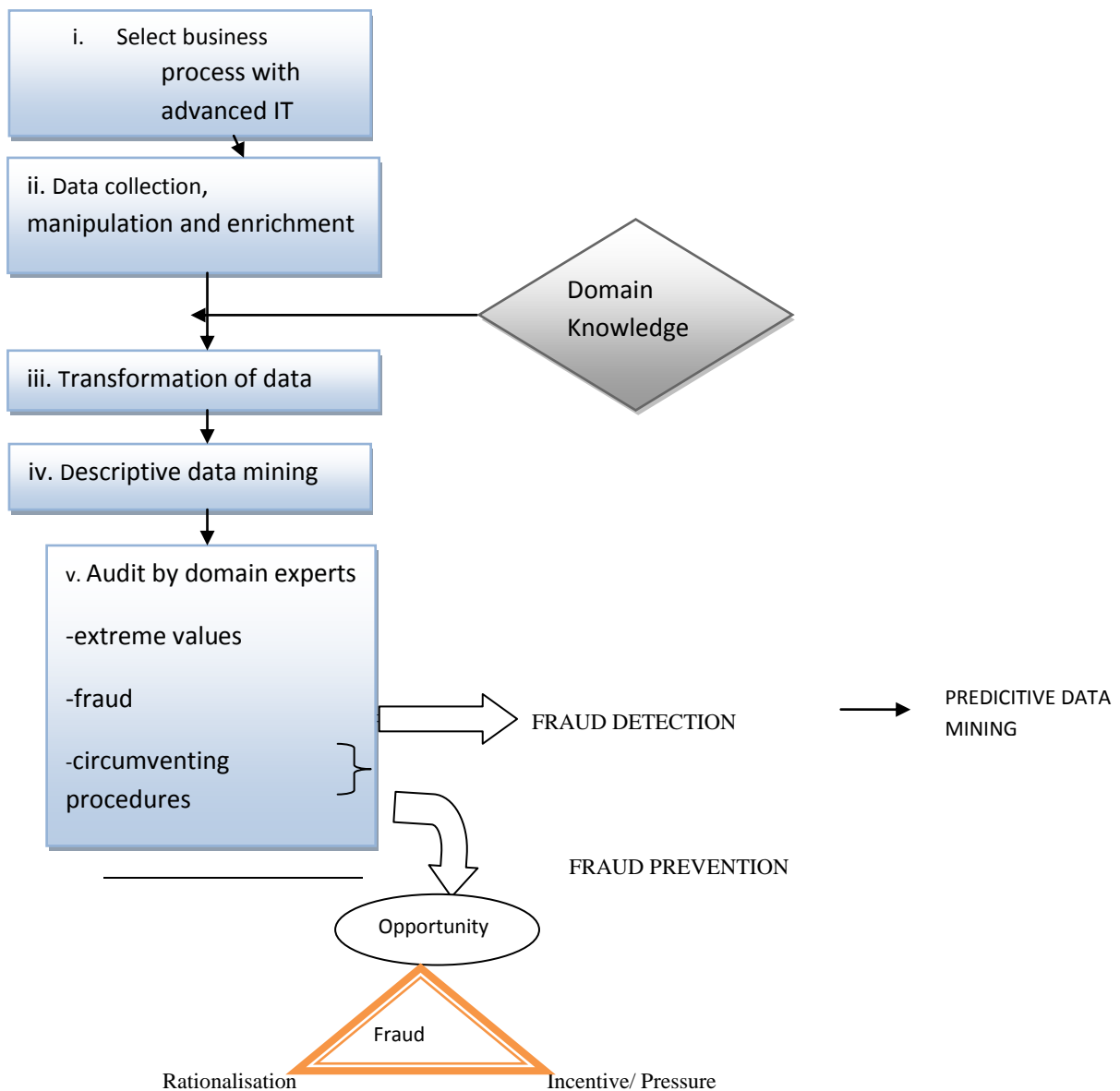


Figure 4.4: Framework of Internal control Techniques Combining Fraud Prevention and Detection Using Data Mining Techniques

Source: Mieke Jans et al. (2010 : 2)

A review of the literature on electronic fraud reveals that most studies concentrated on fraud detection. Only very few mentioned fraud prevention. Out of thirty studies reviewed only two (Estevez et al., 2006 and Sanchez et al., 2008) worked on both fraud prevention and detection. The popularity of fraud detection among scholars is proved by the fact that all the studies examined investigated fraud detection using data-mining techniques, e.g. Fuzzy Set theory (Derrig and Ostaszewski, 1995; Deshmukh and Talluru, 1998; Pathak et al., 2003; Sanchez et al., 2008), Neural Network (Fanning and Cogger, 1998; Dorronsoro et al., 1997; Green and Choi, 1997;

He et al., 1997; Maes et al., 2002; Viaene et al., 2005; Kirkos et al., 2007), Decision Tree, (Bonchi et al., 1999; Fan, 2004; Kim and Kwon, 2006). Neural network comes out as the most common technique used for detection of fraud. The popularity of neural network in regards to credit card, automobile insurance and corporate fraud applications may be due to some of its acclaimed advantages: it is capable of generating robust models, secondly, it is adaptive and lastly, the classification process can be modified anytime new training weights are set (Ngai et al., 2010).

Furthermore, of the 30 studies reviewed, 14 are about insurance fraud (automobile and health care insurance), nine involved credit card, six involved financial statement fraud while only one involved communication fraud. By far the insurance fraud is the largest claiming about 47 per cent of the studies reviewed probably because of the geographical location involved in the study (Europe and America). A study in a developing economy like Nigeria may not reveal the same pattern.

In a more recent study, Ngai et al. (2010) undertook an academic review of literature on the application of data mining techniques in financial fraud detection. Ngai et al. (2010) reviewed 49 journal articles on the subject published between 1997 and 2008. They analysed and classified into four categories of financial fraud: bank fraud, insurance fraud, securities and commodities fraud and other related financial fraud. Ngai et al. (2010) also came up with six classes of data mining techniques (regression, prediction, visualisation, classification, clustering, and outlier detection). The findings of this review agree with earlier studies that data mining techniques are the most commonly applied especially for the detection of insurance fraud and credit cards fraud. However the review finds paucity of research on mortgage fraud, money laundering, and security and commodity fraud. The reason for lack of research in these areas is not known yet. Ngai et al. (2010) study appears to be the first comprehensive literature review of application of data mining techniques in financial fraud detection spanning a period of 12 years (1997 to 2008). An observed limitation is that only literatures written in English language is included in their review. Furthermore, IT innovations are rapidly changing.

Author	Technique Used	Application Area	Detection	Prevention
Bermudez et al. (2008)	Skewed Logic Link and Bayesian Analyses	Automobile Insurance Fraud	Detection	
Brockett et al. (1998)	Kohonen's Self-Organizing Map	Automobile Insurance Fraud	Detection	
Brockett et al., (2002)	Principal Component Analysis	Automobile Insurance Fraud	Detection	
Derrig and Ostaszewski, (1995)	Fuzzy set theory	Automobile Insurance Fraud	Detection	
Kim and Kwon, (2006)	Insurance Fraud Recognition System (Korea)	Insurance Fraud	Detection	
Major and Riedinger (2002)	Electronic Fraud Detection (EFD)	Health Care Insurance Fraud	Detection	
Phua et al. (2005)	Meta-classifiers	Automobile Insurance Fraud	Detection	
Viaene et al. (2005)	Bayesian Neural Network	Automobile Insurance Fraud	Detection	
Viaene et al.,(2007)	Logistics Regression	Automobile Insurance Fraud	Detection	
Yang and Hwang (2006)	Frequent Pattern Mining	Health Care Insurance Fraud	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	Health Care Insurance Fraud	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	
Dorrnsoro 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	Telecommunications Fraud	Detection	Prevention

Table 4.2: Summary of Previous Studies on Fraud Prevention and Detection Techniques

Adapted from Jans, Lybaert and Vanhoof (2009: 14)

The latest data used in their work is that of 2008. A lot might have happened in technological innovations since then.

Table 4.2 above summarises literature review carried out by Jans et al. (2009). It is obvious from the table that prior studies concentrated on fraud detection. Jans et al. (2009) arrived at the conclusion that most studies concentrated on investigating external fraud consequently there is a gap in academic literature on investigation of internal fraud. A few internal frauds reported in the literature concerned financial statement fraud whereas evidence of asset misappropriation by internal operators is numerous (PWC, 2007). One noticeable trend that runs through the selected literature is the popularity of the usage of data mining techniques in the context of fraud detection. This underlines the importance of data analysis technique that encompasses insightful data interpretations and lead to knowledge. This is a step above the traditional data extraction technique that is primarily focused on extracting statistical quantitative data.

4.4.0: Summary of Literature

The main focus of this chapter has been the review of pioneer and current literature on the four main objectives of the thesis identified in chapter one. Attention has been focused upon: (1) assessing the level of ICT usage by Internal Auditors (2) assessing the impact the usage of ICT for internal control has on IAs' independence and objectivity (3) assessing the potential of ICT tools and techniques on electronic fraud prevention and (4) assessing the effectiveness of ICT tools and techniques on electronic fraud detection in order to identify gaps in the body of knowledge. A general review was carried out followed by a specific review of relevant literature in the area of internal control, internal auditing, ICT tools and techniques, knowledge-based system, continuous online auditing, fraud prevention and detection and adoption of ICT. Gaps were identified in the methods adopted, the statistical analysis used, theoretical underpinnings, findings and limitations inherent in previous studies' approaches.

In the next section, research propositions are stated based on the experience and information gathered and gaps identified from the literature reviewed. Examinations

of various theories that are popularly used in ICT research are carried out in order to access the most suitable theory for the study.

4.5.0: Gaps in the Literature

In order to strengthen the efforts of auditors in making qualitative judgement decision aids consisting of decision support systems and highly complex artificial intelligence-based system (knowledge-based expert systems and neural networks) are being deployed (Abdolmol Mohammadi and Usoff, 2001). Some studies emphasised the benefits of decision aids to auditors while some other empirical studies indicated that auditors over-rely on expert systems output (Glover et al., 1996; Swinney, 1999). A review of the literature reveals a paucity of empirical studies related to investigating IT-related activities performed by Internal Auditors in developing countries. Abdul-Gader (1990) stated that most of the previous studies focusing on computing practices in developing countries are mainly descriptive, and much work needed to promote adoption of computer systems on a wider scale. The current study is a response to Abdul-Gader's call by carrying out further empirical research in Nigeria on ICT usage for internal control effectiveness.

The review showed that organisations are increasingly adopting the use of knowledge-based systems to improve the internal control and internal audit process. The quality of internal control procedures (ICP) has been linked to fraud prevention (Rae and Subramaniam, 2008; PWC, 2007) and value of internal evidence (Janvrin, 2008). However there is no agreement among the studies reviewed on the reasons for adoption of ICT. Few studies have examined the impact of ICT on auditing or accounting (Omoteso, 2006) but no study has specifically examined the impact of ICT on internal control effectiveness in the prevention and detection of electronic fraud, especially in a developing economy like Nigeria. Besides, only very few studies focused on homogeneous professional group such as internal auditing which is the focus of the present study (Mahzan and Lymer, 2008; Kim et al., 2009)

Internal Auditor's independence has been a contentious issue in academic literature. While the IIA and COSO through their definitions and frameworks believe that:

“independence and objectivity “are essential for Internal Auditors to carry out their mandate effectively, other commentators believe that Internal Auditor cannot be completely independent since they are responsible to the management. Independence of Internal Auditors has been found to be impaired by using internal audit function as a training ground for higher management positions or by operating a bonus scheme for “outstanding performance” (Sarens and De Beelde, 2006; Christopher et al., 2009; Stewart and Subramaniam, 2010).

Prior studies on Internal Auditors’ independence suffered from lack of theoretical guidance. In addition none of the studies reviewed examined the impact of ICT on Internal Auditors’ independence and objectivity. This study endeavours to minimise the void in the internal auditing literature by contributing empirically to the debate on how ICT impacts Internal Auditor’s independence and objectivity. Another objective of the review is to appreciate the current knowledge stock of the usage of COA. The review showed that adoption of COA is becoming more popular however the readiness of audit professionals and their clients to adopt COA remains a contentious issue (Omoteso et al., 2008). Furthermore another noticeable gap in literature is the scanty research efforts in electronic fraud prevention and detection. The available literature concentrates more on fraud detection than prevention even though the best way to reduce electronic fraud is through prevention technologies. This may be due to the fact that data are difficult to gather from individual and firms because of privacy protection issues. Another reason is that any system designed to detect errors is regarded as a fraud-prevention system. Consequently, there is additional gap in identifying a dominant theoretical framework for exploring electronic fraud prevention and detection. The reason may be partly due to the fact that so many dynamic variables are involved. Man, Machine, Organisation environment, External variables, Regulatory environments are all involved at the same time. All these variables undergo constant changes. The rate of technological changes is so fast and dynamic to the extent that it affects virtually all other variables. Fraudsters are known to be vastly adaptive and capable of circumventing any measure given a little time to study the existing system. Studies in the area of fraud prevention and detection are therefore ongoing as there is a need to stay ahead of fraudsters.

4.6.0: Emergence of Research Propositions from the Literature

This section is a follow up from the discussion on existing literature in chapters three and four. It summarises the studies already reviewed with a view to examining the overall gap that may exist within the body of knowledge. The rapidly changing role of IT in auditing places limitations on the extent to which the existing findings from earlier studies can be relevant to the current audit environment.

There is disagreement in research literatures about the meaning normally given to the terms ‘hypothesis’ and ‘proposition’. In most cases, it generates more confusion when they are used interchangeably. “Research proposition refers to a statement about a concept that may be considered as true or false in relation to observable phenomena. Hypothesis refers to a situation where a statement is created to speculate upon the outcome of an experiment or when a proposition statement is presented for empirical testing” (Cooper and Schindler, 1998: 43). This study makes use of research propositions rather than hypotheses because of the following:

This study intends to push forward the frontier of knowledge by bringing out the relationship between two or more variables rather than establishing cause. Exploratory approach is adopted for the empirical part of this study. The study utilised a more pragmatic approach to make it more meaningful.

4.6.1: Effectiveness of Internal Control

System success itself is a variable that is not easily explained in literature. Several studies adopted surrogate measures for the measurement of the systems success concept. This study viewed systems success as the positive strategic benefits of using ICT to control the operations of the organisation. There is symmetry between system success and effectiveness of Internal controls. Effectiveness of Internal controls connotes provision of reasonable assurance that the entity is achieving efficiency and effectiveness of operations and at the same time compliance with relevant regulations. This study adopts the five-point Likert scale developed for measuring the effectiveness of the system of internal control in the previous studies, (Wise 1990; Romney and Steinbart 2000 and Henderson 2002). The effectiveness of internal control is measured using the perception of Internal Auditors.

4.6.2: Proposition I: Nigerian Internal Auditors are increasingly adopting IT-based tools and techniques

In order to bring out the issues involved clearly, this proposition is broken down into three themes as follows:

(1.1) Internal Auditors' current level of ICT usage for Internal Control purpose is increasing;

(1.2) Financial institutions' current level of provision of ICT for Internal Control purpose is increasing and

(1.3) ICT tools and techniques are useful for Internal Auditors' tasks, efficiency and effectiveness.

The Nigerian business community has engaged the use of ICT as a means of conducting business transactions in order to keep abreast with the rest of the developed world. Ayo et al. (2008: 2) found that 'improved technological development and provision of basic infrastructure will improve e-commerce and e-payment services with overall reduction in the amount of currency in circulation'. In another study, Adeyemi, (2008) opines that electronic payments have increased and actually accounted for N360 billion worth of transactions in 2008 alone. This trend is expected to be sustained with the recent policies of the central bank of Nigeria to discourage the use of cash transactions. Most studies examined ICT usage in the financial sector of the economy (Irechukwu 2000; Agboola 2001; Ayo et al., 2008; Adesina and Ayo 2010) whereas no study has examined the level of usage of IT-based tools and techniques by Internal Auditors in Nigeria.

A Technology Acceptance Model (TAM) has been widely used and tested for investigating users' adoption of IT (Davis et al., 1989; Venkatesh and Davis, 2000; Hasans, 2007; Adesina and Ayo, 2010). TAM is adopted as a model for this proposition. Extensions are introduced to TAM as external variables in order to measure their impact on the acceptance to use IT tools and techniques. The model is shown in Figure 2.8. The external variables include "effectiveness", "Computer Self-efficacy", and "Internal auditors' attitude".

The main purpose of investments in ICT by many organisations nowadays is to achieve maximum efficiency and eventually reduce the cost of operations. It is

paradoxical to note that the benefits that organisations can gain from investing in ICT are influenced by the extent to which users (Internal Auditors) are willing to accept and use technological tools. The productivity paradox has increased interest in understanding factors affecting systems' acceptance and utilisation (Hasan, 2007). Several studies have been carried out on systems' acceptance and use. The reported results in the Information System literature are mixed and inconclusive. An array of researchers used TAM to explain acceptance behaviour as a function of users' beliefs about the usefulness and ease of use of a given system (Davis, 1989; Legris, Ingham, and Collette, 2003; Hasan, 2007). While TAM provided a convenient basis for mapping the effects of external factors on users' internal beliefs of usefulness and ease of use (Davis, 1989), careful attention was given to external variables (computer self-efficacy and system complexity) in Hasan's (2007) study by expanding TAM variables and examining the impact of the external variables on TAM and IS acceptance. Hasan (2007) found that both computer self-efficacy and system complexity affect technology usefulness and ease of use. There is a need to extend the study to examine the effect of perceived system complexity on IAs and internal control effectiveness especially in an emerging economy like Nigeria.

This study is intended to contribute to knowledge by examining the level of usage of IT tools and techniques by Internal Auditors in the Nigerian financial sectors using variables in Gullkvist's, 2003 TAM's model in a developing economy. The study sought explanation as to whether the adoption of IT in the Nigerian financial sector is due to Perceived benefits (including internal control effectiveness), Organisational readiness, Trust, External pressure or any other variables.

4.6.3: Proposition 2: The use of ICT-based tools and techniques in Internal Control impacts positively on Internal Auditors' independence.

The IIA standards emphasised the importance of Internal Auditors' independence for internal control effectiveness. For instance the following Attribute Standards are of relevance:

Standard 1100: says "the internal audit activity should be independent, and Internal Auditors should be objective in performing their work"

Standard 1110: “the internal audit activity should report to a level within the organisation that allows the internal audit activity to fulfill its responsibilities”

Standard 1110.A1: “the internal audit activity should be free from interference in determining the scope of internal auditing performing work, and communicating results”

Standard 1120: “Internal Auditors should have an impartial, unbiased attitude and avoid conflicts of interest”

Pickett (2005: 112) explains the concept of independence to mean “that management can place full reliance on audit findings and recommendations”. He further suggests the concept of Internal Auditors’ independence to mean “objectivity, impartiality, unbiased views, valid opinion, no spying for management, no ‘no-go’ areas, sensitive areas audited, senior management audited and no backing-off when confronted by an assertive manager”.

The impact of ICT usage on internal control can be influenced by the ‘user’ and ‘monitor’ of the system. This may depend on the users’ motivation from management and audit committee. Davis (1989) suggested that users’ motivation can be explained by three elements thus: perceived ease of use, perceived usefulness, and attitude toward using the system. Fadzil and Jantau (2005) concluded in their study on internal auditing practices and internal control that internal auditing practices impact on quality of the internal control system. It is proposed in this study that if ICT usage has a positive impact on Internal Auditors’ independence, it will equally positively impact on perceived usefulness of ICT for internal control in the same direction and vice versa.

An Internal Auditor who has professional and reporting independence is more likely to take advantage of ICT usage in internal control for prevention and detection of fraud. This is in accord with Vaccaro and Madsen, (2009) who predicted that ICT will play a positive role in future ICT-driven ethics and transparency of Internal Auditors. Prior studies have looked at auditors’ independence in relation to External Auditors (Beattle and Fearnley, 2002; Porter et al., 2003; Godwin, 2004). Very few studies examined IAs’ independence in relation to audit committee.

4.6.4: Proposition 3: Internal Auditors' use of ICT-based tools and techniques has the potential of preventing electronic fraud.

Proposition 3 is further divided into three themes for better analysis as follows:

3.1. Internal Auditors' use of ICT has had positive impact on prevention of fraud

3.2. COA has effective fraud prevention control

3.1. The extent of ICT utilisation for prevention of fraud is affected by auditors' demographic characteristics (experience, gender and qualification)

There are two fundamental assumptions in a continuous audit environment. The first is that the auditors have the proficiency to carry out a continuous audit engagement. The second is that the processes that capture, aggregate, store and report information on the subject being audited are highly automated through the use of audit tools and techniques so as to be available in real time.

Continuous online auditing (COA) as a principal technique for internal control gives Internal Auditors the ability to monitor key business systems for both anomalies at transaction level and for data-driven indicators of control deficiencies and emerging risk. According to Seetharaman et al. (2006: 1067) "Fraud Prevention Procedures should have three realistic and measurable goals: viz (1) reduce losses resulting from fraud (2) deter fraud through proactive policies; and (3) increase the likelihood of early fraud detection" Fraud preventive capability of COA makes it unique for internal control. It could be done by deploying appropriate artificial intelligence to monitor control and report anomalies continuously.

The obvious advantage of COA is that it can be applied in two ways: to audit historical records in the same way as traditional audit, i.e. detective orientation (ex-post) or to pre-empt occurrence of errors and frauds by the use of sophisticated data mining techniques (ex-ante) or preventive orientation. Prior studies agree that preventive orientation of COA can be enhanced by incorporating appropriate artificial intelligence in the design which is capable of functioning as Continuous Intelligent Online Validation (CIOV). (Helms, 2002; Omoteso et al., 2008)

While the complexity of IT makes auditing more challenging, it also provides an opportunity to streamline internal audit activities by designing and utilising continuous IT controls. Adoption of COA may reduce the need for detailed annual reviews that have been typical in the traditional accounting setting. COA gives IAs the ability to monitor key business system. COA can also be incorporated into other aspects of the audit process (Coderre, 2005).

Warren and Parker, (2003) explain that under continuous online auditing, technology is an enabler, but must be initiated and managed by the Internal Audit Function.

Cash et al. (1977) noted that the use of computer in accounting induced the development of Electronic Data Processing auditing as a new auditing field. Yu et al., (2000) built on earlier work and noted that the demand for more reliable, relevant and timely decision-making information actually drives the demand for COA which is increasing by the day. According to Searcy and Woodroof (2003) further advantages of COA include reducing wastages commonly associated with the traditional audit process, such as time delay, process cumbersomeness, errors and mistakes, accessibility delay and over auditing.

CICA (2003) noted that automation may apply to three categories of data: routine hard data (e.g. sales price); non-routine hard data (e.g. periodic adjustments entities of accruals); soft data, i.e. a data with a high degree of subjectivity that requires judgment by the clients' staff (e.g. net realisable value of inventory)). Automating this type of data is becoming more or more feasible with advances in information technology such as neural networks and intelligent agents.

Yu et al. (2000) identify and discuss the potential impacts of electronic commerce on auditing practices in the emerging paperless online transaction environment. Yu et al. (2000) develop two auditing process models that incorporate modern network security techniques and show how an audit can be conducted in an e-commerce environment. A periodical auditing process model (PAPM) is proposed to demonstrate how secure electronic technologies can be used to facilitate the auditors' evidence collection and validation process for annual and semi-annual audits. Yu et al. (2000) also present a continuous auditing process model (CAPM) which extends the functions of PAPM for continuous auditing. The main contribution of their work

is that they propose a conceptual framework and corresponding solution processes for validating electronic transactions and for conducting external continuous auditing in an electronic commerce environment. In particular, Yu et al. (2000) provide a first step to answer several issues proposed by Kogan et al. (1999) related to continuous online auditing (COA), (e.g. the architecture of COA, system audit, security of COA and electronic records). Studies have shown that IAs are interested in continuous auditing even though they have difficulties in applying the concept successively as a result of lack of experience, financial resources and necessary training (IIA, 2003). How experience, financial resources and necessary training impacted on Internal Auditors' ability to implement COA in the Nigerian financial sector is yet to be seen.

Several studies have been carried out on fraud detection techniques (He et al., 1997; Brause et al., 1999; Bolton and Hand, 2002; Lin et al., 2003; Fan, 2004; Viaene et al., 2005; Yang and Hwang, 2006; Hoogs et al., 2007; Kirkos et al., 2007; Juszczak et al., 2008) whereas only a few studies examined fraud prevention techniques (Estevez et al., 2006; Sanchez et al., 2008). In view of limited number of studies on fraud prevention, this study hopes to extend the frontier of knowledge by examining the extent of usage of IT tools and techniques by Internal Auditors in Nigerian financial institutions and the ability of Continuous Intelligent Online Validation (CIOV) currently in use to predict and prevent potential financial fraud, quickly and easily authenticate identities online, eliminate manual inefficiencies and identify high-risk applicants who warrant further investigation.

4.6.5: Proposition 4: Internal Auditors' use of ICT-based tools and techniques is effective in detecting electronic fraud.

This proposition is further divided into three themes for better analysis as follows:

- 4.1. Use of ICT in internal control has had positive impact on detection of fraud
- 4.2. COA has effective fraud detection control
- 4.3. The extent of ICT utilisation for detection of fraud is affected by auditors' demographic characteristics (experience, training and qualification).

There is no universally accepted definition of electronic financial fraud. This study adapted the one given by Wang et al. (2008 : 1120): “e-financial fraud is a deliberate act that is contrary to law, rule, or policy with intent to obtain unauthorised financial benefit”. Financial fraud detection is vital for business survival in any part of the world. It manifests in the form of bank fraud (mortgage fraud, asset forfeiture/money laundering and identity fraud, advance fee fraud, foreign exchange fraud) insurance fraud (healthcare insurance, motor insurance, life insurance) and security and commodity fraud (theft from security accounts, wire fraud).

The limited number of relevant journal articles in the area of electronic financial fraud has been traced to difficulty in obtaining sufficient research data. Fanning and Cogger (1998) noted that challenges associated with collection of financial fraud data is a cog in the wheel of financial fraud detection research. All the studies reviewed in electronic fraud detection were based on Data Mining Techniques. For instance, some studies used neural network (Davey et al., 1996; Ezawa and Norton, 1995; Dorronsoro et al., 1997; Green and Choi, 1997; He et al., 1997; Fanning and Cogger, 1998; Brause et al., 1999; Hilar and Mastorocostas, 2008). Some used decision tree, (Bonchi et al.,1999; Viaene et al., 2002; Fan, 2004;). Some used fusion rules, (Derrig and Ostaszewski, 1995; Estevez et al., 2006; Sanchez et al., 2008). These are all frameworks of data mining techniques for financial fraud detection. The existing financial fraud detection research focuses on particular types of data mining techniques or models (Ngai et al., 2010). Furthermore, all the studies were carried out in a developed economy. A replication of some of these studies may not bring out the same result in a developing economy like Nigeria.

This study intends to direct its attention towards finding out how effective are the IT tools and techniques currently being used by IAs in financial fraud detection and suggesting more practical principles and solutions for the practitioners to help them to design, develop, and implement data mining and business intelligence systems that can be applied to financial fraud detection in developing economies.

4.7.0: Summary of Section

This section has examined the four main propositions drawn from literature. The propositions are aimed at providing answers to the research problem. The preceding sections were devoted to the review of relevant literature. A general review was first carried out followed by a targeted review in the area of internal control, internal audit, computer-assisted auditing tools and techniques, knowledge-based expert system; electronic fraud and continuous online auditing. A critical review of content, methodology, statistical analysis adopted, findings and theoretical underpinnings was carried out. This made it possible to assess and identify the gaps that currently exist, some of which this study intends to fill.

In addition, a review of relevant theories commonly used in ICT research is carried out in chapter four in order to assess their relevance to the present study. The next chapter focused on the theoretical framework considerations for this study based on the insight provided by the review of relevant literature in this chapter.

CHAPTER FIVE

THEORETICAL FRAMEWORK

5.0: Introduction

This chapter considers some of different theories that have commonly been used in ICT studies over the last two decades that are considered suitable for this study. Prior scholars on auditing and information systems made use of different theories to underpin their studies depending on their personal inclination and the relevance of such theories to the principal variables in their studies. For instance, those who see auditing as an instrument that may bridge information asymmetries that put question marks on information generated by management (agents) to shareholders (principal) are inclined to use Agency Theory or Agency Structure Theory (ICAEW, 2005). Most common theories in ICT research are considered and the two most suitable theories are selected. A brief summary of the theoretical framework considered useful for the study follows.

Theoretical Framework

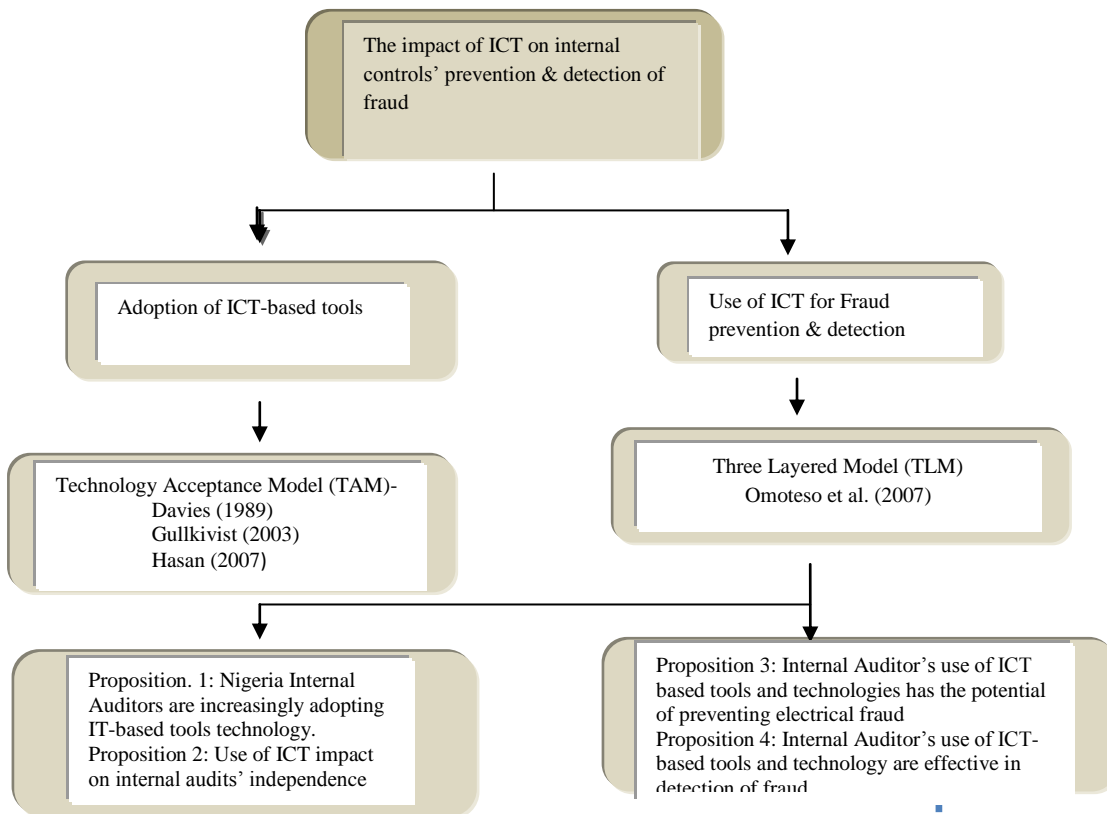


Figure 5.1: Summary of Theoretical Frameworks for the Study

This study considered the most cited theories and models used in the field of ICT in the last two decades (1991 – 2011) in order to situate the most appropriate theory for explaining the impact of ICT on internal control effectiveness in prevention and detection of fraud. The theories are presented in Table 5.1.

Table 5.1: Theories Adopted by the Most Cited Articles and Books on ICT System Implementation and Adoption

	Theory	Author(s),year	Citations	% of 2474
1	Three Layered Model (TLM)	Omoteso et al. (2007)	1	--
2	Technology Acceptance Model (TAM)		869	35.1
	TAM	Davis, 1989	237	
	TRA and TAM comparison	Davis et al., 1989	195	
	TAM, TPB and the decomposed theory of planned Behavior (comparison)	Taylor and Todd, 1995	144	
	Extension called TAM2	Venkatesh and Davis, 2000	129	
	TAM and TPB (comparison)	Mathieson, 1991	90	
	TAM (replication)	Adams et al., 1992	74	
3	Theory of Reasoned Actions (TRA)		502	20.3
	TRA and TAM (Comparison)	Davies et al., 1989	195	
	TRA	Fishbein and Ajzen, 1975	130	
	TRA and DOI (Combination)	Karahanna et al., 1999	100	
	TRA	Ajzen and Fishbein, 1980	77	
4	Diffusion of Innovations (DOI)		497	20.1
	DOI	Rogers, 1983	286	
	DOI	Moore and Benbasat, 1991	111	
	TRA and DOI (Combination)	Karahanna et al., 1999	100	
5	Theory of Planned Behavior (TPB)		331	13.4
	TAM, TPB, and the decomposed Theory of Planned Behavior	Taylor and Todd, 1995	144	

	TBP	Ajzen, 1991	97	
	TAM and TPB	Mathieson, 1991	90	
6	Unified Theory of Planned Behavior (UTAUT)		109	4.4
	UTAUT combines eight models, TRA, TAM and TPB	Venkatesh et al., 2003		
7	Models of the ICT Implementation process	Cooper and Zmud, 1990	85	3.4
8	Information Systems Success Model	Delone and McLean, 1992	81	3.3
	Total		2474	100

Source: Korpelainen (2011:14)

Korpelainen (2011) carried out a critical review on theories of ICT system implementation and adoption. The aim of the research was to examine what influential theories and models of ICT system implementation and adoption are used in management and business research. The data set was limited to 1303 sample articles published in 122 different leading management and business journals between 1999 and 2010. The data were analyzed using citation analysis and qualitative content analysis. The result shows that out of a total of 2474 citations, TAM and TAM extended theories enjoyed 869 (35.1 per cent) citations; Theory of Reasoned Actions (TRA) 502 (20.3 per cent); Diffusion of Innovations (DOI) 497 (20.1 per cent); Theory of Planned Behaviour (TPB) 331 (13.4 per cent); Unified Theory of Acceptance and Use of Technology (UTAUT) 109 (4.4 per cent); Model of the ICT Implementation Process 85 (3.4 per cent); Information Systems Success Model 81 (3.3 per cent). The most cited theory was clearly TAM; this is consistent with Davis, (1989). Among the reasons provided for the popularity of TAM in ICT research were those of its simplicity, appropriateness and understandability.

Korpelainen's (2011) study benefited from the longitudinal approach to data collection and the rich data set provided by the quantum of data obtained no doubt extended the frontier of knowledge. However, the research work could have benefited more if the qualitative and or interpretive approach were used to induce a more novel knowledge and possibly new theories.

Some of the commonly used theories in information system research are now briefly considered vis-à-vis their suitability for this study.

5.1.0: Commonly Used Theories in Information System Research

5.1.1: Theory of Reasoned Actions (TRA)

One of the theories that is popular in the ICT system implementation and adoption research is TRA which has its origin in social psychology. TRA sets out to provide definition between attitudes, beliefs, intentions, norms, and individual behaviours. TRA focuses on the behavioural intentions of the individual which in themselves depend on his or her subjective norms. TRA has been heavily used in consumer behaviour, women and family planning behaviour and research concerning users' pre-adoption and post-adoption behaviour. In most cases, TRA is combined with other theories. TRA is not favoured for this study as the adoption and effectiveness of ICT for internal control do not entirely depend on behavioural intentions of Internal Auditors alone.

5.1.2: Theory of Planned Behaviour (TPB)

TPB is similar in many ways to TRA but focuses more on perceived behavioural control. The theory has been used to underpin studies concerning drinking problems and leisure behaviour and provide effective interventions (Ajzen, 1991). Prior studies have examined the ability of TPB and TAM to either explain behaviour or predict individual intention to use ICT (Mathieson, 1991; Todd, 1995). TPB is considered insufficient for this study as the study involves not only humans but technology, institutions and prevention and detection of electronic fraud.

5.1.3: Diffusion of Innovations (DOI)

DOI was proposed by Roger in 1983. It focused on "how new ideas or innovations are spread and adopted in a community and seeks to explain how communication channels and opinion leaders shape adoption." (Korpelainen, 2011: 16) A five-stage model was proposed by Rogers (1983) for the implementation and adoption of innovation (new ideas) in institutions. DOI has been used successfully to develop "an

instrument designed to measure the various perceptions that an individual may have of adopting an information technology (IT) innovation” (Moore and Benbasat, 1991, 1992 cited in Korpelainen, 2011: 16). This study involved not only IAs but financial institutions and ICT which are increasingly changing with time therefore DOI may not be suitable as theoretical underpinning.

5.1.4: Unified Theory of Acceptance and Use of Technology (UTAUT)

UTAUT is also a popular theory that is being used in ICT adoption research. It is a unified theory because it combines several models such as TRA, TAM, TPB, DOI, PC utilisation model, the motivational model and social cognitive theory. UTAUT focuses on four constructs to determine users’ usage and acceptance behaviour: (i) performance expectancy, (ii) effort expectancy, (iii) social influence, and (iv) facilitating conditions. The four constructs are considered along with four moderating variables: age, experience, gender and voluntariness of use. UTAUT no doubt has a wider application and may be particularly useful to assess the success of ICT and identify the drivers of ICT acceptance. However UTAUT is not considered suitable for this study as it “focuses on users who may be less willing to adopt and use a new system” (Korpelainen, 2011: 17). UTAUT has been criticised by various independent commentators for presenting too many independent variables for predicting intentions and behaviour and “being less parsimonious than TAM and TAM2” (Bagozzi, 2007; Van Raaij and Schepers, 2008)

5.1.5: Model of the IT Implementation Process (MIIP)

MIIP was first introduced by Kwon and Zmud (1978) and later extended by Cooper and Zmud (1990). The model proposed a framework for directing and organising research based on innovation, changes in organisations and technological diffusion. Kwon and Zmud’s (1987) initial model proposed six stages: (i) initiation, (ii) organisational adoption, (iii) adaptation, (iv) acceptance and adoption, (v) routinisation, and (vi) diffusion. MIIP appears to be a much more embracing model than most of the models so far considered. Apart from focusing on the six stages from adoption to diffusion of IT, it also examines intervening variables such as the technology being used, the organisation, the environment, the task in focus, and the

users' community characteristics. MIIP appears to be a good theoretical underpinning for ICT adoption and usage studies. However, it is doubtful if MIIP can be used to sufficiently provide a theoretical framework for a study involving electronic fraud prevention and detection.

5.2.0: Technology Acceptance Model (TAM)

In his initial proposal, Davis (1989) suggested that users' motivation can be explained by three factors: perceived ease of use, perceived usefulness, and attitude toward using the system. Davis (1985) hypothesized that "the attitude of a user toward a system was a major determinant of whether the user will actually use or reject the system. The attitude of the user, in turn, was considered to be influenced by two major beliefs – perceived usefulness and perceived ease of use – with perceived ease of use having a direct influence on perceived usefulness" (Chuttur, 2009: 2)

ICT self-efficacy refers to individuals' judgement about their capability to execute and organise courses of action necessary to carry out a given task. In social cognitive theory, self-efficacy impacts people's behaviours on efforts to exert to achieve a given level of performance. It also influences the level of perseverance needed to overcome obstacles (Bandura, 1986).

According to Moore and Benbasat (1991), perceived system complexity (PSC) can be explained as "the degree to which a computer system is perceived to be difficult to learn or use". It is clear that the perception of the system user (Internal Auditors) is what is referenced here and not the complexity of the system itself. Prior studies on perceived system complexity and systems acceptance found an inverse relationship between PSC, acceptance and usage behaviour (Thompson et al., 1991; Bradford and Florin, 2003).

Hasan (2007) extended prior studies by integrating computer self-efficacy and perceived system complexity as external variables to TAM in order to examine the direct and indirect impacts of these two variables on system acceptance and use. Hasan (2007) surveyed a total of 121 students who were given a 70-minute training presentation on the use of a Unix-based text editing application (PICO). A total of

102 questionnaires were collected the following day, ninety-six (96) of which were usable. Respondents were asked to indicate their confidence level in their ability to use unfamiliar software to complete certain computing tasks and responses were recorded on a 10-point interval scale ranging from (a) not at all confident to (b) totally confident. Hasan (2007) found that computer self-efficacy and system complexity had significant direct effects on perceived usefulness and perceived ease of use. He further developed a model as shown below:

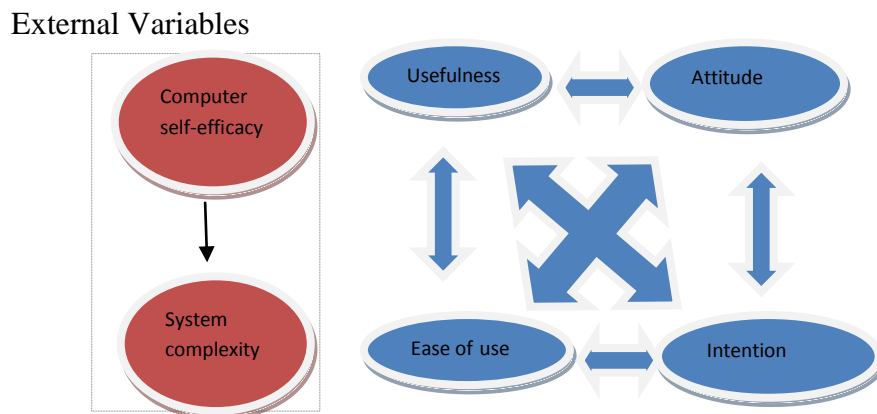


Figure 5.2: TAM and Research Model

The Technology Acceptance Model (TAM) Hasan (2007:79)

Hasan’s (2007) study made useful contributions to the body of knowledge on ICT research and practice by extending TAM and incorporating CSE and PSC as external factors using TAM’s core constructs. However the study’s major limitation is the use of student subjects to test the research model. In order to enhance generalisation of results to other user groups, the choice of subject sample should have been made to take care of diverse organisational settings (Hasan, 2007). However, Hasan’s 2007 model may not be appropriate for a highly skilled set of users like Internal Auditors in that the external variables of CSE and PSC are not likely to have much effect since they can learn fast and adjust to any new technology.

Gullkvist (2003) adapted TAM for the accounting environment and produced his own version by incorporating ‘Trust’ which was earlier suggested by Hart and Saunders (1997). Gullkvist’s (2003) TAM model is considered most suitable for this study because it has already been adapted to the accounting environment. Besides, all the four variables of trust, organisation readiness, perceived benefits and external pressure are relevant to IAs in the internal control environment

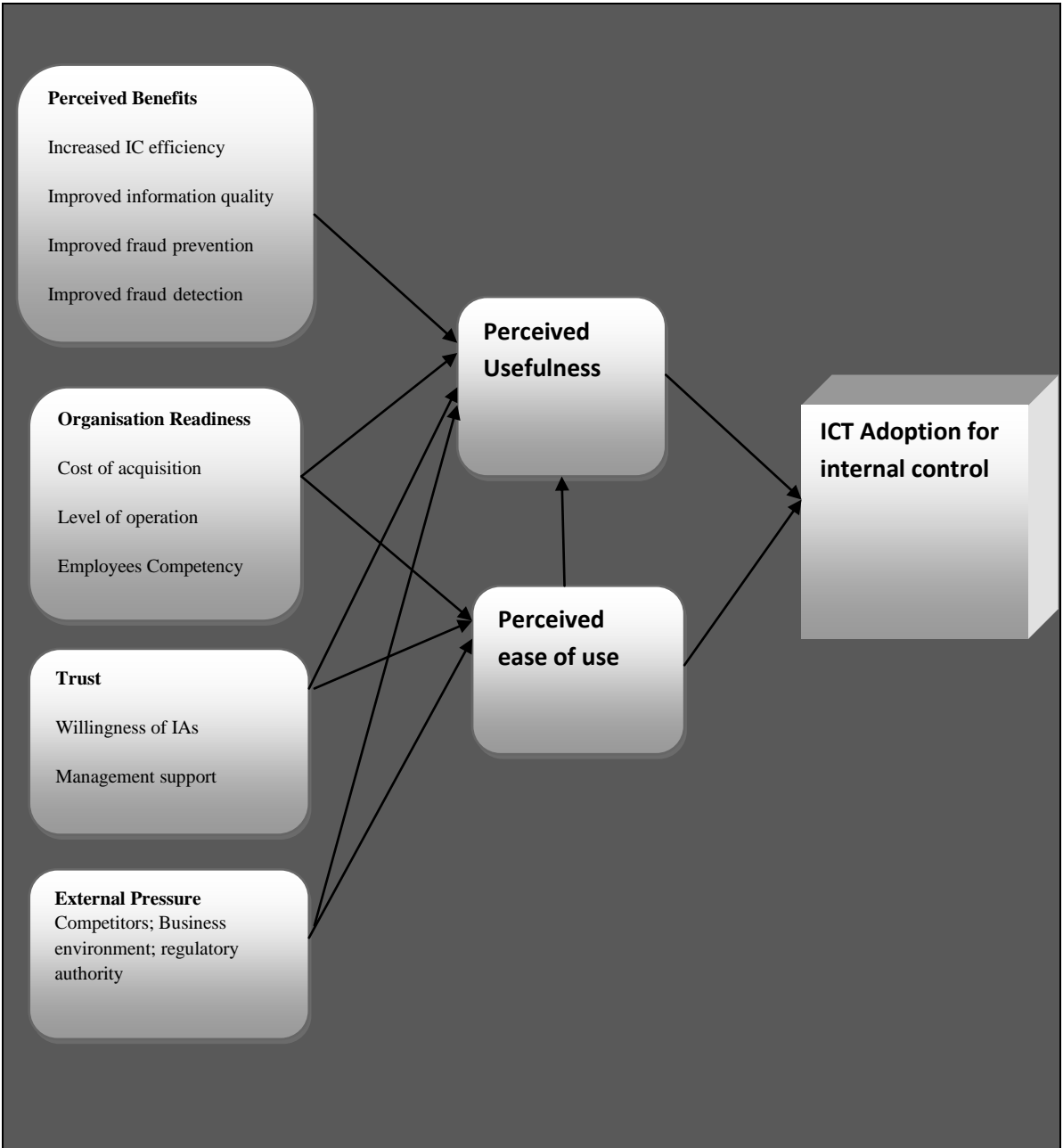


Figure 5.3: TAM Model for Adoption of ICT in Internal Control by Internal Auditors

Adapted from Accounting Adoption Model (Gullkvist, 2003:541)

Perceived benefits are benefits that can be derived from establishing ICT in a business and can be grouped into two. Researchers refer to the first group as direct benefits, which include reduction of transaction cost, increased internal control efficiency and improved information quality. The second group is indirect benefits and this is related to improved operational efficiency, increased ability to compete and improved customer service (Gullkvist, 2003).

Organisational readiness refers to the financial and technological capability of the business, how much finance is available for the installation of the required technology and the level of IT users' know-how within the business (Iacovou et al., 1995).

External pressure to adopt IT is influenced by the business environment. Iacovou et al. (1995) identified the two main sources of external pressure to adopt as "competitive pressure and imposition by trading partners". As trading partners appear to have competitive edge by the adoption of ICT there will be increased pressure on businesses to adopt the technology as well in order to stay relevant and competitive.

Trust is the fourth factor which was added to the model by Hart and Saunders (1997). Trust is considered essential for investment and to discourage opportunistic behaviour. It refers to reliability and openness. Most small businesses are concerned with the reliability of hired managers to transmit accurate data and information (Gullkvist, 2003). Hart and Saunders (1997) observed that some managers in smaller firms appear to resist adoption of EDI technology even when the advantages become obvious to them. The two theoretical underpinnings used in this study are TLM (see section 3.3) and TAM.

Furthermore this study involves some contingency variables such as personal characteristics of Internal Auditors, size and resources of organisation, internal audit departments, people and technology. As a result of increasingly changing technology and the need to acquire new skills, socio-technical and structuration theories are also found useful. Based on evidence obtained from the literature in chapter 2, this study adopts the TLM theoretical frameworks as underpinning to understand the effectiveness of internal control in controlling electronic fraud since the model consists of the consolidation of contingency, socio-technical and structuration theories. TLM is explained in the next section (5.3.0)

5.3.0: The Three–Layered Model from a Meta-Level Perspective

The three theoretical perspectives (Contingency theory, Socio-Technical System perspective and Structuration theory) provide invaluable insight to studies on ICT either individually or when combined together. However, they have been individually severely criticized for their limitations (Wood, 1979; Schoonhoven, 1981; Scott, 1987; Rose, 1998; Rose and Jones, 2004; Omoteso et al., 2007). Some of the identified limitations are summarised below.

Table 5.2: Summary of Criticism of Contingency, Socio-Technical and Structuration Theories.

Contingency Theory	Socio-Technical Perspective	Structuration Theory
Overall strategy clear but its substance is not clear (Schoonhoven, 1981)	The socio-technical perspective relates to failure incidents (Poulymenako and Holmes, 1996)	Criticised in understanding the relationship between ICT and organisations on the basis of its restrictions of “agency” to human capabilities (Rose and Jones, 2004)
Problem of goal conflict and multiple contingencies (Wood 1979)		Problem of reducing structure to action (Rose, 1998)

Source: Author

Some of the identified limitations of the Three Model Theories are based on the contributions of earlier scholars. For instance, Schoonhoven (1981) found that the overall strategy embedded in contingency theory is clear but its substance is not, while Wood (1979) found that there is a problem of goal conflict and multiple contingencies. Both Schoonhoven (1981) and Scott (1987) regard contingency theory as orienting strategy (or meta-theory) rather than a theory on its own.

Omoteso et al. (2007) combine the three theories (Contingency, Socio-Technical and Structuration) into a single model that is more explanatory and provides a more “...illuminating framework for the study of ICT’s impact on organisations” According to Omoteso et al. (2007: 12), TLM advocates in its general form that:

“Effectiveness is achieved within the context of the contingent factors by implementing strategic choices leading to appropriate structures that enable a synergy between ‘efficiency’ of technology and ‘creativity’ of human beings; where strategic choices themselves are representative of human creativity.”

This study aims at evaluating the impact of ICT on effectiveness of internal control in prevention and detection of electronic fraud in the financial sector. A synergy between ‘efficiency’ of technology and ‘creativity’ of human beings is essential to achieve effective internal control in the electronic environment. The essential theoretical underpinning will be provided by TAM and a meta-level perspective enabled by the composite TLM encompassing the contingency, structuration and socio-technical systems theories as suggested by Omoteso et al. (2007). For instance, communication network provides a contingent structural factor for fraud perpetration and since the fraudsters too might be harnessing technology, there is a Socio-technical systems aspect to fraud perpetration. As a result of the nature (electronic) and size of the business transactions, contingent factors will be used to understand the extent of perpetration and control. Furthermore, the challenges of automation have imposed on Internal Auditors the need to acquire a new set of skills besides those learnt traditionally. This conforms to both social-technical systems and structuration theories. According to Omoteso et al. (2007), the socio-technical perspective advocates that, from an organisational viewpoint, the best utilization of technology can only be realised with a due measure of the social actors who work and interact with it to achieve an optimum result in terms of quality, efficiency and effectiveness. While Omoteso et al. (2007) believe that the model is generic with regards to any technology; their main discussion is focused on ICT as the main technology at the heart of the shift from an industrial economy to a knowledge economy.

A Three-Layered Model

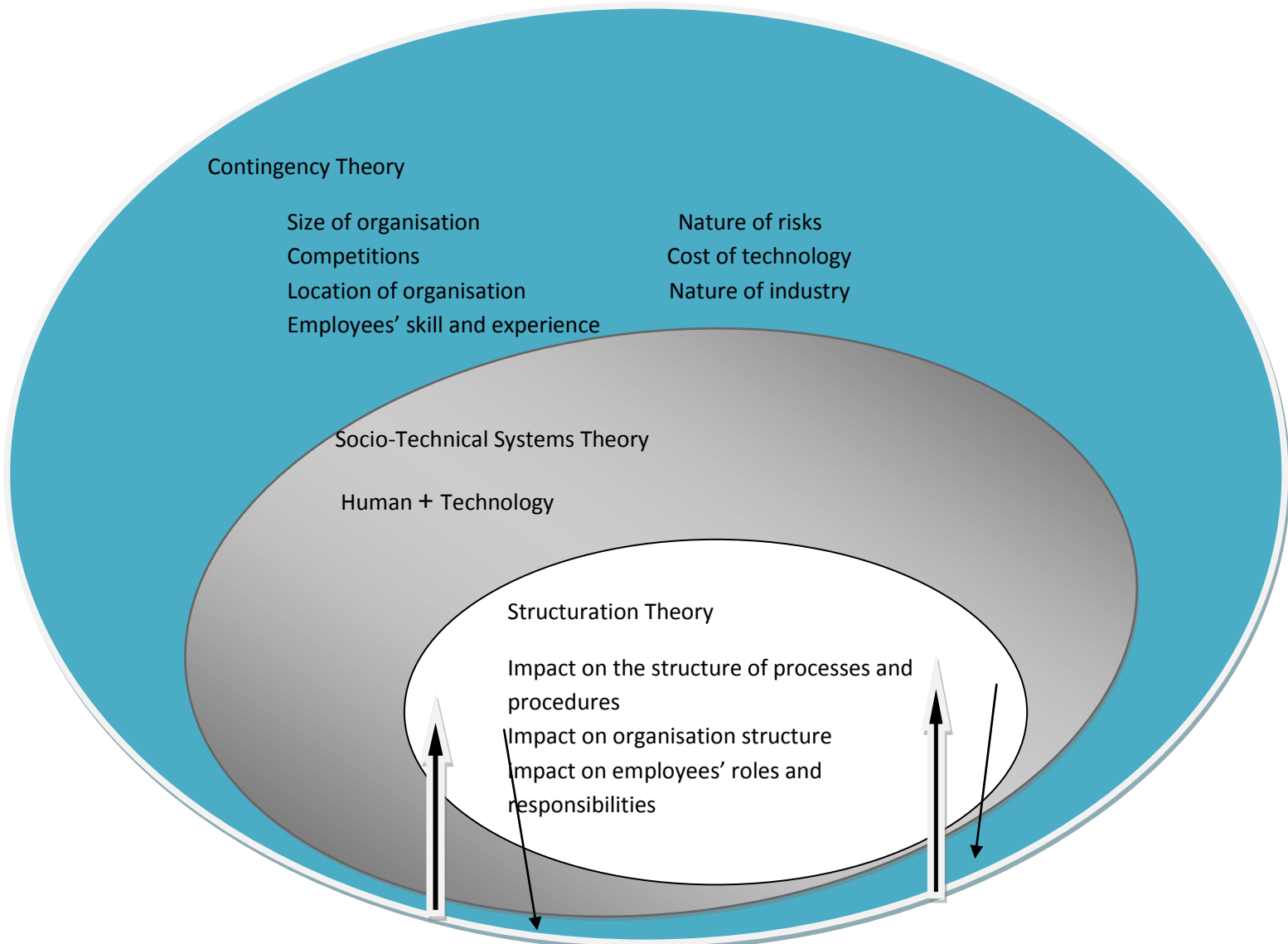


Figure 5.4: A Three-Layered Model

Source: Omoteso et al. (2007)

The thick arrows represent the impact of contingent factors and environmental changes

The thin arrows represent strategic choices made by organisations to counteract or benefit from changes in the environment

Contingency Theory is depicted as an encompassing framework with contingent factors (representing thick arrows) affecting the use of ICT on the first layer of this model. The contingent factors include the location of the organisation, the size of the organisation, competition, the nature of the task, employees' skills and experience

and the relative cost of the ICT tool/technique in terms of purchase, installation, training, maintenance and staffing needs (Omoteso et al., 2007). The model posits that ‘an organisation has to exercise “strategic choices” (representing thin arrows) in order to optimise its effectiveness within the constraints posed by the contingent factors’.

The Socio-Technical Systems Theory is depicted on the second layer of the model. Emphasis is placed on the ‘need to blend attributes of objects such as ICT with relationships, as embodied in human characteristics, to generate greater effectiveness. Achievement of effectiveness is essential in internal control.

The third layer is a reflection of other two layers of organisational structures no matter how pro-active or reactive in nature the organisation might be. It is occasioned by possible reduction in the number of non-skilled workers as they are replaced by technology. There is also a change of managerial focus from operational to more strategic aspects as the structure of employees’ roles and responsibilities change.

Omoteso et al. (2007) found that the interplay of these meta-level theories generates a synergistic frame within which the impact of ICT on organisations can be understood. Omoteso et al.’s (2007) work is an outcome of an exploratory research effort that ordinarily provides a rich framework for further research in the area of ICT-integrated human endeavour. It is the intention of this study to assess the efficacy of the perspective by using TLM as underpinning through empirical research investigation involving the Internal Auditors and the use of ICT tools and techniques in preventing and detecting electronic financial fraud.

The next section explains why the researcher favoured TAM and TLM to underpin this study. The section also explains the relationship between the two theories and why they have to be used together.

5.4.0: TAM and TLM: Competing or Complementary?

In this chapter, the researcher has examined various theories and models most commonly used in the information system and ICT literature. Merits and demerits of each of them are considered in the light of current study. The researcher now

provided the direction as to why TAM and TLM models are favoured for this study and establishes interactions between the two models (showing whether the models are competing or complementary).

TLM and TAM are considered most suitable for this study. TAM has been very popular and is by far the most cited in the ICT implementation and adoption literature (Korpelainen, 2011). TAM is found useful in this study for the understanding of usage of ICT tools and techniques by Internal Auditors in the Nigerian banking and financial sector. This is because prior study has shown that technology adoption and usage depends on so many internal and external factors. These factors mostly boil down to the nature of the 'machine' (system complexity) and the nature of 'man' (attitude and behavioural intention) as Hassan 2007 puts it "computer self-efficacy and system complexity had significant direct effects on perceived usefulness and perceived ease of use as well as indirect effects on attitude and behavioral intention" (Hassan, 2007: 76). TAM is favoured for the present study because it involves internal computing support, internal computing training, management support, subjective norms, voluntariness, output quality, computer self efficacy and objective usability (Davis et al., 1989; Igarria et al., 1997; Venkatesh and Davis, 2000).

The strength of TAM is that it has been well tested in various ICT adoption and acceptance research over the last three decades. TAM had been used as a single theory (Davis, 1989), in comparison with other theories such as Theory of Reasoned Action (Davies et al., 1989), extended as a theoretical concept (Venkatesh and Davis, 2000) or completely replicated (Adams et al., 1992). In the original version Davis (1985, 1989) proposed that "system use is a response that can be explained or predicted by user motivation, which, in turn, is directly influenced by an external stimulus consisting of the actual system's features and capabilities. Davis (1985) further explained users' motivation to mean one or all of the following: "Perceived Ease of Use, Perceived Usefulness, and Attitude toward Using the System" (Chuttur, 2009: 2)

The present study involves adoption and usage of ICT by a professional group, namely Internal Auditors. TAM has been the most useful theoretical model to explain ICT adoption and penetrations in different environments. TAM is found suitable to

explain proposition 1 of this study. While it may not fully explain propositions 2, 3 and 4, TAM provides necessary background for the use of TLM. (See Fig. 5.1)

TLM is a meta-level theory proposed by Omoteso (2006) and was used to underpin a study on impact of ICT on auditing. This is the first time the model will be tested to underpin a study on fraud prevention and detection. The researcher considers TLM relevant to some aspects of this study as it involves: man, technology; professional group; organisation; management and fraud perpetration. While TLM may be useful to fully explain Propositions 2, 3 and 4 it can only partially explain Proposition 1. According to Omoteso (2006: 252), TLM advocates that:

“The use of ICT in audits is a function of certain contingent factors that determine an optional mix of human skills and technological capabilities, which would lead to changes in the nature of auditors’ roles and outputs and audit organisations’ structures”.

The use ICT has been found to be contingent on the size and structure of organisations, and personal characteristics of users such as experience and training. In addition, the adoption of the internet, which makes communication via networks possible, is also a contingent factor for fraud perpetration. In addition, since the fraudsters are also busy harnessing technology, there is a socio-technical dimension to fraud perpetration. Table 5.3 below provides a summary of propositions and the model used to underpin them.

Table 5.3: Summary of Propositions and Models Used for Explanations

PROPOSITIONS	MODEL USED
1.1	TAM
1.2	TAM + TLM
1.3	TAM
2	TAM + TLM
3	TLM
4	TLM

TAM is used to underpin Propositions (1.1) Internal Auditors current level of ICT usage for Internal Control purpose is increasing;

(1.2) Financial institutions' current level of provision of ICT for Internal Control purpose is increasing,

(1.3) ICT tools and techniques are useful for Internal Auditors' tasks, efficiency and effectiveness.

Proposition 2: The use of ICT-based tools and techniques in Internal Control impacts on Internal Auditors' independence. Internal Auditors' adoptions and use of ICT tools and technique for internal control can be predicted by Internal Auditors' motivations (usefulness and ease of use) and external stimulus of computer self-efficacy and system complexity.

Propositions 1.2; 2; as above and Proposition 3: Internal Auditors' use of ICT-based tools and techniques has the potential of preventing electronic fraud and

Proposition 4: Internal Auditors' use of ICT-based tools and techniques are effective in detecting electronic fraud and are explained by TLM because structure and size of organisation, man, machine and Internal Auditors are all involved. The use of ICT in internal control is a function of certain contingent factors that determines an optimal mix of human skills and technological capabilities which would lead to changes in the nature of Internal Auditors' roles and output. However there are areas where neither of the two theories will be sufficient to explain the phenomena involved. This happens in propositions 1.2 and 2 where the two models are combined for the explanations. The aforementioned explanations highlight the complementarities of TAM and TLM in the present study.

The next chapter provides the philosophical and methodological basis for this study. The methods adopted and reasons for favouring these methods over alternative methods are equally explained.

5.5: Summary of Chapter

This chapter has discussed the main theories popular in Information and Communication Technology research in the last two decades. Efforts were made to examine their relative applicability to the present research. The researcher noted that none of the theoretical models will be sufficient when used alone as a single theory. Two theoretical models (TAM and TLM) have therefore been chosen to underpin this study.

The next chapter is explained the philosophical foundation and research methodology adopted for this study. It also stated in details the research approach and steps taken in data collections.

CHAPTER SIX

RESEARCH METHODOLOGY

6.0: Introduction

The purpose of this study is to investigate the impact of ICT audit tools and techniques on the effectiveness of internal control in prevention and detection of electronic fraud incidence. The seeming increase in electronic fraud incidence, and the potential concerns about security and handling of electronic financial information by Internal Auditors motivate this study. Chapter 2 examined the views, opinions and arguments of various authors as presented in existing journals and texts on Computer Assisted Auditing Tools and Techniques, audit automation, internal control, internal auditing and electronic fraud. Chapter 3 looked at suitable theories based on past literature on ICT research to underpin this study. The research propositions were presented in the last section of chapter 2 based on literature reviewed.

This chapter looks at the research methods and/or research techniques. Research method and research technique are used interchangeably to mean the same thing in the literature. For instance Jankowicz (2000) refers to research method as “concentrating on a systematic and orderly approach taken towards the collection and analysis of data so that information can be obtained from those data”. While Bennett (1986) refers to research technique as focusing on particular, step-by-step procedures, which this research follows in order to gather data, and analyse them for the information they contain. As a result, the next section (6.1) is on the philosophical basis that underpinned the methodology chosen for this study. Section 6.2 restates the four research propositions and groups them into two sub-sections based on identifiable gaps from literature. Section 6.3 explains the research designs and pilot study.

6.1.0: Philosophical Foundation

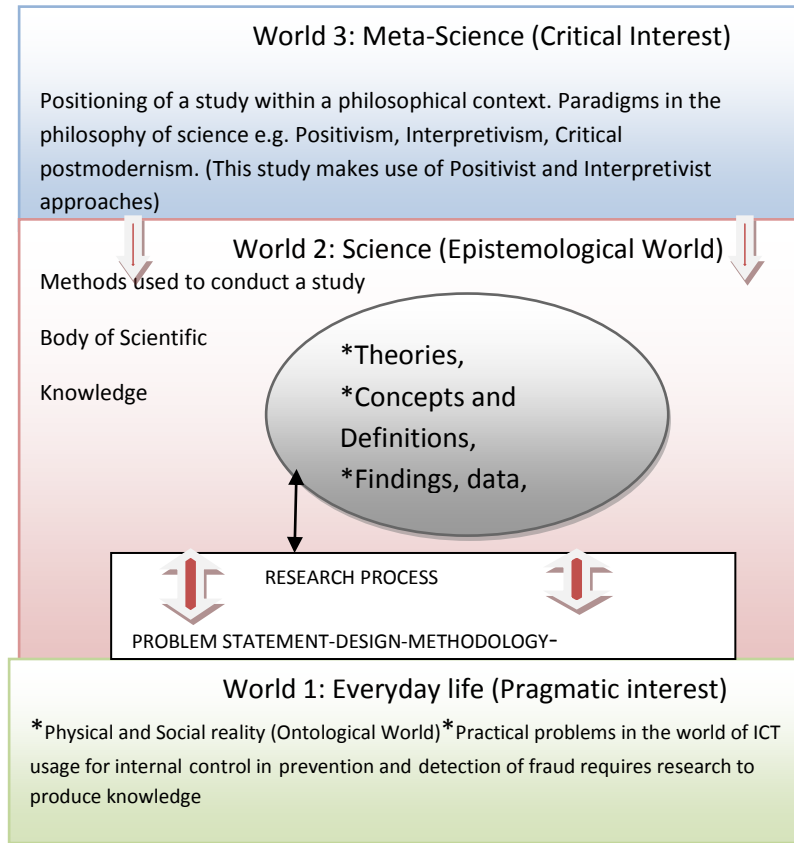


Figure 6.1: The Three-World Framework

Adapted from: Mouton, 1996:10; Mouton, 2001: 139-141

In an attempt to position this study within an appropriate philosophical context, effort is made to adapt Mouton's¹ Three World analogy (Figure 6.1). World 1 is our everyday life. It consists of man, his experience and decisions. In this study it is the world of ICT usage in the financial sector for internal control which is part of Internal Auditors' everyday life. This can be regarded as a subset of World 1. The research problem addresses a need in World 1, viz., how effective is ICT usage in internal control in controlling electronic fraud. In order to find a solution to this problem, there is a need for the researcher to relate to World 2. World 2 is a world of scientific knowledge and comprises theories, concepts and definitions of phenomena

¹ Mouton (1996) identified "three worlds" of knowledge, viz., the world of everyday life; science and scientific knowledge and the meta-science.

identifiable with research problems, viz, exploring effectiveness of ICT tools and techniques for prevention and detection of electronic fraud.

World 3 consists of the world of meta-science and it is imperative to understand it in order to be able to manipulate and engage well with various phenomena in World 2. The philosophical orientation of the researcher influences his/her engagements within the different worlds. The next section will be devoted to a review of different philosophical paradigms with a view to locating the present research within an appropriate philosophical context.

6.1.1: Philosophical Basis of the Methodology

There are three dominant paradigms which form the philosophical platform and all are prominent in contemporary social management research: positivism (sometimes referred to as the quantitative, objectivist or scientific paradigm), interpretivism (phenomenology) and more recently critical postmodernism.

Positivism implies an objective world, hence; it searches for facts conceived in terms of specified correlations and associations among variables. Positivism assumes a state which scientific methods can more or less readily represent and measure, and it seeks to predict and explain causal relations among key variables (Gephart, 1999). Post-positivism is a recent evolution of positivism. Post-positivism agrees with positivism in assuming that an objective world exists but it assumes that the world might not be readily apprehended and that variable relations or facts might only be probabilistic, not deterministic (Gephart, 1999). The positivist traditionally focused on experimental and quantitative methods used to test and verify hypotheses sometimes extended by an interest in using qualitative methods to gather broader information outside of readily measured variables.

Theories in the critical postmodern tradition take many literary and narrative forms (Boje et al., 1996) including historical essays and analysis, case studies, survey and field research. Thus, according to Gephart (1999), rather than methodological differences, it is a commitment to dialectical analysis and to critical/postmodern

theory which most clearly differentiates critical postmodern research from positivism and interpretivism.

Interpretivism (phenomenology) is fundamentally concerned with meaning and it seeks to understand social members' definitions of a situation (Schwandt, 1994). Interpretive theory involves building a second order theory or theory of members' theories (Schutz, 1973). This is in contrast to positivism, which deals with objective reality and meanings thought to be independent of people. According to Gephart (1999), interpretivists assume that knowledge and meaning are acts of interpretation hence there is no objective knowledge which is independent of thinking, reasoning humans. Understandably, interpretive researchers have often preferred meaning- (versus measurement-) oriented methods. Data collection and representation have been accomplished with informant interviewing (Spradley, 1979), ethnography, or the thick description of cultures based on intimate knowledge and participation (Van Maanen, 1988), and even ethnographically linked textual analyses (Gephart, 1993).

The apparent inadequacy of the positivist approach in explaining organisational phenomena encouraged the campaign for interpretive research orientation in accounting and auditing (Adebayo, 2004). Boland (1979) and Covaleski and Dirsmith (1983) demonstrate in their studies that the interpretive approach is more appropriate in the study of organisational/behavioural phenomena.

According to Watts and Zimmerman (1978, 1986), positivist theory attempts to identify and explain behavioural relationships in the context in which the relationships are exhibited. According to Boland (1979), Morgan and Smircirch (1980) and Tomkins and Groves (1983) positivist theory in accounting research largely ignores the assessment of the subjective issues that are inherent in human processes. The positivist theory approach, as it is currently practised in accounting and auditing research, makes use of the rational model approach of conceptual or objective understanding of practitioners' behaviour, and seeks to explain the influence of behavioural and social issues on organisational phenomenon through hypothesis and proposition testing. The interpretive research approach guides the researcher to learn the common-sense understandings of the everyday life of people in

their world by examining organisational events from the perspective of the world of consciousness and humanly created meanings (Lee 1999).

The dominance of positivism in social and management research is increasingly challenged by critics from interpretivism and critical postmodernism. Interpretivism and critical postmodernism proponents raise fundamental philosophical challenges for positivism and offer alternative theoretical, methodological and practical approaches to research on management and social sciences. The argument against positivism is that it strips contexts from meanings in the process of developing quantified measures of phenomena (Guba and Lincoln, 1994).

Investigation of ontological distinctions is an important step in the research process because it helps the researcher to uncover how his/her perceptions of human nature impact on the approach consciously adopted to reveal social truths (David and Sutton, 2004). This study is based on epistemology which is firmly grounded in the “ontological belief that the behaviour of human subjects is manifest of an ordered and rule governed external reality. Accordingly, there is a conceptual perspective that human behaviours and actions are largely determined by stimuli which are not of their own making” (Bracken, 2010:3).

Literature has shown that the form of research methodology which logical positivist epistemology generates suffers from defined limitations. For instance, “it fails to take into consideration the clear epistemological distinctions between knowledge about humans and knowledge about things. In essence, the positivist approach to the social sciences negates the role of human agency, or trivializes it to such an extent that it becomes meaningless. The mixed methods approach is adopted for this study in order to ensure convergence of data findings (Mathieson, 1991) and more importantly to increase the validity of research findings (Mark and Shortland, 1987). This is because the study “combines phenomenological indices such as observer independence, asking how, why, and how much relevance of human interest and actions and positivistic indices such as fairly large sample size, theoretical abstraction, general understanding of physical and technology environment” (Omoteso, 2006:110).

A more comprehensive account of the thing being researched is provided through a mixed methods approach by incorporating a fuller description and/or more complete

explanation of the phenomenon (fraud) being studied and by providing more than one perspective on it. The mixed methods approach will be useful for understanding financial fraud, technology, man and the auditing environment. Published mixed methods studies (Bryman, 2006; Collins et al., 2006; Rocco et al., 2003; Greene et al., 1989) suggest that social researchers use mixed methods strategies for one or more of the following purposes: improved accuracy, providing a more complete picture; compensating for strengths and weaknesses and more especially in developing robust analysis (Denscombe, 2008).

The application and combination of several research methodologies (in this case positivism and interpretivism) in the study of the same phenomenon is generally known as triangulation. The purpose of triangulation in qualitative research is to increase the credibility and validity of the results. These views are emphasised by Cohen and Manion (2000) by defining triangulation as an attempt to map out, or explain more fully, the richness and complexity of human behaviour by studying it from more than one standpoint. Attrichter et al. (1996: 117) submitted “that triangulation gives a more detailed and balanced picture of the situations”. O’Donoghue and Punch (2003), quoted in Ritchie (2003:43-44), also state “that triangulation is a method of cross-checking data from multiple sources to search for regularities in the research data. It refers to extending understanding, or adding breadth and depth to analysis, through the use of multiple perspectives”.

The word ‘triangulation’ is a term borrowed from navigation. It is used to describe a technique for pinpointing the precise position of an aircraft or ship. This is usually done by combining different reference points (Ammenwerth et al., 2003).

In this study, triangulation will serve two main purposes: first, to support (validate) the finding with help from others and second, to extend understanding of the use of ICT in internal auditing by adopting multiple perspectives in data collection, the dual theoretical approach and methodological triangulations.

Initial work on triangulation is credited to Denzin (1970). In the words of Denzin, (1989: 307):

‘.....By combining multiple observers, theories, methods and data sources, (researchers) can hope to overcome the intrinsic bias that comes from single-methods, single observer and single theory studies...’

Denzin (1978) recommended four basic types of triangulation: Investigator triangulation, Data triangulation, Theory triangulation and Methodological triangulation. This study will make use of three types of triangulation out of these four as discussed below.

Data triangulation is used because the study involves various data sources with regards to time, space, persons and technology. For example, Internal Auditors from different financial institutions are interviewed and questionnaire survey is applied at different times. The validity of findings can be checked by using different sources of information by comparing data from different informants through interview.

Theory triangulation is useful to this study as the study makes use of more than one theoretical scheme in the interpretation of the fraud phenomenon. It involves the use of more than one theoretical position in relation to data. Different theories can shape the kind of data that are collected and the way the data are interpreted (Denscombe, 2008). This study makes use of TLM and TAM as theoretical underpinning.

Methodological triangulation is also useful to this study as it involves the use of various methods for data collection and data analysis. Two types of method triangulation can be identified in this study: ‘within-method triangulation (combining approaches from the same research tradition), and between-method triangulation (combining approaches from both qualitative and quantitative research traditions, also called across-method triangulation’ (Ammenwerth et al., 2003: 239) For example the questionnaire contains questions that are directed to access the same phenomenon in order to compare data collected using different questions for the same phenomenon. The questionnaire used in this study provided some space for comments from respondents thus giving a triangulated flavour to the data collection method (Olsen, 2004).

Furthermore this study involves using more than one method (interview and questionnaire) to gather data. Comparisons using different methods can provide a check on the accuracy of findings.

Methodological triangulation is perhaps the most talked about. This is because ‘the term “triangulation” is often seen as strongly related to the term “multi-method evaluation” because methods triangulation is seen as the most often used triangulation approach’ (Ammenwerth, 2003: 239). A debate on methodological pluralism is ongoing. In order to gain a better insight into different methodological approaches used in the past studies, several past studies were selected for examination of the methodological approaches adopted.

6.1.2: Summary of Research Methods from the Literature

Table 6.1 Summary of research methods from literature

Qualitative (interpretivism or Phenomenology)	Quantitative (Positivism or Scientific)	Mixed methods (Triangulation)
Caglio (2003)	Cheung & Lam (1995)	Bryman (2006)
ICAEW (1987)	Wilson and Sangster (1992)	Manson et al. (1997)
Pricewaterhouse Coopers (2004)	Rae and Subramaniam (2008)	Banker et al. (2002)
Cannon and Crowe (2004)	El-Masry and Reck (2008)	Collins et al. (2006)
Manson et al. (2001)	Yu, Yu; & Chou, C. (2000)	Greene et al. (1989)
Bierstaker et al. (2006)	Lehmann & Norman (2006)	Rocco et al. (2003)
Fischer (1996)	Abdolmohammadi and Usoff (2001)	Omoteso (2006)
Bonner et al. (1996)	Ololube (2006)	
Remenyi (1992)	Seyal & Rahim (2006)	
Wright and Wright (2002)	Alon & Dwyer (2010)	
Mpofu & Watkins-Mathys (2012)	Abu-Musa (2006)	

From the 30 relevant literatures shortlisted (Table 6.1 above), the first obvious lesson is that the choice between the three approaches depends on the epistemological inclination and background of the author(s) concerned. Eleven of the studies used qualitative methods in the form of observation, interviews, case studies or action research. Twelve of the studies adopted questionnaire or experiment while seven used the mixed methods approach. However, out of the seven studies that adopted (mixed

methods) triangulation (Bryman, 2006; Collins et al., 2006; Omoteso, 2006; Rocco et al., 2003; Banker et al., 2002; Greene et al., 1989; Manson et al., 1977). Banker et al. (2002) and Omoteso (2006) remain the most comprehensive as they have enjoyed widespread presentation in the form of academic papers by the authors. Their work benefited immensely from one of the advantages of the triangulation method, which lies in the comprehensiveness of its analysis and has direct impact on the quality, wider acceptability, and replicability of results. Triangulation would enhance a better understanding of the phenomenon being studied which is the effectiveness of ICT in prevention and detection of electronic fraud.

Furthermore, most of the previous studies are exploratory in nature and are classified as cross-sectional as against longitudinal study (Manson et al., 1997; Banker et al., 2002; Omoteso 2006) and combine qualitative explanations of respondents with Pearson correlation in their data analysis. This study is exploratory in nature as it simply attempts to seek new insights into the use of ICT in detecting and preventing electronic fraud. It also covers a literature search, conduct interviews and seek questionnaire response from experts (Internal Auditors) in the field (Saunders et al., 2003). The study adopts cross-sectional study, drawing data from banking, insurance, and other financial institutions. The choice of a cross-sectional approach allows the study to be carried out in real life, natural settings in order to bring out the phenomenon being studied clearly thereby increasing the validity.

Longitudinal study could have been more detailed and comprehensive across a fairly long period. However, the research time frame and resources available could not support a longitudinal study.

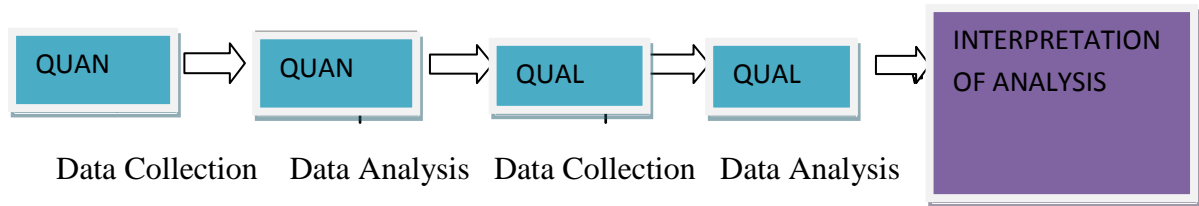
Also, the higher number of participants, the observer's independence, the respondents' independence, the opportunity to evaluate facts qualitatively and quantitatively, the quality of data obtained and the comprehensiveness of the resulting analysis are all combined factors that make a mixed methods (questionnaire and one-to-one in-depth interview) a robust option (Palmerino, 1999; Easterby-Smith et al., 2002). According to Greene (2005), a mixed methods way of thinking also generates questions, alongside possible answers; it generates results that are 'smooth and jagged, full of relative certainties alongside possibilities and even surprises, offering

some stories not yet told'. Care would be taken in using mixed methods as in the end it is perhaps the inappropriate titling of the work that can lead to unfulfilled expectations. In any case, Denscombe (2007) stated that qualitative and quantitative (QUAL/QUAN) distinction tends to oversimplify matters. Even though they are convenient terms to use and understand, a clear dividing line between qualitative and quantitative approaches is hard to sustain at either a practical or philosophical level (Coxon, 2005; Halfpenny, 1997; Hammersley, 1996)

6.1.3: Mixed Methods Sequencing

The intent of this two-phase sequential mixed methods study will be to explore the impact of ICT tools and techniques on internal control in preventing and detecting electronic fraud. In the first phase, quantitative research questions addressed the effectiveness of audit tools and techniques being used by Internal Auditors in financial institutions in Nigeria. Information from this first phase was explored further in a second qualitative phase. In the second phase, qualitative interviews were used to probe further results generated by questionnaire data. The follow up interview was conducted with 21 executive staff selected randomly from financial institutions (banks, insurance, stockbroking firms and mortgage institutions) in Nigeria. The reasons for following up with qualitative research in the second phase are to better understand and explain the quantitative results.

A large number of possibilities exist in sequencing and level of mixed methods research design. This study adopts the suggestion of Creswell et al. (2003) on the approach for sequential exploratory design that is the $QUAN \Rightarrow QUAL$ approach to allow observed gaps to be covered by face-to-face interview after semi-structured questionnaire responses have been collected. In other words, observed gaps in questionnaire responses are covered and explained by interview. Efforts were made not to interview respondents who participated in completion of the questionnaire to avoid positive bias. The analysis of collected data also followed this trend to facilitate meaningful interpretation of the entire analysis (Creswell et al., 2003).



6.2.0: Research Instruments and Validation

In this section, the detailed procedures followed to draw up and validate the questionnaire used as the research instrument for this survey are stated. This study adopted both qualitative and quantitative research methodologies. The quantitative aspect is derived from 510 questionnaires that consisted of a mixture of both open-ended and fixed alternative questions. This is adopted from a questionnaire originally used by Henderson (2002). The open-ended questions were designed to give respondents the opportunity to supply their responses as they thought suitable, while the fixed alternative questions adopt a five-option Likert scale. The number of questionnaires was arrived at to enable the study to cover all the financial institutions registered with the Lagos Chamber of Commerce and industries (LCCI). More than 80 per cent of functional financial institutions in Nigeria are members of the Lagos Chamber of Commerce and have their head offices in Lagos. The respondents are the Internal Auditors/internal control managers in these organisations. The internal control department is usually located in various head offices from where staff are sent to branches on a periodical basis for specific assignments. The qualitative part focuses on semi-structured face-to-face interview with 21 top executives of financial institutions; at least two interview respondents were selected from banking, insurance, stockbroking firms, mortgage institutions and finance houses using non-probability sampling methods to ensure each sector is fairly represented. The primary data collected from pilot interviews helped in setting up the semi-structured questionnaires. The questionnaire was followed by a set of interviews in order to address any deficiency identified in the responses from the questionnaire.

A purposive sampling method is adopted and the conclusion generalised by means of inference and triangulation (Jankowicz, 2000). Purposive sampling is adopted because investigating the effectiveness of audit tools in preventing and detecting

electronic fraud incidence and improving security of internal control cannot be based on a random sampling either across industries or within a particular chosen organisation, as it is subject to peculiar target research. 100 per cent sample frame is adopted since it is convenient to survey the entire population of Internal Auditors in financial organisations where ICT is adopted in Nigeria.

Instrument development is important to achieve effective and valid research output (Straub 1989: 148). The researcher benefits from earlier studies such as Malhotra (1996) and Newsted, Huff and Munro (1998) in order to complete the tasks that need to be completed to bring out a usable research instrument. The following five steps are followed:

- i. Determine sampling and appropriate response rate.
- ii. Determine the measure of constructs that will be used.
- iii. Prepare a draft questionnaire and determine:
 - Question wording
 - Question content
 - Structure and layout
 - Response format
- iv. Internal validity testing
- v. Piloting the questionnaire and assessing reliability, construct validity and content validity.

These tasks are further explained as follows.

6.2.1: Sampling and Response Rate

Due to large sample size and the nature of targeted participants (Internal Auditors who are very busy and not easily accessible) a response rate of about 35 per cent is expected. It is estimated that the total number of Internal Auditors/internal control staff in the financial sector will be 805. The breakdown is estimated as follows:

Banking sector: 24 banks with an average of ten internal audit staff	= 240 staff
Insurance companies: 37 with an average of five internal audit staff	= 185 staff
Mortgage companies: 70 with an average of two staff	= 140 staff

Other financial Institutions 120 with average of two staff	= 240 staff
Total.....	= 805 staff

However, by the nature of the research, only those organisations that substantially deployed ICT for their operations were targeted. These were identified during the piloting period. It was therefore possible to achieve 100 per cent sampling coverage. Five hundred and ten (510) questionnaires were sent out to targeted respondents in financial institutions where ICT is adopted representing 100 per cent of the estimated total population of financial institutions where ICT are substantially deployed.

6.2.2: Construct Measures

There is the need to measure concepts or constructs that are being investigated. According to Newsted, Huff and Munro (1998) it is advisable to search the literature for existing measures of constructs. A review of existing literature may reveal already-designed and validated instruments that may address the same concepts a researcher is trying to measure. The primary purpose of the survey is to evaluate the quality and impact of ICT tools and techniques on effectiveness of internal control in detecting and preventing electronic fraud. From the review of information system literature, what causes information systems to be effective has been a contentious issue in research (Mckeen et al., 1994). The lesson learnt from existing literature is that there is no universally accepted model for measuring ICT effectiveness (Success, Quality and Usefulness) however, the most popular method observed is to measure the level of users' satisfaction connected with the system. The user in this context refers to the Internal Auditors.

Constructs from user satisfaction/effectiveness in information systems have been derived from various sources (Henderson, 2002; Doll and Torkzadey, 1991). This study adopts Doll and Torkzadey's (1991) instrument for measuring user satisfaction using the End User Computing Instrument (EUCI) which divided user satisfaction into five dimensions: content, accuracy, format, timeliness and usability. The first four dimensions indicated the information provided by the system, while the last dimension, usability, refers to users' (IAs) interaction with the system. The survey questionnaire adapted EUCSI because it has been extensively validated in previous

research (Gelderman, 2002). The open-ended qualitative questions are to supplement the data gathered from the construct measures by providing the Internal Auditors' thoughts and suggestions on effectiveness of technology tools and techniques in preventing and detecting fraud.

6.2.3: Drafting the Questionnaire

The questionnaire was drafted carefully to incorporate the process of construct translation (as determined in step two) into meaningful words. The actual wordings are carefully selected for respondents' understanding. In order to avoid misinterpretations by respondents, efforts are devoted to choice of words in the questionnaire design. It is important to make the questionnaire conducive to being answered by the respondents. According to Frazer and Lawley (2000), respondents are more likely to give an accurate answer if the questions are phrased in a lucid, appropriate, relevant and neutral manner. Furthermore, in order to have a rich data set from the respondents, the questionnaire was designed to elicit the two types of responses possible in survey questions posed to respondents: open-ended and closed-ended. The former allows respondents to give free formed opinion answers. This is suitable where the responses cannot be predicted or where there are too many possible answers. The latter refers to a predetermined fixed set of choices for respondents to choose from.

Efforts were also made to ensure simple and attractive structure and layout in the ordering of questions as it may affect the motivation and manner in which participants answer questions. Layout of the questionnaire is made in such a way as not to impede the effective answering of questions. The visual design of the questionnaire is carefully undertaken and cleanly presented to eliminate confusion.

6.2.4: Internal Validity Testing

Frazer and Lawley (2000) refer to internal validity as the degree of confidence the researcher has in the causal effects between variables. To satisfy this task, the researcher carefully reviewed the questionnaire draft to ensure all questions are clear and unambiguous from the researchers' perspective. Furthermore, the questionnaire

questions were given to colleagues within the department to complete, and necessary adjustments were made to arrangements of questions after the feedback.

6.2.5: Reliability Check

The most commonly used reliability check for internal consistency in prior studies is Cronbach's alpha coefficient. According to DeVellis (2003), the recommended Cronbach's alpha coefficient of a scale should be above .7. In their study, Pavot, Diener, Colvin and Sandvik (1991) suggested a satisfaction with life scale that has internal consistency with a reported Cronbach's alpha coefficient of .85, however the questionnaire instrument used for the current study was tested for reliability of internal consistency using SPSS version 18. The result shows a Cronbach's alpha coefficient of .88 as shown in Table 6.2 below:

Table 6.2: Reliability Statistics: Cronbach's Alpha

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No. of Items
.875	.881	12

This is higher than the recommended satisfactory Cronbach's alpha coefficient level of .7 as suggested by DeVellis (2003). This suggests a high reliability check for internal consistency for the questionnaire instrument used in this study.

6.3.0: Research Propositions

Based on the objective of this research and identifiable gaps from the review of relevant literature in chapter two, four research propositions are considered central to the main contribution of this study. These propositions are broadly detailed below.

6.3.1: Current and Potential Implications of ICT Tools and Techniques for Internal Control

1.0 Nigerian Internal Auditors are increasingly adopting IT-based tools and techniques for internal control. This is divided into three themes as follows:

1.1 Internal Auditors' current level of use of ICT tools and techniques for internal control purposes is increasing.

1.2 Financial institutions' current level of provision of ICT tools and techniques for internal control purpose is increasing.

1.3 ICT tools and techniques are useful for internal control's task, efficiency and effectiveness.

2.0 The use of ICT-based tools and techniques in internal control impacts on Internal Auditor's independence.

3.0 Internal Auditors' use of ICT-based tools and techniques has the potential of preventing electronic fraud. This is divided into three themes as follows:

3.1 Internal Auditors' use of ICT has had positive impact on prevention of fraud.

3.2 COA has effective fraud prevention control.

3.3 The extent of ICT utilisation for prevention of fraud is affected by auditors' demographic characteristics (experience, gender, training and qualification).

4.0 Internal Auditors' use of ICT-based tools and techniques are effective in detecting electronic fraud. This proposition is further split into three as follows:

4.1. Use of ICT in internal control has had positive impact on detection of fraud.

4.2. COA has effective fraud detection control.

4.3. The extent of ICT utilisation for detection of fraud is affected by auditors' demographic characteristics (experience, gender, training and qualification).

6.4.0: Research Design

6.4.1: Pilot Study

Pre-testing or piloting the questionnaire is a necessary step to give the questionnaire a trial run. Piloting ensures that any potential problems that may exist in the instrument are discovered and corrected. It gives a clear picture of what to expect when the finalised questionnaires are sent out (e.g. clarity of questions, estimated time of completion etc). The feedback received from pilot run may necessitate questionnaire revisions as many times as necessary.

The study is piloted by testing the questionnaire on a set of people that are not too divergent from the target respondents, in order to detect possible deficiencies in its design and administration. The questionnaires were given to 30 respondents (Internal Auditors and internal control staff in financial institutions) in Nigeria. The pilot study is helpful in that it gives advance warning about where the main research project could fail, where research protocols may not be followed, where proposed methods or instruments are inappropriate or too complicated (De Vaus, 1996: 54). Based on the result of the pilot, the questionnaire is revised to increase internal validity and ensure reliability of the instrument to collect useful and high quality research data. The pilot questionnaire was preceded by a covering letter individually addressed to every respondent explaining the main objectives of the study. The respondents were also assured of their anonymity and of the confidentiality of the data they were expected to supply in the questionnaire. The covering letter was followed by a guideline on how to complete the questionnaire.

6.4.2: Outcome of Pilot Study

The pilot questionnaire is structured as in Table 6.3 below.

Table 6.3: Structure of Pilot Questionnaire

Section	Title	Scaled Item	Open-Ended Questions	Total
A	Personal bio data	9	-	9
B	Use of ICT tools and Techs.	10	-	10
C	IAs' experience	4	-	4

	and ICT utilisation			
D	ICT & Fraud Detection	5	-	5
E	COA and Fraud Detection	9	2	11
F	ICT and Internal Control	5	2	7
TOTAL		42	4	46

Additional space was provided after each question to allow respondents' feedback on each question. Thus, respondents were able to comment on clarity and understandability of any question.

The pilot study commenced in the beginning of April 2011 by forwarding questionnaires to respondents through the researcher's contacts in Nigeria. The researcher followed up and collected the questionnaires back by the middle of May 2011. In all, a total of 18 questionnaires were collected from respondents from four banks, two Insurance firms, two mortgage banks, one stockbroking firm and four professional accountants who participated in the pilot study. The returned questionnaires are analysed in Table 6.4 below.

Table 6.4: Analysis of Returned Questionnaire by Business Type

Organisation	Type of Business	Number of Questionnaire returned
A	Commercial Banks	6
B	Insurance firms	4
C	Mortgage firms	2
D	Stockbroking firms	2
E	Professional Accountants	4
	TOTAL	18

Some respondents were of the view that more open-ended questions should be included to allow for more flexibility. In response to this, some of the scaled questions were converted to open-ended questions to allow for respondents'

explanations of the phenomenon being studied. Also, some respondents suggested that the option on scaled questions be increased to include a “Neither agree nor Disagree” option. An example is as follows:

Only four scaled items are presented. The initial questionnaire does not allow for required flexibility for respondents who do not have the necessary experience or enough information of the task in question. Examples are shown.

	Strongly Disagree	Disagree	Agree	Strongly Agree
I used ICT tools and techniques in.....	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The ‘neither agree nor disagree’ column is added to give opportunity to those respondents who do not have enough experience or information about the phenomenon being asked to respond appropriately.

It now becomes:

	Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
I use ICT tools and techniques to.....	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Table 6.5: Structure of Final Questionnaire

Section	Title	Scaled Item	Open-ended questions	Total
A	Personal Biodata and skills	10	5	15
B	ICT usage and fraud prevention	21		21
C	ICT usage and fraud detection	11	2	13
	TOTAL	42	7	49

The structure of the final questionnaire is as shown in Table 6.5 above.

The final questions were produced after taking care of all the observations. The questionnaire was reduced from six sections to three and from seven pages to five pages.

6.4.0: Collection of Data

This study involved the internal control activities of Internal Auditors in financial institutions in Nigeria. The list of financial institutions in Nigeria was compiled through the internet and Lagos Chamber of Commerce and Industries (LCCI). The list includes banks, insurance companies, mortgage institutions, stockbroking firms and finance houses. An introductory letter was collected from the relevant department of the University to confirm the authenticity of the study and the researchers' identities.

In addition, the researcher personally delivered letters to the head of internal audit of some big financial institutions in August 2010 to request their participation. The organisations visited are as detailed in Table 6.6 below.

Table 6.6: Analysis of Organisations Contacted for the Study

	Organisation Description	Number of Organisations
1	Commercial Banks	24
2	Insurance Companies	29
3	Mortgage Banks	10
4	Stockbroking firms	20
5	Other Finance Companies	28
	TOTAL	121

This study makes use of ‘collection after delivery’ questionnaire and face-to-face interviews to collect primary data. A questionnaire is a research instrument consisting of a series of questions and other prompts that are necessary for gathering information from respondents. The questionnaire is served on all the identified population of banks, insurance companies, stockbroking firms and investment ventures registered with Lagos Chamber of Commerce and Industries (LCCI). LCCI is the premier chamber of commerce in Nigeria with more than 70 per cent of viable businesses in Nigeria as members. For instance, twenty-one (21) of the twenty-four (24) existing commercial banks in Nigeria are members of LCCI. The researcher is assisted by many of his former students and professional colleagues who are working in various organisations to provide necessary access.

6.4.1: Interview

For the face-to-face interview, a convenience sampling method is adopted since it is possible but very difficult to interview the entire population of Internal Audits in financial organisations in Nigeria given the limited resources available to the researcher. Convenience sampling is adopted because investigating the impact of ICT tools and techniques in reducing electronic fraud incidence and improving security of

internal control cannot be based on a random sampling either across industries or within a particular chosen organisation as it is subject to peculiar target research.

The interview is conducted using a tape recorder. The interviewer also noted in writing every gesture and the body language of the interviewee. The recorded interview is transcribed.

Constant comparative method is adopted to analyse the interview data (Glaser and Strauss, 1967; 1993). Iterative approach is adopted as the data is analysed as it is collected and coded. Using open coding afforded the researcher the means to identify and examine common themes of ICT tools and techniques in relation to the context, meanings, and circumstances of internal control.

The data collected through interview involves transcribing the text, and is analysed based on the strength of explanations and arguments obtained from the interviewee. Efforts were made to reconcile and provide a useful link between the purpose of research and the aim and techniques of analysis that relate to the purpose (Crowther and Lancaster, 2009). The researcher made a careful consideration of identified strategies that were suitable for data analysis in IS research, viz., content analysis, grounded theory method, discourse analysis and thematic analysis. The researcher favoured thematic analysis as it is more convenient to code the data through the identification of key points or themes (Strauss and Corbin, 1998; Allan, 2003). The researcher followed the following procedures in processing the interview data.

- i. Interview and field notes are transcribed and the researcher reflects on the contents of the transcript.
- ii. Transcripts and field notes are compared. The researcher reflects on observations made during the interview and web sites visited and identifies any apparent inconsistency.
- iii. The tape is replayed many times and the transcript adjusted to reflect accuracy when compared with verbal interview.
- iv. Deep reflection of evidence is further carried out.
- v. Finally, a key-point coding² is carried out, i.e., Conceptualising stage³.

² Coding is defined as “the analytical processes through which data is fractured, conceptualised, and integrated to form theory” (Strauss and Corbin, 1998:3)

Interviews were coded bearing in mind underlying patterns in the data. The researcher built on initial data analysis as a guide for further and more focused data collection in order to achieve better conceptualisation and refinement of the coding system. Categories were created by isolating similarities and differences in line with the coding scheme. The process continued until conceptual saturation was reached.

For instance, the coding sheet was divided into four columns. The sequence of interview questions was recorded in the first column, the raw interview data were transcribed into the second column and the third column contained space for preliminary code notes and jottings while the fourth column listed the final codes. The ruminations on preliminary codes in the third column transformed into useful impressions that helped to provide necessary transitional link between the raw data and codes:

Example of coding sheet: (see Appendix 1V for detailed example)

COLUMN 1: Question	COLUMN 2: Raw Data	COLUMN 3: Preliminary Code	Column 4: Final Code
-----------------------	-----------------------	-------------------------------	-------------------------

Credibility of the interview data was established using the techniques of persistent observation (Lacey and Luff, 2001). Phone calls were made to some of the interviewees to request their views again and correlate what they said previously on tape. Furthermore peer debriefing was used by presenting analysis and conceptual abstractions of the data to other colleagues in order to explore enquirer biases and also to clarify the meaning and basis of interpretations.

Structure of the final questionnaire

The questionnaire is structured as follows: there are four propositions which are translated into specific relevant questions. Each of the probing questions is expected

³ Conceptualising is an abstract representation of an event, object, or action/interaction that a researcher identifies as being significant in the data. The purpose behind naming phenomena is to enable researchers to group similar events, happenings, and objects under a common heading or classification (Strauss and Corbin, 1998: 103)

to provide illuminating data for evaluating the proposition. The questions are divided into two main sections for convenience: the first section (A) has 13 questions in all about the respondents' personal data and type of organisation; the second section (B) focused on the assessment of internal control on the effectiveness of electronic fraud. This is further broken down into three parts with each part addressing the relevant research question in Table 6.7 below.

Table 6.7: Relevance of the Questionnaire and Interview Questions to the Study

Propositions	Questions to be answered	
	Questionnaire	Interview
Proposition 1		
Nigerian Internal Auditors are increasingly adopting IT-based tools and techniques. These questions are aimed at assessing the perceptions of Internal Auditors on the current level and effectiveness of IT usage for their work. This is further broken down into four themes:		
(1.1) Internal Auditors' current level of use of ICT tools and techniques.	A1 – A11; A12 – A15; B22;B24;B28	C1-C6
(1.2) Financial institutions' current level of provision of ICT tools and techniques for audit purpose.	B26,B30	C4; C6
(1.3) ICT tools and techniques are useful for internal control's task, efficiency and effectiveness.	B1 – B16	C1 – C6, E1; F1 – F4
Proposition 2		
The use of ICT-based tools and techniques impact on Internal Auditors' independence.	B30; B31	D1; D2

Proposition 3

Internal Auditors' use of ICT-based tools and techniques has the potential of preventing electronic fraud.

These questions were aimed at assessing the potential of IT tools and techniques in preventing electronic fraud. The question is divided into three themes as follows:

	A12 to A15; B1 to B17; B19	
Proposition 3.1: IA's use of ICT has had a positive impact on prevention of fraud.	B21; B22; B26	E1;
Proposition 3.2: COA has effective fraud preventive control.	A15, B17, and B22	F3;
Proposition 3.3: The extent of ICT utilisation for prevention of fraud is affected by auditors' demographic characteristics.	B22, A10	F4

Proposition 4

Internal Auditors' use of ICT-based tools and techniques are effective in detecting electronic fraud.

These questions were aimed at assessing the effectiveness of ICT-based tools and techniques in detection of fraud. The question is divided into three themes as follows:

	A12 to A15; B1 to B16; B18	F1-F2
Proposition 4.1: Use of ICT in IC has had a positive impact on detection of fraud.	B21; B22; B23; B27	F3
Proposition 4.2: COA has effective fraud detection control.	A9, A10, A11, B24	F4
Proposition 4.3: The extent of ICT utilisation for detection of fraud is affected by auditors' demographic characteristics.		

6.5.0: Data Analysis

6.5.1: Data Generated From Questionnaire

The next important phase of the research is the analysis of data so far collected. As mentioned earlier in section of this chapter, questionnaire data is analysed first to determine gaps and any further confirmatory evidence required for the study.

Data preparation involves categorising the data, checking and editing data and questionnaire coding (which took place before data collection). For example, respondent's years of experience is coded as follows:

Q8: How many years experience have you had in your present position?

Less than 1	a
1-2 years	b
3-5 years	c
6-10 years	d
10 years and above	e

Enough spaces are provided on the questionnaire for open questions that may need to be post-coded. These steps are associated with data collected through the questionnaire. The next section examines applicable techniques for analysing collected data.

Table 6.8: Common Tasks of Analysis and Applicable Techniques

Purpose	Aims of Analysis	Applicable techniques
Description	Concept formulation	Content analysis
	Classification	Factors analysis
		Cluster analysis
Construction of measurement scales	Multi-attribute scale construction	Uni-dimensional scaling Multi-dimensional scaling
Generation of empirical relationships	Pattern recognition	Correlation methods
	Deprivation of empirical laws	Graphical techniques
Explanation and prediction	Policy analysis	Loglinear analysis Experimental design, model, Regression model,
	Theory generation	Path analysis.

Source: Sharp and Howard (1996: 108)

Sharp and Howard, (1996) provided a taxonomy of common tasks of analysis and applicable techniques which is by no means exhaustive but which has proved valuable for this study.

The purpose of this study is to generate empirical relationships among the identified variables. The aim of analysis has therefore been tilted towards pattern recognition and this favours correlation methods as the chosen applicable technique. This is in agreement with Sharp and Howard (1996). Table 4.9 below explains the main statistical methods adopted in this study.

Table 6.9: Statistical Methods Used for Analysis.

	Statistical Technique	Reason for adopting it
1	Frequency Tables	To simplify the data and provide set of figures for the “what” aspect of the research questions (de Vaus, 1996)
2	Cross-tabulation	To categorise data on the basis of one or more than one variables i.e. Univariate and bivariate analyses (Graziano and Raulin, 2004)
3	Correlation Coefficient and one-way ANOVA	To reinforce cross-tabulation and the outcome of frequency tables in order to provide solution to the “why” aspect of the research questions (de Vaus, 1996: Graziano and Raulin, 2004)

Source: Author

The data generated through the questionnaire is analysed by means of Statistical Package for Social Sciences (SPSS) version 18.0 using descriptive statistical methods i.e. Frequency tables; Cross-tabulations and Correlation coefficients and one-way ANOVA. This is because the questionnaire generated an ordinal dataset which is suitable for Spearman’s rank correlation technique. Furthermore this study intends to use a correlation test to establish a connection or strength of relationship between two or more variables, the outcome of which might serve as a platform for further studies. Correlational research measures at least two variables and the plans for measuring variables are formalised prior to measurement (Graziano and Raulin, 2004: 147). This is different from investigation of possible connections in terms of cause and effect that may require the use of regression analysis.

In order to determine if there is a relationship between two variables in cross-tabulation analysis, researchers always go for a range. In this study a correlation coefficient between 0.25 and 0.75 (plus or minus) will be taken as demonstrating some reasonable correlation between two variables. 0.25 is reasonably weak, and 0.75 is reasonably strong at 10 per cent significance level (two-tailed). To interpret correlation coefficients generated through SPSS, the following criteria were used.

Table 6.10: Criteria Used for Interpreting Correlation Coefficients

RANGE	INTERPRETATION
0.80 to 0.99	A very high degree of positive correlation
0.60 to 0.79	A high degree of positive correlation
0.30 to 0.59	A moderate degree of positive correlation
0.10 to 0.29	A low degree of positive correlation
0.01 to 0.09	No or negligible positive correlation
-0.01 to -0.09	No or negligible negative correlation
-0.10 to -0.29	A low degree of negative correlation
-0.30 to -0.59	A moderate degree of negative correlation
-0.60 to -0.79	A high degree of negative correlation

For calculation of the effect size for independent-samples t-test, this study makes use of Cohen's (1988: 284-7) proposed guidelines for interpreting the value of eta squared as follows:

.01 = small effect

.06 = moderate effect

.14 = large effect

6.5.2: Secondary Data

This study also made use of secondary sources which included professional accounting journals from the Institute of Chartered Accountants of Nigeria, (ICAN), ACCA, CPA, CGA and magazines of regulatory bodies like the Central Bank of Nigeria (CBN), Nigeria Insurance Deposit Corporation (NDIC) and the website of EFCC. Relevant books and journal articles were also assessed in order to review wider theoretical perspectives and results of various research within the area of study.

6.6: The Body of Evidence Used in this Study

This study has benefited from two primary sources of evidence to provide a robust analysis. According to Strauss and Cobin (1998), analysis is the direct or indirect interplay between the researcher and the evidence. Figure 5.1 below shows the different sources of evidence used in this study.

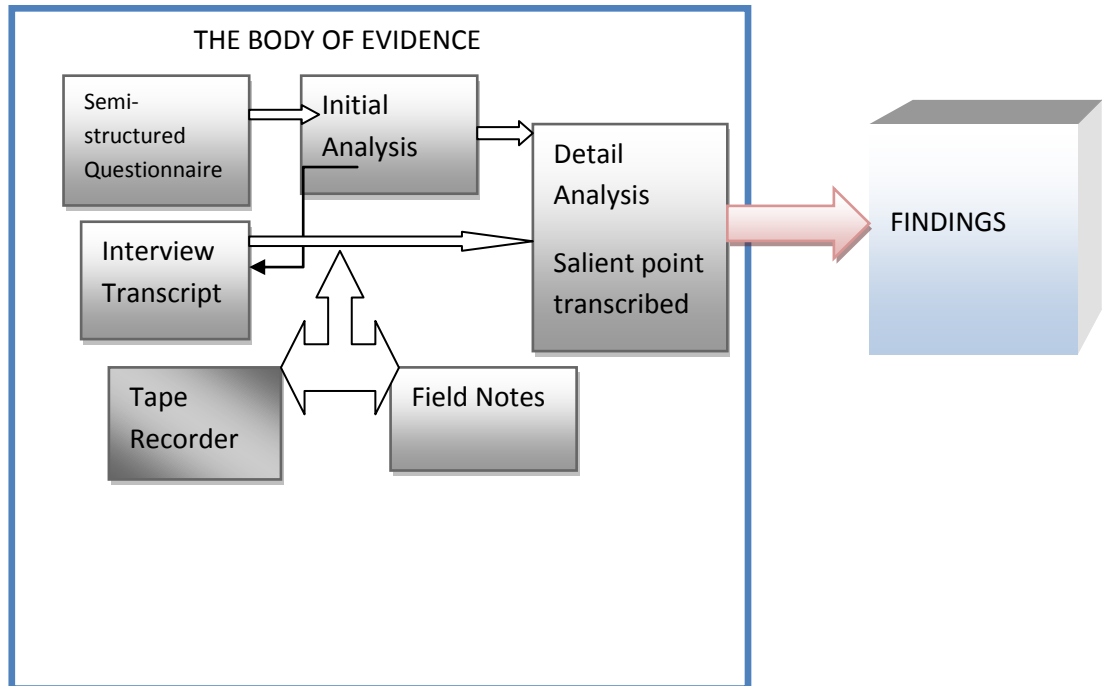


Figure 6.2: The Different Sources of Evidence Used in the Study

Source: Author

6.7: Limitations of the Methodology

The sensitive nature of the information needed for the research (using ICT tools and techniques to detect and prevent fraud) makes accessibility difficult. Apart from the fact that Internal Auditors considered ICT tools they are using as Critical Success Factor (CSF), some of the targeted organisations also believe divulging such vital information may put them at a disadvantage relative to their competitors. Nonetheless, efforts are made to secure access through professional colleagues (fellow chartered accountants) and past former students of the researcher who are in vantage positions in some of these organisations. Furthermore, in order to give the targeted organisations necessary assurance regarding the ethical, confidentiality, and anonymity of individuals involved, as well as judicious use and control of the data given out, the approval of the relevant university authority was sought and obtained.

The main limitation of correlation is that it does not explain cause and effect. For instance, the connection between two variables that might be demonstrated using a correlation test says nothing about which is the independent. It says nothing about which is the cause and which is the effect (Denscombe, 2008: 271). But it establishes that there is a connection, with a specified closeness of fit between the variables.

Prior literature from related studies confirmed that this study could have also benefited from other methods such as case study, action research, ethnography and experiment. For instance, a case study could have equally provided empirical output as it “focuses on one (or just a few) instances of a particular phenomenon with a view to providing an in-depth account of events, relationships, experiences or processes occurring in those particular instances” (Denscombe, 2008: 35). Case study approach could still have answered the salient questions of what, how and why. At the same time, grounded theory approach would have proved invaluable in building relevant theory if the researcher had found the existing theories inadequate for investigating the use of IT tools by Internal Auditors in detecting and preventing electronic fraud.

Ethnography and action research could have also provided the study with opportunity for direct observation, empirical approach, and links with theory, actors’ perceptions and ecological validity. However, the study could have been costly and time consuming considering the limited resources and time available to the researcher. Experimental investigation could have been equally difficult in this instance since it involves “empirical investigation under controlled conditions designed to examine the properties of, and relationship between, specific factors.” (Denscombe, 2008: 48). The nature of the research subject makes both experiment approach and action research difficult alternatives.

Also, data collection through longitudinal approach provides a good basis to draw worthy conclusions and generalise the findings, but it is not considered appropriate for this study because it involves gathering data repeatedly from the same or similar sources at regular intervals over a fairly long period of time (Saunders et al., 2003). The dynamic nature of IT tools and the obvious limitations imposed by limited monetary resources make longitudinal approach a difficult alternative.

6.8: Summary of Chapter

This chapter considered the research approaches and the details involved in collecting, collating and analysing the research data for the study in order to obtain meaningful conclusion and contribute further to knowledge.

The chapter started by examining suitable research philosophies in an attempt to situate the study in an appropriate philosophical context. The study is found to combine phenomenological and positivistic indices and a mixed methods approach has been adopted. The questionnaire data was analysed using frequency tables, cross-tabulations, correlation coefficient, and one-way ANOVA while thematic method was used for the analysis of interview data.

The next chapter concerns the analysis of the interview and questionnaire questions and the responses obtained. This is followed with a discussion on key issues as they become crystallised.

CHAPTER SEVEN

DATA ANALYSIS 1

7.0: Introduction

This chapter introduces analysis of the data collected through detailed questionnaire instrument (quantitative) and subsequent semi-structured interview sessions (qualitative) in order to assess the adoption of IT-based tools and techniques by Internal Auditors in the Nigerian financial sector.

Out of 510 questionnaires sent out to Internal Auditors in the financial sector (banks, mortgage institutions; insurance and stockbroking firms), 218 (representing 42.8 per cent) usable questionnaires were returned.

Descriptive statistics are presented in the form of frequencies tables for initial analysis in order to simplify the data (collected with questionnaire and interview) and provide a set of Figures for the “what” aspect of the research questions (de Vaus, 1996). This is followed with detailed analysis of responses using cross-tabulation, t-test and one-way ANOVA to reinforce the outcome of frequency tables in order to provide a solution to the “why” aspect of the first proposition.

The interviews were conducted by tape recording, mostly at the premises of the firms. The raw interview data was transcribed. Codes are attached to the ‘raw’ data and then grouped into categories. The categories provide a suitable platform under which a number of individual codes can be placed (Denscombe, 2008). Themes and relationships are then identified among the codes and categories. Iterative process is adopted as raw data is visited many times in order to come up with acceptable concepts and suitable generalised statements. The qualitative analysis is presented in the form of thematic analysis as discussed in detail in chapter 6 (6.5.2).

In order to achieve a logical sequence, the quantitative data analysis is first presented for each proposition followed by qualitative data analysis and discussion. To set the background for further analysis, initial data presentation in the form of frequency tables are carried out on responses to questions 1 to 11 in the questionnaire. These are to simplify the data and provide a set of figures for the “what” aspect of the research questions. They are presented in the Appendix.

7.1 Detailed Analysis of Responses

The study made use of responses collected from questionnaire as well as views collated from semi-structured interviews to throw light on propositions and draw conclusions. Previous studies and chosen theoretical underpinnings are further considered before conclusions are drawn regarding the use of audit tools and techniques on internal control and its effectiveness in prevention and detection of fraud. This initial data presentation (Tables 6.1 to 6.8, see Appendix) is to provide set of data for more detailed analysis starting from Table 6.9.

7.2.0: Proposition 1: Nigerian Internal Auditors are increasingly adopting IT-based tools and techniques.

This question is aimed at assessing the perceptions of Internal Auditors on the current level and effectiveness of IT usage for their work. This is further broken down into three themes:

- i. Internal Auditors' current level of use of ICT tools and techniques for internal control purposes is increasing
- ii. Financial institutions' current level of provision of ICT tools and techniques for internal control purposes is increasing
- iii. ICT tools and techniques are useful for internal control's task, efficiency and effectiveness.

Themes (i) and (ii) explore the current state of affairs of Internal Auditors' use of ICT tools and techniques and are expected to illuminate understanding of theme (iii).

7.2.1: Proposition 1.1: Internal Auditors' current level of use of ICT tools and techniques for internal control purposes is increasing.

Table 7.1: A Combined Analysis of Questions 12, 13, 14 and 15 to Answer Research Proposition 1.1

S/N	QUESTIONS	E	S	A	M	N	TOTAL ROW
12	How would you rate the extent of your knowledge in	-	2(1%)	194(89%)	20(9)	2(1%)	218(100%)
13	Internal Auditing?	-	10(5%)	124(56%)	84(39%)	-	218(100%)
14	Internet Usage?	-	8(4%)	94(43%)	116(53%)	-	218(100%)
15	ICT Audit tools techniques? Continuous Online Auditing (COA)	2	4(2%)	52(25%)	158(72%)	2(1%)	218(100%)
	TOTAL COLUMN	2	24	464	378	4	872
				490		382	

Key: E = Extensive, S = Substantial, A = Adequate, M = Minimal. N =None

Responses to question A12 show that a total of 196 respondents (representing 90 per cent) answered in the affirmative, while 22 (representing 10 per cent of the total respondents) answered in the little or no knowledge category. Hence, the practising Internal Auditors have knowledge of internal auditing practice. Question A13 shows that a total of 134 (representing 61.5 per cent of the total) respondents answered in the affirmative, 84 respondents (representing 38.5 per cent of the total population)

answered that they have minimal knowledge in internet usage. The higher percentage affirmation implies that the impact of ICT tools and techniques is appreciably felt by the Internal Auditors. Question A14 shows a total of 102 of the total respondents (representing 46.8 per cent) answered that their knowledge of ICT audit tools techniques is substantial and adequate, while 116 respondents (representing 63.2 per cent) have minimal knowledge of ICT audit tools and techniques. Hence, the responses indicate that the Internal Auditors require workshops, seminars and in-service training to brace them with modern technology. Question number A15 shows that 58 respondents (representing 26.6 per cent) answered in the affirmative, while 160 respondents (representing 73.4 per cent) answered in the negative. Hence, Nigerian Internal Auditors are yet on the road to learn and adopt continuous online auditing. This is similar with the findings of Manson et al. (1997) and Omoteso (2006) who indicate that only large and medium-sized accounting and auditing firms make use of ICT extensively for their work.

Furthermore, it appears there is almost an equal representation of male and female Internal Auditors that are COA literate going by the number of questionnaire returned. Out of 216 questionnaires returned, 104 (representing 48.2 per cent) Male and 112 (representing 51.8 per cent) Female are conversant with COA (See Table 5.2).

The result of cross-tabulation confirms further that on general knowledge of ICT skill, 138 (representing 64 per cent) respondents have adequate or substantial general ICT knowledge while only 78 (representing 24 per cent) respondents either have minimal or no knowledge of ICT at all. However, respondents' knowledge of COA is found to be lower. Only 84 (representing 39 per cent) respondents have adequate, substantial or extensive knowledge of COA, while 132 (representing 61 per cent) have minimal or no knowledge of COA. This result suggests at a glance that the practice of COA is still very low in the Nigerian financial sector. However, a further probe indicates that the practice of COA is gaining ground, especially in almost all commercial banks. Some respondents probably indicate minimal knowledge of COA because they are not directly involved in operating the system and manipulating the software. Some Internal Auditors merely deal with output generated by a system specialist with given input.

Gender * Continuous Online Auditing Cross-Tabulation

Count

Table 7.2 Gender * COA Cross-tabulation

A11 * A15	Continuous Online Auditing				Total
	Minimal	Adequate	Substantial	Extensive	
Gender Male	61(58%)	31(30%)	8 (8%)	4 (4%)	104(100%)
Female	71(63%)	39(35%)	2 (2%)	0 (0%)	112(100%)
Total	132(61%)	70(32%)	10(5%)	4 (2%)	216(100%)

The result of age distribution from the study does not follow the general belief in the literature that the youth have more knowledge of ICT skills than the ageing population. For instance, for those aged less than 25 years, 20 (9 per cent) had minimal knowledge of audit software: while only 8 (4 per cent) had adequate knowledge. A majority of Internal Auditors are less than 45 years old. 86 respondents (representing 40 per cent) have either Adequate or Substantial knowledge of audit software while only 72 (33 per cent) have minimal knowledge of audit software (see Table 7.3).

Table 7.3 Age * Audit Software Cross-tabulation

Count

A10*A14		Audit Software			Total
		Minimal	Adequate	Substantial	
Age	Less than 25 years	20(71%)	8 (29%)	0 (0%)	28(100%)
	Less than 35 years	46(48%)	46(48%)	4 (4%)	96(100%)
	Less than 45 years	26(42%)	36(58%)	0 (0%)	62(100%)
	Less than 60 years	12(40%)	12(40%)	6 (20%)	30(100%)
Total		104(48%)	102(47%)	10 (5%)	216(100%)

For those Internal Auditors who are between the ages 45 and 60 years, 18 (8 per cent) have either adequate or substantial knowledge of audit software, while 12 (6 per cent) have minimal knowledge.

An independent-samples t-test was conducted to compare the Audit IT skills for male and female auditors (see Appendix V1). There was a small significant difference in scores for males (Mean = 2.55, SD = 0.54) and females (Mean 2.68, SD = 0.59), $t(216) = 0.677$, $p = 0.50$, two tailed). The magnitude of the differences in the means (means difference = 0.12, 95% CI: -0.28 to 0.03) was very small (eta squared = 0.012). This suggests that the audit IT skills are almost the same for male and female auditors.

$$\begin{aligned}
 \text{Calculation of Eta Squared: } &= \frac{t^2}{t^2 + (N1 + N2 - 2)} \\
 &= \frac{1.592^2}{1.592^2 + (94 + 124 - 2)} = \frac{2.54}{218.54} \\
 &= 0.012 \text{ (Moderate effects)}
 \end{aligned}$$

In Table 7.4 below, multiple comparisons were undertaken to find out if there is any significant difference in ICT skills in different business types in the financial sector. Only stockbroking and insurance businesses recorded significant differences (.001). This suggests that these two business sub-sectors are still experiencing low usage of ICT tools and techniques compared with commercial banking and mortgage banking. Table 7.4 Comparing Internal Auditors' ICT skills in different business types

Table 7.4 ANOVA

Multiple Comparisons						
iaictUse						
Tukey HSD						
(I) BusinesType	(J) BusinesType	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Banking	Insurance	-.35390	.23017	.417	-.9499	.2421
	Mortgage	.50855	.31253	.366	-.3007	1.3178
	Stockbrokers	1.23932*	.38422	.008	.2445	2.2342
Insurance	Banking	.35390	.23017	.417	-.2421	.9499
	Mortgage	.86245	.33931	.056	-.0161	1.7410
	stockbrokers	1.59322*	.40630	.001	.5412	2.6453
Mortgage	Banking	-.50855	.31253	.366	-1.3178	.3007
	Insurance	-.86245	.33931	.056	-1.7410	.0161
	Stockbrokers	.73077	.45802	.383	-.4552	1.9167
Stockbrokers	Banking	-1.23932*	.38422	.008	-2.2342	-.2445

	Insurance	-1.59322*	.40630	.001	-2.6453	-.5412
	Mortgage	-.73077	.45802	.383	-1.9167	.4552

iaictUse

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	38.009	3	12.670	6.098	.001
Within Groups	444.652	214	2.078		
Total	482.661	217			

Table 7.5 One-Way between group ANOVA

Calculation of Eta Squared = $\frac{\text{Between Groups}}{\text{Total}}$

$$\begin{aligned} \text{Eta Squared:} &= \frac{38.009}{482.661} \\ &= 0.08 \end{aligned}$$

Furthermore, a one-way between groups analysis of variance was conducted to explore the usage of ICT by Internal Auditors among the business group (Table 7.5). They were divided according to their business functions (banking, insurance, mortgage and stockbroking firms). There is a statistically significant difference at the $P < 0.05$ level in scores for the four business groups: $F(3, 214) = 6.09$, $P = 0.001$ (see Appendix). Despite reaching statistical significance, the actual difference in mean scores between the groups was quite small. The effect size, calculated using eta squared, was 0.08 post-hoc comparisons using the Tukey HSD test which indicated that the mean score for banking ($M = 10.24$; $SD = 1.49$); was not significantly different from Insurance ($M = 10.59$; $SD = 1.50$), Mortgage ($M = 9.73$; $SD = 1.19$); was not significantly different from stockbroking ($M=9.00$; $SD = 1.21$).

The one-way ANOVA result suggests that the level of ICT usage in the banking industry is very close to that of insurance companies in terms of sophistication. Also the level of sophistication of equipment and ICT usage in mortgage and stockbroking firms are comparably close to each other.

Table 7.6 Comparing Internal Auditors’ ICT skills with their years of experience

ANOVA

iaictUse

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	41.174	4	10.294	4.966	.001
Within Groups	441.486	213	2.073		
Total	482.661	217			

One-way ANOVA on Internal Auditors’ experience and ICT skills

Calculation of Eta squared = $\frac{\text{Between group}}{\text{Total}}$

= $\frac{41.174}{482.661} = 0.09$

Summary statistics for Table 7.6

Test of Homogeneity of Variances

iaictUse

Levene Statistic	df1	df2	Sig.
3.466	4	213	.009

Tukey HSD^{a,b}

Experience	N	Subset for alpha = 0.05	
		1	2
Less than 1 year	48	9.6250	
3-5 years	45	10.1111	
1-2 years	43	10.1163	
6-10 years	52	10.2885	10.2885
Greater than 10 years	30		11.1000
Sig.		.218	.077

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 42.061.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed

One-way ANOVA on Internal Auditors' Experience and ICT Skills

A one-way between-groups analysis of variance was further conducted to explore the impact of Internal Auditors' job experience on their ICT skills (Table 7.6). On-the-job experience was divided into five groups: (group1 = < 1 year, group2 = 1-2 years, group3 = 3-5 years, group4 = 6-10 years, group5 = > 10 years). There is a statistically significant difference at the $P = < .05$ level for the five groups: $F(4, 213) = 4.97$. Despite attaining what can be considered as statistical significance, the actual difference in mean scores between the groups remains quite small. The effect size, computed using eta squared, was .09. This is a medium effect.

As expected, there is a significant association between the level of work experience of Internal Auditors and their ICT skills. An Auditor with long working experience is expected to have benefited from internal training and practical interactions with IT equipment. This suggests that most Internal Auditors enjoy good in-house training to enhance their jobs. The result tallies with the findings of Samuel et al. (2004) who found that peer mentoring training and experience can produce approximately double competence scores for ICT skills. The result is also in agreement with the pioneering work of Abdolmohammadi and Shanteau (1991) who concluded that the knowledge base needed by an expert auditor may be presumably acquired through experience. The experience effect on a system is expected to be of lesser importance as new recruits are expected to be highly computer literate before they are engaged.

Analysis of question B24:list specific ICT-based audit tools and techniques you use.

The response to this question is similar to that of B25 and B28. This is an open-ended question and 208 respondents (95.4 per cent of the total) answered the question. The pattern of the answer is illustrated below in accordance with respondents' aggregate prioritisation:

Table 7.7: Specific ICT Tools in Use

Software	N = 208	Percentage (%)
Microsoft Office	180	86.5
Audit Command Language (ACL)	48	23.1
Gemini Case ware	41	19.7
Auto audit 2000	32	15.4
ADM-Plus	30	14.4
In house software	25	12.0
Wiz Rule	18	8.7

The analysis of respondents' answer shows that ACL is the most mentioned audit software apart from Microsoft Office, which came first with 86.5 per cent, while Gemini Case-ware came third. 18 respondents were using WIZ Rule package, 25 respondents mentioned an in-house package. It is evident from this analysis that the use of ICT tools and techniques for internal control is improving. More sophisticated internal audit tools and techniques are now being used in the Nigerian financial sector.

7.2.2 Interview Results on ICT Usage

Internal auditors were asked about the level of ICT usage in their organisations. Most interviewees believe that the size of their organisation does not affect the extent of ICT usage, as financial services are generally recognised as information technology intensive. One of the senior managers in one of the new generation banks puts it more succinctly:

“Size does not have any effect on the extent of ICT usage. As a matter of fact some of the older banks that are still very big have not reached the level of computerisation we have reached today. It is obviously difficult to transform your massive manual data into computer form if you don't start with computers from inception. And of course it becomes more expensive as you now have numerous staff members who are computer illiterate and who may not be trainable. So it takes a lot of time and money to acquire computer hardware, software and training of staff members”

Senior Manager A6

Senior Manager A6 is happy to compare his organisation with some other big ones *“As a matter of fact some of the older banks that are still very big have not reached the level of computerisation we have reached today”*. From his body language, he is obviously **‘proud’** about the achievement of his bank in computerisation. This also suggests that the level of ICT usage does not depend only on perceived efficiency but

‘better competitive advantage’ over peers. Senior Manager A6 is very assertive that *‘size does not have any effect’* on the extent of computer usage drawing on his experience. He is probably referring to ease of computerisation rather than system acquisition and in any case underlining the fact that the banking industry is information technology intensive. Manager A6 is sitting next to his assistant during the course of the interview. The assistant keeps giving approval, nodding to Manager A6’s answers. This opinion may be true for banks, and to some extent insurance companies, because they are big enough to absorb budgets associated with acquisition of computer equipment and necessary software. For instance, the minimum paid up capital for banks is 25 billion naira while that of insurance companies is now 2 billion naira. These amounts are big enough to make size of no consequence since they have enough working capital and can equally spend a lot of their budget on ICT acquisition. However, some of the finance houses and stockbroking firms do not have access to large funds and this has an effect on the level of computerisation. One of the managers in a finance house puts it thus:

“ICT tools and techniques are very useful for our operations but we have not been able to buy sophisticated knowledge-based software like others because of cost and the level of our operations. We are still using a package developed in-house for our data analysis and there are some of our operations we still carry out manually. In these circumstances, we cannot talk about COA yet”

Manager, Internal Control (D2)

‘...but we have not been able to buy sophisticated knowledge-based software like others because of cost and the level of our operations’ (Manager D2). The level of operations (size of organisation) and cost are two important factors that affect the level of ICT tools and techniques usage in small financial houses as mentioned here. Of course a lot of their operations are still being carried out manually since the level of transactions is low. This is revealed by Manager D2 above: **‘We are still using a package developed in-house for our data analysis and there are some of our operations we still carry out manually’**. What matters most is for this category of organisation to operate as efficiently as possible. Another fact that emerges from this theme is that this category of organisation cannot operate COA since they cannot afford acquisition of required knowledge-based systems.

The interview results in Table 5.8 below show that 17 (81 per cent) out of 21 participants are of the opinion that the current levels of ICT skills of Internal Auditors have improved.

Table 7.8: Interview Results on ICT Usage

	NO. N = 21	Percentage %
Current levels of ICT skills of Internal Auditors have improved.	17	81
New Internal Auditors are no longer employed without a good knowledge of ICT skills	14	67.7
Internal auditors are being trained on a regular basis to improve the use of ICT skills and techniques	15	71.4
There is increased usage of ICT tools and techniques for internal control/internal audit purposes	15	71.4

The same number of interviewees 15 (71.4 per cent) are of the opinion that there is increased usage of ICT tools and techniques for internal control/internal audit purposes (this is consistent with PricewaterhouseCooper's 2007 findings that Internal Auditors will rely more and more on the use of ICT tools and techniques for their assurance work) and that Internal Auditors are being trained on a regular basis to improve on the use of ICT skills and techniques. 14 out of 21 (66.7 per cent) interviewees are of the opinion that new Internal Auditors must exhibit a good knowledge of ICT skills as part of the interview process before they are engaged. This is consistent with the socio-technical aspect of the three-layered model which predicts that ICT will continually create new sets of experts as new ways of getting transactions done through information technology are discovered.

7.2.3: Interview Questions on ICT Usage and Staffing Requirements

Only six interviewees were of the view that ICT tools and techniques do not necessarily reduce staff but merely shift emphasis to employment of quality staff. However, almost all the interviewees 18 out of 21 (85.7 per cent) are of the view that

the use of ICT tools and techniques reduced the quantity of time required to interact with colleagues, thereby affecting inter-personal working relationships. One of the auditors interviewed has this to say:

“I do not subscribe to people who believe that ICT is increasing unemployment. My view is that the use of ICT tools and techniques affects quality of staff requirements. Accountants and Auditors must be able to use simple programs on the system before they can be relevant in this dispensation. If you are unskilled in computer usage then retrain to become relevant”

Internal auditor A3

The view of internal auditor A3 that “ ***the use of ICT tools and techniques affects quality of staff requirements***” suggests that professional qualification as an auditor or accountant may not be enough to be ‘relevant’ as an Internal Auditor. This is pointing to the need for accountants to be trained on the use of “***simple programs on the system before they can be relevant in this dispensation***”

Opinions of the interviewees are divided as to whether ICT has reduced the number of staff requirements in the internal audit department. More interviewees, 15 out of 21 (representing 71.4 per cent), are of the view that the use of ICT tools and techniques has taken away jobs and therefore fewer staff are now required.

Table 7.9: Interview Result on ICT Usage and Staffing Requirements

	NO. N = 21	Percentage (%)
The use of ICT tools and techniques has reduced the number of internal audit staff especially non-skilled staff	15	71.40
I don't think the use of ICT tools and techniques affect the number of staff requirements. It merely shifts emphasis to quality of staff.	6	28.60
ICT tools and techniques has reduced the quantity of time required to interact officially with colleagues at work as you now interact more with machines	18	85.70

7.2.4: Discussion

The sum total of these findings is that ICT is regarded as a labour-replacing technology. In a developing economy like Nigeria where there are legions of unemployed, semi-skilled youths, this opinion may have some policy implications on development of the ICT industry as a whole.

While opinion supports the view that ICT literacy is increasing among internal audit professionals, the impact of ICT on the economy and unemployment is not yet settled in literature. Meng and Li (2001) reviewed the earlier study conducted by Moss (1996) to reach a conclusion that “if the widespread adoption of ICT leaves more people unemployed, it is understandable that developing countries are reluctant to encourage its rapid development” (Meng and Li, 2001: 2).

If ICT has a negative impact on unskilled workers in terms of employment it follows that the training of professional auditors must incorporate modern ICT skills in order to be relevant. This study’s findings revealed that ICT skill is one of the major criteria for recruiting new professional staff into the financial sector. This is similar with the results obtained by Manson et al. (2001), who showed that audit automation has had a small indirect impact on the recruitment of new auditors, and Omoteso (2006) who showed in addition that automation had a fairly significant impact on auditors’ promotion. This can be explained in the context of the Three-Layered Model (TLM) which suggested that “the use of ICT in audits is a function of certain contingent factors that determine an optimal mix of human skills and technological capabilities, which would lead to changes in the nature of auditors’ roles and outputs. The requirement of ICT knowledge for new recruits is due to the changing roles and responsibility of the internal auditor which can be discussed under the socio-technical aspect of TLM. The complementarities of Technology Acceptance Model (TAM) with TLM can be shown here as the requirement of ICT knowledge for new recruits imposed on graduates and professionals to retrain before employment, thereby positively impacting on the ease of use of ICT tools and techniques.

Linking ICT knowledge with economic development (Meng and Li, 2001) the policy makers must be aware that government needs to urgently sponsor students abroad to

learn new skills by following the experience of China, which has sponsored over 260,000 students in 113 different countries to learn different aspects of technology in the past two decades. There is proven evidence of availability of IT experts in abundant supply now in China (Meng and Li., 2001). The internal control function needs the right mix of human experience and technology for it to be effective. This is captured by the socio-technical aspect of TLM.

7.2.5: The Use of ICT Tools and Techniques and the Size of Organisation.

Previous contingency studies suggested that organisational growth increases communication and control problems. In other words an organisation's size may have a direct effect on the method of system design and management systems adopted (Merchant, 1981, 1984). Previous contingency studies further suggested that an organisation control process becomes more specialised and sophisticated as it increases in size (Ezzamel, 1990; Libby and Waterhouse, 1996; Hoque and James, 2000). A correlation has been established between availability of resources and internal differentiation. The need for a more sophisticated control system becomes obvious as the organisation operations becomes larger (Duncan et al., 1999).

This study builds on the findings of previous studies by empirically examining whether size of the firm plays any role in the use of ICT tools and techniques in financial institutions in a developing country, as most available previous studies took place in developed countries of Europe, America or Canada. In some businesses other than banking and finance firms, direct involvement by top management is more favoured than a more expensive sophisticated control system.

Question B25: ...list specific audit software you use for your work.

Question B25 is similar to questions B24 and B28. The questionnaire responses were analysed based on the type of institution of the respondents.

Table 7.10: Packages/ICT Equipment Use by Participants' Institutions

	Microsoft Office only	In house Software	Microsoft ACL/Gemini case-ware etc	+ Total
Banks	-	-	84 (100%)	84 (100%)
Insurance	-	05 (09%)	51(91%)	56 (100%)
Mortgage	15 (34%)	21 (48%)	08 (18%)	44 (100%)
Stock/Finance	18 (75%)	04 (16%)	02(9%)	24 (100%)
TOTAL	33	30	145	208

Table 7.10 shows that banks and insurance institutions invest heavily in ICT tools and equipment. Out of 208 respondents whose questionnaires are usable, 84 respondents (representing 100 per cent) come from banking firms and use Microsoft Office and ACL/Gemini case-ware etc. This is followed by insurance firms with 51 respondents (representing 91 per cent) using sophisticated ICT. In contrast stock/finance firms have the lowest investment in ICT, as most of them that is 18 respondents (representing 75 per cent) use only Microsoft Office. This is followed by mortgage institutions with 15 respondents (representing 34 per cent) also using only Microsoft Office. The stockbroking/finance houses are relatively small firms. For instance, central bank regulation makes it mandatory for commercial banks to have 25 billion Naira (about £100,000,000.00) as paid-up capital. Insurance companies have 5 billion Naira as paid-up capital while stockbroking firms' paid-up capital is fixed at the sum of two billion Naira. The use of ICT tools and techniques in these institutions can therefore depend on size, level of perceived risk by management/auditors or even environmental uncertainty outside the organisations. Analysis of interview responses made the position clearer.

7.2.6: Interview Responses on the Use of ICT Tools and Techniques and Size of Organisations

In response to the question on what the Internal Auditors think is the most determinant of level of investment in ICT in their organisation, the majority of those responded (14, representing 67 per cent) are of the opinion that the use of ICT tools and techniques in their organisation is dependent on the size of their organisation and volume of operation. 5 respondents (representing 24 per cent) are of the opinion that the use of ICT tools and techniques is dependent on risk associated with the business and the specific industry. Only 2 respondents (representing 8 per cent) are of the view that the use of ICT tools and techniques is dependent on perceived environmental uncertainty relating to the organisation. The results obtained thus far are further reinforced by the responses of two of the Internal Auditors interviewed.

“Internal control is the bedrock of any organisation whether small or big. But investments on control instruments must be commensurate with the level and volume of transaction. If the operation is small there is no need going for sophisticated knowledge-based systems when the same objective can be achieved by adopting manual control that will be less expensive. So, as far as I know the acquisition of ICT tools and techniques and hence their usage in an organisation is dependent much more on size than anything else”.

-Assistant Manager D5

“I have worked in one of the old generation banks for many years and we kept a very good internal control system manually. We were able to keep fraud to a minimum. But things are changing very rapidly. We now have more transactions being processed within a very limited time. Most customers are now in a hurry to get their banking transactions through. All these cost a lot of money. The cost must be matched with the benefit before the investment in new technology can be justified. In any case this is a mortgage institution with less daily transactions than what you have in commercial bank environment. Size of the organisation therefore plays a major role in deciding which technology to adopt”.

-Manager – C8

The two managers emphasised cost and benefit as important for the decision to acquire expensive ICT tools and equipment. The level of transactions generated is also important as reflected in the quote by Manager C8: ‘.....*this is a mortgage*

*institution with less daily transactions than you have in ’ The more transactions you have to process, the more you need more sophisticated ICT to capture them effectively. This is reflected in the quote by Manager C8: **‘I have worked in one of the old generation banks for many years and we kept a very good internal control system manually But things are changing very rapidly (emphatic)’.***

What is changing? There are more customers now than before; there are more banks now than before; level of customer sophistication has changed etc. And more importantly he is laying emphasis on the fact that transactions processed by electronic means have to be controlled by the same means **“We now have more transactions being processed within a very limited time”**. This seems to suggest that internal, external and environmental factors have a role to play in deployment of ICT.

Manager C8 and Assistant Manager D5 agree that size is very important in a decision to adopt ICT equipment. Assistant Manager D5 was very emphatic: **“So as far as I know the acquisition of ICT tools and techniques and hence its usage in an organisation is dependent much more on size than anything else”**.

7.2.7: Discussion

These findings suggest that an organisation’s size may determine the types and sophistication of ICT tools and techniques to be used in an organisation. This result supports the view of early contingency researchers that an organisation’s size may affect the organisation’s choice of designing and adopting management systems (Hoque and James, 2000; Merchant, 1981, 1984). The result also supported Omoteso’s 2006 Three Layered Model which proposed that the use of ICT in audits is a function of certain contingent factors including size of organisation. This result is slightly different from that obtained by Jokipii (2010) which indicated that firms adapt their internal control structure to deal with environmental uncertainty and to achieve observed control effectiveness, and that the organisation’s strategy has more statistically significant effects on internal control structure than organisation size.

7.3: Proposition 1.2: Financial institutions' current level of provision of ICT tools and techniques for internal control purposes is increasing.

Question B28 asked respondents to state which auditing package/software they are using for their work. The result shows that 15.4 per cent use Microsoft Office software to generate audit reports and specific analysis of data. 18.2 per cent use software developed in-house (the majority of this category comes from the insurance industry and finance houses). The majority of respondents (44.2 per cent) uses Audit Command Language (ACL), 21.2 per cent use Gemini case-ware/case-view. Only 1 per cent of the respondents indicate they use ADM Plus software. 10 participants (representing 4.6 per cent of the sampled population) did not indicate what they use, probably because of the sensitive nature of the question. This result is consistent with what was obtained below for B26 (my organisation operates COA) and B30 (my organisation provides a knowledge-based expert system). Slightly above 60 per cent of respondents are positive.

B28. Which of the following tools/packages do you use?

Table 7.11: Packages/tools Use by Internal Auditors in Nigeria

	Frequency	Percentage	Valid Percentage	Cumulative %
Valid				
Microsoft Office application			15.4	15.4
Microsoft Office application			18.3	33.7
Software developed in-house			44.2	77.9
Microsoft Office application				
Software developed in-house				
Gemini Case-ware/case view				
ACL				
Microsoft Office application			21.2	99.0
Software developed in-house				
Gemini Case-ware/case view				
ACL/IDEA/ADM-Plus				
Microsoft Office application +			1.0	100.0
Total			100.0	

Questions B22 and B30 WAS are further analysed for the sake of comparison since the questions are similar. The results are presented in Table 7.12 below:

Table 7.12: Calculated WAS for questions B26 and B30

	5	4	3	2	1	
	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Weighted Average Statistics
B26						
My organisation operates COA	102 (46.7%)	10 (4.6%)	4 (1.8%)	22 (10.6%)	80 (36.8%)	686/218 = 3.15
B30						
My organisation provides a knowledge-based expert system	97 (44.5%)	23 (10.6%)	6 (2.7%)	14 (6.4%)	78 (35.8%)	701/218 = 3.22

Calculated WAS for B26 (My organisation operates COA) and B30 (My organisation provides a knowledge-based expert system) are very close (3.15 and 3.22). The result corroborates the view of prior researchers that COA can only thrive on knowledge-based expert systems (Rezaee and Elam, 2000; Shaikh, 2005). Since the maximum WAS obtainable is 5, the result shows that more than 60 per cent of those sampled are using knowledge-based expert system and are operating COA. This opinion is supported by the interview responses that follow:

There is an increased usage of ICT tools and techniques by financial institutions either because it makes them more efficient (perceived benefits), competitive or because financial regulators (external pressure) make it obligatory for them. Furthermore, as discussed in the preceding proposition, organisation readiness and trust are evidenced as financial institutions are ready to spend as much as possible to

acquire the necessary ICT equipment and train staff in order to trust them with effective use of that equipment. One of the officers in a new generation bank put it thus:

“Today banking is a competitive business. You cannot survive the competition without deploying a lot of resources on IT. Apart from the reasons of efficiency and competition, the regulators, especially the CBN are monitoring very strictly and ‘recommends’ update of IT systems. In most cases, failure to follow ‘advise’ may attract sanctions.”

Officer C2

It is evident from what officer C2 said above that the financial institutions can be said to increase acquisition of ICT tools and techniques for three reasons: for **efficient** operations, to stay **competitive**, and to satisfy **regulatory** guidelines. Attainment of efficiency of operation is an internal factor while competitive and regulatory may be regarded as external pressure.

Table 7.13: Interview Result on Usage of ICT Tools and Techniques by Financial Institutions

	NO.	Percentage (%)
N = 21		
Financial institutions are now using more ICT tools and techniques more than before to be competitive	11	52.4
Financial institutions are now using more ICT tools and techniques than before because financial regulators make it mandatory	10	47.6
Financial institutions are now using more ICT tools and techniques to be more efficient in their operations	13	61.9

Field interview, 2011

13 Interviewees out of 21 (61.9 per cent) are of the opinion that financial institutions are now using more ICT tools and techniques in order to be more efficient in their operations. 11 out of 21 (52.4 per cent) are of the view that financial institutions are now using more ICT tools and techniques more than before to stay competitive.

Furthermore, 10 out of 21 (47.6 per cent) are of the view that financial institutions are now using more ICT tools and techniques than before because financial regulators make it mandatory.

7.3.1: Discussion

External pressure to adopt IT is influenced by the business environment. Iacovou et al. (1995) identified the two main sources of external pressure to adopt as competitive pressure and imposition by trading partners. This finding is in agreement with prior researchers that used TAM to explain acceptance behaviour as a function of users' beliefs about the usefulness and ease of use of a given system (Davis, 1989; Hu, Chau, Sheng and Tam, 1999; Legris, Ingham, and Colletette, 2003 and Hasan, 2007).

The findings are also in agreement with Gullkvist (2003) who found that adoption of IT is due to Perceived benefits (including internal control effectiveness), Organisational readiness, Trust, External Pressure or any other variables. Perceived benefit here includes making organisations more efficient in their operation, while external pressure consists of competition from other businesses offering similar services, and directives from regulatory authorities.

Apart from a few mortgage institutions and stockbroking firms who cannot afford the acquisition of knowledge-based auditing software for reasons of cost or small level of operation, almost all banks have appropriate technology for online, real-time operations. This is in agreement with the result of a survey on Internal Auditors carried out by PricewaterhouseCoopers (2007) which forecast that by 2012 Internal Auditors will depend more and more on ICT for effective performance of their work.

There is agreement between the findings obtained by questionnaire and those of interview. For instance, 51.4 per cent of interview participants agreed or strongly agreed that their organisations operate COA, while 55 per cent agreed or strongly agreed that their organisations provide a knowledge-based expert system. This shows that financial institutions are investing in ICT tools and techniques. The numbers of financial organisations adopting ICT are increasing. This follows the trend observed by NICTP (2012) in the table 2.1 provided in chapter two, of this thesis. This has

been mainly explained by TAM as the usefulness of ICT tools and techniques for internal control/audit operations.

The study further finds that about 40 per cent of respondents who say they do not use knowledge-based systems are constrained by one or more TLM contingent factors, such as size of organisation, cost of acquiring the technology, size of transactions involved etc.

7.4: Proposition 1.3: ICT Tools and Techniques are Useful to Internal Audit's Task, Efficiency and Effectiveness

Questionnaire questions B1 to B16 addressed the usefulness of ICT tools and techniques to internal audit's task, efficiency and effectiveness. The results of the respondents are summarised from frequency tables (see Appendix) as shown in Table 7.14 below. The results are grouped into three categories of those who agree or strongly agree that ICT tools and techniques are useful for specific audit tasks, Disagree or strongly disagree, and those who neither agree nor disagree. The percentage of those who agreed or strongly agreed ranges between 65 and 95 per cent, except for question B3 (ICT tools and techniques are useful for evaluation of audit risk) which has 48 per cent. This is to be expected, as evaluation of audit risk involves a lot of professional judgement which cannot be completely transferred to computer. The second category is those who disagree or strongly disagree with the proposition (ranges between 1 per cent and 20 per cent, except for B3 which is 39 per cent), while those who neither agree nor disagree ranges between 1 per cent and 16 per cent.

Table 7.14: Summary of Frequency Tables for Questions B1 to B16

ICT tools and techniques are useful for	Agree and agree	Strongly disagree	Strongly disagree	Neither agree nor disagree
B1 Evaluation of risk management	(142) 65%	(44) 20%	(32) 15%	
B2 Evaluating audit risk assessment	(170) 78%	(13) 06%	(35) 16%	
B3 Control within payroll application	(104) 48%	(85) 39%	(29) 13%	
B4 Control of e-payment application	(203) 93%	(15) 07%	(0) 0%	
B5 Control of e-purchase	(194) 89%	(16) 07%	(8) 4%	
B6 Control of e-sales	(176) 81%	(28) 13%	(14) 6%	
B7 Control of e-receipt	(182) 83%	(22) 11%	(14) 6%	
B8 Control of identity	(201) 92%	(8) 04%	(9) 4%	
B9 Testing internal control weaknesses	((199) 91%	(9) 04%	(10) 5%	
B10 Quality of internal control	(204) 94%	(11) 05%	(3) 01%	
B11 Testing general control	(207) 95%	(2) 01%	(9) 04%	
B12 Identifies transaction flows	(200) 92%	(4) 02%	(14) 06%	
B13 Control e-funds transfer	(196) 90%	(12) 05%	(10) 05%	
B14 Authorisation control	(184) 84%	(14) 07%	(20) 09%	

B15 Segregation of duty control	(184) 84%	(16) 8%	(16) 08%
B16 ICT useful for security standard	(170) 78%	(14) 06%	(34) 16%

Source: Field Questionnaire, 2011

This result is further reinforced by cross-tabulation of Type of Organisation against Internal control quality. This is because the quality of internal control is perceived to be related to internal audit efficiency and effectiveness. Out of 218 respondents 11 (5 per cent) either disagree or strongly disagree, and 204 (94 per cent) respondents agree or strongly agree that ICT tools and techniques improve internal control quality, while only 3 (1 per cent) neither agree nor disagree. The result supports the proposition that ICT tools and techniques improve internal audit's task, efficiency and effectiveness. The responses cut across banks, insurance companies, mortgage institutions and stock houses sampled.

Furthermore, Spearman's rank correlation is computed using Internal control quality and Business type. The internal control quality was ranked according to the perception of Internal Auditors in the questionnaire responses while business types represent the number of business types contacted for the survey. 91 Internal Auditors agree that banking firms have high internal control quality. The highest is ranked as 1 while the lowest is ranked 6.

Table 7.15 Spearman's Ranking Table

Firms	Internal Control Quality X	Business Type Y	Rank X	Rank Y	X ²	Y ²	XY
Banking	91	9	1	3	1	9	3
Insurance	41	11	3	2	9	4	6
Mortgage	52	14	2	1	4	1	2

Stock Firm	15	8	4	4	16	16	16
Finance House	10	4	5	5	25	25	25
Others	4	2	6	6	36	36	36
TOTALS			21	21	91	91	88

$$r_s = \frac{n \sum XY - \sum X \sum Y}{\sqrt{(n \sum x^2 - (\sum x)^2)(n \sum y^2 - (\sum y)^2)}}$$

$$= \frac{6 \times 88 - 21 \times 21}{105} = \frac{87}{105}$$

$$= \underline{0.83}$$

The Spearman's rank correlation result of .83 indicates a positive ranked correlation between internal control quality and Business types.

7.4.1: Interview Results on Usefulness of ICT Tools and Techniques

18 interviewees (representing 85.7 per cent of the population) interviewed are of the view that ICT tools and techniques improve the overall efficiency of Internal Auditors' task. One of those interviewed has this to say:

“From internal auditing perspective, the use of ICT tools and techniques has been of immense advantage for effective internal control. It helps in immediate tracking of online transactions that might otherwise constitute a problem for lack of adequate audit trail. Another important aspect is the timely generation of audit reports, most especially the exception report....”

Deputy Manager A4

Emphasis is on 'effective internal control' as well as 'immediate tracking of online transactions'. This indicates that ICT tools and techniques improve the overall efficiency of the Internal Auditor's task. In addition the mention of 'timely generation of audit reports' shows that the use of ICT tools and techniques support timely generation of various audit reports and consequently save time and cost.

The results of the interview is summarised as detailed below in Table 7.16

Table 7.16: Interview Question C3

	NO.	Percentage
	N = 21	
ICT tools and techniques improve the overall efficiency of the Internal Auditor's task	18	85.7
ICT tools and techniques save more audit man hours than manual operations and enable reports to be generated on time	15	71.4
ICT tools and techniques save cost. It results in reduction in operating cost.	13	61.9

Furthermore, 15 interviewees (representing 71.4 per cent) are of the view that ICT tools and techniques save more audit man hours than manual operations and enable reports to be generated on time. This view supports those who believe that ICT tools and techniques reduce numbers of available unskilled jobs since computers are capable of doing tasks at a faster rate. 13 out of 21 interviewees (61.9 per cent) are of the view that ICT tools and techniques save costs.

Interviewees were also asked to mention specific areas of audit task that are benefiting from the use of ICT. The responses are tabulated below in order of priority.

Table 7.17: Interview Question C1

Audit Task	NO. N = 21	Percentage (%)
Interrogation and Analysis of Data	16	76.2
Communicating	13	61.9
Reporting	13	61.9
Recording and Documenting	11	52.4
Planning	10	47.6
Controlling	10	47.6
Risk Assessment	9	42.9
Data Storage	6	28.6
Selection of Samples	4	19.0
Testing Sampled Data	3	14.3
Transaction Monitoring	1	4.8

The views analysed in Table 7.17 are reinforced by the assertion of two Assistant Managers in the internal control department of a bank.

“ICT has helped a lot in making us to be more efficient in internal control and in particular in fraud prevention and detection. Some of us are also very comfortable with the technology we use. Before I joined this bank six years ago I could not operate any computer. I could not even manipulate simple e-mail on my computer. I was already a chartered accountant but I was so used to the old system of getting things done through my secretary. But now the story has changed. You can see for yourself that everybody in this room has a computer. Without it there is no job done, simple”

Assistant Manager A2

“Banks have numerous daily transactions that are being generated by bank staff, bank customers and third party. These are made possible by the use of online real-time technology. Going through these transactions one by one manually is impossible with the time and manpower available. The only visible option is to deploy appropriate software that is capable of interrogating and analysing data as they occur”

An Assistant Manager in bank A4

The response from Assistant Manager A2 above suggests that ICT tools and techniques have been very useful to strengthen internal control processes for effective prevention and detection of fraud. The phrase **‘before I joined this bank six years ago I could not operate any computer. I could not even manipulate simple e-mail on my computer.....’** suggests that staff are being trained properly for the use of ICT and there is adequate provision of necessary tools and equipment. The body language exhibited by one of the respondents, as suggested by the satisfaction on his face, also suggests a positive attitude towards the use of ICT for his assignments.

The Assistant Manager in Bank A4 emphasised the usefulness of ICT tools and equipment. *“Going through these transactions one by one manually is impossible with the time and manpower available. The only visible option is to deploy appropriate software that is capable of interrogating and analysing data as they occur”* This suggests that ICT is helpful in making the Internal Auditors more efficient in internal control assignments.

However, the above results notwithstanding, interviewees are of the view that the use of ICT-based tools and techniques has some limitations. The view of the head of internal control in one of the big insurance companies is presented below:

“There is no way ICT tools and techniques will take over internal control and internal audit process completely. You need professional audit judgement which cannot be left entirely to technology to decide. Don’t forget, it is the internal auditor that takes responsibility for effective internal control, including prevention and detection of electronic fraud not the technology no matter how sophisticated.”

Head, Internal Control B2

Apart from the ‘factual’ information presented on the limitation of the use of ICT-based tools and techniques we can see some emphatic denial in the view expressed and the body language as demonstrated by the swinging of his hands for emphasis. For instance ‘*there is no way*’ – this is very emphatic denial which was further echoed in the ‘*don’t forget*’ – very forceful; ‘*auditor takes responsibility... ..not the technology however sophisticated*’ – emphasises the role of humans in the process. Furthermore, the use of certain terms like ‘*professional audit judgement*’ connotes that trained, experienced, time-served, effective individuals are required to man the ICT tools and techniques for effective prevention and detection of fraud. This conforms with the socio-technical aspect of TLM which recommends ‘an optimal mix of human skills and technological capabilities’.

7.4.2: Discussion

The interviewee’s view that the use of ICT-based tools and techniques have some limitations is in agreement with the findings of Ashton (1990) and Sutton et al. (1994) which found that there is a risk of over-reliance on IT by auditors for audit and decision taking. Since technology does not reduce auditors’ responsibility in any way, auditors must be diligent in interpreting output from the system. This calls for the use of professional judgement.

Furthermore, there is agreement in the result of interview and questionnaire analyses, that ICT tools and techniques improve the overall efficiencies and effectiveness of Internal Auditors’ tasks. This may be one of the motivating factors for increased use of ICT tools and techniques by Internal Auditors. This finding corroborates Pinsker’s (2008) study which indicated that TAM and absorptive capacity represent appropriate theories for studying adoption of technology. Pinsker’s (2008) hypothesised that technology adoption would occur if the decision maker perceived ICT to be highly useful in the job and if the decision maker had a favourable attitude toward technology. The data from questionnaire respondents and interviewees suggests that Internal Auditors find technology to be very useful to their work and have a positive attitude towards understanding the usage of ICT. According to Al-Gahtani (2001),

one of the major purposes of TAM is to provide a theoretical basis for understanding the impact of external factors on internal beliefs and attitudes toward technology adoption as its key variables to predict IT adoption.

7.5: Proposition 2: The Use of ICT-based Tools and Techniques Impacts on Internal Auditors’ Independence.

This research proposition tests if the use of ICT tools and techniques impacts on the independence of Internal Auditors. Questionnaire questions B30 and B31 are analysed in order to shed light on this proposition.

Table 7.18 Questionnaire Responses on Internal Auditors’ Independence

		5 Strongly Agree	4 Agree	3 Neither Agree Nor Disagree	2 Disagree	1 Strongly Disagree	WAS
B 30	ICT-based tools and techniques positively affects Internal Auditors’ reporting independence	78 37.1%	102 48.6%	15 7.5%	15 7.5%	0 0%	873/ 210= 4.16
B 31	ICT-based tools and techniques positively affects Internal Auditors’ expression of professional opinion	68 32.4%	113 53.8%	18 8.6%	11 5.2%	0 0%	868/ 210= 4.13

Based on 5 Likert scale, similar WAS of 4.16 and 4.13 were generated from the response to question B30 and B31. This shows that most respondents (86 per cent) support the view that the use of ICT tools and techniques impacts positively on auditors’ reporting and professional independence. Only 12.4 per cent of the respondents did not support the view while 15.7 per cent of respondents neither support it nor disagree. Furthermore a similar WAS of 4.16 and 4.13 means that

opinion of the Internal Auditors is similar about positive effects ICT has on their reporting and professional independence.

Interview Analysis on Internal Auditors' independence

The result obtained under the questionnaire is further supported by the view of the Assistant Head of internal control in a mortgage institution, i.e. that ICT tools and techniques provide good environment where Internal Auditors can express an opinion based on the output of the system without being unjustifiably reprimanded.

“It is quite a lot easier to put audit reports forward to management and audit committee no matter how indicting the report might be to them since the report is a direct output from the machine and not manually generated. The manual reports that are indicting are often looked at as witch hunting. Thus there is leverage on professional freedom for Internal Auditors”

Assistant Head, Internal control C3

Assistant Head, Internal Control C3 pointed to the fact that ICT provides necessary **“...leverage on professional freedom for Internal Auditors”** The use of the word **‘leverage’** and **‘professional freedom’** suggests ICT usage has a positive association with auditors' reporting independence. A report generated manually may have to be approved by an immediate boss who may decide to ‘redecorate’ it or completely step it down. A system-generated report may not need such approval and might be copied to several managers at the same time.

An officer in one of the three old banks has this to say:

“ICT tools and techniques allow me to take a lot of official routine and non-routine decisions without referring them further to my boss”

Officer A7

The tone at which Officer A7 expressed his view and the facial expression suggest that he was very '**motivated**' to take a decision on his own with the help of ICT tools and techniques and without undue intervention from the boss.

Transferring control to ICT tools and techniques can also lead to a sense of independence. Most controls are now machine dependent and so subordinates do not need to seek approval and authorisation from their supervisors before a transaction is concluded. This is further confirmed by a deputy manager in one of the new generation banks.

“ICT tools and techniques provide a lot of motivation and job satisfaction for me. At the moment my job requires a lot of authorisations and transactions approvals which are machine dependent. Jobs can be done with minimal human interference and control.”

Deputy Manager A2

The quote '*ICT tools and techniques provide a lot of motivations and job satisfaction for me.*' suggests that the use of ICT tools and techniques motivates staff and stimulates a positive attitude towards effective usage. There is expression of '**satisfaction**' on the face of Deputy Manager A2 throughout the interview apart from deliberate emphasis placed on “...**a lot of**” to place the response in a definitive perspective. Also “*authorisations and transactions approvals which are machine dependent*” suggests reporting independence.

7.5.1: Discussion

Prior research looked at the independence of External Auditors in relation to their clients. Literature is scant on the impact of ICT tools and techniques on the independence of Internal Auditors. Most authors prefer to look into Internal Auditors' objectivity instead. Professional objectivity is closely linked with individual independence. Internal Auditors operate under Management and audit committees. It is expected that without freedom from the control and influence of management and audit committees it will be difficult for Internal Auditors to maintain the necessary objectivity needed to perform their functions creditably well.

As a structuration process, the findings support the view that ICT tools and techniques impact positively on Internal Auditors' roles and responsibilities. In other words, devolution of more ICT tools and techniques resources has a positive impact on Internal Auditors' ability to carry out their duties with independence and an objective attitude. This finding is similar to Al Twaijry et al. (2004) who found that reliability may not be placed on Saudis' Internal Auditors when they lack professionalism and independence and that devolution of more resources for the internal auditor will establish independence. The result so far is also comparable with Vaccaro and Madsen (2009) who predicted that ICT will play a positive role in future ICT-driven ethics and transparency of Internal Auditors. Omoteso (2006: 269) found that "ICT could enhance auditor independence as a result of various factors: the auditors' ability to access more data; the ability to generate their own audit trail in the client system; less contact with clients' staff because of remote access to information..." Omoteso (2006) relates more to External Auditors. The present study relates solely to Internal Auditors and supports the view that the use of ICT by Internal Auditors impacts positively on their reporting and operational independence. It provides motivation and increased job satisfaction for Internal Auditors. The present study appears to be a pioneer work in this area and is expected to generate more reactions and comments in future.

7.6: Summary of Chapter

In this chapter attempts are made to analyse relevant bio-data collected with descriptive statistics to provide necessary input data for further analyses. This is followed with a detailed analysis in support of proposition 1 which was further broken down into three (3) related themes. In the quantitative section, descriptive statistics were strengthened with cross-tabulation, t-test and One-way ANOVAs. The findings of quantitative analysis were reinforced with qualitative analysis of interview data. Thematic analyses of key issues were undertaken. The results obtained were compared with results from similar previous studies. Efforts were also made to compare results from quantitative analysis with those obtained from qualitative analysis to see if they complement each other or differ. The next chapter is devoted to analysis of propositions III and IV.

CHAPTER EIGHT

DATA ANALYSIS II

8.0: Introduction

Continuing the data analysis started in chapter 7, this chapter attempts to push the analysis further in order to find solutions to propositions 3 and 4. Similar to the previous chapter, univariate analysis in the form of frequency tables are combined with bivariate analysis in the form of cross-tabulations for the quantitative analysis. These are reinforced with t-test and one-way ANOVA in order to bring out the central themes properly.

In addition to qualitative analyses, the outcomes of interviews are transcribed and coded. Thematic analysis is carried out to bring out themes that are relevant to propositions 3 and 4.

8.1.0: Proposition 3: Internal Auditors' use of ICT-based tools and techniques has the potential of preventing electronic fraud.

Proposition 3 is broken down into three themes as follows:

- 3.1. Internal Auditors' use of ICT has had a positive impact on prevention of fraud.
- 3.2. COA has fraud preventive control.
- 3.3. The extent of ICT utilisation for prevention of fraud is affected by auditors' personal characteristics (experience, training, qualifications).

8.1.1: Proposition 3.1: Internal Auditors' use of ICT has had a positive impact on prevention of fraud

Table 8.1: Calculated WAS for Questions B14, B16, B19 and B20

	5 Strongly agree	4 Agree	3 Neither agree nor disagree	2 Disagree	1 Strongly disagree	WAS
B20: ICT is useful for generating exception report	58 (26.6%)	82 (37.6%)	60 (27.5%)	18 (8.3%)	0 (0%)	834/218 = 3.83
B16: ICT is effective in security procedure evaluation	82 (37.6%)	88 (40.4%)	34 (15.6%)	12 (5.5%)	2 (0.9%)	890/218 = 4.08
B19: ICT is effective for internal check	78 (35.8%)	101 (46.3%)	16 (7.3%)	19 (8.7%)	4 (1.8%)	884/218 = 4.06
B14: ICT is effective in authorisation control	87 (39.9%)	97 (44.5%)	20 (9.2%)	12 (5.5%)	2 (0.9%)	909/218 = 4.17

Source: Field Questionnaire, 2011

The calculated WAS on a Likert scale of five for questions B15, B17, B18 and B23 are as shown in Table 8.1. Question B20 (ICT is useful for generating exception report) generated the lowest WAS of 3.83 and the highest proportion of respondents who neither agree nor disagree (27.5 per cent). However questions B14, B16 and B19 have similar WAS that ranges between 4.08 and 4.17 that tends towards agree or

strongly agree. The majority of the respondents agreed that ICT tools and techniques are effective in evaluating security procedures, in conducting effective internal check and instituting authorisation control which are all crucial for effective fraud prevention. This result also supports the result obtained earlier on the usefulness of ICT tools and techniques for internal control's task, efficiency and effectiveness. To probe further the extent of ICT utilisation for fraud prevention, responses to question B26 are analysed below.

Table 8.2: Types of fraud ICT tools and techniques have prevented

Question B26. '.....list the types of fraud you have used ICT-based tools and techniques to prevent'.

Types of fraud prevented	Respondents out of 218	Percentage (%)	Ranking
Identity fraud	208	95	1st
E-funds transfer	192	88	2nd
Hacking	120	55	3rd
Fraudulent bills settlement	65	30	4th
Payroll fraud	23	01	5th
Money Laundering	22	01	6th

Source: Field Questionnaire, 2011

Table 8.2 above summarises responses to open-ended question B26. All the respondents have more than one type of fraud prevented. This means they all use ICT tools and techniques to prevent electronic fraud. In all, six types of fraud were identified as having been prevented. 208 respondents, representing 95 per cent have prevented identity fraud; second on the list is e-fund transfer with 192 respondents (88 per cent); hacking is also popular, coming 3rd with 120 respondents (55 per cent); fraudulent bills settlement is in the 4th position with 65 respondents (30 per cent).

payroll fraud 23 (1 per cent) and money laundering 22 (1 per cent) are in 5th and 6th positions respectively.

A multiple comparisons of ICT usage and fraud prevention were undertaken in all the financial business types.

Table 8.3: ICT Fraud Prevention by Business Type

Multiple Comparisons						
ICTFPrevent						
Tukey HSD						
(I) BusinesType	(J) BusinesType	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
banking	insurance	-.29465	.32363	.799	-1.1326	.5433
	mortgage	1.00000	.43944	.107	-.1379	2.1379
	stockbrokers	2.48077*	.54024	.000	1.0819	3.8796
insurance	banking	.29465	.32363	.799	-.5433	1.1326
	mortgage	1.29465*	.47710	.036	.0593	2.5300
	stockbrokers	2.77542*	.57129	.000	1.2962	4.2547
mortgage	banking	-1.00000	.43944	.107	-2.1379	.1379
	insurance	-1.29465*	.47710	.036	-2.5300	-.0593
	stockbrokers	1.48077	.64401	.101	-.1868	3.1483
stockbrokers	banking	-2.48077*	.54024	.000	-3.8796	-1.0819
	insurance	-2.77542*	.57129	.000	-4.2547	-1.2962
	mortgage	-1.48077	.64401	.101	-3.1483	.1868

*. The mean difference is significant at the 0.05 level.

The result shows that stockbroking firms are significant compared to banking and insurance firms. This may be due to the fact that the insurance and banking industries are able to use more sophisticated ICT tools and techniques because they have more resources and are able to accommodate bigger budgets than their stockbroking counterparts. One-way ANOVA is further carried out to confirm the results obtained so far.

Table 8.4: ANOVA on ICT Fraud Prevention

ANOVA					
ICTFPrevent					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	118.885	3	39.628	9.647	.000
Within Groups	879.096	214	4.108		
Total	997.982	217			

Calculation of eta squared

$$\begin{aligned}
 &= \frac{\text{Between Groups}}{\text{Total}} \\
 &= \frac{118.885}{997.982} \\
 &= \underline{0.12}
 \end{aligned}$$

Furthermore a one-way between-groups analysis of variance was conducted to explore the impact of ICT on fraud prevention (ICTFPrevent). The group was divided into four (banking, insurance, mortgage and stockbroking). There was a statistically significant difference at the $p = .05$ level in ICT fraud prevention score for the four groups: $F(3, 214) = 9.7$. It is worthy of mention that statistical significance

notwithstanding, the actual difference in mean scores between the groups was quite small. The effect size, calculated using eta squared, was 0.12. Post-hoc comparisons using the Tukey HSD test indicated that the mean scores for banking (M = 12.23, SD = 2.0), insurance (M = 12.53, SD = 1.82), and mortgage (M = 11.23, SD = 2.23) did not differ significantly from each other but were significantly different from stockbroking (M = 9.75, SD = 2.54).

This result is indicative of the premium placed on fraud prevention and the level of ICT tools and equipment being used by banking, insurance, and mortgage institutions. This is significantly different from stockbroking firms.

7.1.2: Proposition 8.2: COA has fraud preventive control.

The responses obtained from Questions A15, B17 and B22 are analysed in Table 8.5 below:

Table 8.5: COA Preventive Control

Questionnaire Questions	5 Strongly agree	4 Agree	3 Neither agree nor disagree	2 Disagree	1 Strongly disagree	WAS
A15 Internal auditors' knowledge of COA	62 (26.6%)	78 (37.6%)	60 (27.5%)	18 (8.3%)	0 (0%)	853/218 =3.91
B17 COA effective in preventive control	71 (32.0%)	75 (33.0%)	58 (26.7%)	14 (6.3%)	0 (0%)	857/218 = 3.93
B22 Organisation operates COA	60 (27.3%)	85 (39.0%)	58 (26.7%)	15 (7.0%)	0 (0%)	844/218 = 3.87

Source: Field Questionnaire, 2011

The analysis in Table 8.5 shows that the calculated WAS ranges between 3.87 and 3.93. This shows a good level of agreement between respondents about the knowledge of COA and the potential of COA for effective prevention of fraud.

In order to find out the correlation between COA and different groups in the financial sector an analysis using Spearman's rank correlation was carried out in Table 8.6 below. Ranking of COA preventive control was undertaken with the responses received from 218 Internal Auditors. 87 ranked banking as the highest with COA preventive control, therefore ranked as number 1 on the table while other money market businesses were ranked lowest with 6. Business Types ranking followed the number of financial institutions that participated in the survey. The result obtained (0.77) indicates a positive correlation between COA preventive control and business types.

Table 8.6: Spearman's Ranking Table

Firm	Busine ss Types X	COA Preventive Control Y	Rank X	Rank Y	X²	Y²	XY
Banking	9	87	3	1	9	1	3
Insurance	11	63	2	2	4	4	4
Mortgage	14	44	1	3	1	9	3
Stockbroking	8	16	4	4	16	16	16
Finance House	4	5	5	5	25	25	25
Others	2	3	6	6	36	36	36
TOTAL			21	21	91	91	87

$$r_s = \frac{n \sum XY - \sum X \sum Y}{\sqrt{(n \sum x^2 - (\sum x)^2)(n \sum y^2 - (\sum y)^2)}}$$

$$= \frac{6 \times 87 - 21 \times 21}{105} = \frac{87}{105}$$

$$= \underline{0.77}$$

This suggests a strong relationship between types of organisation (commercial banks, mortgage institutions, insurance companies and stockbrokers) and the use of COA preventive control for electronic fraud.

8.1.1: Interview Analyses on the effectiveness of Continuous Online Auditing (COA) for Prevention of Fraud.

The following comments from various managers are necessary for detailed evaluation:

“With over 200 branches scattered around the country it would be impossible to carry out a good job, in good time considering the human and material resources available for our use without COA in place. It enables us to work in different locations at the same time. It also enables real-time communication of data among audit staff. It saves a lot of time while 100 per cent interrogation and checking of data is now possible.”

Manager, A5

“COA is very relevant for the prevention of errors and fraud. The advantage over the traditional system is that errors and frauds are discovered and pointed out instantly because of its real-time capability. They are not left for months or possibly the end of year before they are discovered.”

Senior Manager, B3

“It is hoped that most financial organisations will make use of COA to enhance the standard of internal control processes as most transactions are now done online real time. ‘Audit risk’ can be substantially reduced and decision usefulness of financial statements enhanced”

Manager C2

The quotes from managers A5, B3 and C2 above suggest that COA is very useful and improves the standard of internal control. For instance, C2 says ‘.....organisations will make use of COA to enhance the standard of internal control...’ and B3 says ‘COA is very relevant for the prevention of errors and fraud. The advantage over the traditional system is that errors and frauds are discovered and pointed out instantly because of its real-time capability’. This strongly suggests that COA has fraud preventive capability. Also, because ‘..... 100 per cent interrogation and checking of data is now possible’ (Manager A5), COA detective capability is assured.

Another important identified capability of COA is that it enhances decision usefulness of financial reports. As a result of the recently discovered problem of bad

corporate governance practices in the financial system in Nigeria (Abiola, 2012), the Central Bank of Nigeria (CBN), the Security and Exchange Commission (SEC), and the Nigeria Deposit Insurance Corporation (NDIC) separately issued code of governance guidelines to be followed by individual firms. It is the contention of the regulatory authorities that adoption of ICT in processing and auditing financial data will help good corporate governance practices and improve decision usefulness of financial statements.

The usefulness of COA for prevention and detection of fraud notwithstanding, it is the views of some interviewees that COA has its limitations. According to a manager in one of the old generation banks, since COA operates on real-time online accounting, discoveries are often made after the deed has been done. Inasmuch as the fraudsters illegally have access to customers' passwords and relevant security identity questions, so funds can be illegally transferred and payments illegally made to persons online. The view of Manager A3 is stated below:

“One major drawback of COA to my mind is that since it operates on real-time online accounting, illegal transactions such as funds transfers and online payments are done swiftly with stolen identity before discovery is made. In order words, COA may not be very helpful for prevention of fraud as it is for detection”

Manager A3

Another limitation of COA identified by one of the officers in a mortgage institution is cost. His view is that benefits derived from COA must be related to the cost of establishing and maintaining it.

“It is my view that COA is effective in prevention of fraud but the start up cost and the operating cost of COA is too high for the level of our operations. We use a software developer locally for our analytical review and to highlight exceptional items but these cannot compare with knowledge-based software that is more sophisticated and capable of data mining”.

Officer C2

From the various quotes above (Manager A3; Officer C2), the major limitation of COA is the cost of setting it up and the cost of maintaining it. For instance, the view of Officer C2 that ***“...COA is effective in prevention of fraud but the start-up cost and the operating cost of COA is too high for the level of our operations”*** suggests

that COA is effective for prevention of fraud. The barriers for the use of COA identified are set up cost and maintenance cost. Maintenance cost can be significant in Nigeria because the power supply is not stable and a standby power supply for 24 hours daily may be costly for a small operation. The quote from Manager A3 that ‘....*funds transfers and online payments are done swiftly with stolen identity before discovery is made* ***COA may not be very helpful for prevention of fraud as it is for detection***’ may be unfounded because it is based on the fact that ‘...illegal transactions such as funds transfers and online payments are done swiftly with stolen identity...’ which may not be easily prevented by use of additional sophisticated software. If identity is stolen, it becomes difficult for the system to fish out fake users from original users.

A total of 15 interviewees (representing 71.40 per cent) are of the view that COA is effective in prevention of fraud. This means more interviewees are of the view that COA is more effective in fraud prevention. 20 interviewees are of the opinion that COA enhances the value of internal control and hence the work of Internal Auditors. This should also be a welcome proposition for the advancement of corporate governance. The other three interviewees who underplayed the capability of COA to prevent fraud are not using COA in their establishments. It is therefore correct to say that all interviewees who are using COA agree that it is effective for prevention of fraud. The views of some of the officers interviewed are summarised in Table 8.7 below:

Table 8.7: Interview on Continuous Online Auditing

	No. N = 21	Percentage (%)
Continuous Online Auditing is effective in prevention of electronic fraud	15	71.40
Continuous Online Auditing enhances the value of internal control	20	95.20

Source: Field Interview, 2011

8.1.3: Proposition 3.3: The extent of ICT utilisation for prevention of fraud is affected by auditors’ demographic characteristics (experience, training, gender and qualifications)

Table 8.8: Internal Auditors’ Qualifications and Experience and Relationship with Prevention of Electronic Fraud.

ANOVA					
ICTFPrevent					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	23.163	4	5.791	1.265	.285
Within Groups	974.818	213	4.577		
Total	997.982	217			

$$\begin{aligned}
 \text{Calculation of eta Square} &= \frac{\text{Between Groups}}{\text{Total}} \\
 &= \frac{23.163}{997.982} \\
 &= \underline{0.02}
 \end{aligned}$$

A one-way between-group analysis of variance was conducted to explore the impact of Internal Auditors’ qualifications on fraud prevention when using ICT tools and techniques. Participants were divided into five groups according to their qualifications: (group1: OND; group2: HND/Bsc; group3: Msc/PhD; group4: ACA/ACCA/CPA etc; group5: others). There was statistically significant difference at the $p < .05$ in level of fraud prevention for the five qualification groups: $F(4, 213) = 1.03$, $p = .39$. The actual difference in mean scores between the groups was small. The effect size, calculated using eta squared, was .02

Table 8.8a: Internal auditors' experience and relationship with the use of ICT

Multiple Comparisons						
ICTFPrevent						
Tukey HSD						
(I) Experience	(J) Experience	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Less than 1 year	1-2 years	.10636	.46452	.999	-1.1717	1.3844
	3-5 years	-.12639	.44390	.999	-1.3477	1.0949
	6-10 years	.07127	.41909	1.000	-1.0818	1.2243
	Greater than 10 years	-.90417	.49790	.367	-2.2740	.4657
1-2 years	Less than 1 year	-.10636	.46452	.999	-1.3844	1.1717
	3-5 years	-.23275	.47132	.988	-1.5295	1.0640
	6-10 years	-.03509	.44803	1.000	-1.2677	1.1976
	Greater than 10 years	-1.01053	.52249	.303	-2.4480	.4270
3-5 years	Less than 1 year	.12639	.44390	.999	-1.0949	1.3477
	1-2 years	.23275	.47132	.988	-1.0640	1.5295
	6-10 years	.19766	.42661	.990	-.9761	1.3714
	Greater than 10 years	-.77778	.50424	.536	-2.1651	.6095
6-10 years	Less than 1 year	-.07127	.41909	1.000	-1.2243	1.0818
	1-2 years	.03509	.44803	1.000	-1.1976	1.2677
	3-5 years	-.19766	.42661	.990	-1.3714	.9761
	Greater than 10 years	-.97544	.48254	.259	-2.3030	.3522
Greater than 10 years	Less than 1 year	.90417	.49790	.367	-.4657	2.2740
	1-2 years	1.01053	.52249	.303	-.4270	2.4480
	3-5 years	.77778	.50424	.536	-.6095	2.1651
	6-10 years	.97544	.48254	.259	-.3522	2.3030

A one-way between-groups analysis of variance was also conducted to explore the impact of auditors' experience on levels of prevention of fraud when using ICT tools and techniques. Participants were divided into five groups according to the number of years spent on the job: (group 1: < 1 year; group 2: 1-2 years; group 3: 3-5 years; group 4: 6-10 years; group 5: >10 years) There was statistically significant difference at the $p < .05$ level of fraud prevention for the five experience groups: $F(4, 213) = 1.3, p = .29$. The difference in mean scores between the groups was small. The effect size, calculated using eta squared, was .02. Post-hoc comparisons using the Tukey HSD test indicated that the mean score for Group 1 ($M = 11.90, SD = 1.99$); was not significantly different from group 2 ($M = 11.79, SD = 2.41$); group 3 ($M = 12.02, SD = 1.83$) was also not significantly different from group 4 ($M = 11.82, SD = 2.29$), and group 5 ($M = 12.8, SD = 2.14$).

8.1.2: Discussion

Prior studies have investigated financial and economic viability and the technological feasibility of COA (Alles et al., 2002; Razaee et al., 2002; Vasarhelyi, 2002; Pathak et al., 2005), the adoption of COA using TAM (Painsker, 2008), and the application of COA in the UK (Omoteso et al., 2008). The main aim of this proposition is to investigate the usefulness of COA to prevent fraud. Both the interview and questionnaire results support the view that COA has preventive capability. Those respondents that are of the view that COA may not be helpful for prevention of fraud as it is for detection are probably not aware that when COA is enhanced by using appropriate artificial intelligence such as Continuous Intelligent Online Validation (CIOV), a detective orientation and preventive capability will be achieved (Omoteso, 2006). The ex-ante (preventive) is confirmed while the ex-post (detective) orientation of COA will be tested under proposition 4.2.

The adoption of COA for prevention of fraud is reinforced by the regulatory authorities who advise banks and other financial institutions to adopt COA in order to

strengthen their internal control capacity. The regulatory authorities in Nigeria are now advising banks and mortgage institutions to adopt COA in their operations in order to catch up with the global trend. Even though regulatory authorities' directives are advisory, complying with it signifies a 'good' practice. It is therefore expected that virtually all operating banks and mortgage institutions in Nigeria will adopt COA in the near future. An Assistant Manager in one of the banks agrees with this:

“COA is recommended by the regulatory authorities (CBN, NDIC, NICOM) for effective and timely capture of errors and fraud in banks, mortgage institutions and insurance companies in Nigeria. Although their recommendation is advisory, most organisations are now adopting it and in the near future almost all financial institutions will have fully adopted it.”
Assistant Manager A5

This suggests that regulatory authorities have taken COA to be more effective for “.. *timely capture of errors and fraud....*” than the manual alternatives, otherwise it would not be recommended. This suggests that COA has the capacity for instantaneous analysis of raw data with high probability of identifying internal control deficiency. The fact that organisations are now adopting it based on the advice of regulatory authorities and the '*perceived benefits*' suggests that it is becoming a standard for financial institutions to adopt appropriate ICT. This is obvious from the assertion of Assistant Manager A5 above: “*most organisations are now adopting it and in near future almost all financial institutions....*”

This result is similar to the result of PricewaterhouseCoopers' (2007) survey (chapter 2; page 69-70) which predicted that by 2012 technology will be rated highest in impacting internal audit roles, responsibility and functions. The present level of impact of ICT tools and techniques on internal control and audit functions calls for redesigning of training of Internal Auditors to incorporate a good knowledge of IT skills. The present study confirms Razaee et al.'s (2002) suggested conditions to be fulfilled by auditors in a COA environment. For instance, it is necessary for Internal Auditors to have good knowledge of the business, be conversant with the flow of transactions that ensure validity and reliability in order to make use of a control-risk-oriented audit plan that focused on adequacy and effectiveness of internal control in the ICT environment.

Furthermore the findings generated statistically significant difference when tested with different financial groups' ability to prevent fraud. It is noted that stockbroking firms have the lowest ability to prevent fraud probably because most of the firms in the stockbroking group adopt limited ICT tools and techniques capabilities for reason of size and cost as earlier discussed in chapter 5. Some of the firms that fall into the small group adopt less expensive and probably less sophisticated ICT tools and techniques.

8.2.0: Proposition 4: Internal Auditors' use of ICT-based tools and techniques are effective in detecting electronic fraud.

This proposition is further broken down to three themes as follows:

Proposition 4.1: Use of ICT in internal control has had a positive impact on detection of fraud.

Proposition 4.2: COA has effective fraud detection control.

Proposition 4.3: The extent of ICT utilisation for detection of fraud is affected by auditors' demographic characteristics (experience, gender, training and qualifications).

8.2.1: Proposition 4.1: Use of ICT in internal control has had a positive impact on detection of fraud.

Questions B18; B19; B20 and B23 in the questionnaire probed into the use of ICT-based tools and techniques by IAs to detect electronic fraud. This is presented in Table 8.9 below.

Responses to all these four questions (B18, B19, B20 and B23) generated a WAS of between 3.47 and 4.14 each. This indicates that respondents, irrespective of the type of financial industry they work in, tend to agree that ICT tools and techniques can be effective in detection of electronic fraud.

Table 8.9: Use of ICT-based tools and techniques to detect electronic fraud

	5 Strongly agree	4 Agree	3 Neither agree nor disagree	2 Disagree	1 Strongly disagree	WAS
B18.....I use ICT tools and techniques for fraud detection	76 (34.9%)	108 (49.5%)	24 (11.00%)	8 (3.8%)	2 (0.8%)	902/218 = 4.14
B19...ICT tools and techniques are effective for internal check of transactions	78 (35.8%)	101 (46.3%)	16 (7.3%)	19 (8.7%)	4 (1.9%)	884/218 = 4.06
B20....ICT tools and techniques are useful for generating exceptional reports	84 (38.5%)	98 (45%)	24 (11%)	6 (2.75%)	6 (2.75%)	902/218 = 4.14
B21....ICT makes monitoring of transaction flow more effective	46 (21.5%)	59 (27.6%)	68 (31.8%)	31 (14.5%)	10 (4.6%)	742/214 = 3.47

In addition, an attempt was made to probe further to find out if there is any link between respondents' audit-specific IT skills and their opinion on the usefulness of ICT tools and techniques for electronic fraud detection through the use of cross-tabulation. Questions A13 and B18 are selected for this purpose. This is because question A13 addresses the skills of the auditors in using IT while question B18 addresses the usefulness of ICT tools and techniques in fraud detection.

Table 8.10: Audit IT Skill* Fraud Detection Cross-tabulation (A13* B18)

Count		Fraud detection					Total/Percentage
		Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree	
Audit IT Skill	None	0 (0%)	2 (1%)	0 (0)	2 (1%)	0 (0%)	4 (2%)
	Minimal	2 (1%)	4 (2%)	12 (5%)	40 (18%)	22 (10%)	80 (36%)
	Adequate	0 (0%)	2 (1%)	12 (6%)	66 (30%)	48 (22%)	128 (59%)
	Substantial	0 (0%)	0 (0%)	0 (0%)	0 (0%)	6 (3%)	6 (3%)
Total		2 (1%)	8 (3%)	24 (11%)	108 (50%)	76 (35%)	218 (100%)

Also since questions B18, B19, B20 and B23 generated a similar WAS, they are likely to yield similar results when cross-tabulated with a similar variable.

The majority of respondents that have above the minimal level of IT skills, 182 (83.5 per cent), agree positively that ICT tools and techniques are effective in detecting electronic fraud. Only 10 (4.5 per cent) do not agree while 24 (11 per cent) neither agree nor disagree.

To confirm the results obtained so far, an open-ended question (B27) asked the respondents to state the types of fraud ICT-based tools and techniques have detected. The responses are summarised in Table 8.12 below:

B27 ...list the types of fraud you have used ICT-based tools and techniques to detect. All 218 respondents answered this question.

Table 8.12: Types of fraud ICT-based tools and techniques have detected

Types of fraud detected	Frequency (f)	% Ranking
Identity fraud	192 (88.1%)	1st
ATM fraud	185 (84.7%)	3rd
e-fund transfer	186 (85.3%)	2nd
Money laundering	85 (40.0%)	4th
Payroll fraud	52 (23.8%)	7th
Bills payments	65 (29.8%)	6th
Hacking	82 (37.6%)	5th

The result obtained in B27 above is related to the result previously obtained in B26. This may be because most variables responsible for fraud prevention are also affecting fraud detection. Respondents agree that identity fraud, 192 (representing 88.1 per cent) is the most detected. This is not surprising as most electronic frauds involve false identity of the perpetrators. This is in agreement with the outcome of Jones and Levi (2000) who found that identity fraud accounted for 96 per cent of Visa members' bank credit card fraud losses of \$407.00 million in 1997.

E-fund transfer (186 representing 85.3 per cent) is the second most prominent fraud detected. This is also in line with the findings of Chapman and Smith, (2001) which noted that irrevocable transfer of funds, usually offshore, is extremely difficult to prevent, especially when perpetrators typically use fictitious identities. According to Chapman and Smith, (2001), over 50 per cent of banks surveyed reported having been the victim of electronic funds transfer fraud.

ATM fraud, which enjoyed a low preventive rate in the previous analysis, now has a high detective rate, 185 (representing 84.7 per cent) and WAS = 5.09. This means most ATM frauds are only discovered after they have been committed.

Money laundering has a frequency rate of 85 (representing 40 per cent). This is relatively low compared with previous studies which describe money laundering as the infiltration of the banking system by organised criminals who make use of electronic non-bank transfer and cyber-banking, and many other sophisticated techniques. It is estimated that one trillion dollars is laundered every year (Financial Action Task Force, 2001; Williams, 1997; 239). Nigeria has been classified as one of the countries where money laundering is still rampant (FATF, 2001)

Table 8.12a: One-Way ANOVA Result for Groups of Financial Institutions

ANOVA					
ICTFDetection					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	65.577	3	21.859	2.316	.077
Within Groups	1972.376	209	9.437		
Total	2037.953	212			

$$\text{Effect Size} = \frac{\text{Between Groups}}{\text{Total}}$$

$$= \frac{65.577}{2037.953}$$

$$= 0.03$$

To strengthen the analysis obtained so far, a one-way between-group analysis of variance was conducted (Table 8.12a above) to explore the impact of ICT on fraud detection among various groups of financial institutions. The groups were divided into four according to their functions (banking, insurance, mortgage and

stockbroking). There was statistically significant difference at the $p < .1$ level in the scores obtained for the four groups $F(3, 209) = 2.3, p = .08$. The effect size, calculated using eta squared, was .03. Post-hoc comparisons using the Tukey HSD test indicated that the mean scores for the group banking ($M=14.62, SD = 3.02$), insurance ($M = 15.47, SD = 2.91$), mortgage ($M = 14.15, SD = 2.46$), stockbroking ($M = 13.5, SD = 4.58$) are weakly significant at 10 per cent.

The result obtained here is different from what was obtained for ICT fraud prevention among the same group of businesses in the previous section. The result for prevention shows statistically significant difference at the $p < .05$ level in the scores obtained for the four groups. This is because financial businesses follow the old dictum that “prevention is better than cure” by placing more premium on fraud prevention rather than detection.

Proposition 4.2: COA has effective fraud detection control.

Responses to questionnaire questions A15, B22 and B23 were analysed to test proposition 4.2.

Table 8.13: Internal Auditors’ perception on COA capability to detect fraud

	5	4	3	2	1	WAS
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	
Extent of COA Knowledge	62 (26.6%)	78 (37.6%)	60 (27.5%)	18 (8.3%)	0 (0%)	853/218 =3.91
My Organisation operates COA	60 (27.3%)	85 (39.0%)	58 (26.7%)	15 (7.0%)	0 (0%)	844/218 = 3.87
COA is effective in detecting Fraud	72 (33.0%)	79 (36.2%)	61 (28.0%)	6 (3.0%)	0 (0.0%)	871/218 = 4.0

Source: Field Questionnaire. 2011

It is evident from the analyses in Table 7.13 above that the perception of Internal Auditors on COA capability to detect fraud is high (69.2 per cent and WAS of 4.0). It is interesting that those Internal Auditors who believe in the efficacy of COA to detect fraud is not limited to those who are operating COA in their organisations (66.3 per cent). The percentages of those who fall into the 'Neither agree nor disagree' group are relatively high because most of them do not operate COA in their organisations.

The result obtained above is complemented with the interview results. A manager, in one of the new generation banks has this to say:

“COA is very useful for fraud detection. I can confirm to you from experience that most successful frauds in banks are fake identity related and sometimes undetected by COA since transaction update and checking are instantaneously done but often detected by other ICT. I don't see how you can operate online real time transactions in the banking industry without complementing it with COA.”

Manager A4

The assertion of Manager A4 above that **“COA is very useful for fraud detection”** suggests a strong conviction that COA is effective for fraud detection. Also he confirmed that **“I don't see how you can operate online real time transactions in the banking industry without complementing it with COA”**. This suggests that operating online real time transactions without COA may cause a problem of late detection or no detection of fraud at all. But he further cast doubt on the first assertion by stressing that **“I can confirm to you from experience that most successful frauds in banks are fake identity related and sometimes undetected by COA since transaction update and checking are instantaneously done but often detected by other ICT equipments** this appears contradictory to the first assertion of the manager that COA **“is very useful for fraud detection”**. It also contradicts the questionnaire response on Internal Auditors' perception on COA capability to detect fraud in Table 7.13 above. This contradiction may emerge from the inability of respondents to differentiate fraud prevention from fraud detection. The researcher therefore probed further through telephone follow up interview to two managers in two different banks. The responses are as follows:

“The software we use is capable of instantaneous discovery of errors and frauds. I can confirm that most frauds are preventively discovered before they are actually committed except for those involving identity thefts which sometimes not discovered by COA and are actually committed before discovery is made through special investigation as a result of complaint or red flag alert”.

Manager Bank A5

“May I say that I don’t remember any fraud detected by COA even though we have used COA to prevent a lot of errors and fraud. This is done as a matter of fact on a daily basis. But that does not mean that we don’t use ICT for detection of fraud. For instance we use Analysis note book and Auto Fraud Investigation software for data analysis and checking of approval limits. This sometimes throws out surprises.”

Manager, bank A2

The assertion of manager A5 that **“The software we use is capable of instantaneous discovery of errors and frauds”** suggests that COA is being used in his organisation. He went on to say that **“frauds are preventively discovered”** and that those frauds like that of electronic transfer of funds are extremely difficult to prevent when perpetrators typically use fictitious identity. The implication of this is that if COA is instantaneously done as the transactions occur then it may not be useful for fraud detection purposes except where transaction update cycles are delayed as in a batch processing environment. This is not a likely proposition in financial industries.

Manager A2 was categorical by saying that **“May I say that I don’t remember any fraud detected by COA....”** this supports the view that COA is not used for fraud detection in this organisation but for fraud prevention. However some software such as Analysis note book and Auto Fraud Investigation may be used in isolation to probe isolated cases for detection of fraud. This supports the earlier findings that ICT is useful for fraud detection.

The contradiction in the result for this proposition is resolved in favour of interview results. This is because it is possible by respondents answering questionnaire questions superficially by confusing fraud detection with fraud prevention despite the piloting efforts of the researcher.

Proposition 4.3: The extent of ICT utilisation for detection of fraud is affected by auditors’ demographic characteristics (experience, gender, training and qualifications).

Independent T-test results on fraud detection and gender

An independent-samples t-test was conducted to compare detection of fraud using ICT tools and techniques for male and female auditors (see Appendix). There was no significant difference in scores for males (Mean = 4.18, SD = 0.80) and females (Mean 4.10, SD = 0.83), $t(216) = 0.677, p = 0.50$, two-tailed). The magnitude of the differences in the means (means difference = 0.08, 95% CI: -0.15 to 0.23) was very small (eta squared = 0.002). The results suggest that fraud detection using ICT tools and techniques has weak correlation with gender. This result is similar to what was obtained previously under proposition 1 when comparing the means of audit IT skills scores for male and female auditors. The question of gender characteristics and how they affects auditors’ work and decision making in audit have not been fully resolved by prior studies in spite of increasing interest in this area.

Table 8.14: Internal Auditors’ Experience and the use of ICT Tools and Techniques to Detect Electronic Fraud

Multiple Comparisons						
ICTFDetection						
Tukey HSD						
(I) Experience	(J) Experience	Mean Difference (I- J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Less than 1 year	1-2 years	-.25694	.68412	.996	-2.1396	1.6257
	3-5 years	.35417	.64384	.982	-1.4176	2.1259

	3-5 years	.28009	.61553	.991	-1.4138	1.9739
	Greater than 10 years	-.87917	.72216	.741	-2.8664	1.1081
1-2 years	Less than 1 year	.25694	.68412	.996	-1.6257	2.1396
	3-5 years	.61111	.69383	.904	-1.2982	2.5204
	3-5 years	.53704	.66764	.929	-1.3002	2.3743
	Greater than 10 years	-.62222	.76705	.927	-2.7330	1.4886
3-5 years	Less than 1 year	-.35417	.64384	.982	-2.1259	1.4176
	1-2 years	-.61111	.69383	.904	-2.5204	1.2982
	3-5 years	-.07407	.62630	1.000	-1.7976	1.6494
	Greater than 10 years	-1.23333	.73136	.445	-3.2459	.7793
6-10 years	Less than 1 year	-.28009	.61553	.991	-1.9739	1.4138
	1-2 years	-.53704	.66764	.929	-2.3743	1.3002
	3-5 years	.07407	.62630	1.000	-1.6494	1.7976
	Greater than 10 years	-1.15926	.70656	.473	-3.1036	.7851
Greater than 10 years	Less than 1 year	.87917	.72216	.741	-1.1081	2.8664
	1-2 years	.62222	.76705	.927	-1.4886	2.7330
	3-5 years	1.23333	.73136	.445	-.7793	3.2459
	3-5 years	1.15926	.70656	.473	-.7851	3.1036

In order to explore the impact of Internal Auditors' experience on the use of ICT tools and techniques to detect electronic fraud one-way between-group analysis of variance was conducted. Participants' experience was divided into five groups according to years of experience (group1: < 1 year; group2: 1-2 years; group3: 3-5 years; group4: 6-10 years, group5: >10 years). There was statistically significant difference at the $p < .1$ level in experience scores for the five experience groups: $F(4, 208) = 0.9, p = .5$. The difference in scores between the groups was quite small. The effect size

calculated using eta squared, was .02. post-hoc comparisons using the Tukey HSD test indicated that the mean score for group1 (M = 14.7; SD = 3.4),

Table 8.14a Auditors’ Experience and ICT Fraud Detection

ICTFDetection					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	35.348	4	8.837	.918	.454
Within Groups	2002.605	208	9.628		
Total	2037.953	212			

Calculation of Effect size = $\frac{\text{Between Groups}}{\text{Within Groups}}$

$$= \frac{35.348}{2037.953}$$

$$= 0.02$$

group2 (M = 14.9; SD = 2.5), group3 (M = 14.3; SD = 3.4), group4 (M = 14.4; SD = 3.2), group5 (M = 15.6; SD = 3.1) did not differ significantly from each other.

Table 8.15 Internal Auditors’ Qualifications and the use of ICT Tools and Techniques to Detect Electronic Fraud

Multiple Comparisons						
ICTFDetection Tukey HSD						
(I) Qualification	(J) Qualification	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound

OND	HND/BSc	-.56039	.62450	.898	-2.2789	1.1581
	Msc/PhD	-.90261	.63588	.616	-2.6525	.8473
	ACA/CPA/ACCA	-.53699	.61689	.907	-2.2346	1.1606
	Others	.21739	1.35099	1.000	-3.5003	3.9351
HND/BSc	OND	.56039	.62450	.898	-1.1581	2.2789
	Msc/PhD	-.34222	.61086	.981	-2.0232	1.3388
	ACA/CPA/ACCA	.02339	.59106	1.000	-1.6031	1.6499
	Others	.77778	1.33940	.978	-2.9080	4.4636
Msc/PhD	OND	.90261	.63588	.616	-.8473	2.6525
	HND/BSc	.34222	.61086	.981	-1.3388	2.0232
	ACA/CPA/ACCA	.36561	.60308	.974	-1.2940	2.0252
	Others	1.12000	1.34474	.920	-2.5805	4.8205
ACA/CPA/ ACCA	OND	.53699	.61689	.907	-1.1606	2.2346
	HND/BSc	-.02339	.59106	1.000	-1.6499	1.6031
	Msc/PhD	-.36561	.60308	.974	-2.0252	1.2940
	Others	.75439	1.33587	.980	-2.9217	4.4305
Others	OND	-.21739	1.35099	1.000	-3.9351	3.5003
	HND/BSc	-.77778	1.33940	.978	-4.4636	2.9080
	Msc/PhD	-1.12000	1.34474	.920	-4.8205	2.5805

ANOVA

ICTFDetection					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	22.952	4	5.738	.592	.669
Within Groups	2015.001	208	9.688		

Total	2037.953	212			
-------	----------	-----	--	--	--

Furthermore, a one-way between-groups analysis of variance was conducted to explore the impact of auditors' formal qualifications on the use of ICT tools and techniques to detect electronic fraud. Participants were divided into five groups according to the paper qualifications they had acquired (Group1: OND, group2: HND/Bsc, group3: Msc/PhD, group4: ACA/CPA/ACCA, group5: Others). There was statistically significant difference at the $p < .1$ level in qualification scores for the five groups: $F(4, 208) = .6, p = .7$. The difference in mean scores between the groups was quite small. The effect size, calculated using eta squared, was .01. Post-hoc comparisons using the Tukey HSD test indicated that the mean score, for the group1 ($M = 14.2, SD = 3.0$); group2 ($M = 14.8, SD = 3.4$); group3 ($M = 15.1, SD = 3.2$); group4 ($M = 14.8, SD = 2.8$); group5 ($M = 14.0, SD = 3.2$) were not significantly different from each other.

8.2.1: Discussion

While ICT has been found to be useful and has a positive impact on fraud prevention and detection, COA enhances fraud prevention but is not found to support fraud detection contrary to prior studies which stated that appropriate artificial intelligence acts as "Continuous Intelligent Online Validation (CIOV) and [is] capable of both preventive orientation and detective capability (ex-post)" (Omoteso, 2006:268). This result is contrary to the studies by Helms (2002) and Omoteso (2006) which found that COA has preventive and detective capabilities.

The question of auditors' demographic characteristics (experience, qualifications, training and gender) and how they affect work and decision making as Internal Auditors have not been fully resolved by prior studies. Comparing the present study with previous ones, while Abdolmohammadi and Wright (1987) observed that task complexity acts as a moderating variable, Choo (1989) and Colbert (1989) reported mixed results from literature on auditors' experience separately reviewed. David and Solomon (1989) suggested that experience may not be the appropriate characteristics

but instead proposed performance as defined by the efficiency and effectiveness of an audit. The feasibility of measuring effectiveness, which is often done through a proxy, has made the approach suggested indefensible.

Bonner et al. (1990) examined the role of task-specific knowledge and experience effects in auditing. Specifically, the study by Bonners' et al. (1990) focused on "experience effects in analytical risk assessment and control risk assessment". The result supported the view that "task-specific knowledge aided the performance of experienced auditors in both the cue selection and cue weighting components only in analytical risk assessment" (Bonner et al., 1990:1). This result supported the findings of Abdolmohammadi and Wright (1987) as discussed earlier.

Extending prior research, Estes and Reames (1990) studied effects of demographic characteristics on materiality decisions using multivariate analysis. The study was administered on 596 CPAs. The personal characteristics tested were experience, education, and place of work, frequency of materiality decision, gender and age. The result of multivariate analysis indicated that age and place of employment may affect materiality decisions and the confidence in materiality decisions may be affected by years of external auditing experience, place of employment, frequency of materiality decisions and gender. The study is significant as the choice of subject was restricted to expert group unlike most prior studies that made use of novice group to test the difference in problem representation.

Lehmann and Norman (2006) posited that more experienced auditors have more concise problem representations than novices and that some types of concepts featured in problem representation are associated with judgement notwithstanding the level of experience. Lehmann and Norman's (2006) position was a result of experimental investigation involving students and professional accountants. The result obtained is not quite explicit on the impact of experience on the level of efficiency of auditors. The present study is designed to empirically investigate effects of experience of Internal Auditors on the use of ICT tools and techniques for fraud prevention and detection.

The results obtained so far do not agree with some of the prior studies as no association is found between auditors' demographic characteristics (qualifications

and experience) and the use of ICT for fraud detection. However, none of the previous studies used homogeneous professional group (Internal Auditors) like the present study. The present study did not consider task complexity because the respondents are highly educated staff who can easily comprehend system complexity.

8.3.0: Key Findings from the Study

The major findings from the study are summarised based on the four main research propositions of the study as detailed below.

8.3.1: Nigerian Internal Auditors are increasingly adopting IT-based tools and techniques (Proposition 1)

This study tested understanding of usage of ICT tools and techniques for internal control by Internal Auditors in the Nigerian financial sector. Prior studies (Bandura, 1986; Hasan, 2007) suggested that the usage of ICT depends on internal factors such as usefulness; ease of use; attitude and intention; and external factors such as the system's complexity and computer self-efficacy. Proposition 1 was divided into three themes as follows:

8.3.2: Internal Auditors' current level of use of ICT tools and techniques for internal control purposes are increasing. (Proposition 1.1)

First, this study has provided evidence that shows that Internal Auditors' current level of use of ICT tools and techniques as a means of internal control has increased substantially in recent times⁴. This finding corroborates the results of the PricewaterhouseCoopers (2007) which predicted that by 2012 a good number of Internal Auditors would depend more on ICT for effective performance of their work even though PricewaterhouseCoopers' (2007) survey drew data from America, North

⁴ Please refer to Tables 7.11 and 7.13 on pages 181 and 183 for results of quantitative analysis and interview (qualitative analysis) result. Also results reflected in Tables 7.16 and 7.17 on pages 188 and 189 which detailed the usefulness of ICT tools and techniques support this assertion.

America and Europe. The practical implication of this is that Nigeria is increasingly responding to global changes in business and technology with direct consequences on policy formulations.

Secondly, the study found significant positive association between the levels of Internal Auditors' work experience, training and ICT skills⁵. More experienced and older Internal Auditors have a higher level of ICT skills. The result tallies with the findings of Samuel et al. (2004) who found that peer mentoring training and experience can produce approximately double competence scores for ICT skills. This finding is different from the 2011 UK Department of Business Innovation and Skills survey of literacy, numeracy and ICT levels in England which found that "age carries two-thirds of the model's explanatory power and that those aged 16 and 34 performed much better in ICT assessment than those in the aged 54 and above category". (BIS, 2012:110) The reason for this difference may be due to difference in past educational policies between the two countries. For instance, individuals in England are likely to be exposed to computers at a very early age unlike individuals in Nigeria where the majority do not have access to a computer until after graduation from University.

Thirdly, the study contributes empirical evidence to the debate on how the use of ICT tools and techniques has reduced the number of staff required for various tasks in organisations. The debate on whether the deployment of ICT actually reduces employment opportunities is an ongoing one in academic literature. The study found that the use of ICT tools and techniques reduced the number of internal audit staff, especially non-skilled staff⁶. The implication of this is that the use of ICT in audits has led to changes in the nature of auditors' roles and their expected outputs and by implication on internal audit organisations' structures. This is in accord with the position of Omoteso (2006, 252) as depicted in TLM.

"The use of ICT in audits is a function of certain contingent factors that determine an optimal mix of human skills and technological capabilities, which would lead to changes in the nature of auditors' roles and outputs and audit organisations' structures."

⁵ The result of One Way ANOVA to explore the impact of Internal Auditors' job experience on their ICT skills can be found on page 169.

⁶ This is reflected in the results obtained in Table 7.9 on page 175.

Fourthly, the study found that for banking businesses, all the companies involved are big enough to be able to afford the purchase of sophisticated knowledge-based systems but this is not the case with small finance houses and stockbroking firms. One of the managers in a finance house puts it clearly:

“ICT tools and techniques are very useful for our operations but we have not been able to buy sophisticated knowledge-based software like others because of cost and the level of our operations. We are still using a package developed in house for our data analyses and there are some of our operations we still carry out manually. In these circumstances, we cannot talk about COA yet”.

The last sentence from the above statement – “In these circumstances, we cannot talk about COA yet” – clearly indicates a structure based on the best combination of humans and technologies as per Socio-Technical system theory. Organisations will start utilising COA when their budget and size of operation can support highly skilled staff as well as sophisticated technology. This is further supported by the manager’s statement above: “.....because of cost and the level of our operations”; this suggests that the use of ICT tools and techniques in internal control is contingent on ‘cost’ and ‘size of operation’ in small finance houses. This result is in line with the findings in Omoteso’s (2006: 265) study which found “that large organisations are likely to use more ICT tools and techniques than small and medium organisations: the use of ICT tools and techniques in audits will be more widespread as cost of technology decreases”. This study has empirically proven that the predictions by prior studies (Omoteso, 2006; PricewaterhouseCooper, 2007) are true even now as the cost of ICT tools and techniques are coming down and more organisations are adopting them. Sophisticated knowledge-based systems are likely to be more widespread as the cost of technology decreases and becomes affordable to small and medium businesses in the near future. However in the case of Nigeria what can slow down this trend in the near future is the increasing cost of maintenance and inadequate electricity power generation. Most organisations have to generate their own electricity to power ICT equipment. Some are found to be on generating set for 24 hours on daily basis as they operate continuous online real time systems. The overall cost of maintenance becomes more and more significant as the cost of diesel oil increases in the

international markets. This is part of external factors of contingency theory which impacts adoption of ICT-based tools and techniques (see Figure 9.1).

Fifthly, the study found that the use of ICT tools and techniques in the Nigerian financial sector depends on TAM variables, that is, the perceived usefulness of the equipment to the various firms and external pressure of competition from firms offering similar products as well as pressure from regulatory authorities⁷.

8.3.3: Financial institutions' current level of provision of ICT tools and techniques for audit purposes is increasing. (Proposition 1.2)

The study found that most banks and insurance companies are using sophisticated knowledge-based systems and software such as Audit Command Language, IDEA, ADM plus, Gemini Case-ware/Case View in addition to Microsoft Office. The small and medium mortgage institutions, finance houses and stockbroking firms are using auditing applications developed in house in addition to Microsoft Office⁸. Three important reasons were found to have motivated financial institutions to acquire ICT tools and techniques for their use. The first one is efficiency. The need to be more efficient in their operations is now more compelling than before. The second reason is competition. As more and more competitors are coming to the market with similar products, the manner in which the product is delivered to the customer determines business market shares. The third reason is that financial institutions regulatory authorities are making it mandatory for banks, insurance business and mortgage institutions to acquire ICT tools and techniques for their operations. These findings are consistent with TAM variables of perceived benefit (to improve internal control effectiveness, making organisations more efficient in their operations), organisational readiness (organisations can afford the cost of technology, improving employees' competency), trust (this involves the willingness of Internal Auditors to use the system effectively), external pressure (competitions from other businesses offering similar services and directives from regulatory authorities).

⁷ Please see analysis in Table 7.14 and 7.16 on pages 186-188

⁸ Please see analysis in Tables 7.11-6.13 on pages 180-183

8.3.4: The Usefulness of ICT Tools and Techniques for Internal Audit's Task Efficiency and Effectiveness (Proposition 1.3).

As mentioned in chapter 3, there is symmetry between system success and effectiveness of internal controls/internal audit. Effectiveness of internal controls connotes provision of reasonable assurance that the entity is achieving efficiency and effectiveness of operations and at the same time compliance with relevant regulations.

The COSO (1994) framework noted five components of internal control that lead to effective internal control. COSO (1994) goes further to recognise differences in internal control effectiveness in different firms but failed to offer explanation as to why the differences exist. Prior research used the contingency theory approach to explain control effectiveness (Jakipii, 2010; Fisher, 1998; Simon, 1987).

The usefulness of ICT tools and techniques to Internal Auditors' tasks, efficiency and effectiveness is a subjective judgement as to whether there is a reasonable assurance that the objectives of internal control are being met. Internal Auditors are the chosen observers of efficiency and effectiveness of ICT tools and techniques in this study for three reasons: first, Internal Auditors have professional and detailed insight into operation of internal control systems (COSO, 1994). Secondly, establishing, evaluating and supervising internal control is the direct responsibility of Internal Auditors. Lastly, most previous studies have mainly concentrated on the view of external parties as against internal parties (see Jokipii, 2010).

This study found that ICT tools and techniques have been substantially useful to Internal Auditors' tasks, efficiency and effectiveness. Over 70 per cent of respondents agree that ICT tools and techniques have been useful for the following services in order of importance: testing general control; testing quality of internal control; control of e-payment; control of identity; identifying transaction flows; testing internal control weaknesses; control of e-fund transfer; control of e-purchase; authorisation control; segregation of duty control; control of e-receipt; control of e-sales; evaluation of security procedure; control of payroll; audit risk assessment; and evaluation of

audit risk. The evaluation of audit risk is the most frequent task Internal Auditors perform with ICT tools and techniques.⁹

The study found strong evidence that ICT tools and techniques have a positive impact on the overall efficiency of Internal Auditors' tasks and valuable time (audit man hours) is saved compared to manual operations and reports are able to be generated on time. Efficiency results in reduction in operating cost.¹⁰

The study also found limitation to usefulness of ICT tools and techniques as tendency of Internal Auditors to rely too much on it. This is captured by what one of the audit managers said:

“There is no way ICT tools and techniques will take over internal control and internal audit process completely. You need professional audit judgement which cannot be left entirely to technology to decide. Don't forget, it is the internal auditor that takes responsibility for effective internal control including prevention and detection of electronic fraud not the technology no matter how sophisticated.”

The implication of this is that exercise of professional judgement by the Internal Auditors is important to complement the use of ICT tools and techniques for effective results.

8.4: The Use of ICT-based Tools and Techniques Impact on Internal Auditors' Independence and Objectivity (Proposition 2)

Internal auditors operate under management and audit committee. It is expected that without freedom from the control and influence of management and audit committee it would be difficult for Internal Auditors to maintain the necessary objectivity needed to perform their functions creditably. The IIA (2002) envisaged that independence of internal auditor is important for their assurance assignment. This is reflected in the Internal Auditors' definition.

⁹ There is agreement between the quantitative result and the qualitative result. See Tables 7.14 to 7.17 on pages 185 to 191

¹⁰ There is agreement between the quantitative result and the qualitative result. See Tables 7.14 to 7.17 on pages 185 to 191

This study found that the use of ICT tools and techniques provided an enabling environment for Internal Auditors to be objective in performing their duties. This study provides strong evidence to show that ICT has a positive impact on reporting and operational independence of Internal Auditors. In prior studies, independence is looked at in relation to External Auditors¹¹. Since Internal Auditors report to management, they are regarded as not independent of top management. This study looks at Internal Auditors' independence from the perspective of objectivity in carrying out their assignments with respect to line managers. This is important in an environment like Nigeria where a young Internal Auditor may find it difficult to demand appropriate audit explanations from an elderly line manager for cultural reasons. The use of ICT was found to have a positive impact on Internal Auditors' reporting and operational independence. This finding indicates a socio-technical perspective which implies that organisations become task oriented rather than person oriented. A further implication of this is that ICT has affected those influences which were traditionally placed higher up in the organisations' power structures to the extent that they now moved down to the shop floor. The view of an assistant head of internal control summarises this finding:

“It is quite easy to push audit reports forward to management and audit committee no matter how indicting the reports might be to them since the report is a direct output from the machine and not manually generated. The manual reports that are indicting are often looked at as witch hunting. Thus there is leverage on professional freedom for Internal Auditors to communicate as appropriate.”

Two important findings can be deduced from this: one, ICT supports reporting freedom of Internal Auditors; two, ICT supports professional freedom of Internal Auditors. Reporting freedom is important for internal audits anytime there is a need to report identified deviation from normal. The findings obtained are similar with those of Vaccaro and Madsen (2009) which proposed a new conceptualisation of corporate transparency as an ICT-driven dynamic process of communication. Vaccaro and Madsen's (2009) study was designed to extend the earlier work of Tapscott and Ticoll (2003) which predicted that transparency will become more important in effective communication with internal and external stakeholders and that the role of ICT will become increasingly prominent in achieving corporate transparency. This is

¹¹ See Table 7.18 on pages 193-196 for the analysis and discussion

explained with structuration theory. As the technology impacted on actions of individual agents (the Internal Auditors) the internal structure of organisations are being affected (Figure 9.1).

8.5: Internal Auditors' use of ICT-based Tools and Techniques has the Potential of Preventing Electronic Fraud (Proposition 3)

Prior studies concentrated mostly on fraud detection rather than fraud prevention. The recent paradigm shift in internal audit function to that of assurance and consulting value added activities emphasises the importance of fraud prevention. This study contributes to academic literature on fraud prevention by providing empirical evidence on the use of ICT tools and techniques by internal audits for fraud prevention. This proposition is divided into three themes:

8.5.1: Proposition 3.1: Internal Auditors' use of ICT has had a positive impact on prevention of fraud.

This study found that ICT tools and techniques (IDEA, Gemini Caseware; Audit Command Language; ADM plus and Auto fraud investigator) have a better e-fraud preventive control than manual operation (see analysis on pages 228 to 231). The study shows that identity fraud is the most prevented followed by e-fund transfer; hacking; fraudulent bills settlement; payroll fraud and money laundering in order of importance.

Identity fraud is found to be common to all types of different frauds. Most fraudsters use stolen identity to perpetrate their crime. It is noteworthy to discover that credit cards are not common in the Nigerian financial environment hence there is no mention of it at all by the respondents. ATM fraud is common but the study found that most ATM-related frauds are discovered only after they have been committed.

The study shows that there is no significant difference among the business types (banking, insurance, mortgage, and stockbroking firms) and the use of ICT tools and techniques for fraud prevention. All the business types in the group are equally concerned about fraud prevention.

8.5.2: Proposition 3.2: Continuous Online Auditing's (COA) has effective fraud preventive control.

Prior studies have looked at COA as a potential tool for effective auditing of online real time business transactions for Internal and External Auditors (Vasarhelyi, 2002; Alles et al., 2002; Pathak et al., 2005; Omoteso, 2006). The need to equally improve the reliability of electronic transactions increases proportionately as businesses adopt electronic commerce at an increasing rate across the globe. This study looked at COA effectiveness for the prevention of e-fraud.

The study found that COA has a positive impact on internal control and is also found to be effective in fraud prevention. The views of managers interviewed summarised the result:

“With over 200 branches scattered around the country it will be impossible to carry out a good job, in a good time considering human and material resources available for our use without COA in place. It enables us to work in different locations at the same time. It also enables real-time communication of data among audit staff. It saves a lot of time while 100 per cent interrogation and checking of data is now possible.”

“COA is very relevant for the prevention of errors and fraud. The advantage over traditional system is that errors and frauds are discovered and pointed out instantly because of its real-time capability. They are not left for months or possibly end of year before they are discovered.”

As a result of the decision usefulness of COA, the financial regulatory authorities in Nigeria (Central Bank of Nigeria; Nigeria Insurance Deposit Corporation and Nigeria Stock Exchange) recommended COA and issued code of governance guidelines to be followed by individual firms in order to standardise governance practices and improve decision usefulness of financial statements.

One major limitation against the widespread adoption of COA across financial industries in Nigeria is cost. As the cost of acquiring and maintaining online real time technologies comes down, it is expected that more non-banking organisations will

adopt COA for internal control and internal audit purposes. This is in line with the views of a manager in an insurance company.

“It is hoped that most financial organisations will make use of COA to enhance the standard of internal control processes as most transactions are now done online real time. ‘Audit risk’ can be substantially reduced and the decision usefulness of financial statement enhanced.”

8.5.3: Proposition 3.3: The extent of ICT utilisation for prevention of fraud is affected by auditors’ demographic characteristics (experience, qualifications, training and gender).

The study found that two personal characteristics tested, qualifications and experience, have no statistically significant difference among the groups (see analysis and results on pages 206 and 209). The implication of this is that neither experience nor qualifications have discernible impact on the use of ICT tools and techniques for prevention of e-fraud. However, the study found that training has a positive influence on Internal Auditors in using ICT tools and techniques to prevent e-fraud.

8.6: Internal Auditors’ use of ICT-based tools and techniques are effective in detecting electronic fraud. (Proposition 4)

There is a strong association between the use of ICT tools and techniques and strong internal control. The proposition is divided into three themes as below.

8.6.1: Proposition 4.1: Use of ICT in internal control has had positive impact on detection of fraud.

Evidence gathered from questionnaire and interview analyses shows that the use of ICT in internal control has had positive impact on detection of fraud, especially in a batch transaction environment. This is consistent with the work of Matsumura and Tucker (1992) which found that a strong internal control is consistent with a high fraud detection rate. In their study, Matsumura and Tucker (1992) found that “auditors are expected to better detect fraud when penalties for not detecting fraud are increased, when testing requirements are increased, or when clients’ internal controls

are strong. Managers are expected to be less likely to commit fraud when testing requirements are increased or when clients' internal controls are strong. An experimental market using accounting students and economic gains and losses to represent benefits and costs in this setting found results consistent with the expectations" (The Auditors Report, 2001:3) The majority of the frauds are not properly investigated beyond detection level because of the relatively small amount involved. The majority of financial institutions believe that the cost of further investigation is prohibitive and in any case funds defrauded may never be recovered.

8.6.2: Proposition 4.2: COA has effective fraud detection control.

This study found that Internal Auditors have a strong perception that COA is not suited for fraud detection control. This is different from the result from Omotesos' 2006 and Helms' 2002 studies which found that COA has preventive and detective capabilities. The study further found that there is no statistically significant difference among different groups of financial institutions practising COA as far as level and rate of electronic financial fraud detection is concerned. This means the rate of fraud detection (if any) is at the same level for all the participants. This is different from the result obtained for the same group in fraud prevention which shows that banking businesses put more emphasis on prevention probably because of the nature of banking business and the prevalent use of COA in banking than other groups of financial institutions.

8.6.3: Proposition 4.3: The extent of ICT utilisation for detection of fraud is affected by auditors' demographic characteristics (experience, qualifications and training).

This study found that there is no association between the use of ICT tools and techniques for fraud detection and auditors' demographic characteristics (experience, qualifications and gender) (see pages 219 to 225). The implication of this is that detection of fraud using ICT tools and techniques is not contingent on personal characteristics (experience, qualification and gender). However, there is a significant association with the rate of electronic fraud prevention and level of sophistication of ICT tools and techniques. Firms using knowledge-based systems confirm having prevented more frauds than those using simple software packages. This is consistent with socio-technical system where only the optimum mix of human and technology

can achieve effective internal control for prevention and detection of fraud (see Figure 9.1)

8.7.0: Summary of Chapter

This chapter concluded the analyses of data collected through questionnaires and interviews. Following the trend started in chapter six, the analyses were conducted by means of Weighted Average Statistics, Cross-Tabulation, Independent T-Test and One-Way ANOVA for data generated through the questionnaire. Interview data were analysed through thematic analysis. Tests were carried out on continuous online auditing for prevention/detection of fraud, types of fraud ICT-based tools and techniques have detected, the use of ICT-based tools and techniques to detect electronic fraud, ICT fraud prevention by business types and Internal Auditors' qualifications and the use of ICT tools and techniques to detect electronic fraud. There is agreement between the findings generated through questionnaires and that of interviews. The next chapter considers the key findings with a view to drawing conclusions and make appropriate recommendations.

CHAPTER NINE

CONCLUSIONS AND RECOMMENDATIONS

9.0: Introduction

This chapter concludes the study by synthesising and bringing out the main themes in the previous chapters. The chapter will further demonstrate how the stated objectives are achieved in the context of investigations carried out. The major findings and contribution of the thesis are discussed. The researcher highlighted the theoretical implications of the findings as well as the challenges and limitations experienced in the course of the study. Finally the researcher sheds light on future research and provides some policy recommendations.

9.1.0: An Overview of the Thesis

In order to achieve the stated objectives of this study, the researcher segmented the thesis into three main parts. The first part (Chapters 1 to 5) provided an opportunity to set a proper theme for the thesis. The first chapter introduced the thesis and presented the synopsis of other chapters. The chapter stated the research problem and scope of the study while highlighting the research propositions, originality and key outcome of the study. Chapters 2 to 5 provided detailed background to the study. Specifically, Chapter 2 provided detailed background of the economic and political environment of Nigeria where the research was actually carried out. The chapter considered the internal control and internal auditing practices in Nigeria and highlighted reported fraudulent cases in the financial sector. Chapter 3 and 4 provided the definitions of internal control and internal auditing, a review of relevant literature in the area of internal control models, internal auditing functions, ICT tools and techniques usage in auditing and fraud prevention and detection. Research propositions were discussed after highlighting gaps in the literature. Chapter 5 discussed various theoretical concepts that are useful in underpinning research work in ICT. Specifically the researcher considered seven models: Theory of Reasoned Action, Theory of Planned Behaviour, Diffusion of Innovation, Unified Theory of Acceptance and Use of Technology, Model of the IT Implementation Process, Technology Acceptance

Model and Three Layered Model. The merits and demerits of each model were considered and TAM and TLM were considered most suitable for the study. The second part of the thesis consists of chapter 6 only. The researcher presented detailed discussion on the methodology of the research. The philosophical justification was thoroughly discussed while giving reasons for not adopting alternative methods. The lesson the researcher learnt from 30 relevant studies shortlisted was that the research approach adopted by an individual researcher depends on their epistemological inclination and background. Mixed methods approach is adopted for this study in order to ensure convergence of data findings (Mathieson, 1991) and to increase the validity of research findings (Mark and Shortland, 1987). A complete explanation of the phenomena being studied (ICT, Fraud, Control and Human) is provided by the multi-perspective method approach. In order to ensure a more detailed and balanced picture of the situation under study, quantitative and qualitative methodologies are triangulated (Attricher et al., 2008). This conforms with Denzin (1989:307) who stated that “...by combining multiple observers, theories, methods and data sources, (researchers) can hope to overcome the intrinsic bias that comes from single methods, single observer and single theory studies.”

The third part of the thesis consists of chapters 7, 8 and 9. The empirical analyses and results are presented for each of the research propositions. TAM is used to underpin propositions 1.1, 1.2, 1.3 and 2 for Internal Auditors’ adoptions and use of ICT tools and techniques for internal control because it can be predicted by Internal Auditor’s motivation (usefulness and ease of use) and external stimulus (competition, regulatory recommendation) of computer self-efficacy and system complexity which are all variables of TAM. Propositions 1.2, 2, 3, and 4 are explained by TLM because structure and size of organisation, human, technology and Internal Auditors are all involved. The use of ICT in internal control is a function of certain contingent factors that determine an optimal mix of human skills and technological capabilities which would lead to changes in the nature of Internal Auditors’ roles and output. However there are areas where neither of the two models will be sufficient to explain the phenomena involved. This happens in propositions 1.2, 1.4, and 2 where the two models are combined for the explanations.

At the beginning of this research work a number of research objectives were put forward. These objectives were primarily developed from research aims concerning the impact of ICT tools and techniques on internal control effectiveness in prevention and detection of electronic fraud. The increasing reports on Internet fraud across the world, and most especially in developing countries, is a pointer to the doubts about the positive impact the ICT tools and techniques may be having on internal control effectiveness in prevention and detection of fraud (EFCC, 2012). In the developing countries, apart from the fact that infrastructural provisions are still rudimentary, the provision of ICT tools and techniques are in most cases inadequate. A number of researchers have worked on the impact of ICT on auditing or accounting (Omoteso, 2006; PricewaterhouseCooper, 2007; Mahzan and Lymer, 2008). However there is paucity of literature on the subject of the impact of ICT on internal control effectiveness for prevention and detection of fraud. This provided a key motivation for the study. The stated objectives were as follows:

- i. To assess the level of ICT usage by Internal Auditors in internal control systems in Nigeria
- ii. To examine the role ICT plays in Internal Auditors' independence and objectivity
- iii. To assess the potential impact of ICT tools and techniques on electronic fraud prevention, and
- iv. To assess the effectiveness of ICT tools and techniques on electronic fraud detection.

9.1.1: A Self-Appraisal on Research Objectives

In this section, the researcher undertakes a self appraisal of the present study. The relevant question to answer here is “have the research objectives been met?” The researcher stated four main objectives in chapter 1 which are briefly re-stated above. These research objectives have been met. In chapter 6, the researcher explored the first objective through the first research proposition: IAs are increasingly adopting IT

based tools and techniques for internal control. This was rigorously explored by dividing the propositions into three themes and by using TAM and TLM to understand the phenomena involved: the findings confirmed an increase in the adoption of ICT for internal control purposes by financial institutions and that size of organisation and cost limit ICT usage.

The second research objective was to explore the role ICT plays in Internal Auditors' independence: this objective has been met. This is done by exploring research proposition 2 using both quantitative and qualitative analyses in chapter 7. The result provided evidence to show that ICT positively enhanced reporting and operational independence of Internal Auditors.

The third and fourth research objectives were addressed in chapter 8. This is done by rigorously analysing propositions 3 and 4. The two propositions were divided into three themes each to ensure appropriate coverage. This study provided strong evidence to support the findings that ICT enhances fraud prevention and detection and that IAs' audit experience and personal characteristics have no effects on the use of ICT tools and techniques for fraud prevention and detection. Also COA is found to enhance fraud prevention but has little or no impact on fraud detection. Thus, the third and fourth objectives were met.

9.2.0: Placing the Findings within the Context of Applicable Theories

The major theories underpinning this study are presented in chapter 5. The Technology Acceptance Model (TAM) and the Three Layered Model (TLM) are found to be the dominant theoretical underpinnings of the investigation. The two theoretical models TAM and TLM have been used in previous studies. The roles each of the two theories played are also discussed in section 5.9 of chapter 5. This section is intended to shed more light on how clearly the theoretical underpinnings have been explained by the findings from this study.

9.2.1: Technology Acceptance Model (TAM) and Adoption of ICT Tools and Techniques by Internal Auditors

TAM as a model is mostly used to underpin studies involving technology adoption and the reasons why the researcher considered it appropriate for the present study have been documented in chapter 5 under section 5.3. TAM is used in the present study to underpin research proposition 1, that is, Internal Auditors are increasingly adopting IT-based tools and techniques. TAM variables found very useful for this study are perceived benefits, organisational readiness, trust and external pressures. These are explained below.

Perceived Benefits

The study found strong evidence to show that Internal Auditors' perceived benefits of ICT tools and techniques include increased internal control efficiency; improved information quality; improved fraud prevention; improved fraud detection; improved operational efficiency, increased ability to compete and improved customer services. This is similar to perceived usefulness which was defined by Davis et al. (1989, 320) as "the degree to which a person believes that using a particular system would enhance his or her job performance". There is a consensus among Internal Auditors that ICT tools and techniques have improved their operational efficiency. This result is similar to Venkatesh et al. (2003) who proposed TAM's extension, called Unified Theory of Acceptance and use of Technology (UTAUT) where Performance Expectancy (PE) and Facilitating Conditions (FC) were found to directly influence the Internal Auditors' motivation to adopt Computer Assisted Audit Tools and Techniques (Mahzan and Lymer, 2008). Performance expectancy and facilitating conditions are combined in this study to form perceived benefits.

The study found that perceived ease of use has no significant effect on intention to adopt ICT for internal control purposes. This might be because the respondents in this study, the Internal Auditors are professionals who believe that with little training they can use any system effectively. This accords with the findings in Hu et al. (1999) that

perceived usefulness is supported while perceived ease of use is not significant in their study of physicians' acceptance of telemedicine technology.

Organisational Readiness

The study found that cost is not significant to banking organisations in acquiring ICT tools and techniques, unlike the outcome of prior studies (Omoteso, 2006). Most of the banks and insurance companies studied have increased their paid up capital substantially; besides, some of them have branches in other African countries, Europe and the United States. The most viable option open to them is to harness technology for their operations. However, low level of operations may be a barrier to smaller firms. A few mortgage and stockbroking institutions are constrained by cost and level of operations in acquiring knowledge-based systems. However, organisations are ready to meet the challenges of new technology by employing capable professional workers and training the same appropriately as the level of IT users' (Internal Auditors) knowhow is found to be high.

Igbaria et al. (1997) examined organisational factors. They proposed that organisational factors can be divided into two: intraorganisational factors, which include internal support, training and management support and extraorganisational factors which include external support and training. This study is in agreement with the views of Igbaria et al. (1997) that "management and external support have more influence on technology acceptance than internal support and training". However this study found that organisational readiness has a positive effect on ICT acceptance by IA through perceived usefulness rather than perceived ease of use as indicated above under perceived benefit.

Trust

Trust is concerned with reliability and openness of Internal Auditors to transmit accurate data and information. This is particularly important in a developing country where a lot of workers still believe in helping themselves first and foremost to overcome poverty before observing work-place ethical norms. Prior study found that some hired managers may indirectly resist adoption of new technology if they nurse an ulterior motive and may deliberately not be open-minded even when the

advantages become obvious to them (see Hart and Saunders, 1997). Trust refers to reliability and openness. Most small businesses are concerned with the reliability of hired managers to transmit accurate data and information (Gullkvist, 2003). This study found that Internal Auditors are willing to adopt new technology to improve their work irrespective of their knowledge of ICT. Again this supports perceived usefulness more than perceived ease of use.

External pressures

The business environment has direct influence on external pressure. Financial institutions in Nigeria are influenced by global best practices as they move their operations across geographical borders by way of expansion. This process may be referred to as internationalisation and nationalisation factors. Most Nigerian banks and insurance companies are now operating in other African countries, Europe and America, for example, Zenith bank, Guarantee Trust bank, UBA, and Ecobank have branches in London and New York in addition to their branches in other West African countries like Ghana, Sierra Leone and Gabon. This is in addition to the fact that Nigeria is a big country and some of the banks have a network of over 300 branches within the country. To effectively control such a huge branch network needs reliable ICT support. There is also a discernible level of competition among them as they offer similar products; what becomes important is how well the products are delivered to individual customers, hence the need to leverage on ICT tools and techniques.

Furthermore, the study found that regulatory authorities (Central Bank of Nigeria, Nigeria Deposit Insurance Corporation, Security and Exchange Commission) exert a lot of regulatory pressure on financial institutions to adopt ICT tools and techniques in processing and strengthening their internal control. Even though their inspection comments may be advisory, non-compliance is regularly met with penalties.

Image of the organisation and social factors is another filtered reason found in this study. Some of the institutions see themselves as leaders in provision of technology-based services. As they strive to remain so, they continue to increase their budgets on

ICT and invest proportionately in staff training. Thus perceived benefits, organisational readiness, trust and external pressure have an impact on adoption of ICT-based tools and techniques and consequently on internal control. These are depicted in the TEPEM model of internal control in Figure 9.1.

The value of internal audit is apparent in both prevention and detection of fraud as “prevention is better than cure”. A weak internal control creates opportunities for fraud.

9.2.2: The Three Layered Model (TLM) and Effectiveness of ICT Tools and Techniques for Prevention and Detection of Fraud

The TLM was explained in section 5.3 of chapter 5. The model was originally used to underpin a study on the impact of ICT on auditing. The model postulates that “the use of ICT in audits is a function of certain contingent factors (nature of audit, size of the firm/client, auditor’s experience and cost of technology) that determine an optimal mix of human skills and technological capabilities, which would lead to changes in auditors’ roles and outputs, audit organisations’ structures and the structure of the audit profession” (Omoteso, 2006: 272).

The study found that large financial organisations such as banks are financially capable of meeting the huge cost required for audit automation. Apart from this, they have large branch networks both in Nigeria and abroad that make the business manually uncontrollable. Smaller organisations such as mortgage banks and stockbroking firms, on the other hand, cannot acquire sophisticated audit software because of cost and size. This is explained by the TLM model in that “the extent of audit automation is contingent upon the size of an organisation”.

The study found, however, that fraud prevention and detection by Internal Auditors with the use of ICT tools and equipment are not contingent upon their personal characteristics such as Internal Auditors’ education, experience and gender. In other words, experience, education and gender have no impact on the use of ICT for fraud prevention and detection. This result appears to be contrary to the result of similar prior studies, for example Omoteso (2006) found in his study of impact of ICT tools and techniques on auditing that auditors’ use of ICT techniques is contingent upon

their experience and level of seniority. However his study was biased more towards External Auditors than Internal Auditors.

The study also found that Internal Auditors are aware that they have to allow professional judgement to bear on the output of ICT tools and techniques for appropriate decision making. This is put in proper perspective by one of the interviewees.

“There is no way ICT tools and techniques will take over internal control and internal audit process completely. You need professional audit judgement which cannot be left entirely to technology to decide. Don’t forget, it is the Internal Auditor that takes responsibility for effective internal control including prevention and detection of electronic fraud, not the technology no matter how sophisticated.”

In other words an optimum mixture of technology (technical system) and human (i.e. professionals like Internal Auditors) are required for effective internal control including prevention and detection of electronic fraud. The fraudsters also harness technology to commit fraud. There is a need to stay ahead of fraudsters in terms of technological training by Internal Auditors. These are the essential components of socio-technical aspect of TLM which says “...an optimal mix of human skills and technological capabilities...” are required. In the case of this study, Internal Auditors (and the environment created for them by management) make up the social system while ICT tools and techniques constitute the technical system.

The study found that Internal Auditors’ reporting and operational independence are correlated with the use of ICT tools and techniques. This is evidenced with operational and reporting independence. Internal Auditors are able to communicate, disseminating reports with transparent candour with all internal and external stakeholders including top management and the audit committee. The implication of this is that the established ways of getting things done are being changed by the use of ICT with consequent impact on internal structures of organisation. Thus the structuration process has impacted the internal audit department structure, task structure and allocation of individual responsibility. The internal audit departmental structure is now flatter than before as clerical work is being eliminated and professional staffs are engaged. This is in agreement with Caglio (2003) which considered ERP as a structuration process and documented changes in accountants’

positions and practices. This is also explained by TLM model that predicts “...changes in the nature of auditors’ roles and outputs and audit organisations”. It is also consistent with the work of Tapscott and Ticoll (2003) as they predict that transparency will become an important basis for gaining and maintaining required trust and collaborative relationships with internal and external stakeholders, and that the role of ICT will progressively become more prominent in attaining corporate transparency.

The TLM has proved beneficial for the study of impact of ICT on internal control effectiveness in prevention and detection of fraud. The use of ICT tools and techniques in internal audit is a function of already identified contingent factors which determines an optimal mix of human skills and technological capabilities that lead to changes in the nature of Internal Auditors’ roles and outputs and departmental structures. But this cannot fully explain the phenomena involved in this study hence it has been combined with TAM to complement each other for detailed explanation. (see Tables 5.3 on page 127 for propositions and models used).

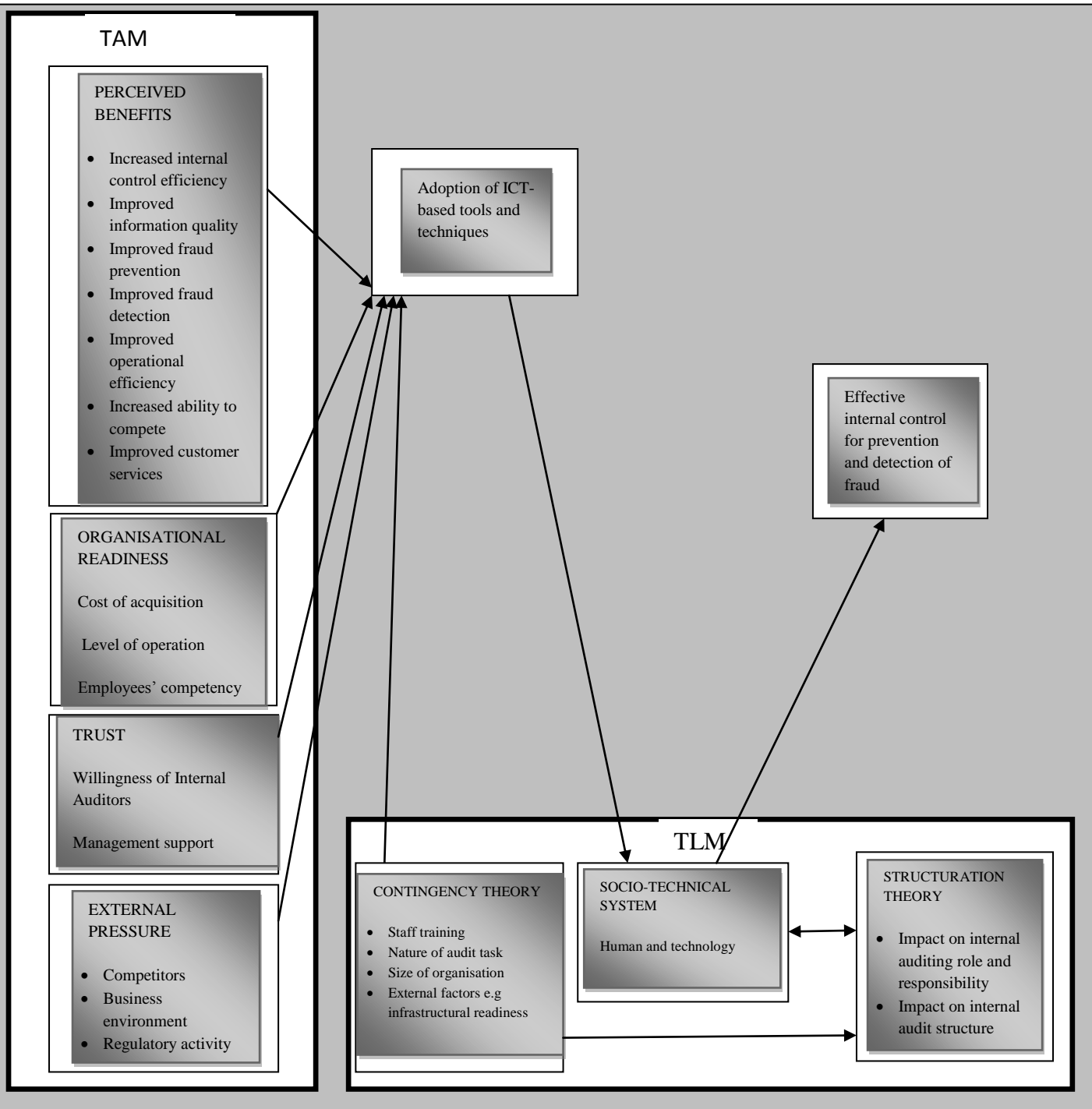


Figure 9.1: Technology Effectiveness Planning and Evaluation Model (TEPEM)

9.3.0: Technology Effectiveness Planning Evaluation Model in Internal Control

TAM and TLM (a meta-level theoretical model encompassing contingency theory, socio-technical systems theory and structuration theory) are the two models identified from literature as suitable for underpinning a study on the impact of ICT tools and techniques on internal control in prevention and detection of electronic fraud. TAM

explained the initial adoption of ICT in internal control by Internal Auditors with four variables (Perceived benefits; Organisational readiness; Trust; and External pressure). All four variables have been identified as having an impact on adoption of ICT-based tools and techniques. The initial plan was to use the two models to complement each other for the analyses and conclusions on the propositions outlined in chapter 2. However, the analyses conducted so far indicated some linkages and interconnections among the two models. For instance while cost, staff training and level of operations are classified as organisational readiness as a TAM internal variable they are regarded as a contingency factor in TLM. In the same sense, while the impact of competition, business environment, and regulatory authority were explained under external pressure in TAM, they are considered under contingency theory because they are all variables that either impact on auditing role and responsibility or organisation structures of Internal Auditors. In the same vein, employees' training is considered under contingency theory as staff ability to adapt to new technology becomes imperative and at the same time considered under employees' competency in TAM as an aspect of organisational readiness. The combination of the two models generates a synergy that produces a good understanding of ICT impact on internal control for prevention and detection of fraud.

The planning process in TEPEM is a unique one to developing economies like Nigeria. For instance, issues like electricity generation and stable regulatory environment are assumed to be constant in developed economies where TAM and TLM have been individually applied but call for careful planning in developing economies. External factors are of utmost importance as a contingent factor as it concerns the macro environmental variables like effective maintenance capability, availability of steady electricity power and government regulations. Lack of constant electricity supply is a major contingency variable in developing countries like Nigeria. Adoption of ICT by the finance industry has been noted to be gradual as each phase of adoption needs planning. The customers and the banking public equally need access to online facilities to be able to transact their businesses. The massive adoption of mobile telephone technology in Nigeria (Nigeria teledensity as at January 2013 according to the Nigerian Communication Commission, 2013 is 81.78 per cent) and the introduction of internet enabled iphone and ipad, provided a cheaper

alternative to computers as they can easily be powered by battery and solar energy. Most commercial banks now encourage their customers to use their telephone banking facilities. These are external contingency variables that also affect the level of organisational readiness under TAM. Similarly, constant regulatory changes affect all the TAM and TLM variables. A recent change cited by one interviewee was an instruction to cancel all ATMs not within the premises of a bank. This resulted in a colossal waste of investment for most banks that have a lot of offsite ATMs. There is need for careful planning that will ameliorate foreseeable regulatory activity that may exert damaging external pressure. Thus while planning may not be so important in an advanced economy for the adoption and effective usage of ICT in internal control, it is of utmost importance in a developing economy like Nigeria.

Moreover the use of ICT to generate and distribute reports has positively impacted on an Internal Auditor to overcome the cultural obligation to respect elders that may make it difficult for him or her to seek necessary audit explanation from an elderly line manager. This, in a way, has impacted the structuration process of the organisation. Equally having impact on ICT adoption are contingency variables of size of the organisation, nature of the audit/internal control task, capability of staff in terms of training and external factors. For instance the size of organisation determines the size of the internal audit department, the volume of transactions and the nature of the internal control task. The human expert attributes which combine to form the socio-system include knowledge, skills, attitudes, values and needs while the technical system is represented by the ICT tools and techniques. Once ICT is adopted, there is a need to ensure a balanced mix between human expertise and machine capability. Thus, socio-technical system most often leads to changes in the configuration of internal control/internal audit department and in turn impacts on internal auditing structure, role and responsibilities as a structuration process. In addition, innovative changes are introduced constantly as a structuration process, in terms of technology in order to be ahead of the fraudsters who are also capable of upgrading their tricks. This process leads to effective prevention and detection of fraud. The model postulates that:

Technology effectiveness is a function of TAM variables (perceived benefits, organisational readiness, trust, external pressure), contingent factors (size of

organisation, cost, staff training and infrastructure readiness), and optimal mix of human and technological capabilities.

9.3.1: Relevance of Technology Effectiveness Planning and Evaluation Model to Previous Studies

The significance of TEPEM can be examined further by analysing prior studies on the impact of adoption of ICT on audit. Some of these studies were able to bring out benefits associated with audit automation (Omoteso, 2006; Bierstaker et al., 2006; Abdolmohammadi and Usoff, 2001). Omoteso (2006) used TLM to underpin the impact of ICT tools and techniques on auditing and brought out essential elements leveraging on contingency perspective, socio-technical and structuration approaches. However, the use of TEPEM could have been more helpful in providing explanations for adoption of ICT by auditors using TAM variables of perceived benefits; organisational readiness; trust and external pressure. Furthermore TEPEM would have brought into focus the human efforts involved in planning in order to achieve an optimum level of human and machine mix. In their studies, Bierstaker et al. (2001) and Abdolmohammadi & Usoff (2001) could have provided a more comprehensive explanation for the benefits associated with audit automation by leveraging on contingency, socio-technical, and structuration approaches as well as TAM variables if TEPEM were used.

Mahzan and Lymer (2008) examined the adoption of CAATs by Internal Auditors in the UK. Mahzan and Lymers' (2008) work benefited from the use of Unified Theory of Acceptance and Use of Technology (UTAUT). The focus of their work was to explore the application of UTAUT to the domain of adoption of CAATs by Internal Auditors. The objective of the study was achieved by coming up with a new model with four dimensions that provided explanations on: "factors that influence motivation, implementation best practices, criteria for performance measurements and challenges/barriers to successful implementation" (Mahzan and Lymer, 2008: 1). UTAUT appears to be a comprehensive model, however the complexity involving the use of ICT tools and techniques for internal audit tasks and assignments could have been better underpinned by the contingency approach and the appropriate combination of ICT tools and human (Internal Auditors) capabilities could have been

appropriately explained by socio-technical approach. Even though UTAUT contains TAM elements, the use of TEPEM would have made the components of TLM available in addition.

Curtis and Payne (2008) examined contextual factors and individual characteristics affecting auditors' decisions on the use of ICT in audit engagement. The unified Theory of Acceptance and Use of Technology (UTAUT), as proposed by Venkatesh et al. (2003), were modified to accommodate specific requirements of public accounting. The issue of auditors' experience, size of organisation and cost of technology could have been better discussed under the contingency approach. Likewise there is a need to balance human efforts with the right mix of technology which is appropriately explained by the socio-technical approach that may be applied to different situations in public or industry accounting.

9.4.0: Summary of Research Contributions

The research has achieved its main objectives as set out in chapter 1. Despite various limitations noted in section 9.5 of this chapter, the thesis has contributed to the body of knowledge in understanding the impact of ICT tools and techniques on internal control in prevention and detection of fraud in a developing economy. It has shed more light on the trend of ICT adoption for internal control in a developing economy.

9.4.1: Contribution to Professional Practice

The study has provided strong evidence to show that the use of ICT tools and techniques (such as IDEA, Gemini Caseware; Audit Command Language; ADM plus and Auto Fraud Investigator) has had a positive impact on the effectiveness of internal controls for prevention of fraud. Internal Auditors agree that more potential frauds are now prevented as a result of the deployment of ICT tools and techniques in internal control. This result has pushed the frontiers of knowledge forward considering that prior studies focused on the use of ICT in audits (Omoteso, 2006; PricewaterhouseCooper, 2007; Mahzan and Lymer, 2008).

Secondly, while prior studies advocated the applicability of complex data mining techniques (such as decision tree, regression, neural networks and Bayesian networks) to financial statement fraud detection (Debreceeny and Gray, 2010; Zhou

and Kapoor, 2010; Ravisankar et al., 2010), this study provided empirical evidence to show that the use of simpler ICT tools and techniques such as Auto Fraud Investigator; Data Analytics; Analysts' Notebook; Wiz Rule for investigation of isolated cases and batch processing transactions in internal control has proved effective for detection of fraud. Respondents supported the view that the rate of fraud detection is high with the use of ICT tools and techniques in internal control rather than manual operation.

Prior studies (Carr, 1985; ICAEW, 2005; and PricewaterhouseCoopers, 2007) predicted a steady increase in the use of ICT by the audit profession. The study found that there is a steady increase in the number of ICT tools and techniques being deployed for internal control and Internal Auditors' use. This study has shown that technology has a great impact on internal audit functions now and is more likely to have a greater impact in the near future.

9.4.2: Contribution to Academic and Theoretical Debates

The study established a positive impact of ICT on Internal Auditors' operational and reporting independence and objectivity in relation to line managers. Prior studies concentrated on the independence of auditors in relation to External Auditors. This study is privileged to be the first that the researcher is aware of to explore the impact of ICT tools and techniques on Internal Auditors' independence. The concept of independence and objectivity are central to the work of Internal Auditors and by extension to the effectiveness of internal control. Evaluating the Internal Auditors' reporting and operational independence in relation to line managers is a means of assessing control environment factors which include ethical values, integrity, competence of staff and philosophy of management which may impact the effectiveness of ICT usage for internal control purposes (COSO, 1992). The control environment sets the tone of an organisation influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people, management's philosophy and operating style, the way management assigns authority and responsibility, and

organises and develops its people, and the attention and direction provided by the board of directors (COSO, 1994).

With ICT, reports are generated automatically and distributed to recipients without any interference. Also it is found that most approvals are machine dependent instead of waiting on supervisors and line managers to give their blessing before a transaction can be concluded. Audit queries are equally automatically generated thus enabling the Internal Auditor to overcome cultural barriers of demanding explanations directly from line managers who are in most cases more elderly staff.

With respect to theoretical perspectives, the study is able to push the frontiers of knowledge forward by being the first to successfully apply TLM model on ICT fraud-related research to augment TAM after it was proposed by Omoteso et al. (2007). This study suggests that TLM has a wide area of coverage as it can be used to underpin research on ICT audit (Omoteso et al., 2007) and ICT fraud as it is the case in the present study.

A new model TEPEM on technology effectiveness has emerged (Figure 9.1 on page 252) from the study as a result of using TAM and TLM as a framework for the understanding of issues involved in this study. The model has been helpful in explaining the phenomena involving adoption and effective usage of technology in a developing country like Nigeria by incorporating external contingencies such as inadequate power supply. The model is able to capture and explain the infrastructural inadequacy, constant regulatory changes, cultural dimension and insecurity surrounding technology adoption, and the planning and effectiveness process.

Apart from organisational readiness as highlighted in TAM, the model has been able to underline the importance of infrastructural readiness as one of the important variables for adoption of ICT tools and techniques, especially in a developing economy where electricity generation is in short supply and constant regulatory changes are common. Inadequate electricity power supply has necessitated encouragement of telephone banking in Nigeria because less electricity is required to power such equipment. This may introduce fresh internal control challenges.

The model postulates that:

Technology effectiveness is a function of TAM variables (perceived benefits, organisational readiness, trust, external pressure), contingent factors (size of organisation, cost, staff training, and infrastructural readiness), and optimal mix of human and technological capabilities.

9.5: Possible Implications for the Policy Makers

The researcher conducted a detailed and extensive study on the impact of ICT tools and techniques on internal control and its effectiveness in prevention and detection of fraud. The following conclusions are expected to be of value to the policy makers.

Nigeria keeps featuring on the grey list of the Financial Action Task Force (FATF), a task force established in 1989 by G-7 countries to fight against money laundering and terrorism. Nigeria is listed in group two among non-performing countries such as: Cuba, Bolivia, Ethiopia, Ghana, Indonesia, Kenya, Myanmar, Nigeria, Pakistan, Sao Tome and Principe, Sri Lanka, Syria, Tanzania, Thailand and Turkey. According to Adeseyoju (2012), no country in West Africa has done more than Nigeria to enhance anti-money laundering and combating the financing of terrorism regimes. This study found that the use of ICT has helped and actually improved prevention and detection of money laundering activities. But policy makers have to motivate the small financial firms in this regard who do not have enough financial muscle, probably in the form of tax concessions, to acquire the necessary sophisticated knowledge-based real-time equipment that is capable of money laundering prevention and detection and performing Customer Due Diligence (CDD) requirements.

The draft of the first Nigeria National policy on ICT (NICTP, 2012) has just been released. The mission of the NICTP is to “fully integrate information and communication technologies into the socio-economic development and transformation of Nigeria into a knowledge-based economy” (NICTP, 2012: 3). Based on the findings of this study, the cost of maintenance is more likely to serve as a constraint to achieving this mission than the cost of initial acquisition of equipment. As the cost of purchase of most computer hardware and software comes down in the international market, the cost of maintenance is going up locally. The cost of

generating electricity¹² to power the equipment, the cost of repairing the equipment and providing spare parts are very prohibitive for small businesses. Some of the banks sampled are on electricity generating set for 24 hours every day as the central electricity supply is still very unreliable. Government should make electricity available to businesses at a subsidised rate to enable small businesses to take advantage of full computerisation.

Secondly, Section 302 of the Sarbanes-Oxley Act 2002 makes it mandatory for the periodic statutory financial reports to include certifications by the executive director that:

- “The signing officers are responsible for internal controls and have evaluated these internal controls within the previous ninety days and have reported on their findings
- A list of all deficiencies in the internal controls and information on any fraud that involves employees who are involved with internal activities
- Any significant changes in internal controls or related factors that could have a negative impact on the internal controls” (Sarbanes-Oxley Act, 2002 section 302)

The provision of the Sarbanes-Oxley Act 2002 is seen as representing good practice and is being adopted in most developing countries. For instance, the Nigerian Companies and Allied Matters Acts 1990, section 359 (6) imposed similar duties on the chairman of the audit committee. The directors and audit committees rely on the work of Internal Auditors for the assessment of internal control therefore it is imperative for the Internal Auditor to be independent from the influence of line managers. This study has found that the use of ICT tools and techniques in internal control has positive impact on Internal Auditors’ operating and reporting independence.

Training of accountants who ultimately become Internal Auditors must be redesigned to include modules on the effective usage of sophisticated software and equipment. For the accountants and auditors to be professionally relevant in future they must equip themselves with relevant technical expertise necessary for effective operation

¹² Power supply in Nigeria is still very problematic. All organisations visited invested in standby electricity generating plants to power their ICT equipment.

of knowledge-based systems. Such skills are needed for data extraction and analysis to evaluate key risk indicators. This is necessary if the use of non-audit professionals who are currently engaged as IT professionals helping auditors for data mining and analysis is to be reduced or eliminated. As the need to leverage on technology to improve audit effectiveness is being felt, Internal Auditors interviewed called for the incorporation of IT audit within traditional audit programmes. It is expected that as more and more technology is being used for internal control and internal audit functions the lines separating IT and non-IT audits will continue to disappear. This is in agreement with the findings of PricewaterhouseCoopers (2012).

As varieties of technology become available to strengthen internal control and for the Internal Auditors to draw upon to assist with their work, the fraudsters are also drawing on newer technology and techniques. As auditors there is the need to stay ahead of fraudsters in order to be effective. This calls for conducting audits on a targeted basis. In this way Internal Auditors will be able to harness technology to focus on risky areas and increase the possibility of early signals for problem areas. This is more relevant in the case of Nigeria where telephone banking is getting more popular and less educated customers are being encouraged onto the telephone banking platforms.

The need to have a strong Association of Internal Auditors is now felt in Nigeria more than at any other time. There are two main accounting associations recognised by law in Nigeria at the moment: The Institute of Chartered Accountants of Nigeria (ICAN) and the Association of Nigeria Accountants (ANAN). The business sector of the economy is dominated by ICAN members while most ANAN members operate in Government ministries and parastatals. At the moment, ICAN has a faculty dedicated to continuous education in auditing. The challenges facing External Auditors are quite different from those of Internal Auditors. The ICAN present arrangement may not adequately address the needs of Internal Auditors who are faced with challenges of ever-changing technology. The need for local professionals to associate with and benefit from experiences of international members worldwide is felt more now than ever. The importance of internal control and Internal Auditors in corporate governance cannot be overemphasised. The position and functions of Internal

Auditors may be much more valuable to the existence of businesses in future than that of External Auditors.

9.6.0: Limitations of the Study

There are obvious restrictions on time and finances. These place constraints on the scope and coverage of the study. For instance, as mentioned in chapter 5, a longitudinal approach could have been a more robust alternative since the study involves technology that is ever changing. Data collected over a time frame could have proved more dynamic. In the same vein, observation and experimental techniques could have been employed. However the use of questionnaire to complement interviews provided a good alternative.

The distance of Nigeria from the United Kingdom also places some restrictions on data collection. The researcher used targeted sampling rather than random sampling in order to obtain required data within the set time frame of personal visits to Nigeria. Therefore there is a probability that non-use of random selection might have affected the research findings. However to mitigate these effects, the questionnaire was administered to 63 per cent of the total estimated population of 805 Internal Auditors in financial sector of the Nigerian economy.

Similar to the above is the nature of the research itself. A study probing the effectiveness of ICT in prevention and detection of fraud is not an attractive proposition that will easily elicit a positive response from the financial sector. In most cases, officials consider the issue of fraud and the way it is prevented and detected a secret of each entity and therefore not to be divulged. In addition to this, most organisations visited did not want to divulge the types of technology equipment they were using for fear that competitors may take advantage of it. The researcher mitigated this by resorting to targeted sampling as indicated above. The researcher relied on his former students at the MBA School former old colleagues to facilitate access.

Respondents chosen for the study, Internal Auditors, are very busy and often work with preset targets. The only basis to secure their participation in the study is

‘interest’. Their interest in the study was ensured through old contacts of the researcher as explained above. This also further explains why random sampling may not be appropriate in the circumstances. Apart from this, the opinions of Internal Auditors form the basis of evidence in the study. This may place some limitations on their responses as they can be regarded as an ‘interested party’ in internal control operations. Even though one of the advantages of the interview method is that it is more likely to produce data based on informants’ priorities, opinions and ideas nevertheless data is often based on what people ‘say’ rather than what they ‘do’.

9.7.0: Recommended Areas for Future Research

These suggestions are made for future research to complement and/or extend the frontier of knowledge concerning the present findings based on previously identified limitations and contributions of the study.

A future research work on the same topic but using a case study approach is not likely to produce the same result. Future research topics can be extended to explore the impact of ICT tools and techniques on independence and objectivity of Internal Auditors in different settings. The concept of independence is important to Internal Auditors for effective discharge of their responsibilities and assurance of effective internal control. A conceptual contribution to the debate on the independence and objectivity of Internal Auditors in different environments will be valuable. This is because culture may affect the impact of technology on Internal Auditors’ independence. A cross-sectional study on the subject area involving developing countries and developed countries will provide interesting findings as the impact of ICT tools and techniques on Internal Auditors’ independence in relation to line managers may be affected by culture and environment.

Nigeria, like most other countries is having problems with corporate governance issues, especially in the banking industry. The concern over corporate governance comes from the knowledge that good governance practices by banks and other organisations result in higher firms’ market value, higher profitability and lower cost of funds (Block, Jang and Kim, 2006; Claessen, 2006). Internal auditing function is regarded as one of the important pillars of corporate governance (Abiola, 2012). This study has identified ICT as a strong factor impacting Internal Auditors’

independence. Since the present study explored the impact of ICT on Internal Auditors who are regarded as important pillars of corporate governance, a future study can probe into the impact of ICT on the effectiveness of corporate governance.

Technology Effectiveness Planning and Evaluation Model has proved to be very useful in explaining issues involved in this study, especially those involving external contingencies. Future studies should further test the TEPEM model to determine its usefulness in ICT-based research apart from its relevance to internal control effectiveness.

REFERENCES

- AAA, (2001): "Fraud: A Review of Academic Literature" Special Issue on Fraud Detection: American Accounting Association Volume 24, No. 2 Winter
- Abbott, L.R., Parker, S., and Peters, G.F., (2001): "The Effectiveness of Blue Ribbon Recommendations in Mitigating Financial Misstatements: An Empirical Study" Paper Presented at Auditing Mid-year Conference, Houston, TX
- Abdolmohammadi, M and Boss, S.R (2010): "Factors Associated with IT Audits by the Internal Audit Function" Internal Journal of Accounting Information Systems 11 140-151
- Abdolmohammadi, M and Usoff, C. (2001): "A Longitudinal Study of Applicable Decision Aids for Detailed Tasks in a Financial Audit" International Journal of Intelligent Systems in Accounting, Finance and Management 10: 139-154
- Abdolmohammadi, M., and Shanteau J. (1991): Personal Attributes of Expert Auditors. Unpublished Paper prepared for a Special Issue on "Experts and Expert Systems".
- Abdolmohammadi, M., and Wright, A. (1987): "An Examination of the Effects of Experience and Task Complexity on Audit Judgments" The Accounting Review January, 1-13.
- Abdul-Gader, A. (1990): "End-user computing success factors: further evidence from a developing nation", Information Resources Management Journal, 3 (1); 2-13.
- Abiola, J.O. (2012): "Corporate Governance in Nigerian Banking Sector and Relevance of Internal Auditors" British Journal of Arts and Social Sciences Vol. 5 No. 1
- Abu-Musa A. A. (2008): "Information Technology and its Implications for Internal Auditing; An Empirical Study of Saudi Organisations" Managerial Auditing Journal, Vol.23 Iss5 pp435-466

Abu-Musa, A. A. (2006a): "Evaluating the Security Controls of CAIS in Saudi Organizations: the Case of Saudi Arabia", *The International Journal of Digital Accounting Research*, 6 (11); 25-64.

Abu-Musa, A. A. (2006b): "Exploring Perceived Threats of CAIS in Developing Countries: the Case of Saudi Arabia", *Managerial Auditing Journal*, 21(4); 387-407.

ACFE (2006): "ACFE Report to the Nation on Occupational Fraud and Abuse" Technical Report, Association of Certified Fraud Examiners, Texas.

Achimugu, P., Oluwagbemi, O and Afolabi, B. (2009): "Adoption of Information & Communication Technologies in Developing Countries: An Impact Analysis", *Journal of Information Technology Impact* Vol. 9 No. 1. Pp. 37-46.

Adams, D., Nelson, R. and Todd, P (1992): "Perceived Usefulness, Ease of Use and Usage of Information Technology: A Replication" *MIS Quarterly*, 16 (2), 227-247

Adams, M.B (1994): "Agency Theory and the Internal Audit" *Managerial Auditing Journal* Vol.9: Iss.8: pp8-12

Addison, S., (2001): "Risk and governance issues for ERP enterprise applications". *IS Control Journal* (4): 53-54.

Adebayo, A.O. (2004): "Developing a Theory of Auditing Behavior in the Electronic Business Environment": Unpublished Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy at Virginia Commonwealth University.

Adekunle, P.A., and Tella, A., (2008): "Nigeria SMEs Participation in Electronic Economy: Problems and the Way Forward" *Journal of Internet Banking and Commerce* December vol.12, no. 3

Adeseyoju, A. (2012): "Anti Money Laundering: FATF Moves Against WMDs" *Financial Action Task Force (FATF)* available @ <http://www.momentng.com/en/news/6879/anti-money-laundering-fatf-moves-against-wmds.html> accessed 20 august 2012

Adesina, A.A., and Ayo, C., (2010): “An Empirical Investigation of the Level of User’s Acceptance of E-Banking in Nigeria” *Journal of Internet Banking and Commerce* April Vol, 15 No. 1

Adesola, A., (2007). “Government’s Anti-Corruption Initiative: The Role of Computer Assisted Audit Techniques in Fraud Detection and Prevention” 37th Annual Accountants Conference, Abuja, Nigeria

Adewumi, O. (1986): “Fraud in Banks: An Overview” in *Frauds in Banks* Chartered Institute of Bankers, Nigeria.

Adewumi, O. (2004): “Perspective of Risk Management”, A Paper presented at Alliance of African Institutes of Bankers” Conference, Kampala, Uganda.

Adewunmi, O. (2009): “Finance, Entrepreneurship and Economic Development: The Missing Nexus” University of Lagos Inaugural Lecture Series

Adeyemi, A. (2008): “Adoption of e-Banking Services Rising in Nigeria” E-Banking Customer Survey Report, Trade InvestNigeria

Agboola, A.A. (2001): “Impact of Electronic Banking on Customer Services in Lagos, Nigeria” in *Ife Journal of Economics and Finance*, Department of Economics OAU, Ile-Ife, Nigeria, Volume 5, Numbers 1 and 2

Aggarwal, R., and Rezaee, Z. (1994): “Introduction to EDI Internal Controls” *IS Audit and Control Journal* Volume 11: P. 64-68

Aggarwal, R., Rezaee, Z., and Soni, R (1998): “Internal Control Considerations for Global Electronic Data Interchange”: *International journal of commerce and Management*. 8, pg. 71

Ahuja, Vijay (1997): “Secure Commerce on the Internet” New York: Academic Press

Ahunwan, B., (2002): “Corporate Governance in Nigeria” *Journal of Business Ethics*, Kluwer Academic Publishers, The Netherlands 37: 269-287

AICPA (1974): “Statement on Auditing Standards No 48: The effects of EDP on the Auditor’s Study and Evaluation of Internal Control” AICPA, New York, NY.

AICPA (1984): "Statement on Auditing Standards No. 48: The effects of Computer Processing on the Examination of Financial Statements" AICPA, New York, NY.

AICPA (1988): "SAS 55: Consideration of Internal Control in a Financial Statement Audit" AICPA, New York, NY.

AICPA (1995): "SAS 78: Consideration of Internal Control in a Financial Statement Audit: An Amendment to Statement of Auditing Standards No. 94" AICPA, New York, NY.

AICPA (2009): "The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit" AICPA, New York, NY

Ajzen, I. (1991) "The Theory of Planned Behavior", *Organizational Behavior and Human Decision Processes* 50, pp. 179-211.

Alali, F, Grant, H.G. and Miller K.C. (2008): "IT Control Deficiencies that Impact Financial Reporting" *International Auditing* Jul/Aug. 23, 4

Al-Gahtani, S. (2001): "The Applicability of TAM Outside North America: An Empirical Test in the United Kingdom", *Information Resources Management Journal*, Vol. 14 (3): 37-46

Allan, G. (2003): "A Critique of Using Grounded Theory as a Research Method" *Electronic Journal of Business Research Methods*, 2(1): 1-10

Allen, R.D.; Hermanson D.R.; Kozloski T.M and Ramsay R.J. (2006): "Auditor Risk Assessment: Insight from Academic Literature" *Accounting Horizons* 20(2): 157-177

Alles, M., A. Kogan, and M. Vasarhelyi (2004): "Restoring Auditor Credibility: Tertiary Monitoring and Logging of Continuous Assurance Systems" *International Journal of Accounting Information Systems* Vol. 5 No. 2 183-202 (July)

Alles, M.A.; Kogan, A; Vasarhelyi, M.A. (2002): "Feasibility and Economics of Continuous Assurance", *Auditing: A Journal of Practice and Theory*, vol. 21 (1): 123-138.

Alon, A and Dwyer, P. (2010): “The Impact of Groups and Decision Aid Reliance on Fraud Risk Assessment” *Managerial Research Review* Vol. 33 Issue 3 PP 240-256

Altricher, H; Posch, P and Somekh, B (1996): “Teachers Investigate Their Work: An Introduction to the Methods of Action Research” London Rutledge

Al-Twajjry, A., Brierley, J.A. and Gwilliam, D.R. (2004): “An Examination of the Relationship Between Internal and External Audit in the Saudi Arabian Corporate Sector”, *Managerial Auditing Journal*, 19(7): 929-944.

American Institute of Certified Public Accountants (AICPA), (2005): “Information Security Tops Technical Issues for 2005”. *Accounting Web* (January 4). Available at: <http://www.accountingweb.com/cgi-bin/item.cgi?id=100297>.

Ames, S. (2001): “Dot-Coms Making a Comeback?” *ZDNet News*. December 27 Available @ <http://zdnet.co.co/2100-1106-277420.html> accessed 6/09/2012

AMF (2004): “The Internal Control Systems: Reference Framework” Presentation of the Work Performed by the Working Group Set up by the AMF

Ammenwerth Elske, Iller Carola and Mansmann Ulrich (2003): “Can Evaluation Studies Benefit from Triangulation? A Case Study,” *International Journal of Medical Informatics* 70, 237-248.

Anderson, J., Lowe, D., and Reckers, P., (1993): “Evaluation of Auditor Decisions: Hindsight Bias Effects and the Expectation Gap” in J.E. McEnroe and S.C. Martens. 2001, ‘Auditors’ and Investors’ Perceptions of the ‘Expectation Gap’; *Accounting Horizons*, 15(4):345-358

Anderson, Ross (2001): “Security Engineering: A Guide to Dependable Distributed Systems”. New York Wiley

Apostolu, B.A., Hassell, J.M., Webber, S.A., and Summers, G.E., (2001): “The Relative Importance of Management Fraud Risk Factors”. *Behavioral Research in Accounting* (May): 1-24.

Arena, M., Arnaboldi, M. and Azzone, G. (2006): "Internal Audit in Italian Organizations: A Multiple Case Study", *Managerial Auditing Journal*, 21 (3): 275-292.

Arnold, V., and Sutton, S.G., eds (2002): "Research Accounting as an Information System Discipline". Sarasota, FL: American Accounting Association.

Ashamu S.O. and Abiola J. O. (2012): "The Impact of Global Financial Crisis on Banking Sector in Nigeria" *British Journal of Arts and Social Sciences*: Volume 4 No. 2

Ashton, R.H (1990): "Pressure and Performance in Accounting Decision Settings: Paradoxical Effects of Incentives, Feedback, and Justification" *Journal of Accounting Research*, Vol.28 Supplement pp148-180

Attrichter, H., Fieldmar A., Posch, P., and Somekh, B (2008): "Teachers Investigate their Work; An Introduction to Action Research Across the Professions", Routledge P147 (2nd edition).

Audit Commission (1987): "Survey of Computer Fraud and Abuse", H.M.S.O. Auditing Practices Committee.

Auditing Practices Board (APB) (2006): *Fundamental Principles of Auditing*

Awad, E.M (1988): "Management Information Systems: Concept, Structure and Applications" California: The Benjamin/Cummings Publishing Company Inc

Ayo, C.K., Adebisi A.A., Fatudimu I.T., and Ekong O.U. (2008): "Framework for e-Commerce Implementation: Nigeria a Case Study", *Journal of Internet Banking and Commerce*, August 2008, Vol.13, no.2

Bae, B., and Ashcroft, P., (2004): "Implementation of ERP Systems: Accounting and Auditing Implications". *The Information Systems Control Journal* (4): 43-48

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 N.A., and Vendirzyk, P.V., (2000): "The Changing Role of IS Audit Among the Big Five US-Based Accounting Firms" *Information Systems Control Journal* 5: 33-37

Bailey, A.D., Jr., Grambling, A.A., and Ramamoorti, S., eds (2003): "Research Opportunities in Internal Auditing" Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation.

Balkaran L. (2008): "Two Sides of Auditing: Back to Basics" *Internal Auditing*, August.

Bandura, A. (1986). "Social Foundations of Thought and Action: A Social Cognitive Theory". Englewood, NJ: Prentice-Hall.

Banker, R.D; Chang, H and Kao, Y. (2002): "Impact of Information Technology on Public Accounting Firm Productivity" *Journal of Information Systems* 16(2): 209-223

Barki, H., and Hartwick, J., (1989): "Rethinking the Concept of User Involvement" *MIS Quarterly*. 13(1). 53-63.

Barki, H., and Hartwick, J., (1994): "Measuring User Participation, User Involvement and User Attitude" *MIS Quarterly* 18(1) 203-225

Barnes, D and Hilton, M (2004): "Performance Measurement in e-Business in Remenyi, D (ed) *Proceedings of the 11th European Conference on Information Technology Evaluation*, Amsterdam, Netherlands, 11-12 Nov Reading MCIL: 43-50

Baronas, A.M.K. and Louis, M.R. (1988): "Restoring a Sense of Control During Implementation: How User Involvement Leads to System Acceptance". *MIS Quarterly*. 12(1) 111-124

Baroudi, J.J., Olson, M.H., and Ives, B. (1986): "An Empirical Study of the Impact of User Involvement on System Usage and Information Satisfaction" *Communications of the ACM*. 29(3) 232-238

Bartels, A., Pohlmann, T., Brown, K., and Young, G. O. (2006): "Security Environment Tops the List of Enterprises Critical Priorities on a Global Basis" *Forrester Research Report Executive Summary*. Available @

<http://www.forrester.com/research/document/exerpt/0.7211.39445.00.html> accessed 06/09/2012

Bastol, K.M., and Martin, D. C., (1994): “Management” Second Edition, New York Mc Graw- Hill Inc

Beasley, M., and Salterio, S., (2001): “The Relationship Between Board Characteristics and Voluntary Improvements in the Capability of Audit Committees to Monitor” *Contemporary Accounting Research* 18 (4): 539-70

Beattie, V and Fearnley, S. (2002): “Auditor Independence and Non-Audit Services: A Literature Review”, Institute of Chartered Accountants in England and Wales, London.

Beckinsale M. and Ram M (2006): “Delivering ICT to Ethnic Minority Businesses: An Action Research Approach”. *Environment and Planning C: Government and Policy* 24(6), pp847 – 867.

Bennett, M. J. (1986): “A Developmental Approach to Training for Intercultural Sensitivity” *International Journal of Intercultural Relations*, 10, 179-195. doi:10.1016/0147-1767(86)90005-2

Bermudez, J. M., Ayuso, M., Gomez, F.J., and Vazquez, A. (2008): “Bayesian Dichotomous, Model with Asymmetric Link for Fraud in Insurance” *Insurance: Mathematics and Economics* 42 (2) 779-786

Bierstaker, J.L, Brody, R.G. and Pacini, C. (2006): “Accountants’ Perceptions Regarding Fraud Detection and Prevention Methods”, *Managerial Auditing Journal*, 21(5): 520-535.

BIS, (2012): “The 2011 Skills for Life Survey: A Survey of Literacy, Numeracy and ICT Levels in England” Department of Business Innovation and Skills Paper 81

Blili, S., Raymond, L., and Rivard, S., (1998): “Impact of Task Uncertainty, End-User Involvement, and Competence on the Success of End-User Computing” *Information & Management*. 33(3), 137-153

Blocher, E., (1993): "The Role of Analytical Procedures in Detecting Management Fraud". Montevale, NJ: Institute of Management.

Block, B.S: Jang, H and Kin, W (2006): "Does Corporate Governance Predict Firms Market Values? Evidence from Korea" *Journal of Law, Economics and Organisation* 22 (2): 3-13

Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committee (BRC) 1999: Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees. New York, NY: New York Stock Exchange and National Association of Securities Dealers.

Boje, D., Gephart, R and Thatchenkary, T. (1996): "Postmodern Management and Organisation Theory" Newbury Park CA: Sage

Boland, L. A. (1979) "A critique of Friedman's Critics" *Journal of Economic Literature*, June 17, 503-22

Bologna, G., and Lindquist, R., (1995): "Fraud Auditing and Forensic Accounting" John Wiley & Sons, New Jersey

Bolton R.J and Hand D.J (2002): "Statistical Fraud Detection: A Review" *Statistical Science* 17 (3) 235-255

Bonchi, F., Giannotti, F., Mainetto, G., and Pedreschi, D. (1999): "A Classification-Based Methodology for Planning Audit Strategies in Fraud Detection" *Proceedings of the Fourth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, NY, USA

Bonner, S.E., Libby, R. and Nelson, M.W.(1996) "Using Decision Aids to Improve Auditors' Conditional Probability Judgements" *The Accounting Review*, 71 (2): 221-240

Boritz, E., (2002): "Information System Assurance" in V. Arnold, S. G. Sulton (eds) *Research Accounting as Information System Discipline*, American Accounting Association, Sarasota, pp. 231-256

Bort, R., and Bielfeldt, G. K., (1995): "Handbook of EDI" Boston MA: Warren, Gorham and Lamont

Botosan, C.A. and Harris, M.S. (2000): "Motivations for a Change in Disclosure Frequency and its Consequences: an Examination of Voluntary Quarterly Segment Disclosures", *Journal of Accounting Research*, vol.38 No. 2, pp.329-53.

Bracken, S. (2010): "Discussing the Importance of Ontology and Epistemology Awareness in Practitioner Research" *Worcester Journal of Learning and Teaching*, Issue 4

Bradford, M., and Florin, J. (2003): "Examining the Role of Innovation Diffusion Factors on the Implementation Success of Enterprise Resource Planning Systems" *International Journal of Accounting Information Systems*, 4(3), 205-225.

Brady, M., and Postal, A.D., (2005): "Tweaking SOX: Regulators Ease up on Compliance Cost" *National Underwriter Property and Casualty Risk & Benefits Management Edition* (May 23): 31-32.

Braun, Robert L., and Davis, Harold E., (2003): "Computer-Assisted Audit Tools and Techniques: Analysis and Perspectives" *Managerial Auditing Journal*: 2003;18, 9

Brause, R., Langsdorf, T., and Hepp, M., (1999): "Neural Data Mining for Credit Card Fraud Detection" *Proceedings of the 11th IEEE International Conference on Tools with Artificial Intelligence*, Chicago, IL. USA

Brockett, P.L., Derrig, R.A., Golden, L.L., Levine, A and Alpert, M (2002): "Fraud Classification Using Principal Component Analysis of RIDITs" *The Journal of Risk and Insurance* Volume 693: 341-371

Brockett, P.L., Xia. X., and Derrig, R.A. (1998): "Using Kononen's Self-Organising Feature Map to Uncover Automobile Bodily Injury Claims Fraud" *The Journal of Risk and Insurance* 65 (2) 245-274

Brown, D.A., (1999): "Public Accounting at a Crossroads" Available on the Web at <http://www.osc.gov.on.ca/en/about/>

- Brown, S., Massey, A., Montoya-Weiss, M., and Burkman, J., (2002): "Do I Really have to? User Acceptance of Mandated Technology" *European Journal of Information Systems* 11: 283-95
- Bryman, A. (2006): "Integrating Quantitative and Qualitative Research: How is it Done" *Qualitative Research*, 6(1); 97-113.
- Burns, T., and Skilker, G.M., (1966) "The Management of Innovation" (Second Edition) London: Tavistock
- Burton, R.N., (2000) "Discussion of Information Technology-Related Activities of Internal Auditors", *Journal of Information Systems*, 14 (1): 57-60, Supplement.
- Caglio, A.(2003): "Enterprise Resource Planning Systems and Accountants: Towards Hybridisation"? *The European Accounting Review*
- Camp, L.J, and Sirbu, M., (1997): "Critical Issues in Internet Commerce. IEEE" *Communications Magazine* 35: may, 58-62
- Canadian Institute of Chartered Accountants (CICA) (2003): "Using Ethical Hacking Technique to Assess Information Security Risk" Toronto, ON: The Canadian Institute of Chartered Accountants.
- Cannon, D.M. and Crowe, G.A. (2004), "SOA Compliance: will IT Sabotage your Efforts?", *The Journal of Corporate Accounting and Finance*, 15(5): 31-37.
- Caplan, D., and Emby, C., (2003): "An Investigation of Whether Outsourcing the Internal Audit Function Affects Internal Controls" Working Paper Iowa State University and Simon Fraser University.
- Carcello, J.V., Hermanson, D.R., and Neal, T.L., (2002): "Disclosure in Audit Committee Charters and Reports" *Accounting Horizons* (December): 219-304.
- Carcello, J.V., Hermanson, D.R., and Raghunandan, K., (2005): "Factors Associated with U.S Public Companies' Investment in Internal Auditing," *Accounting Horizons*, 19(2), 69-84.

Carey, P., Subramaniam, N., and Ching, K.C.W (2006): “Internal Audit Outsourcing in Australia” *Accounting and Finances* 46(1): 11-30

Carr, J.G. (1985): “Summary and Conclusions. IT and the Accountant” Aldershort: Gower Publishing Company Ltd/ ACCA

Cash, J.I., Jr., Bailey, A.D., Jr., and Whiston, A.B. (1977): “A Survey of Techniques for Auditing EDP Based Accounting Information Systems” *The Accounting Review* (October): 812-831.

Castanheira, N; Rodrigues, L.L and Craig, R. (2010): “Factors Associated with the Adoption of Risk-based Internal Auditing” *Managerial Auditing Journal* Vol. 25 Iss:1 pp79-98

Casualty Actuarial Society Framework (2003): “Enterprise Risk Management”

Central Bank of Nigeria (CBN) (2009) “Corporate Governance Code for Banks and Other Financial Institutions” Available at <http://www.cenbank.org/>

Central Bank of Nigeria/Nigeria Deposit Insurance Corporation (1995) “Distress in the Nigerian Financial Services Industry”, A CBN/NDIC Collaborative Study, Lagos, Nigeria.

Chan H; Lee, R; Dillon, T and Chang E (2001): “E-Commerce Fundamentals and Applications” Chichester, John Wiley

Chan, C. (2004): “Sarbanese-Oxley: The IT Dimension”, *The Internal Auditor*, 61(1): 31-33.

Chandra, A., and Calderon, T.G., (2003): “Toward Biometric Security Layer in Accounting Systems”. *Journal of Information Systems* (Fall): 51-70.

Chapman, A and Russell, G. S., (2001): “Controlling Financial Services Fraud” *Trends and Issues*, February, No. 189

Cheung, B.Y.H., and Lam, I.S.K (1995): “Application of EDI in Hong Kong: Survey Evidence on Accountants” *Proceedings of Pan Pacific Conference on IS*, June 29th – July 2nd Singapore 448-456

Chiejine, F.C., (2010): “Corporate Governance in Nigeria Banking System” Unpublished Msc Theses, University of Pennsylvania.

Choo, F. (1989): “Cognitive Scripts in Auditing and Accounting Behavior”. *Accounting Organisations and Society* 14 (5-6); 481-493.

Christ, M. Y. (1993): “Evidence on the Nature of Audit Planning Problem Representations: An Examination of Auditor Free Recalls” *The Accounting Review* 68(2): 304-322.

Christopher, J., Sarens, G. and Leung, P. (2009): “A Critical Analysis of the Independence of the Internal Audit Function: Evidence from Australia”, *Accounting, Auditing and Accountability Journal*, Vol. 22 No 2, pp200-220

Church, B.K., and Schneider, A., (1995): “Internal Auditors’ Memory for Financial Statement Errors”. *Behavioral Research in Accounting* 1: 17-36.

Chuttur, M.Y. (2009): “Overview of the Technology Acceptance Model: Origins, Developments and Future Directions” *Indiana University, USA Sprouts: Working Papers on Information Systems*, 9(37)

Claessens, S., (2006): “Corporate Government and Development” *The World Bank Research Observer*, 21(1) 91-1

Clarke, R. V. (1999): “Hot Products. Understanding, Anticipating and Reducing the Demand for Stolen Goods”, *Police Research Series Paper 98* London: Home Office

Clough, B., and Mungo, P., (1992): “Approaching Zero: Data Crime and the Computer Underworld” London: Faber and Faber

COBIT, (1998): “Information Systems Audit and Control Foundation” *Control Objectives for Information and Related Technology (ISACF, Rolling Meadows, IL.*

Coderre, D. (2005): “Continuous Online Auditing” *The Internal Auditor* 57 (4): 25-27

Cohen, J.(1998): “Statistical Power Analysis for the Behavioral Sciences” (2nd Edition) Hillsdale, NJ: Erlbaum

Cohen, J., Krishnamoorthy, G., and Wright, A (2002): “Corporate Governance and the Audit Process” Contemporary Accounting Research Vol. 19 No. 4 (Winter) pp.573-594

Cohen, L., and Manion, L., (2000): “Research Methods in Education”. Routledge P.254 (5th editions)

Colbert, J. (1989): “The Effect of Experience on Auditors’ Judgments” Journal of Accounting Literature. 8: 137-149

Colbert, J.L., and P.L. Bowen (2005): “A Comparison of Internal Controls” Available at:
[Http://www.isaca.org/PrinterTemplate.cfm?section+HomeandCONTENTID=8174andTEMPLATE=/](http://www.isaca.org/PrinterTemplate.cfm?section+HomeandCONTENTID=8174andTEMPLATE=/)

Collier, P., and Gregory, A., (1999): “Audit Committee Activity and Agency Costs” Journal of Accounting and Public Policy 18 (Winter):311-32

Collier, P.A. (1984): “The Impact of IT on the Management Accountant”, London: ICMA

Collins (1995): “English Dictionary” Free Online edition

Collins K.M.T., and O’Cathain A., (2009) “Ten Points About Mixed Methods Research to be Considered by the Novice Researcher” International Journal of Multiple Research Approaches 3: 2-7

Collins, K. M. T., Onwuegbuzie, A. J. and Sutton, I. L. (2006): “A Model Incorporating the Rationale and Purpose for Conducting Mixed-Methods Research in Special Education and Beyond, Learning Disabilities”: A contemporary Journal, 4(1): 67-100.

Committee of Sponsoring Organizations (COSO) (2004a): “Enterprise Risk Management-Integrated Framework: Executive Summary Framework”. Jersey City, NJ: AICPA

Coombs, R., Knights, D., and Willmott, H., (1992): "Culture, Control and Competition: Towards a Conceptual Framework for the Study of Information Technology in Organizations". *Organization Studies*, 13 (1): 51-72

Cooper, D.R., and Schindler, P.S., (1998): "Business Research Methods" 6th Edition

Cooper, R.B., and Zmud, R.W., (1990): "Information Technology Implementation Research: A Technological Diffusion Approach" *Journal of Institute for Operations Research and the Management Sciences* vol. 36 No.2 Feb. 1990

Coram, P., Ferguson, C., and Moroney, R., (2006): "The Value of Internal Audit in Fraud Detection" Department of Accounting and Business Information Systems, Melbourne 3010, Australia.

COSO (1992): "Internal Control: Integrated Framework" Committee of Sponsoring Organizations of the Treadway Commission, New York, NY.

COSO (1994): "Committee of Sponsoring Organisation of Treadway Commission." *Internal Control-Integrated Framework* New York: AICPA

COSO (2004), "Enterprise Risk Management – Integrated Framework", Committee of Sponsoring Organisations, available at: www.coso.org/Publications/ERM/COSO_ERM_Executive_Summary.pdf (accessed 19 January 2012)

Covaleski, M.A., and Dirsmith, M.W., (1983): "Budgeting as a Means for Control and Loose Coupling", *Accounting, Organizations and Society*, Vol. 8 No. 4 pp.323-40

Coxon, A.P., (2005): "Integrating Qualitative and Quantitative Data: What does the User Need?" in Denscombe, M. (2007) *The Good Research Guide*; Open University Press 3rd edition.

Cravens, K., Oliver, E., and Ramamoorti, S., (2003): "The Reputation Index: Measuring and Managing Corporate Reputation". *European Management Journal* 21 (2): 201-212.

Creswell, J.W., (2009): "Research Design; Qualitative, and Mixed Methods Approaches", Sage Publications 3rd ed.

Creswell, J.W., Plano, C.V.L., Gutmann, M.L., and Hanson, W.E., (2003): "Advanced Mixed Methods Research Designs" In A. Tashakkori and C. Teddlie (eds) Handbbok of Mixed Methods in Social and Behavioural Research Thousand Oaks, CA: Sage Publications: pp 209-240

Crites, S., (2008): "Best Practices in Accounting Online Cash Management Security" Commercial Lending Review New York Aspen Publishers Vol. 23, 3 p.21-25

Crowther, D., and Lancaster, G., (2009): "Research Methods: A Concise Introduction to Research in Management and Business Consultancy" (Second Edition) Oxford Elsevier Butterworth: Heinemann

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 104-121.

Curtis, M.B., and Wu, F.H., (2000): "The Components of a Comprehensive Framework of Internal Control". The CPA Journal (March): 64-66.

Curtiss, R.H., (1995): "Four Years after Massive War Expenses Saudi Arabia get its Second Wind" The Washington Report on Middle East Affairs, September, 48-52.

D'Aquila, J. (1998): "Is the Control Environment Related to Financial Reporting Decisions"? Managerial Auditing Journal 13(8), 472-478

Das, H., (1986): "Organisational and Decision Characteristics and Personality as Determinants of Control Actions: A laboratory Experiment." Accounting, Organisations and Society, 11(3), 215-231

Davey, N., Field, S., Frank, R., Berseon, P., and Mcaskie, G., (1996): "The Detection of Fraud in Mobile Phone Networks" Neural Network World, Vol.64: 477-484

David, J., and Solomon, I. (1989): "Experience, Expertise, and Expert-Performance Research in Public Accounting". Journal of Accounting Literature 8: 150-164.

David, M., and Sutton, C., (2004): "Social Research: the Basics" Thousand Oaks, CA: Sage

Davis, F. (1989): "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology" *MIS Quarterly*, 13(3), 319-40

Davis, F., (1985): "A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results" Being a Thesis Submitted to the Sloan School of Management, MIT in partial fulfilment of the Degree of PhD in Management On-line.

Davis, F.D.; Bagozzi, R.P. and Warshaw, P.R. (1989): "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models" *Managerial Science Journal* 35(8):982-1002

De Vaus, D. A. (1996): "Surveys in Social Research". Fourth Edition, London: UCL

De Vaus, D.A. (1991): "Surveys in Social Research". London; North Sydney, NSW, Australia: UCL. Press: Allen and Unwin.

Dearing, B. (1990): "The Strategic Benefits of EDI" *The Journal of Business Strategy*, January/February 4-6

Debreceeny, 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* 20(6):605-18

Debreceeny, R., and Gray, G (2010): "Data Mining Journal Entries for Fraud Detection: An Exploratory Study" *International Journal of Accounting Information Systems* pp. 157-181

Denscombe, M. (2008): "The Good Research Guide" 3rd. edition, Open University Press.

Denzin, N. K., (1970): "Strategies of Multiple Triangulation", in N.K. Denzin (ed). *The Research Act in Sociology: A Theoretical Introduction to Sociological Method*. New York: McGraw-Hill, pp. 297-313.

Denzin, N. K., (1989): "The Research Act", 3rd edition Englewood Cliffs, NJ: Prentice Hall.

Denzin, N.K., (1978): "Sociological Methods: A Source Book" N.Y: McGraw Hill Second Edition

Derrig, R.A and Ostaszewski, K.M., (1995): "Fuzzy Techniques of Pattern Recognition" The Journal of Risk and Insurance, Volume 623: 447-482

Deshmukh, A., and Talluru, I., (1998): "A Rule-Based Fuzzy Reasoning System for Assessing the Risk of Management Fraud" International Journal of Intelligent Systems in Accounting, Finance and Management 7 (4) 223-241

DeVellis, R.F. (2003): "Scale Development: Theory and Applications" (2nd edn) Thousand Oaks, California; Sage

DeZoort, F.T., and Salterio, S., (2001): "The Effects of Corporate Governance Experience and Financial Reporting and Audit Knowledge of Audit Committee Members' Judgements, Auditing": A Journal of Practice and Theory 20 (September):31-47

Dillard, J.F., and Yuthas, K., (2002): "Ethics in Action: An Application of Structuration Theory in Professional Service Firms" Proceedings of Critical Perspective on Accounting Conference, April 25-27, New York, US.

Dittenhofer, M. (2001): "Internal Audit Effectiveness: an Expansion of Present Methods" Managerial Auditing Journal,16 (8); 435-450.

Doll, W.J., and Torkzadey, G., (1991): "A Discrepancy Model of End-User Involvement" Management Science, 35(10). 1151-1171.

Dorronsoro, J.R., Ginel, F., Sanchez, C., and Cruz, C.S., (1997): "Neural Fraud Detection in Credit Card Operations" IEEE Transactions on Neural Networks 8(4): 827-834

Duncan, J., Flesher, D., and Stocks, M. (1999): "Internal Control Systems in US Churches. An Examination of the Effects of Church Size and Denomination on

Systems of Internal Control” Accounting, Auditng and Accountability Journal, 12(2), 142-163

Easterby-Smith, M., Thorpe, R., and Lowe, A., (2002): “Management Research: An Introduction” 2nd Edition, Sage Publication, London

Economic and Financial Crimes Commission (EFCC) (2012) Publication of Media and Publicity departments Available on Web at <http://www.efcc.org> accessed on 4-5-2012

Edstrom, A., (1977): “User Influence and the Success of MIS Projects: A Contingency Approach” Human Relations 30(70) 589-607.

Elliott, R., (1997): “Assurance Service Opportunities: Implications for Academia” Accounting Horizons 11 (4): 61-74

EL-Masry, E., and Reck, J.L., (2008): “Continuous Online Auditing as a Response to the Sarbanes-Oxley Act” Managerial Auditing Journal Volume 23 No. 8.

Ernst and Young (2006): “9th Global Fraud Survey” Ernst and Young Publication

Estes, R., and Reames, D. D. (1990): “Effects of Personal Characteristics on Materiality Decisions: A Multivariate Analysis” Accounting and Business Research. Vol. 18, No. 72 pp. 291-296.

Estevez, P., Held, C., and Perez, C. (2006): “Subscription Fraud Prevention in Telecommunications Using Fuzzy Rules and Neural Networks” Expert Systems with Applications Volume 31: 337-344

Ezawa, K., and Norton, S.W. (1995): “Knowledge Discovery in Telecommunications Services Data Using Bayesian Network Models 100-105 in Fayyad and Uthurusamy 1995

Ezzamel, M., (1990): “The Impact of Environmental Uncertainty, Managerial Autonomy and Size on Budget Characteristics” Management Accounting Research, 1, 181-197

Fadzil, F.H., and Jantan, M. (2005) “Internal Auditing Practices and Internal Control System”, *Managerial Auditing Journal*, 20(8): 844-866.

Fan, W. (2004): “Systematic Data Selection to Mine Concept-Drifting Data Streams” *Proceedings of the 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Seattle, WA, USA

Fanning, K.M and Cogger, K.O (1998): “Neural Network Detection of Management Fraud Using Published Financial Data” *International Journal of Intelligent Systems in Accounting, Finance and Management* 7 (1) 21-41

FATF (1989; 2001): Committee of G-7 Countries. Financial Action Task Force

Fichman, R.G., (1992): “Information Technology Diffusion: A Review of Empirical Research” *Proceedings of the 13th International Conference on Information Systems (ICIS)*: 195-206

Fischer, M.J. (1996): “Realizing the Benefit of a New Technology as a Source of Audit Evidence: An Interpretive Study” *Accounting, Organisation and Society* 21(2); 219.

Fisher, J. (1998): “Contingency Theory, Management Control Systems and Firm Outcomes: Past Results and Future Directions” *Behavioral Research in Accounting*, 10, 47-64

FITC (1992): “Fraud in Banks” Financial Institutions Training Centre FITC. Lagos, Nigeria.

FITC (2004): “Workshop on Fraud Detection, Prevention and Control” Financial Institutions’ Training Centre FITC, Lagos.

Fox, C., and Zonneveld, P., (2004): “IT Control Objectives for Sarbanes-Oxley: The Importance of IT Design, Implementation, and Sustainability of Internal Control Over Disclosure and Financial Reporting” Rolling Meadows, IL: Guidance document: Information technology Governance Institute.

Franz, C.R., and Robey, D., (1986): “Organisational Context, User Involvement, and the Usefulness of Information Systems”. *Decision Sciences*. 17(3). 329-356.

Frazer, L. and Lawley, M. (2000): "Questionnaire Design and Administration: A Practical Guide", Milton, QLD: John Wiley and Sons

Friedlob, G.T., Plewa, F.J., Schleifer, L.L.F., Schou, C.D., (1997): "An Auditor's Guide to Encryption". Altanote Springs, FL: The Institute of Internal Auditors Research Foundation.

Fung, A., Graham, M., and Weil, D. (2007): "Full Disclosure; The Perils and Promise of Transparency" Cambridge University Press

Gelderman, Maarten (2002): "Task Difficulty, Task Variability and Satisfaction With Management Support Systems" Information and Management 39: 593-604

Gelinas, U., Sutton, S., and Oran, A (1999): "Accounting Information Systems", South-Western College Publishing, Cincinnati, OH.

Gendron, Y., J. Bedard, and M.Gosselin (2004): "Getting Inside the Black Box: A Field Study of Practices in 'Effective' Audit Committees". Auditing: A Journal of Practice and Theory (Spring): 153-171.

Gephart, R.P. (1993): "The Textual Approach: Risk and Blame in Disaster Sense Making" Academy of Management Journal 36(6): 1465-1514

Gephart, R.P. (1999): "The Textual Approach: Risk and Blame in Disaster Sense Making", University of Texas, Arlington

Gibbs, S., Sequeira, J., and White, M.M (2007): "Social Networks and Technology Adoption in Small Business" International Journal of Globalisation and Small Business, Vol.2; No. 1 pp.66-87

Giddens, A., (1984): "The Constitution of Society: Outline of the Theory of Structuration": University of California Press

Ginzberg, M.J., (1979): "A Study of the Implementation Process". TIMS Studies in the Management Sciences. 13. 85-102

Glaser, B and Strauss, A (1967): "The Discovery of Grounded Theory", London; Weidenfield and Nicolson 1st ed.

Glaser, B and Strauss, A (1993): “The Discovery of Grounded Theory” London; Weidenfield and Nicolson 4th ed.

Gloeck, J.D and Jager, H. (2005): “Fraud Profiles of Public Sector Institutions in South Africa” Southern African Journal of Accountability and Auditing Research Vol.6, PP 49-65

Glover S.M., and Romney M.B., (1998): “Software: The Next Generation –how and if- Internal Audit Shops are Employing Emerging Technologies” International Auditing Journal 55(4):47-55

Glover, S., Prawitt D., and Spilker B., (1997): “Decision Aids and Users Behaviour: Implications for Knowledge Acquisition and Inappropriate Reliance” Organisational Behaviour and Human Decision Process 72 (2): 232-255

Glover, S.M., Prawitt, D.F., and Spilker, B.C. (1996): “The Influence of Decision Aids on User Behaviour: Implications for Knowledge Acquisition and Inappropriate Reliance” In L. Swinney, 1999, ‘Consideration of the Social Context of Auditors’ Reliance on Expert System Output During Evaluation of Loan Loss Reserves’: International Journal of Intelligent Systems in Accountiung, Finance and Management 8: 199-213

Godwin, J. (2004), “A Comparison of Internal Audit in the Private and Public Sectors”, Managerial Auditing Journal, 19 (5): 640–650.

Godwin, Jenny and Yeo, T.Y., (2001): “Two Factors Affecting Internal Audit Independence and Objectivity: Evidence from Singapore” International Journal of Auditing 5: 107-125

Godwin-Stewart, J., and Kent, P. (2006) ‘The Use of Internal Audit by Austrailian Companies’, Managerial Auditing Journal, 21(1): 81-101.

Goldsmith, R.W. (1955). “Financial Structure and Economic Growth in Advanced Countries, Capital Formation and Growth”, Princeton, NJ: Princeton University Press.

Gorman, J.F., and Hargadon, J.M. (2005): "Accounting Futures: Healthy Markets for a Time-honored Profession". *Journal of Financial Service Professionals* (January): 74-79.

Grabski, S.V., (1986): "Auditor Participation in Accounting Systems Design: Past Involvement and Future Challenges. *Journal of Information Systems* (Fall): 3-23.

Grabski, S.V., Reneau, J.H., West, S.G., (1987). "A Comparison of Judgement, Skills, and Promoting Effects Between Auditors and Systems Analysts". *MIS Quarterly*, 11(2), 151-161.

Gramling, A.A., and Myers, P.M., (2006): "Internal Auditing's Role in ERM", *Internal Auditors*, Vol.63 No. 2. Pp.52-8

Gramling, A.A., Maletta, M.J. Schnelider, A. & Church, B.K. (2004) "The Role of Internal Audit Function in Corporate Governance: A Synthesis of the Extant Internal Auditing Literature and Directions for Future Research" *Journal of Accounting Literature*, Vol.23, pp. 194-244

Grant, A., David, F., and Grabosky, P., (1997): "Child Pornography in the Digital Age", *Transitional Organised Crime*, 3(4): 171-88

Graziano, A. M. and Raulin, M. I. (2004): "Research Methods, Process of Inquiry". Fifth Edition, Pearson. USA

Green, P., and Choi, J.H., (1997): "Assessing the Risk of Management Fraud Through Neural Network Technology" *Auditing: A Journal of Practice and Theory* 16 (1) 14-28

Greene, J. C., Caracelli, V.J. and Graham, W.F. (1989): "Towards a Conceptual Framework for Mixed-Method Evaluation Designs", *Educational Evaluation and Policy Analysis*, 11(3); 255-74.

Guba, E.G., and Lincoln Y.S., (1994): "Competing Paradigms in Qualitative Research"

Gullkvist, B., (2003): "Adoption and Impact of e-Accounting" *Frontier of e-Business Research* 536-544

Hadden, L.B., DeZoort, F.T., and Hermanson, D.R.(2003): "IT Risk Oversight: the Roles of Audit Committees, Internal Auditors", *Internal Auditing* 18(6): 28-31

Halfpenny, P., (1997): "The Relationship Between Quantitative and Qualitative Social Research, *Bulletin de Methodologie Sociologique*, 57: 49-64

Hamaker, S., (2004): "Principles of IT Governance". *The Information Systems Control Journal* 2: 47-50.

Hammersley, M., (1996): "The Relationship Between Qualitative and Quantitative Research: Paradigm Loyalty Versus Methodological Eclecticism," in J.E.T Richardson (ed) *Handbook of Qualitative Research Methods for Psychology and the Social Sciences*. Leicester: British Psychological Society, pp. 159-74

Handscombe, K., (2003): "Continuous Online Auditing: Practical Experiences" *Proceedings of the European Auditing Research Network Symposium, Manchester, United Kingdom*.

Hangen, S. and Stein J.R. (1999): "Identifying and Controlling Computer Crime and Employee Fraud" *Journal of Industrial Management and Data System*, 99 (8): 340-4

Hannye, L.G., (1977): "Auditors and DP'ers Benefits from Association in the Development Process" *The Internal Auditor* 34(6). 67-70

Hansen, J.V., and Hill, N. C., (1989): "Control and Audit of Electronic Data Interchange" *MIS Quarterly* Vol. 3 No. 4 PP 403-414

Hargraves, K., Lione, S.B., Shackelford, K.L., and Tilton, P.C., (2003): "Privacy Assessing the Risk" Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation.

Harrington, L.J., (1997): "A New Vision" *Internal Auditor*, Vol.54 No.2, pp26-31

Harrington, L.J., and Shepard, M., (1996): "Career Strategies for Turbulent Times" *Internal Auditors* Vol.53 No.3, pp48-52

Hart, P., and Saunders, C. (1997): "Power and Trust: Critical Factors in the Adoption and Use of Electronic Data Interchange" *Organisational Science* (8:1) PP 23-42

Hartwick, J., and Barki, H., (1994): “Explaining the Role of User Participation in Information System Use” *Management Science*. 40(4) 440-465.

Hasan, B., (2007): “Examining the Effects of Computer Self-Efficacy and System Complexity on Technology Acceptance”. *Information Resources Management Journal* Vol. 20, Issue 3

Hashim, J., (2007): “Information Communication Technology (ICT) Adoption Among SME Owners in Malaysia” *International Journal of Business and Information*. Vol. 2 No. 2

Hass, S., Abdolmohammadi, M.J. and Burnaby, P. (2006): “The Americas Literature Review on Internal Auditing” *Managerial Auditing Journal*, Vol. 21 No.8 pp. 835-844

He, H; Wang, J; Graco, W., and Hawkins, S., (1997): “Application of Neural Networks to Detection of Medical Fraud” *Expert Systems with Applications* 13 (4) 329-336

Helms, G.L. (2002): “Traditional and Emerging Methods of Electronic Assurance”, *The CPA Journal*, vol. 72 (3): 26-31.

Henderson, S.A., (2002): “IS Auditor Participation in Developing Electronic Commerce Systems: The Impact on System Success” Unpublished dissertation Alabama, May 11

Hermanson, D., Hill, M.C., and Ivancevich, D.M., (2000): “Information Technology –Related Activities of Internal Auditors” *Journal of Information Systems*.

Hermanson, D.R., and Rittenberg, L.E., (2003): “Internal Audit and Organizational Governance Research Opportunities in Internal Auditing” Edited by A.D.

Hermanson, D.R., Hill, M.C. and Ivancevich, D.M. (2006): “Information Technology-Related Activities of Internal Auditors” *Journal of Information Systems*, 14(1): 39-53, Supplement.

Hermanson, D.R., Hill, M.C. and Ivancevich, D.M. (2010): “Reply to Discussion of Information Technology-Related Activities of Internal Auditors” Journal of Information Systems, 12(1): 29-35, Supplement.

Hilas, C.S., Mastorocostas, P.A (2008): “An Application of Supervised and Unsupervised Learning Approaches to Telecommunications Fraud Detection” Knowledge-Based Systems, Vol.21 (7):721-726

Hirst, D.E., and Koonce, L., (1996): “Audit Analytical Procedures: A Field Investigation” Contemporary Accounting Research 13 (3): 457-86

Holtfreter, K., (2004), “Fraud in US Organisations: An Examination of Control Mechanisms” Journal of Financial Crime,. Vol. 12 No. 1 pp. 88-96

Hoogs, B; Kiehl, T; Lacombe, C; and Senturk, D (2007): “A Genetic Algorithm Approach to Detecting Temporal Patterns Indicative of Financial Statement Fraud” Intelligent Systems in Accounting, Finance and Management Volume 15: 41-56

Hooks, K; Kaplan, S., and Schultz, J. Jr. (1994): “Exchanging Communication to Assist in Fraud Prevention and Detection” Auditing: Journal of Practice and Theory, 13, 86-117

Hopwood, W.S., Leiner J.J., and Young, G.R. (2008): “Forensic Accounting” Mc Graw-Hill/Irwin.

Hoque, Z., and James, W., (2000): “Linking Balanced Scorecard Measures to Size and Market Factors: Impact on Organisational Performance” Journal of Management Accounting Research, 12, 1-17

Hsu, L., (2005): “System Effects on Performance for Interaction Between Suppliers and Buyers’ Industrial Management”, Data Systems, 105 (7): 857

http://www.efcnigeria.org/20120419_ECOWAS_needs.html

http://www.lagoschamber.com/Biz_Econ/members_list_files/sheet013.htm

http://www.pcaob.org/Standards/Staff_Questions_and_Answers/Auditing-Internal-Control_over_Financial_Reporting-2005-05-16.pdf.

<http://www.theiia.org/itaudit/index.cfm?fuseaction=printandfid=5396>.

Hu, P., Chan, P.Y.K., Liu, P., Sheng, O.R and Tam, K.Y., (1999): “Examining the Technology Acceptance Model Using Physician Acceptance of Telemedicine Technology” *Journal of Management Information System* 16(2): 91-112

Huber, N. (2002) “Business Scandals Put IT on the Spot”. *Computer Weekly* (September): 16.

Hunton, J. E., and Beeler, J. D., (1997): “Effects of User Participation in Systems Development: A Longitudinal Field Experiment”. *MIS Quarterly*. 21(4) 359-388.

Hunton, J., Wright, A. and Wright, S (2004): ‘Are Financial Auditors Overconfident in Their Ability to Assess Risks Associated with Enterprise Resource Planning Systems?; *Journal of Accounting Information Systems*, 18(2): 7-28.

Hunton, J.E. (2002): “The Participation of Accountants in all Aspects of AIS in Researching Accounting as an Information Systems Discipline”, Edited by V.Arnold and S.G. Sutton. Sarasota, FL: American Accounting Association Information Section.

Iacovou, C.L., Benbasat, I., and Dester, A.S., (1995): “Electronic Data Interchange and Small Organisations: Adoption and Impact of Technology” *MIS Quarterly* 465-485

ICAEW (1987): “Countering Computer Fraud” Publication of Institute of Chartered Accountants England and Wales.

ICAEW (2007): “An Investigation into Accounting Professional Development in West Africa Sub Region” Institute of Chartered Accountants England and Wales Publication.

ICAEW (2007): “The Accounting Profession in British West Africa” The Institute of Chartered Accountants of Scotland ICAS Website <http://www.icas.org.uk/research>

ICAEW(2005): “Auditors Use of Continuous Auditing” Institute of Chartered Accountants England and Wales Publication.

ICAN (1965): “Establishment Act of Parliament” Institute of Chartered Accountants of Nigeria.

IFAC (1995): “Information Technology in the Accounting Curriculum, Education Guideline, 11, International Federation of Accountants” New York, NY.

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.

Igbara, M., Zinatelli, N.; Cragg, P., and Cavaye, A., (1997): “Personal Computing Acceptance Factors in Small Firms: A Structural Equation Model” MIS Quarterly 21(3):279-302

IIA (1999a): (The) Institute of Internal Auditors, Available at www.theiia.org/index.cfm?doc_id=1617 (accessed 24 June 2009).

IIA (2002): “Auditing in Computer Information Systems Environment”. International Standard on Auditing 401

IIA (2003) “Internal Audit Use of Continuous Auditing: Current Use and Future Potential” Institute of Internal Auditors Research Foundation, www.theiia.org/iaa/download.cfm?file=493, accessed 17/10/2010

IIA (2004): “The Professional Practices Framework” Institute of Internal Auditors Altarmonte Springs, FL:

IIA (2008): “The Corporate Governance framework” Institute of Internal Auditors Research Foundation

IIA-UK and Ireland (2003): The Corporate Governance Framework, The IIA-UK and Ireland in Association with KPMG, London, England

Irechukwu, G. (2000): “Enhancing the Performance of Banking Operations Through Appropriate Information Technology in Nigeria Banking Industry”, Ibadan: Spectrum Books

ITGI, (2004): "IT Governance Global Status Report." IT Governance Institute Rolling Meadows, IL: The IT Governance Institute.

Ivancevich, D.M., Hermanson, D.R. and Smith, I.M., (1998): "The Association of Perceived Disaster Recovery Plan Strength with Organizational Characteristics" *Journal of Information Systems* (Spring):31-40.

Ives, B., and Olson, M.H., (1984): "User Involvement and MIS Success: A Review of Research". *Management Science* 30(5) 785-793.

Iyayi, F.E. (2006): "The Role of Government in Creating Sustainable Development in the Niger Delta: The Role of Labour" Being Paper Presented at the Labour Seminar on Law, Order, Security and Sustainable Peace Organised by SPDC on Friday 8th December at Wellington Hotels, Warri Nigeria

Jamal, K., Muier, M., and Sunder, S., (2003): "Privacy in e-Commerce: Development in Reporting Standards, Disclosure and Assurance Services in an Unregulated Market" *Journal of Accounting Research* May: 285-310

Jamal, K., Muier, M., and Sunder, S., (2005): "Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of e-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom" *Journal of Accounting Research* March: 73-96

James, K.L. (2003): "The Effects of Internal Audit Structure on Perceived Financial Statement Fraud Prevention" *Accounting Horizons* 17(4): 315-327

Jankowicz A.D. (2000): "Business Research Projects" 3rd Edition Centage Learning Inc.

Jans, M., Lybaert, N. and Vanhoof, K., (2009): "A Framework for Internal Fraud Risk Reduction at IT Integrating Business Processes: The IFR2 Framework" *The International Journal of Digital Accounting Research* Vol. 9, pp.1-29

Janvrin, D., (2008): " To What Extent Does Internal Control Effectiveness Increase the Value of Internal Evidence" *Managerial Auditing Journal* vol. 23 No. 3. Pp262-282

Janvrin, D., Bierstaker, J., and Lowe, D.J. (2008): “An Examination of Audit Information Technology Use and Perceived Importance” *Accounting Horizons* Vol. 22, No. 1 pp.1-21

Johnstone, D., Tate, M., and Bonner, M., (2004): “Bringing Human Information Behavior into Information Systems Research: An Application of System Modeling”; *Information Research*. Vol. 9 No. 4 July.

Jokipii, A., (2010): “Determinants and Consequences of Internal Control in Firms: A Contingency Theory Based Analysis” *Journal of Management and Governance*, 14 (2), 115-144

Jones, G., and Levi M., (2000): “The Value of Identity and the Need for Authenticity” Research Paper, in *Foresight (2000) Turning the Corner*, London: Department of Trade and Industry, Crime Prevention Panel, DTI/Pub 5185/5k/12/00/NP, URN 00/136 CD Annex.

Joseph G.W., and Engle T.J. (1996): “Controlling EDI Environment” *The Journal of Systems Management* July/August pp 42-49 55

Joseph, G.W., and Engle, T.J., (1996): “Controlling EDI Environment Consistent with CoBIT and COSO” *IS Audit and Control Journal* Vol 4 pp 36-41

Juszczak, P; Adams, N.M; Hand, D.J; Whitrow, C; and Weston, D.J. (2008): “Off-the-Peg and Bespoke Classifiers for Fraud Detection” *Computational Statistics and Data Analysis*, Volume 52 (9): 4521-4532

Kalakota, R., and Whinston, A.B. (1997): “Electronic Commerce: A Manager’s Guide”. Addison-Wesley: Reading MA.

Kaplan, S.E., Reneau, J.H., and Whitecotton, S., (2001): “The effects of Predictive Ability Information Locus of Control and Decision Maker Involvement on Decision Aid Reliance” *Journal of Behavioural Decision Making* (14):35-50

Karahanna, E., Straub, D.W., and Chervany, N.L., (1999): “Information Technology Adoption Across Cross-Sectional Comparison of Pre-Adoption and Post Adoption Beliefs” *MIS Quarterly* Vol.23 No. 183-213

Katz, R.A., (1998): “Telephonic Interface Game Control System” Technology US581551

Kenny, S., (2004): “Assuring Data Privacy Compliance” The Information Systems Control Journal 4: 31-33.

Kim, E., and Lee, J., (1986): “An Exploratory Contingency Model of User Participation and MIS Use” Information and Management: 11(2) 87-97.

Kim, H and Kwon, W.J. (2006): “A Multi-Line Insurance Fraud Recognition System: A Government-Led Approach in Korea” Risk Management and Insurance Review Volume 92: 131-147

Kim, H.J; Mannimo, 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 10, 214-228

King, C.G., (2001): “Protecting Online Privacy” The CPA Journal (November): 66-67

King, W. R., and Lee, T. H., (1991): “The Effects of User Participation on System Success: Toward a Contingency Theory of User Satisfaction”. Paper Presented at the Twelfth International Conference on Information Systems. New York. NY.

Kinney, W.R., (2003): “Auditing Risk Assessment and Risk Management Processes”. In Research Opportunities in Internal Auditing

Kirkos, E; Spathis, C and Manolopoulos, Y (2007): “Data Mining Techniques for the Detection of Fraudulent Financial Statements” Expert Systems with Applications 32 (4) 995-1003

Kleffner, A.E. (2003): “The Effect of Corporate Governance on the Use of Enterprise Risk Management: Evidence From Canada”. Risk Management and Insurance Review (Spring): 53-74.

Kleinig, John (2000): “The Burdens of Situational Crime Prevention: An Ethical Commentary”, in Andrew von Hirsch, David Garland and Alison Wakefield (eds),

Ethical and Social Perspectives on Situational Crime Prevention. Oxford: Hart Publishing, pp. 4-42

Kogan, A.; Sudit, E.F.; Vasarhelyi, M. (1996): "Implications of Internet Technology: On-Line Auditing and Cryptography", IS Audit and Control Journal, vol. 3: 42-48.

Kogan, A.; Sudit, E.F.; Vasarhelyi, M. (1999): "Continuous Online Auditing: An Evolution", Journal of Information Systems, vol. 1(3): 87-103.

Korpelainen, E., (2011): "Theories of ICT System Implementation and Adoption – A Critical Review" Working Papers, Department of Industrial Engineering and Management, Aalto University, Helsinki.

KPMG (2005), African Fraud and Misconduct Survey 2005

KPMG, (1999) "Fraud Survey Results 1999" New York: KPMG

Krauss, L.I., and MacGahan A., (1979): "Computer Fraud and Countermeasures" Prentice Hall.

Krishnamoorti, G., (2001): "A Cascaded Inference Model for Evaluation of the Internal Audit Report" Decision Sciences (Summer): 499-520.

Kwon, T.H., and Zmud, R.W., (1987): "Unifying the Fragmented Models of Information Systems Implementation" In J.R. Boland and R.H. Hirshheim (eds), Critical Issues in Information Systems Research, New York John Wiley 1987

Lacey, A. and Luff, D. (2001): "Qualitative Data Analysis" Trent Focus for Research and Development in Primary Health Care

Lai, F., and Hsieh, C.T., (2007): "On Network External, E-business Adoption and Information Asymmetry" Industrial Management and Data Systems 107(5), 728-746

Lal Balkaran (2008): "Two sides of Auditing" The Institute of Internal Auditors, Florida

Lawrence, P.R and Lorsch J.W. (1965): "Organization and Environment" Boston: Harvard University

Lee, C. S., (1999): "A meta- Analysis of Single Subject Design, Intervention Research for Students with LD" Journal of Learning Disabilities March vol. 33 no. 2 114-136

Lee, C., (2001): "An Analytical Framework for Evaluating e-Commerce Business Models and Strategies" Internet Research: Electronic Networking Applications and Policy 11(4), 349-359

Leech, N.L., and Onwuegbuzie, A.J., (2009): "A Typology of Mixed Methods Research Designs" Quality and Quantity International Journal of Methodology, 43: 265-275.

Legris, P., Ingham, J., and Collerette, P., (2003): "Why do People Use Information Technology? A Critical Review of the Technology Acceptance Model" Information and Management 40: 191-204

Lehmann, C. M., and Norman, C. S. (2006): "The Effects of Experience on Complex Problem Representation and Judgment in Auditing: An Experimental Investigation" Behavioral Research in Accounting Vol. 18. Pp. 65-83

Leinicke, L.M., Ostrosky, J.A., Rexroad, W.M., Baker, J.R. and Bechman, S. (2005): "Interviewing as an Auditing Tool", The CPA Journal, Vol. 75 No. 2 pp 34-9

Leithhead, B.S., and McNamee, D., (2000): "Assessing Organizational Risk". Internal Auditor (June): 68-69.

Levinsohn, A., (2005): "First-year Verdict of SOX 404: Burdensome, Costly, and Confusing". Strategic Finance (June): 67-68.

Levitt, A., (1998): "The Numbers Game" Available on the Web at <http://www.rutgers.edu/accounting/raw/aa/newsare/pr101898.htm>.

Levitt, A., (1999): "Levitt Plays up Shareholder Rights to Directors, Investor Relations" Business, April 12, 2

Li, S., and Park, S.H., (2004): "The Great Leap Forward: The Transition From Relationship Based Governance to Rule Based Governance" Organisational Dynamics Volume 33(1) 63-78

Li, S., Huang, S., and Lin, Y., (2007): "Developing a Continuous Auditing Assistance System Based on Information Processed Model" *The Journal of Computer Information Systems* Volume 48: pp 2-14

Libby, T., and Waterhouse, J., (1996): "Predicting Change in Management Accounting Systems" *Journal of Management Accounting Research*,8,137-150

Lightle, S.S., and Vallario, C.W., (2003): "Segregation of Duties in ERR" *Internal Auditor* (October): 27-31.

Lin, J.W., Hwang, M.I., and Becker, J.D., (2003): "A Fuzzy Neural Network For Assessing the Risk of Fraudulent Financial Reporting" *Managerial Auditing Journal* 18 (8) 657-665

Link, A.N., and Siegel, D.S., (2002): "The Economics of Science and Technology" Kluwer Academic Publishers (Boston)

Lombardi, Mark (1998): "The Offshore Phenomenon: Dirty Banking in a Brave New World" *Cabinet No 2* Spring P 86

Lowe, D.J, Geiger, M.A. and Parry, K. (1999): "The Effects of Internal Audit Outsourcing on Perceived External Auditors Independence" *Auditing: A Journal of Practice and Theory* 18 (Supplement): 7-26

MacDonald, B., and Colombo, L., (2001): "Creating Value Through Human Capital Management" *Internal Auditor*, Vol 58 No 4 pp 69-75

Maes, S; Tuyls, K; Vanschoenwinkel, B and Manderick, B. (2002): "Credit Card Fraud Detection Using Bayesian and Neural Networks" *Proceedings of the first International ICSC Conference on Neuro-Fuzzy Technologies, Havana, Cuba*

Mahzan, N., and Lymer, A., (2008): *Adoption of Computer Assisted Audit Tools and Techniques (CAATTs) by Internal Auditors: Current Issues in the UK: Draft Paper Submitted for BAA Annual Conference, Blackpool, April*

Mainoma, M.A.M., (2004) "An Assessment of Internal Audit as a Tool for Accountability of a Firm in Nigeria: Prudence, Transparency and Accountability" *Bayero University, Kano Nigeria*

Major, J.A., and Riedinger, D.R., (2002): “ EFD: A Hybrid Knowledge/Statistical-Based System for the Detection of Fraud” *The Journal of Risk and Insurance* 69 (3) 309-324

Malhotra, N. K. (1996): “Marketing Research: An Applied Orientation”, 2nd edition. Englewood Cliffs, NJ: Prentice-Hall.

Mann, David and Sutton, Mike (1998): “Netcrime”, *British Journal of Criminology*, 38(2): 201-29

Manson, S., Mc Cartney, S., and Sherer, M., (1997) “Audit Automation: The Use of Information Technology in the Planning, Controlling and Recording of Audit Work”. Edinburgh: ICAS

Manson, S; Mccantney, S; and Sherer, M., (2001): “Audit Automation as Control Within Audit Firms” *Accounting, Auditing and Accountability Journal*, 14 (1); 109 – 130

Manueli, K, Latu, S., and Koh, D., (2007): ”ICT Adoption Models 20th Annual Conference of the National Advisory Committee on Computing Qualifications’ (NACCQ)” Nelson, New Zealand Samuel Mann and Noel Bridgeman (Eds) Available at www.naccq.ac.nz Accessed on 20 March 2012.

Marcella, A.J., and Greenfield, R.S., eds (2002) “Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crime”. Boca Raton, FL: Auerbach Publications, CRC Press LLC.

Mark, M.M., and Shortland, R.L., (1987): “Alternative Models for the Use of Multiple Methods, in Mark M.M., and Shortlads R.L. (eds). *Multiple Methods in Program Evaluation: New Directions for Program Evaluation*, 35: 95-100

Mathieson, K. (1991) “Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior”, *Information Systems Research* (2)3, pp.173-191.

Matsumura, E.M., and Tucker, R.R., (1992): “Fraud Detection: A Theoretical Foundation” *The Accounting Review* 67 (Fall): 753-782

McEvoy, S., (2001) “Youth, Violence and Conflict Transformation Peace Review” A Transnational Quarterly 13: 1 March: 89-96

McKeen, J.D., Guimaraes, T., and Wetherbe, J.C. (1994): “The Relationship Between User Participation and User Satisfaction: An Investigation of Four Contingency Factors”, MIS Quarterly. 18(4) 427-451.

McNamee, D., and Selim, G.M. (1998): “Risk Management: Changing the Internal Auditor’s Paradigm” Altamonte Springs. FL: The Institute of Internal Auditors Research Foundation.

Meiners, C. (2005): “Detecting and Eliminating the Unintentional Perk”, Risk Management, vol.52 No. 4, pp 50-4.

Meng, Qingxuan and Li, Mingzhi (2001): “New Economy and ICT Development in China” United Nations University, World Institute for Development Economic Research, Discussion Paper No. 2001/76

Menon, K., and Williams, J.D., (1994): “The Use of Audit Committees for Monitoring” Journal of Accounting and Public Policy 13 (2): 121-39

Merchant, K. (1981): “The design of the Corporate Budgeting System: Influences on Managerial Behaviour and Performance.” The Accounting Review, 56, 813-829

Merchant, k. (1984): “Influences on Departmental Budgeting: An Empirical Examination of Contingency Model”, Accounting, Organisation and Society, 9(3-4), 291-307.

Meredith, M., and Akers, M., (2003): “Internal Auditor Participation in Systems Development Projects” Internal Auditor Participation in System Development Project Vol. 7 No 2

Meyer, N.D., (2004): “Systematic IS Governance: An Introduction” Information Systems Management (Fall): 23-34.

Mieke Jans; Nadine, L, and Koen Vanhoof (2010): “A Framework for Internal Fraud Risk Reduction at IT Integrating Business Processes: The IFR2 Framework” The International Journal of Digital Accounting Research Vol 09 No 15

- Mills, R. (1997): "Internal Control Practices Within Large UK Companies. In K Keasey and M. Wright (eds) Corporate Governance, Responsibilities, Risks and Remunerations" Chichester: Wiley
- Mitchell, M.L and Jolley, J.M (2006): "Research Design Explained" (6th ed) Belmont, CA: Wadsworth
- Mock, T.J., and Wright, A.M., (1999): "Are Audit Programs Risk-adjusted?" Auditing: A Journal of Practice and Theory (Spring): 55-74.
- Mooney, J.L., Harrell, H.W., and Ludwig, S.E. (2000): "Audit Software that Help Your Company Stop Fraud" The Journal of Corporate Accounting and Finance. Volume 11 Issue 4 pp 17-23 May/June
- Moore, G. C., and Benbasat, I. (1991): "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation" Information Systems Research, 2(3), 192-222.
- Moorman, R.H.(1991), "Relationship Between Organisational Justice and Organisational Citizenship Behaviours: Do Fairness Perceptions Influence Employee Citizenship?" Journal of Applied Psychology, Vol. 76, pp. 845-55
- Morgan, G. and Smircich, L. (1980): "The Case for Quantitative Research" The Academy of Management Review (pre-1986); Oct. 1980; 5, 00004 pg 491
- Mouton, J (2001): "How to Succeed in Your Master's and Doctoral Studies: A South African Guide and Resources Book. Pretoria: Van Schaik
- Mouton, J. (1996): "Understanding Social Research" Pretoria: Van Schaik
- Mpofu, K.C., Milne, D. and Watkins-Mathys, L. (2012): "ICT Adoption and Development of E-business Among SMEs in South Africa", Buckinghamshire New University. U.K.
- Nagy, A.L. and Cenker, W.J. (2002): "An Assessment of the Newly Defined Internal Audit Function", Managerial Auditing Journal, 17 (3): 130 – 137.

NDIC (2007): “Annual Reports and Statement of Accounts” Nigeria Deposit Insurance Corporation

Ndubisi, N.O. and Jantan, M (2003): “Evaluating IS Usage in Malaysian Small and Medium-sized Firms Using the Technology Acceptance Model” *Logistics Information Management*, 16(6), 440-450.

Nehmer, R., (2003): “Transaction Agents in e-Commerce, A Generalized Framework. In *Trust and Data Assurances in Capital Markets: The Role of Technology Solution*, Edited by S.J. Roobani, Smithfield, RI: PriceWaterHouseCoopers.

Newman, Graeme R. and Clarke, R.V.G (2003): “Superhighway Robbery; Preventing E-Commerce Crime” Willan Publishing

Newsted, P., Huff, S. and Munro, M. (1998), *Survey Investments in IS*, *MIS Quarterly*, vol.22 (4), pp. 553-554

Ngai, E.W.T; Hu, Yong; Wong, Y.H. Chen, Y., and Sun, Xin (2010): “The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature” *Decision Support Systems* 50: 550-569

NICTP (2012): “Penetration of Information Technology in Nigeria” National Information Communication Technology Policy

NPC (2007): “Revised Census Figures” National Population Commission

Nwankwo, G.O. (1975) “Bank Lending in a Developing Economy: The Nigerian Experience”. *Journal of African Law*, 19 (1/2, International Conference on Banking Law and Development in Africa) 84-104

Nwankwo, G.O. (1991): “Bank Management Principles and Practice” Malthouse Press Ltd, Lagos, Nigeria.

Nwaze, C., (2006): “Bank Fraud Exposed with Cases and Preventive Measures” Control and Surveillance Associates Ltd, Lagos.

O'Donoghue, T. and Punch, K. (2003): "Qualitative Educational Research in Action: Doing and Reflecting". Routledge. P.78

O'Leary, C and Stewart, J. (2007): "Governance Factors Affecting Internal Auditors' Ethical Decision Making: An Exploratory Study" *Managerial Auditing Journal*, Vol. 22 No. 8, pp787-808

O'Leary, D.E. (2000): "Enterprise Planning Systems: Systems, Life Cycle, Electronic Commerce, and Risk" Cambridge, U.K: Cambridge University Press.

O'Regan, D. (2008), "The CPA's transition to the world of internal auditing", *The CPA Journal*, August, pp. 11-13

Oghojafor, B.E.A; Olayemi, O.O.; Okonji, P.S., and Okolie, J.U. (2010): "Poor Corporate Governance and its Consequences on the Nigerian Banking Sector" *Serbian Journal of Management* 5(2) (2010) 243-250

Ogunbunka, N.M. (2002): "Risk Analysis and Management in a Competitive Banking Environment", in *Risk and Internal Control Management in Financial Institutions*, Ogunbunka N.M. (ed), The Chartered Institute of Bankers of Nigeria, Lagos.

Ogunleye, G.A. (2007): "Proactive Measures to Guard Against Fraud/Cash Theft in the Banking Industry and in Organizations, *NDIC Quarterly*, Sept/Dec. 31-53.

Okike, E., (1994): "Curious Auditing Regulations in Nigeria: A Case Study of Cultural/Political Influence on Auditing Practice", *The International Journal of Accounting*, Vol. 29, pp. 78 - 91

Okike, E., (2004): "Management of Crises: The Response of the Auditing Profession in Nigeria to the Challenges to its Legitimacy", *Accounting, Auditing & Accountability Journal*, Vol. 17 Iss: 5 pp. 705 – 730

Okike, E., (2009): "Seeding Corporate Integrity: the Challenges to Accounting and Auditing in Nigeria" *Global Corruption Report, 2009 Transparency International* pg136 – 138

Olojo, A., (2006): "Curbing Fraud Within the Banking System: A Banker's Perspective" Bolabay Publications, Lagos.

Ololube, N.P. (2006): “Appraising the Relationship Between ICT Usage and Integration and the Standard of Teacher Education Programs in a Developing Economy” International Journal of Education and Development Using ICT vol.2 No. 3

Olsen, W., (2004): “Triangulation in Social Research: Qualitative and Quantitative Methods Can Really Be Mixed” Developments in Sociology : Ed M. Holborn Ormskirk: Causeway Press

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 Pg. 23-44

Omoteso, K., (2006): “The Impact of Information Communication Technology on Auditing”: Unpublished P hD Thesis, De Montfort University, UK

Omoteso, K., Patel, A., and Scott, P., (2007): “Information and Communications Technology and Organisations: A Meta-Level Perspective” The Journal of Technology, Knowledge and Society, 3(3): pg 19-27.

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, Issue 2, pg 147-162 July.

Onwuegbuzie, A.J., and Collins, K.M.T., (2007): “A Typology of Mixed Methods Sampling Designs in Social Science Research” The Qualitative Report, 12(2). Retrieved December 20 2009, from <http://www.nova.edu/ssss/QR/QR12-2/onwuegbuzie2.pdf>

Organisation for Economic Co-operation and Development (OECD), (1999): OECD Principles of Corporate Governance. Available at <http://www.oecd.org>

Orlikowski, W.J., (1992): “The Duality of Technology: Rethinking the Concept of Technology in Organisations” Organisation Science, 3(3): 398-427

Orman, L.V., (2001): “Database Audit and Control Strategies”, Information Technology and Management, vol.2 (1): 27-51.

Oyeyinka, O.B., and Adeya, C.N., (2002): "Internet Access in Africa: An Empirical Exploration" Discussion Papers 05, United Nations University, Institute for New Technologies.

Paape, L., Scheffe, J., and Snoep, P., (2003): "The Relationship Between the Internal Audit Function and Corporate Governance in the EU-A Survey" *International Journal of Auditing* 7: 247-262.

Pacini, C., and Sinason, D., (1999): "The law and CPA Web trust" *Journal of Accountancy* (February): 20-25.

Pallant, J., (2010): "SPSS Survival Manual: A Step by Step Guide to Data Analysis Using SPSS" 4th Edition McGraw-Hill, UK

Palmerino, M.B., (1999): "Take a Quality Approach to Qualitative Research" *Marketing News*, Vol. 33, No. 12 pp. 35-36

Panurach, P., (1996): "Money in Electronic Commerce: Digital Cash, Electronic Fund Transfer, and E-Cash" *Communications of the ACM* 39(6) June, 45-50

Parker, X.L (2001): "An e-Risk Primer" Altamonte Springs. FL: The Institute of Internal Auditors Research Foundation.

Pathak, J., (2003): "IT Auditing and Electronic Funds Transfers", *Internal Auditing*, Vol.18 No. 5 p.28

Pathak, J., Chaouch, B.; Sriram, R.S. (2003): "Minimizing the Cost of Continuous Audit: Counting and Time Dependent Strategies", *Journal of Accounting and Public Policy*, vol. 24: 61-75

Pathak, J; Vidyarthi, N., and Summers, S.I., (2005): "A Fussy-Based Algorithm for Auditors to Detect Elements of Fraud in Settled Insurance Claims" *Managerial Auditing Journal* 20 (6) 632-644

Paulson, J. (1993): "EDI An Implementation Review" *Production and Inventory Management Journal*, Second Quarter 77-81

Pavot, W., Diener, E., Colvin, C.R, and Sandvik, E., (1991): “Further Validation of the Satisfaction with Life Scale: Evidence for the Cross Method Convergence of Well-Being Measures” *Journal of Personality Assessment*, 57, 149-61

Payne, E.A., and Ramsay, R.J., (2005): “Fraud Risk Assessments and Auditors’ Professional Skepticism” *Managerial Auditing Journal* Volume 20 Issue 3 PP 321-330

Peters, T.J., (1987): “Thriving on Chaos: Handbook for a Management Revolution” Knopf (New York)

Phua, C., Lee, V., Smith, K., and Gayler, R., (2005): “A Comprehensive Survey of Data Mining-Based Fraud Detection Research” *Artificial Intelligence Review* pp. 1-14

Pickett, K.H.S., (2005): “The Essential Handbook of International Auditing” John Wiley and Sons Ltd

Pinsker, Robert, (2008): “An Empirical Examination of Computing Theories to Explain Continuous Disclosure Technology Adoption Intentions Using XBRL as the Example Technology” *The International Journal of Digital Accounting Research* Vol. 8, N. 14, pp. 81-96

Plumly, M., and Dudley, E., (2002): “Building a Successful Audit Organisation” *The Internal Auditor* (Online) Available at: <http://proquest.umi.com/pdqwebindex=6anddid=147410001&srchmode=1andsid=3fmt=4andvinst=pro> downloaded 10-03-2012

Porter, B., Simon, J, and Hatherly, D., (2003): “Principles of External Auditing” (3rd ed.) Chichester: Wiley

Porter, M.E., (2001): “Strategy and the Internet” *Harvard Business Review*, Boston March

Porter, W.T., and Perry, W.E., (1983): “EDP; Controls and Auditing, Boston: Kent Publishing.

PricewaterhouseCoopers (2003): "Technology Forecast" 2003-2005. Menlo park. CA: PricewaterhouseCoopers.

PricewaterhouseCoopers (2004): "Enables TSX Group to be First in Canada to Publish Financials in XBRL" available at http://www.pec.com/en_Gx/gx/xbrl/pdf/tsx.pdf assessed on 26/7/2012

PricewaterhouseCoopers (2006): "A Survey on Internal Audit" Menlo park. CA: PricewaterhouseCoopers

PriceWaterHouseCoopers (2007): "State of the Internal Audit Professional Study: Pressures Build for Continual Focus on Risk" PwC Advisory Publication

PricewaterhouseCoopers (2012): State of the Internal Audit Professional Study: PwC Advisory Publication

Public Company Accounting Oversight Board (PCAOB), (2005): "Staff Questions and Answers on Auditing Standard No.2- Internal Control. Available at: <http://www.pcaob.org/standards/staff-Questions-and Answer/Auditing>. accessed 10/09/2012

Public Oversight Board (1993): "A Special Report by the Public Oversight Board of the SEC Practice Section, AICPA

Public Oversight Board (POB) (2008): "Statement of Internal Control" A Report by the Public Oversight Board of SEC Practice Section

Punch, (2009): "Stealing Regime in the Banking Sector" The Punch Newspaper Publications, September, 25

Pyle, R. (1996): "Electronic Commerce and the Internet" Communications of the ACM 39(6): June, 22-23

Rae, K., and Subramaniam, N., (2008): "Quality of Internal Control Procedures: Antecedents and Moderating Effects on Organisational Justice and Employee Fraud" Management Auditing Journal vol. 23 No. 2 pp104-124.

Ramomoorti, S., and Traver, R.O., (1998): "Using Neural Networks for Risk Assessment in Internal Auditing: A Feasibility Study." Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation.

Ramsay, I., (2001): "Independence of Australian Company Auditors: Review of Current Australian Requirements and Proposals for Reform (Ramsay Report). Available on the Web at <http://www.treasury.gov.au/>

Ravisankar, P., Ravi, V., Rao, G., and Bose, I. (2010): "Detection of Financial Statement Fraud and Feature Selection Using Data Mining Techniques" Decision Support Systems 50: 491-500

Remenyi, D., (1992): "Researching Information Systems: Data analysis Methodology Using Content and Corresponding Analysis"; Journal of Information Technology, 7 76-86

Rezaee, Z. Sharbartoghlie, A., Elam, R., and McMickle P.L. (2002): "Continuous Auditing: Building Automated Auditing Capability." Auditing: A Journal of Practice and Theory (March): 147-163.

Rezaee, Z., and Reinstein, A., (1998): "The Impact of Emerging Information Technology on Auditing" Managerial Auditing Journal Vol. 13 No. 8, pp 465-471

Rezaee, Z., Ford, W. and Elam, R. (2000): "Real-time Accounting Systems", Internal Auditor, April, pp. 63-7.

Rezaee, Z.; Elam, R.; Sharbatoghlie, A. (2001): "Continuous Auditing: The Audit of the Future", Managerial Auditing Journal, vol. 16(3): 150.

Riahi Bel Kaoui, A; and Picur, R.D. (2000): "Understanding Fraud in the Accounting Environment," Managerial Finance, 2b (ii): 33-40

Richtel and Matt (2002): "Credit Card Theft is Thriving Online as Global Market" The New York Times

Rishel, T.D., and Ivancevich, S.H., (2003): "Additional Opportunities for Internal Auditors in IT Implementations" Internal Auditing Vol. 18 No. 2, pp 35-39

Ritchie, C., (2003): "Parenting and Adolescent Well-being," Doctoral thesis, University of Oxford.

Robitaille, D.B., (2004): "World-Class Audit and Control Practices" Internal Auditor Vol 61 No.1 pp 74-80

Rocco, T.S., Bliss, L. A., Gallagher, S., and Perez-prado, A., (2003): "Taking the Next Step: Mixed Methods Research in Organizational Systems. Information Technology," Learning and Performance Journal, 21(1): 19-29.

Romney, M. B., and Steinbart, P.J., (2000): "Accounting Information systems" (8th ed.). Upper Saddle River. NJ: Prentice-Hall.

Rose, J. (1998): "Evaluating the Contribution of Structuration Theory to the Information Systems Discipline" Proceedings of the 6th European Conference on Information Systems, Beats, W.R.J. (Ed.) Euro-Arab Management School, Granada

Rose, J., and Jones, M., (2004): "The Double Dance of Agency: A Socio-Theoretical Account of How Machines and Human Interact" ALOIS Workshop: Action in Language, Organisations and Information Systems, Linkoping University, Sweden

Rusch, J., (2001): "The Rising Tide of Internet Fraud" Internet Fraud Cybercrime 11: United States Attorney's Bulletin Vol 49 No 3

Samuel, M., Coombes J.C., Miranda, J.J., Melvin, R., Young E. J.W., and Azarmina, P., (2004): "Assessing Computer Skills in Tanzanian Medical Students: An Elective Experience" Available at <http://www.biomedcentral.com/1471-2458/4/37>

Sanchez, D; Vila, M.A. Cerda, I., and Serrano, J.M., (2008): "Association Rules Applied to Credit Card Fraud Detection" Expert Systems with Applications 36 (2) 3630-3640

Sanusi, J.O., (1986): "Management Control Systems and the Prevention and Detection of Frauds in Banks". A Paper Presented at the Seminar on Frauds in Banks Organized by the Nigerian Institute of Bankers, Lagos, Nigeria.

Sarbanes-Oxley Act 2002: IS Control Journal (1): 17-21.

Sarens, G., and De Beelde, I., (2006): “Building A Research Model for Internal Auditing: Insights from Literature and Theory Specification Cases” *International Journal of Accounting Auditing and Performance Evaluation* Vol. 3 No. 4: 452-470

Sarens, G., and De Beelde, I., (2006a): “The Relationship Between Internal Audit and Senior Management: An Analysis of Expectations and Perceptions” *International Journal of Auditing* Vol. 10, No. 3: pp 219-241

Sarner, A (2004): “It’s Time to Re-Energize Business-to Consumer e- Commerce”. Gartner Research Report <http://www.gartner.com> accessed 06/09/2012

Saunders, M.N.K., Lewis, P., and Thornhill, A., (2003): “Research Methods for Business Students” (3rd ed) Harlow: FT Prentice Hall

Sawyer, L.B., (1995): “An Internal Audit Philosophy”, *Internal Auditor*, August, pp. 46-55.

Scarborough, D.P., Rama, D.V. and Raghunandan, K., (1998): “Audit Committee Composition and Interaction with Internal Auditing: Canadian Evidence” *Accounting Horizons*, Vol.12 No. 1, pp.51-62

Schoonhoven, C.B., (1981): “Problems With Contingency Theory: Testing Assumptions Hidden Within the Language of Contingency “Theory” *Administrative Science Quarterly*, 26(3): 349-377

Schutz, A., (1973) The Structures of the Life-World Evanston (111), Northwestern University Press.

Schwandt, T.A., (1994) in Handbook of Qualitative research by Denzin, Norman K; Lincoln; Yvonna S; Thousands Oaks, Sage Publications

Scott, W.R., (1987): *Organizations, Rational, Natural and Open Systems*. Second Edition, London, Prentice Hall.

Searcy, D., Woodroof, J. and Behn, B. (2003): “Continuous Audit: the Motivations, Benefits, Problems, and Challenges Identified by Partners of a Big 4 Accounting Firm” *Proceedings of 36th Hawaii International Conference on System Sciences*, (January) pp. 2109.

Searcy, D.L., and Wood, Roof J.B. (2003): “Continuous Auditing: Leveraging Technology” The CPA Journal (May): 46-48.

SEC (2009): “Corporate Governance Code for Listed Companies in Nigeria” Security and Exchange Commission

SEC (2010): “Corporate Governance Issues in Quoted Companies” Security and Exchange Commission Available at: [http: www.nsec](http://www.nsec)

Seetharaman, A; Senthilvemurugan, M., and Periyanyagami, R., (2006): “Anatomy of Computer Accounting Frauds” Managerial Auditing Journal, Bradford, 19(8/9); 1055-1072

Seyal, A.H., and Rahim, Md M., (2006): “A Preliminary Investigation of Electronic Data Interchange Adoption in Bruneian Small Business Organisations” The Electronic Journal of Information Systems in Developing Countries Volume 24

Shaikh, J.M., (2005): “E-commerce Impact: Emerging Technology – Electronic Auditing” Managerial Auditing Journal; 20, 4

Sharp, J.A., and Howard, K., (1996): “The Management of a Student Research Project” 2nd Edition

Shaw, E (1973): “Financial Deepening in Economic Development” New York: Oxford University Press.

Shiels, H., Melvor, R.; and O’Reilly, D (2003): “Understanding the Implications of ICT Adoption: Insights from SMEs” Logistics Information Management 16(5), 312-326.

Sieber, Ulrich (2006): “The International Handbook on Computer Crime: Computer-Related Economic Crime and the Infringements of Privacy”, Wiley 276 Pages

Silltow, J., (2003): “Shedding Light on Information Technology Risks” The Internal Auditor, Vol.60 No.6 p.22

Simon, R., (1987): “Accounting Control Systems and Business Strategy: An Empirical Analysis” Accounting, Organisation and Society, 12(4), 357-374.

Simone, D. (2012): "Risk Management Imperatives for 2012" Australian Security Magazine, May

Smith, R. G., (2001): "Cross-Border Economic Crime: The Agenda for Reform", Trends and Issues in Crime and Criminal Justice (Australian Institute of Criminology), No. 202, April

Sobel, P.J., and Reding, K.F., (2004): "Aligning Corporate Governance with Enterprise Risk Management". Management Accounting Quarterly (Winter): 29-37.

Soludo, Charles C (2007): "Macroeconomic Monetary and Financial Sector Developments in Nigeria" CBN Website: www.cenbank.org

Spinello, R., (1998): "Privacy Rights in the Information Economy". Business Ethics Quarterly (October 4): 723-763

Spira, J.F., and Page, M., (2003): "Risk Management: The Reinvention of Internal Control and The Changing Role of Internal Audit" Accounting, Auditing and Accountability Journal, Vol. 16 No. 4, pp. 840-661

Spraakman, G., (1997): "Transaction Cost Economist: a Theory of Internal Audit", Managerial Auditing Journal, 17 (7); 323-30.

Spradley, J.P., (1979): "The Ethnographic Interview" New York: Rine Hart and Winston

Srivastava, A.; Kundu, A; Sural, S and Majumdar, A.K. (2008): "Credit Card Fraud Detection Using Hidden Markov Model" IEEE Transactions on Dependable and Secure Computing 5 (1) 37-48

Staff (1999): "US and Video Game Makers Lost More Than \$3 Billion Worldwide in 1998 Due to Software Piracy: Greater China Paraguay, Thailand and Malaysia Top List" Business Wire, 16th February

Staff (2000): "E-commerce and Security – A European View" International Security Review, March/April, No. 115, pp. 10-13

Staff (2002): "Go on, Watch Me", The Economist, 17th August, p.12

Stanfield, M and Grant, K. (2003): “An Investigation into Issues Influencing the use of Internet and Electronic Commerce Among Small-Medium Sized Enterprises” Journal of Electronic Commerce Research, Volume 4: Number 1. PP 15-33

Stanfield, M., and Grant, K., (2003a): “An Investigation into Issues Influencing the use of Internet and Electronic Commerce Among Small-Medium Sized Enterprises” Journal of Electronic Commerce Research, Volume 4: Number 1. PP 15-33

Stern J. (2002): “Web Metrics: Proven Methods for Measuring Web Site Success” Wiley Books, Third Edition

Stern, L.W., and Kaufmann, P.J., (1985): “Electronic Data Interchange in Selected Consumer Goods Industries: An Inter-Organisational Perception” in ‘Marketing in Electronic Age’ R. Buzzell (ed), Boston, MA, Harvard Business School Press PP 52-74

Stewart J and Subramaniam, N (2010): "Internal Audit Independence and Objectivity: Emerging Research Opportunities", Managerial Auditing Journal, Vol. 25 Iss: 4, pp.328 – 360

Stolfo, S; Fan, W; Lee, W; Prodromidis, A and Chan, P.K. (2000): “Cost-Based Modelling for Fraud and Intrusion Detection: Results from the JAM Project” Proceedings of the DARPA Information Survivability Conference and Exposition, Volume 2: 1130-1144 IEEE Computer Press

Straub, D. W., (1989): “Validating instruments in MIS research”, MIS Quarterly, vol. 13 pp. 147-169.

Strauss, A.L. and Corbin, J.M. (1998): “Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. 2nd Edition Thousand Oaks, CA: Sage

Stuart, Loh (2002): “Using Continuous Assurance to Detect Fraud in E-Commerce Transactions” Unpublished Thesis, The University of New South Wales

- Subramaniam, N., Ng. C., and Carey, P. (2000): "Outsourcing Internal Audit Services: An Empirical Study on Queensland Government Entities" *Australian Accounting Review*, Vol.14 No.3, pp.86-95
- Sutton, S.G., Arnold, T.D., and Arnorld, V., (1994): "An Integrative Framework for Analysis of the Ethical Issues Surrounding Information Technology Integration by the Audit Profession". *Research on Accounting Ethics* 5: 21-36.
- Swanson, E. B., (1974): "Management Information Systems: Appreciation and Involvement". *Management Science*, 21(2), 178-188
- Swinney, L (1999): "Consideration of the Social Context of Auditors' Reliance on Expert System Output During Evaluation of Loan Loss Reserves" *International Journal of Intelligent Systems in Accounting, Finance and Management* 8(3): 199
- Sydney, I.F. (1986): "Management Control System, Prevention and Detection of Frauds", A Paper Presented at the Seminar on Frauds in Banks Organized by the Nigerian Institute of Bankers, Lagos, Nigeria.
- Tait, P., and Vessey, I., (1988): "The Effect of User Involvement on System Success: A Contingency Approach". *MIS Quarterly*, 12(1). 91-108.
- Tapscott, D., and Ticoll, D. (2003): "The Naked Corporation" New York: Free Press
- Taylor, J.C. (1978): "The Socio-Technical Approach to Work Design" in UK Legge and E Mumford (eds.) *Designing Organizations for Satisfaction and Efficiency* (England Gower Press, 1978) PP.95-107.
- Taylor, S. and Todd, P.A. (1995): "Understanding Information Technology Usage: A Test of Competing Models", *Information Systems Research* 6(2): 144-176
- Tenenbaum, J.M., Chowdhry, T.S., and Hughes, C., (1997): "Eco System: An Internet Commerce Architecture" *IEEE Computer* 30(5): May 48-55
- Thompson, R. L., Higgins, C. A., and Howell, J. M., (1991): "Personal Computing: Towards a Conceptual Model of Utilization." *MIS Quarterly*, 15(1), 125-143.

Thong J., Hong, W., and Tam, K., (2002): “Understanding User Acceptance of Digital Libraries: What are the Roles of Interface Characteristics, Organisational Context, and Individual Differences” *International Journal of Human-Computer Studies* 57(3) 215-242

Tillinghast-Towers, Perrin (2001): “Enterprise Risk Management: Trends and Emerging Practices”. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

Todd, P.A., (1995): “Understanding Information Technology Usage: A Test of Competing Models” *Information Systems Research* 6:144-176

Tomkins, C., and Groves, R., (1983): “The Everyday Accountant and Researching His Reality” *Accounting, Organisations and Society*, 8 (4): 361 – 74

Treadway Commission, (1987): “National Commission on Fraudulent Financial Reporting” Washington, D.C., Government Printing Office.

Turkey, S. and Zaman, M., (2007): “Audit Committee Effectiveness: Informal Process and Behavioural Effects”, *Accounting, Auditing and Accountability Journal*, Vol.20 No.5, pp.765-788

Umoh, P.N., (2004): “An Overview of Risk Management Practices in the Nigerian Banking Industry”, *NDIC Quarterly*, Vol. 12 No. 4, Abuja, Nigeria.

United States General Accountability Office (1998) available at <http://www.gao.gov/> accessed on-line on 20-9-2012

Vaccaro, A., and Madsen, P., (2009): “Corporate Dynamic Transparency: The New ICT-Driven Ethics” *Ethics, Information and Technology* 11:113-122

Van Gansberghe, C.N., (2005): “Internal Auditing in the Public Sector: A Consultative Forum in Nairobi, Kenya, Shores up Best Practices for Government Audit Professionals in Developing Nations”, *Internal Auditor*, 62 (2) ; 69-73.

Van Maanen, J., (1988): “Tales of the Field” Chicago: University of Chicago Press

- 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, no.3, pp. 838-852
- Vanasco, R.R., (1998): "Fraud Auditing" *Managerial Auditing Journal*, Bradford, 13(1); 4-71
- Vasarhelyi, F.B., and Ezawa, K.J., (1991): "The Continuous Process Audit System: A UNIX-Based Auditing Tool" *The EDP Auditor Journal*, Vol.111, 85-91
- Vasarhelyi, M. (1998): "Towards an Intelligent Audit: Online Reporting; Online Audit and Assurance Services" *Advances in Accounting Information Systems* Volume 6 pp 207-21
- Vasarhelyi, M.A., (2002): "Concepts in Continuous Assurance" in Sutton, S.; Arnold, V. (eds): *Researching Accounting as an Information Discipline*, Florida: American Accounting Association.
- Vasarhelyi, M.A., and Harper, F., (1991): "The Continuous Audit of Online Systems" *Auditing: A Journal of Practice and Theory* 10(1) 110-125
- Venkatesh, V., and Davis, F. (2000): "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies" *Management Science* 46(2): pp 186-204
- Venkatesh, V., Morris, M., Davis, G., Davis, F., (2003): "User Acceptance of Information Technology: Toward a Unified View" *MIS Quarterly*, 27(3), pp. 425-478
- Viaene, S., Ayuso, M., Guillen, M., Cheel, D. V., and Dedene, G., (2007): "Strategies for Detecting Fraudulent Claims in the Automobile Insurance Industry" *European Journal of Operational Research* 176 (1) 565-583
- Viaene, S., Dedene, G., and Derrig, R.A., (2005): "Auto Claim Fraud Detection Using Bayesian Learning Neural Networks" *Expert Systems with Applications* 29 (3) 653-666

Viaene, S., Derrig, R.A., Baesens, B., and Dedene, G., (2002): “A Comparison of State-of the-Art Classification Techniques for Expert Automobile Insurance Claim Fraud Detection” *Journal of Risk and Insurance* 69 (3) 373-421

Wang, Q., Wong, T., and Xia, L., (2008): “State Ownership, the Institutional Environment and Auditor Choice: Evidence from China” *Journal of Accounting and Economics* 46: 112-134

Warren, J.D., and Parker, X.L., (2003): “Continuous Auditing Potential for Internal Auditors” *The Institute of Internal Auditors Research Foundations* September

Warren, J.D., Edelson, L.W., and Parker, X.L., (1998): “Handbook of IT Auditing” Warren, Gorham and Lamont

Watts and Zimmerman (1978): “Towards a Positive Theory of the Determination of Accounting Standards” *The Accounting Review* 53 January pp 112 – 134

Weidenmier, M.L., and Ramamoorti, S., (2006): “Research Opportunities in Information Technology and Internal Auditing” *Journal of Information Systems* Vol.20 No., 1 pp205-219

Weil, D., Fung, A., Graham, M., and Fagotto, E., (2006): “The Effectiveness of Regulatory Disclosure Policies” *Journal of Policy Analysis and Management* 25(1),155-181

Will, Knight (2001): “Hacking Will Cost World \$1.6 Trillion this Year”, Report of PricewaterhouseCoopers Study in 30 Different Countries. Available @ <http://www.zdnet.com/hacking-will-cost-world 1.6> accessed 6/09/2012

Williams, Phil (1997): “Emerging Issues: Transnational Crime and its Control” in Graeme Newman (ed.), *Global Report on Crime and Justice*. New York: Oxford/UNCICP.

Wilson, R.A., and Sangster, A., (1992): “The Automation of Accounting Practice”, *Journal of Information Technology*, 7; 65-75.

Wise, T. M., (1990): “Looking at the Systems Development Audit” *Internal Auditing*. 6(1). 69-74.

Wood, S., (1979): "A Reappraisal of the Contingency Approach to Organisation" *Journal of Management Studies*, 16 (October): 334-354

Wortley, Richard (1997): "Reconsidering the Role of Opportunity in Situational Crime Prevention", in Graeme Newman, Ronald V. Clarke and S., Giora Shoham (eds), *Rational Choice and Situational Crime Prevention*. Aldershot: Ashgate, pp. 65-81

Wright, S., and Wright, A.M., (2002): "Information System Assurance for Enterprise Resource Planning Systems: Unique Risk Considerations" *Journal of Information Systems (Supplement)*: 99-114.

Wu, R., (1992): "The Information Systems Auditor's Review of the Systems Development Process and its Impact on Software Maintenance Costs". *Journal of Information Systems (Spring)*: 1-13.

Xiangdong, W., (1997): "Development Trends and Future Prospects of Internal Auditing" *Managerial Auditing Journal*, 12 (4/5); 200-204.

Yang, W., and Hwang, S., (2006): "A Process-Mining Framework for the Detection of Healthcare Fraud and Abuse" *Expert Systems with Applications* 31 (1) 56-68

Yu, C., Yu, H., and Chou, C., (2000): "The Impact of Electronic Commerce on Auditing Practices: An Auditing Process Model for Evidence Collection and Validation" *International Journal of Intelligent Systems in Accounting, Finance and Management*. 9 195-216.

Yusuf, M.O., (2005): "Information and Communication Technologies and Education; Analysing the Nigerian National Policy for Information Technology" *International Education Journal*, 6(3), 316-321

Zappala, S., and Gray, C.W.J., (eds) (2006): "Impact of e-Commerce on Consumers and Small Firms". London, Ashgate.

Zhou, W., and Kapoor, G (2010): "Detecting Evolutionary Financial Statement Fraud", *Decision Support Systems*: 50, 570-575

Ziegenfus, D.E. (2000): "Developing an Internal Auditing Department Balanced Scorecard", *Managerial Auditing Journal*, 15 (1/2); 12-19.

Zimbelman, M.F., (1997): "The Effects of SANS No. 82 on Auditors' Attention to Fraud Risk Factors and Audit Planning Decisions". *Journal of Accounting Research (Supplement)*: 75-97.

APPENDICES

Appendix (i): Ethical Approval for the study

Appendix (ii): Introductory Letter for data collection

Appendix (iii): Questionnaire questions

Appendix (iv): Interview questions

Appendix (v): Copy of One Example of Interview Coding

Appendix (vi): Response from one of the banks

Appendix (Vii): Initial frequency Tables

Appendix (vii): EFCC Cases

APPENDIX (i)

ETHICAL APPROVAL FOR THE STUDY

FACULTY OF BUSINESS AND LAW - BUSINESS SCHOOL

ADVANCE APPROVAL OF RESEARCH ACTIVITY INVOLVING HUMAN RESEARCH
ETHICS - BUSINESS SCHOOL

Staff/Student Name

Programme/Diet (if relevant)

JAMES ABIOLA

PhD Forensic Accounting

Title of Research Project

Internal Audit and Electronic Fraud: A study of the
Nigerian Financial/Commercial Sector

I agree that in conducting the above research project I will comply with the Market Research Society Code of Conduct as published in their revised July 1999 statement. The rights of respondents are recognised in sections B3 through B8 of the code as per attached to this form. In cases where it is not appropriate to provide written statements, respondents will always receive a verbal statement that their co-operation is voluntary, that anonymity will be preserved, and the purpose for which information is being collected.

I further agree that I will always carry with me and show to respondents my staff/student identification card.

Signature of Researcher/Student



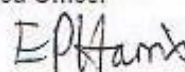
Date: 10-03-09

Signature of Director of Studies/Supervisor



Date: 16-03-09

Signature confirming approval by Designated Officer



Date: 23/03/09

APPENDIX (ii)

INTRODUCTORY LETTER FOR DATA COLLECTION

25th May, 2011

Re: James Olusola ABIOLA

This is to confirm that James Olusola Abiola is currently carrying out a research on "The Impact of ICT Tools and Techniques on Internal Auditors' Role in Prevention and Detection of Electronic Fraud" in the Department of Accounting and Finance, Leicester Business School, De Montfort University, United Kingdom.

The study is in partial fulfilment of his Doctor of Philosophy degree and I can confirm that the University code of conduct on ethics and associated procedures will be followed in this research. Therefore, respondents and focus organisations are guaranteed anonymity and confidentiality.

I shall be grateful if co-operation and assistance are accorded him. Do feel free to contact me in case of further enquiries.

Yours faithfully,



Dr. Kamil Omoteso (BSc MSc PhD PGCHE CPA MCFI MAPM FHEA)
Senior Lecturer in Accounting
Leicester Business School (HU4.64)
De Montfort University
Leicester LE1 9BH, UK
Tel.: +44 (0) 116 257 7448
E-mail: komoteso@dmu.ac.uk

APPENDIX (iii)

QUESTIONNAIRE QUESTIONS

The Impact of ICT on Internal Controls' Prevention and Detection of Fraud

The purpose of this survey is to evaluate the impact of ICT tools and techniques on effectiveness of internal control in prevention and detection of electronic fraud in financial sector of Nigeria economy.

Please complete all sections as much as possible by selecting the best responses for each question. Kindly be rest assured that your responses will be treated with utmost confidentiality.

Thank you for your participation.

James Abiola

SECTION A

This section contains question about the person completing the questionnaire and the organization. Kindly answer each question in the space provided or thick the appropriate box.

1. Firm's name
.....
2. Please tick the primary business activity of your organization.
(a) Banking (b) Insurance (c) Mortgag (d) Stock
brokers
(e) Others.....
3. Which department are
you.....
4. What is the size of your internal audit department in terms of audit staff?
(a) Zero (b) 1-2 (c) 3-5 (d) 6-10 (e) > 10
5. Which section are you?.....
6. How many staff are in your section
.....
7. What is your current position?.....
8. How many years experience have you had in your present position
(a) Zero (b) 1-2 years (c) 3-5 years (d) 6-10 years
(e) > 10 years
9. What is your qualification?
(a) OND (b) HND/BSC (c) MSC/PHD (d) ACA/CPA etc
(e) Other Specify
10. Please tick appropriate box for your age
(a) < 25 (b) < 35 (c) <45 (d) < 60 (e) above 60

11. Please tick appropriate box for your gender? (a) Male..... (b)Female.....

How would you rate the extent of		None	Minimal	Adequate	Substantial	Extensive
Your knowledge in						
12.	General ICT Skills?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13.	Audit Specific IT Skills	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14.	Audit Software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15.	Continuous Online Auditing (COA)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

SECTION B: ICT and Fraud Prevention

This section contains information about the job you do. Kindly tick appropriate box

B		Strongly agreed	Agreed	Neither agreed/nor disagreed	Disagreed	Strongly Disagreed
(1)	I used ICT Tools and techniques in evaluating risk management.					
(2)	ICT tools and techniques improve level of Audit risk assessment					
(3)	I use ICT tools and techniques to test control within payroll application					
(4)	I use ICT tools and techniques to test control within e-payment application					
(5)	I use ICT tools and techniques to test control within e-purchase application					

(6)	The use of ICT tools and techniques to test control within e-sales application					
(7)	I use ICT tools and techniques to test control within e-receipt application					
(8)	I use ICT tools and techniques to test control within individual identity application					
(9)	I use ICT tools and techniques to identify weaknesses in internal control					
(10)	ICT tools and techniques improve Quality of internal control					
(11)	I use ICT tools and techniques to carry out tests on effectiveness of general control					
(12)	I use ICT tools and techniques to carry out tests on identity transaction flows					
(13)	ICT tools and techniques are used to test control within electronic funds transfer application					
(14)	I use ICT tools and techniques to periodically evaluate authorization control					
(15)	I use ICT tools and techniques to periodically carry out tests on segregation of duties					
(16)	I use ICT tools and techniques for the evaluation of security standards and procedures					
(17)	Continuous online auditing is effective in preventive control					
(18)	I use ICT tools and techniques for fraud detection					
(19)	ICT tools and techniques are effective in internal checks of transaction					
(20)	I use ICT tools and techniques to generate exception reports					
(21)	The use of ICT tools and techniques has made monitoring of transactions flow more effective as they occur					

Internal auditor’s use of ICT-based tools and techniques are effective in detecting electronic fraud

(22)	My organisation operate continuous on-line auditing				
(23)	Continuous on-line auditing is effective in detecting e-fraud				
(24)	Kindly list specific ICT-based audit tools and techniques you use				
(25)	Kindly list specific audit software you use for your work.....				
(26)	Kindly list the types of fraud you have used ICT-based tools and techniques to prevent				
(27)	Kindly list the types of fraud you have used ICT-based tools and techniques to detect.				

(28). Which of the following tools/ packages do you use (please tick)

Microsoft office application		Gemini Case-ware/Case view	
Bespoken software system		Property software packages developed by audit firm	
Audit software developed in-house		IDEA	
AS/2		Galileo	
Win EWP		ACL	
Financial Crime Investigator		DATAS for IDEA	
WIZ Rule		ADM plus	
Auto 2000		Expert Choice	
Pentana Tracker		Audit Master Plan	
Auto Audit SE		Others.....	

		Strongly agreed	agreed	Neither agreed/nor disagreed	disagreed	Strongly disagreed
(29)	My organisation provides knowledge based expert system					
(30)	ICT-based tools and techniques positively affects internal auditors reporting independence					
(31)	ICT-based tools and techniques positively affects internal auditors expression of professional opinion					

Thank you very much for your time.

APPENDIX (iv)

INTERVIEW QUESTIONS

Interview Questions

Impact of ICT on Internal Control Systems' Prevention and Detection of Fraud in Nigeria Financial Sector

James Abiola, PhD Research Student, Department of Accounting & Finance, Leicester Business School, De Montfort University, Leicester

Introduction

The purpose of this interview is to understand how internal auditor can be effective in handling the challenges of obtaining and evaluating electronic information using ICT tools and techniques in the e-business environment.

This study adopts Glover et al., (2001) definition of e-business as “the use of information technology and electronic communication networks to exchange business information and conduct transactions in electronic, paperless form”

(C) Level of ICT usage by Internal Auditors

1. In your opinion, which area of your audit work are benefiting from the use of ICT?
2. Which area of Internal Control do you think should be left exclusively for manual operations (human intervention)
3. What are the benefits and limitations derived from the use of ICT tools and techniques in Internal audit process?
4. What are the main computer hardware and software you are using for Internal Control/Internal audit purposes?
5. In what ways do you think your training needs are being met in terms of efficient usage of computer hardware and software provided by your organisation?
6. In what ways do you think the use of ICT tools and techniques affected the staffing needs of internal audit department?

(D) ICT and internal auditor independence

1. In what ways has the use of ICT affected your reporting responsibility?
2. In what ways has the use of ICT affected your operational responsibility?

(E) ICT and Prevention of e-fraud

1. What types of errors and frauds have been prevented by ICT tools and techniques?

(F) ICT and Detection of e-fraud

1. What types of frauds have been detected by the use of ICT tools and techniques?
2. Apart from using ICT tools and techniques for internal control purposes, what other impact(s) does the usage have on your organisation generally?
3. What role(s) do you think COA has for effective prevention/detection of frauds?

4. What is your assessment of the current and future directions of ICT tools and techniques and internal control in Nigeria financial sector?

APPENDIX (V)

COPY OF ONE EXAMPLE OF INTERVIEW CODING

CODING OF INTERVIEW DATA

ASSISTANT MANAGER, BANK A4

COLUMN 1: Question	COLUMN 2: Raw Data	COLUMN 3: Preliminary Code	Column 4: Final Code
C1	<p>“Size does not have any effect on the extent of ICT usage. As a matter of fact some of the older banks that are still very big have not reached the level of computerisation we have reached today. It is obviously difficult to transform your massive manual data into computer form if you don’t start with computer from inception. And of course it becomes more expensive as you now have numerous staff members who are computer illiterate and who may not be trainable. So it takes a lot of time and money to acquire computer hardware, software and training of staff members”</p>	<ol style="list-style-type: none"> 1. SIZE 2. TRAINING 3. COST OF ACQUISITION 	A1. ADOPTION OF ICT
C2	<p>“ICT tools and techniques are very useful for our operations but we have not been able to buy sophisticated knowledge based software like others because of cost and the level of our operations. We are still using a package developed in-house for our data analysis and there are some of our operations we still carry out manually. In these circumstances, we cannot talk about COA yet”</p>	<ol style="list-style-type: none"> 4. COST OF ACQUISITION 	A1. ADOPTION OF ICT

C3	“ The benefits of using ICT tools and techniques for internal control include on-line real-time tracking of records; on-line monitor of transactions; control and approval transfer to computer; generation of timely reports. The major disadvantage is lost of audit trails because of instantaneous nature of electronic transactions”	5. PERCEIVED BENEFITS	A1. ADOPTION OF ICT
C4	Don't want to say for security reasons and fear of competitors	-	--
C5	“We are being trained regularly . I can confirm to you that I could not use computer at all when I joined this bank 6 years ago. But now I am computer literate and well able to use some of our packages. I have done several trainings both locally and overseas”.	6. TRAINING 7. MANAGEMENT/ ORGANISATIONAL SUPPORT	A1. ADOPTION OF ICT
C6	“ICT has affected the staffing requirements of internal audit department. The bank now recruits well qualified staff that can be trained easily. Apart from the fact that the regulatory authority insisting on qualified accountants to man internal audit. The emphasis is now on qualified staff. Of course number of staff are reducing unlike when we depend on manual operations”	8. REDUCED STAFF 9. QUALIFIED STAFF	A1. ADOPTION OF ICT
D1	“It is quite easier to put audit reports forward to management and audit committee no matter how indicting the report might be to them since the report is a direct output from the machine and not manually generated. The manual reports that are indicting are	10. REPORTING INDEPENDENCE 11. PROFESSIONAL REPORT	A2. AUDITORS' INDEPENDENCE

	often looked at as witch hunting. Thus there is leverage on professional freedom for internal auditors”		
D2	“ICT tools and techniques allow me to take a lot of official routine and non-routine decisions without referring them further to my boss”	12. MOTIVATION 13. REPORTING INDEPENDENCE	A2. AUDITORS’ INDEPENDENCE
E1	“We have benefited from the use of ICT tools and technique in preventing errors and fraud in the area of money laundering, hacking, identity fraud which is very common, e-funds transfer, fraudulent bill settlement, and payroll fraud. The last two are internal fraud common with our staff.	14. PERCEIVED BENEFITS	A3. ICT USAGE A4. FRAUD PREVENTION
F1	ICT-based tools and techniques has helped us in timely fraud detection especially in identity fraud, e-fraud transfer, ATM fraud, money laundering, payroll fraud, bills payments, and hacking	15. PERCEIVED BENEFITS	A3. ICT USAGE A5. FRAUD DETECTION
F2	“Banks have numerous daily transactions that are being generated by bank staff, bank customers and third party. These are made possible by the use of on-line real-time technology. Going through these transactions one by one manually is impossible with the time and manpower available. The only visible option is to deploy	16. PERCEIVED BENEFITS	A3. ICT USAGE

	appropriate software that is capable of interrogating and analysing data as they occur ”		
F3	<p>“With over 200 branches scattered around the country it will be impossible to carry out a good job, in a good time considering human and material resources available for our use without COA in place. It enables us to work in different locations at the same time. It also enables real-time communication of data among audit staff. It saves a lot of time while 100 percent interrogation and checking of data is now possible. COA is very relevant for the prevention of errors and fraud. The advantage over traditional system is that errors and frauds are discovered and pointed out instantly because of its real-time capability. They are not left for months or possibly end of year before they are discovered.”</p>	<p>17. COA PREVENTS FRAUD 18. ALLOWS 100% POPULATION CHECK</p>	A4. FRAUD PREVENTION
F4	<p>“From internal auditing perspective, the use of ICT tools and techniques has been of immense advantage for effective internal control. It helps in immediate tracking of on-line transactions that might otherwise constitute a problem for lack of adequate audit trail. Another important aspect is</p>	<p>19. FUTURE OF ICT 20. EXTERNAL FACTOR</p>	A6. EXTERNAL PRESSURE

	<p>the timely generation of audit reports, most especially the exception report. There is no doubt that the use of ICT-based tools and techniques in processing transactions and indeed in internal control will be more popular especially in financial institutions as the regulatory authorities are now more concerned in it. They even show regulatory interest in the type of software you adopt for your operation.”</p>		
--	---	--	--

APPENDIX (vi)

RESPONSE FROM ONE OF THE BANKS

Appendix vi

Dear Mr Abiola,

“..... your area of research seems to be very interesting. However we will not be able to grant you any interview as a matter of policy unless we have your written assurance that the name of our bank will not be mentioned in any of your work. As you may aware banking.....
.....

If you are prepared to abide by this policy then let me hear from you again shortly while wishing you the best in your research endeavour”

AGM (Human Capital)

APPENDIX (vii)

INITIAL FREQUENCY TABLES

Frequency Tables for Initial Analyses

Table 6a: Analysis of participating organisation by business type:

	Frequency		Percentage		Cumulative %	
	Q	I	Q	I	Q	I
Banking	117	11	53.7	52.4	53.7	52.4
Insurance	59	6	27.1	28.6	80.7	81
Mortgage	26	3	11.9	14.2	92.7	95.2
Stock brokers	16	1	7.3	4.8	100	100
Total	218	21	100	100	100	100

Q = Questionnaire respondents, I = Interview respondents

Table 6a above indicates that internal auditors in the banking sector responded more than their counterparts in other financial sectors (172 representing 78.9 percent) Insurance, Mortgage and Stock-broking firms represent (46) 21.1 percent. The interview data also follows this trend with 11 (53.7 percent) interviewed in the banking sector while 10 (46.3 percent) were interviewed in insurance, mortgage and stock-broking institutions put together. The study will rely on these responses as the banking sector appears to be the dominant unit judging from the turnover of the banking unit, which is more than triple the size of turnover of all other units within the financial sector.

6b: Analysis of Respondents by Gender

Table 6b: Respondents' Gender

	Frequency		Percentage		Cumulative %	
	Q	I	Q	I	Q	I
Male	112	12	51.4	57.1	51.4	57.1
Female	106	9	48.6	42.9	100	100
Total	218	21	100	100	100	100

Q = Questionnaire responses I = Interview responses

Although there are more male participants in the questionnaire survey 112 (51.4 percent), the difference from that of the female participants 106 (48.6 percent) is marginal. The interview also follows this trend. Out of 21 interviews conducted 12 (51.4 percent) are male while 9 (48.6 percent) are female.

6 c: Qualification of Respondents

Question A9what is your qualification? (please tick)

Qualification

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid OND	47	21.6	21.6	21.6
HND/BSc	54	24.8	24.8	46.3
MSc/PhD	51	23.4	23.4	69.7
ACA/CPA/ACCA	60	27.5	27.5	97.2
Others	6	2.8	2.8	100.0
Total	218	100.0	100.0	

Table 6c Respondent’s qualification

A good number of respondents (more than 90 percent) have a college degree and or professional qualifications. Only 7.3 percent of the respondents are working without a degree or professional qualifications

Analysis of Respondent’s Age

Question A10.....Select appropriate box for your age.

Age

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Less than 25 years	28	12.8	12.8	12.8
Less than 35 years	97	44.5	44.5	57.3
Less than 45 years	63	28.9	28.9	86.2
Less than 60 years	30	13.8	13.8	100.0
Total	218	100.0	100.0	

Table 6d: Age of respondents.

More than 98 percent of the respondents fall below 45 years of age. Only a negligible percentage 1.8 percent is more than 45 and less than 65 years of age. This means the industry is dominated by age group between 25 and 45 years.

Analysis of Work Experience

QA11..... How many years have you worked in your current position?

Experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 1 year	48	22.0	22.0	22.0
	1-2 years	43	19.7	19.7	41.7
	3-5 years	45	20.6	20.6	62.4
	6-10 years	52	23.9	23.9	86.2
	Greater than 10 years	30	13.8	13.8	100.0
	Total	218	100.0	100.0	

Table 6e Respondents' experience in current position

Table 6e above shows that 86.2 percent of respondents have spent between 1 and 10 years in their current position as internal auditors. Only about 13.8 percent has more than 10 years internal auditing experience. Those internal auditors with six to ten years on the job experience dominated the group (52 representing 23.9 percent).

Analysis of Respondents' Current Position

	Frequency		Percentage		Cumulative %	
	Q	I	Q	I	Q	I
Officer	96	1	44	4.8	44	4.8
Assistant Manager	73	5	33.5	23.8	77.5	28.6
Manager	29	6	13.3	28.5	90.80	57.1
Senior Manager	20	9	9.2	42.9	100	100
Total	218	21	100	100	100	100

Q = Questionnaire respondents, I = Interview respondents

Table 6f Participants' current position

Table 6f above shows that the highest number of participants, 96 (44 percent) are officers while 73 (33.5 percent) are assistant managers. The number of Managers 29 (13.3 percent) and Senior Managers 20 (9.2 percent) are comparatively small. Conversely, senior managers have the highest participants for the interview, 9 (42.9 percent), 6 (28.5 percent) for Managers, 5 (23.8 percent) for assistant managers and only 1 (4.8 percent) for the officer.

Analysis of Respondents' Department

	Frequency		Percentage		Cumulative %	
	Q	I	Q	I	Q	I
Internal Control	155	15	71.1	71.4	71.1	71.4
Internal Audit	63	6	28.9	28.6	100	100
Total	218	21	100	100	100	100

Q = Questionnaire respondents, I = Interview respondents

Table 6g participants' department

Table 6g shows that participants indicated internal control 155 (71.1 percent), internal audit 63 (28.9 percent); it appears what name given to each organisation is a matter of choice as the two nomenclatures cut across all units in the financial sector. However, internal control is most dominant in the banking sector, while Insurance companies mostly use internal audit. This trend is also noticeable with interview participants, with 15 (71.4 percent) indicating that they come from internal control department while six (28.6 percent) indicate their department as internal audit. The study takes the two departments, internal control and internal audit, to mean the same thing.

Staff Population in Internal Audit Department

Staff Population

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid < 2 staff	14	6.4	6.4	6.4
2 staff	22	10.1	10.1	16.5
3 to 5 staff	87	39.9	39.9	56.4
6 to 10 staff	52	23.9	23.9	80.3
>10 staff	43	19.7	19.7	100.0
Total	218	100.0	100.0	

Table 6h: Number of staff members in internal audit department.

Table 6h shows that 43 (19.7) percent of participants' organisations have ten or more staff in their internal audit department, 52 (23.9) percent have between six and ten staff, while 87 (39.9) percent have between three and five staff. 22 (10.1) percent have either one or two staff. However 14 representing 6.4 percent have only one person in audit department.

APPENDIX (viii)

EFCC DECIDED CASES

Economic and Financial Crimes Commission (EFCC) Cases Involving Internet Fraud

A sample of concluded cases as reported by the Media and Publicity Unit of the commission (EFCC) are reproduced here. Within a time frame of 36 months there are more than 1000 reported internet related fraud cases. Some of these cases involved advanced fee fraud and money laundering.

288 Jailed for Interne Fraud–EFCC



Mohammed Bello Adoke, AGF , Minister of Justice, Joanna Hewitt, A.O. Special envoy of Australian P.M to West Africa with the Executive Chairman, EFCC, Ibrahim Lamorde at the “Regional engagement meeting on transnational fraud for West African Law Enforcement Agencies holding at the EFCC Academy, Karu, Abuja.

The Chairman of EFCC , Ibrahim Lamorde has revealed “that the Commission has convicted more than 288 persons over sundry Internet crimes. He also disclosed that four fugitives were extradited to the United States and another 234 cases are still being prosecuted in courts across the country” (Media and Publicity Unit, EFCC, 2012)

Sample Cases from EFCC websites

Case 1

EFCC Arraigns Two Over \$149,000.00 Love Scam

“The Economic and Financial Crimes Commission, EFCC, has arraigned two internet fraudsters, Olubode Olukotun and Olamide Adekeye on a 22 count charge bordering on obtaining money under false pretence, to the tune of One Hundred and Forty

Nine Thousand Dollars (\$149,000.00) before Justice Akinteye, of the Oyo State High Court, Ibadan.

The accused persons were alleged to have obtained the sum from two American citizens, Janet Nelson and Louise Cecchni, in a romance scam. When the charges were read to the accused persons, they pleaded not guilty to the charges.

The prosecuting counsel, Kayode Oni asked the court to remand the accused persons in prison custody while requesting for a date for the commencement of trial. However, defence counsel, Olaniyi, told the court that he had already filed a bail application since April 1st, and served the prosecution since April 17.

However, Oni countered that it was against the law to file for bail when the accused had not been arraigned Olaniyi therefore pleaded that the accused be remanded in SSS custody. Justice Akinteye adjourned the matter till May 15th, 2012 and ordered that the accused be remanded in prison custody.

The accused persons were arrested on June 14, 2011 at Borem Inn, Ibadan by operatives of the Department of State Security, SSS and handed over to the EFCC on June 28, 2011. Adekeye, a 25-year old student of Biochemistry, Ajayi Crowther University, Oyo confessed to scamming one Janet Nelson, an American lady online in a dating gambit. He claimed to have met her through yahoo messenger where he saw her pictures. He dated her using the false identity of a David Donovan, a successful American. He successfully fleeced her of Ninety Thousand Dollars (\$90,000.00) which she sent to him in various instalments through Western Union money transfer and also through GoldExPay. From the proceeds of the crime he bought a Peugeot 407 saloon car for himself.

On his part, 28-year old Olubode, a fresh graduate of University of Ilorin, awaiting call up to National service posed as Scott Ferguson, a Caucasian to fleece Louise Cecchni of the sum of Fifty Three Thousand dollars (\$53,000.00) in various installments. He obtained the money under the guise of a short loan facility, with a promise to refund his internet lover. Both signed a promissory note to that effect and she started wiring him the hard currency through a GoldExPay account he maintained with Liberty Reserve. From proceeds of the heist, Olubode bought for himself an infinity M35x 2007 model saloon car for four million four hundred thousand Naira (N4.4million)" (EFCC, 2012)

Case no 2

Court Extradites Nigerian to US Over Fraud

“Justice James Tsoho of the Federal High Court Ikoyi, Lagos on Monday, May 28, 2012 granted the request of the Attorney General of the Federation that one Godwin Chiedo Nzeocha be extradited to the United States of America to face criminal charges over alleged Health Care Benefit Fund fraud involving \$30 million. Nzeocha, 54 worked with the city nursing services in Houston, Texas, USA as a physical

therapist aide between 2007 and 2009. There, he was alleged to have conspired with others and submitted claims worth \$45 million to the Medicare and Medicaid for health care services on behalf of some patients who are beneficiaries of the health insurance claims” (EFCC, 2012)



Court Extradites Nigerian to US Over \$30m Fraud

“In a related case involving \$3.2million scam, Olaniyi Jones Makinde faces extradition. Justice James Tsoho of the Federal High Court, Lagos will on May 30 2012 hear the extradition request filed by the office of the Attorney General of the Federation against 26-year old Olaniyi Jones Makinde who is wanted in the United States of America for alleged criminal offences bordering on wire fraud.

Olaniyi Jones is wanted in the United States for criminal offences committed by his syndicate, which include six other persons: Karlis Karkins, Charles Chidi, Waya Nwaki, Osarhieme Obaygbona, Marvin Dion Hill and Alphonsus Osuala.

Between August 2009 and June 2010, Olaniyi and his six co-defendants worked together across three continents as part of a conspiracy to steal approximately Three

Million Two Hundred Thousand United States Dollars (\$3.2million) from payroll companies and banks. To do so they used internet “phishing attacks” and bogus websites to trick unwitting consumers into giving up their online user names and passwords. After obtaining this personal identification information, Karlins, Chidi and other members of the syndicate added fake employees to the payroll accounts of victim companies at payroll processing companies. They used these victims’ online accounts to ‘pay’ the fake employee through electronic transfers. The syndicate then shared the proceeds by transferring them to accounts that they controlled overseas via bank wire, Western Union and Money gram. The Federal Bureau of investigation, FBI reveals that Olaniyi Jones had two specific roles in the conspiracy. First he opened bank accounts in Nigeria into which the fraudulent proceeds of the scheme were wired. Olaniyi also used a fraud commonly known as ‘romance scam’, where he assumed the false identity of a young European woman online, to trick men into believing that they were having a romantic relationship with a “Brenda Stuart” He operates e-mail accounts in the name of Brenda Stuart” (EFCC, 2012)

Case no. 3

Court Jails Undergraduate 20 Years Over Internet Scam

“Justice Mohammed I Shuaibu of the Federal High Court, sitting in Kaduna, on June 5, 2012, sentenced an undergraduate of the University of Ilorin, Imonina Kingsley, 25, to 20 years imprisonment on a four count charge of impersonation, possession of fraudulent documents and attempt to obtain money by false pretences preferred against him by the Economic and Financial Crimes Commission, EFCC.

One of the four count charges for which he was sent to jail reads: ‘That you, Imoina Kingsley “M” on or about 4th April 2008 at Ilorin, Kwara state within the jurisdiction of the Federal High Court did obtain by false pretence the sum of One Thousand US dollars (\$1000.00) from one Mr. Christopher De Troy through the use of a scam letter via your mail box thomasduke4luv@yahoo.com thereby committed an offence contrary to section 8(a) and punishable under section 1(3) of the Advance Fee Fraud and other Fraud Related Offences Act 2006”.

Kingsley, who is to spend five years on each of the four count charges gave his address as at the time of his arrest as Rubby Hostel, Tipper Garage, Tanke Ilorin, Kwara State. He hails from Ndokwa East Local Government Area of Delta State.

The suspect who was arrested on April 4, 2008, during a special operation code-named Operation Cyber Storm 1 at wave Network Cyber Cafe located along Pipeline Road, Tanke, Ilorin, Kwara State, used the false identity of a Mr. Thomas Duke a supposed gay from the United Kingdom with the e-mail

address given as thomasduke4luv@yahoo.com to send fraudulent mails with intent to defraud the unsuspecting victims.

In other instances, he also claimed to be one Muyiwa Akanbi, a Beninoise and Mary Jones.

In his confessional statement, Kingsley admitted that the e-mail address: thomasduke4luv@yahoo.com belongs to him and that he is into the “business” to make money and pay his fees at the University of Ilorin, Kwara State where he was studying Geology and Mineral Sciences. He also confessed that on February 12th, 2008, he sent an e-mail to Luis Barco, attaching a photograph of an unknown man which he downloaded from the internet and claimed to be a gay by the name Muyiwa Akanbi.

At another time, he mailed a message and presented himself to one Mr. Andrew Corrigan as a Uk born gay but based in Africa. Another of his victim is Mr. Christopher De Troy of America, whom he hoodwinked into parting with \$1,000.00 via Western Union when he presented himself as a gay from the Republic of Benin” (EFCC, 2012)

In a related development “EFCC has secured a conviction in the case involving Jacob Chinenye Isintume a.k.a. Price Williams Mbeki who was charged to court on a three count charge of unlawful possession of documents of false pretence, Justice L Akanbi on Wednesday June 13th 2012 at the Federal High Court sitting in Port Harcourt, Rivers State, convicted and sentenced Jacob Chinenye Isintume to seven years imprisonment without an option of fine, on two out of the three count charges preferred against him.

It would be recalled that Isintume was arrested on January 2nd 2012, at Ocabik Planet Hotel. Off Stadium Road, Port Harcourt, Rivers State, by officers of the Intelligence Detachment Headquarters, JTF Operation Restore Hope. At the time of his arrest, he was in possession of a laptop computer with various forged documents stored in it, as well as a superimposed image of himself on pictures of the former United States President, Mr. George W. Bush and former British Prime Minister Mr. Tony Blair” (EFCC, 2012)

Case No. 4

Court Jails Banker Six Months Over 12 Million Naira (about £48,000.00) ATM Fraud

“A former banker with First Monument Bank Plc (FCMB), Olajide Ogundipe, was on February 15th, 2012 sentenced to 6 months imprisonment by a Federal High Court presided by Justice Alaba Ajileye in Lokoja, Kogi State, over a 12.3 million Naira

ATM fraud. Ogundipe, a cash officer with the bank was arraigned by Economic and Financial Crime Commission in March for eight (8) count charge bordering on criminal conspiracy and theft to which he initially pleaded not guilty. As the case commenced and more evidences against the accuse person emerged through the prosecution witness, the accused person changed his plea and pleaded guilty to all the charges. He was subsequently sentenced to six months imprisonment with an option of fine of ten thousand naira on each of the charge. In sentencing the accused, the judge took consideration of the fact of Ogundipe's ill health and refund of entire stolen sum to the bank through the EFCC even before he was charged to court" (EFCC, 2012)

Case No. 5

Two Billion Naira¹³ Money Laundering Suspect Arraigned by the EFCC

"The Economic and Financial Crimes Commission, EFCC, on June 18th 2012, arraigned twelve persons before Justice Gladys Olotu of the Federal High Court, sitting in Abuja on a twenty-two count charge bordering on money laundering to the tune of over two billion naira (2 billion naira).

Those arraigned are seven individuals and five corporate bodies. They are Chidi David Adabanya, Uzoma Ibe, Feyaikeban Ebakpa, Kwokwo Ebiki Bina, Beneth Ezekiel-Hart, Bolouwenimo Kwokwo, and Presley Ebakpa. Others are Forstech Technical Nig Limited, Gastroil Ventures Limited, Bilyiis Integrated Services Limited, Fun-Ala Nigria Ltd and Fambo Integrated Services Limited.

¹³ About £8 million (British pounds)



Suspects of Money Laundry Arraigned by the EFCC at the Federal High Court, Maitama, Abuja

Between April 2010 and July 2010 in Abuja, Adabanya and Forstech Technical Nigeria Limited were alleged to have transferred the total amount of Nine Hundred and Twenty seven Million, One hundred and Ninety One Thousand, Two Hundred and Seventy Seven Naira Ninety Eight Kobo (927,191,277.98 Naira). The amount is alleged to have been deducted from an illegal act from the account of Forstech Technical Nigeria Limited in Stanbic IBTC Bank Plc to the account of Gastroil Ventures Limited with Stanbic IBTC stockbrokers limited.

The seven persons pleaded not guilty to the twenty two count charges read to them. The Judge granted bail to the accused persons in liberal terms. Each was granted bail in the sum of five million naira and one surety in like sum. The Judge said that if the surety is not a civil servant, he must have a landed property which should be verified by the court. The court then adjourned hearing to October 2nd 3rd and 4th 2012". (EFCC, 2012)

Foreign Interests in Nigeria Internet Crime Prevention

Foreign governments and agencies like Federal Bureau of Investigation (US); Australian Federal Police (AFP), Canadian Police and British Interpol are all interested in the success of EFCC because internet crime is not limited by geographical boundaries. They have volunteered resources as well as technical knowhow to help EFCC combat internet fraud.

In fulfillment of this aim, the Australian Police recently signed a Memorandum of Understanding with the EFCC.

EFCC and Australian Police signed MoU



“The Chairman of the EFCC, Mr. Ibrahim Lamorde, signing the MoU, (centre) and from (left to right) the Australian Ambassador to Nigeria Mr. Ian McConville, Superintendent Richard Stanford, Liason Officer of the Australian Federal Police based in Pretoria, South Africa and the Commission Secretary, Emmanuel Akomaye. The MoU will foster understanding and enhance law enforcement partnership between Nigeria and Australia. In addition to the MoU, a “three day regional workshop on cyber crime was convened by the Economic and Financial Crime Commission, EFCC, and the Australian Federal Police, AFP, ended in Abuja on Wednesday, April 18th 2012, with a call on the Economic Community of West Africa States, ECOWAS, to establish a convention on cyber crime to fashion a common law among member states in order to promote cooperation among them in the fight against cyber crimes”. (EFCC, 2012)

