



**The Impact of the SysTrust's Framework as an
Internal Control of AIS Process upon Business
Performance via the Mediating Role of
Financial Quality Reporting: An Integrated
Model**

A Thesis Submitted for the Degree of Doctor of Philosophy

By

Ahamed Hani Al-Dmour

April 2018

ABSTRACT

This study aims to examine and validate the impact of the implementation of SysTrust's framework (principles and criteria) as an internal control method for assuring reliability of Accounting Information System on the business performance via the mediating role of the quality of financial reporting among Jordanian public listed companies. Based upon the literature review and contingency theory, an integrated conceptual framework was developed to guide this study. The study's conceptual framework consists of three major constructs: The SysTrust's service framework (availability, security, integrity processing, confidentiality, and privacy), the business performance (financial and non-financial indicators) and the quality of financial reporting. Descriptive correlational survey design approach is used in this study used as it sought to describe and establish the relationships among the study variables and it employs quantitative method to test the hypotheses first, and then to answer the research questions. Data were collected through self-administrated questionnaire with 239 respondents. Several statistical techniques were used to analyse the collected data. The model fitness and the constructs' validity and reliability were tested, followed by the validation of the conceptual model and research hypotheses.

The findings of the study support the proposition that availability of SysTrust requirements as internal method for assuring the reliability of AIS is positively linked to business performance via the mediating role of the quality of financial reporting. Therefore, a better understanding of the influence of SysTrust principles upon business performance and quality of financial reporting should be viewed as whole rather than isolated fragments. The magnitude and significance of the loading estimate indicate that all of these five principles of SysTrust are relevant in predicating business performance and quality financial reporting.

Thus, this study and its findings have number of contributions and managerial implications. In terms of theoretical contributions, this study has extended the reliability of AIS literature by providing the following: First, it explained the unexplored relationship among the reliability of AIS, the quality of financial reporting using the IASB's framework fundamental qualitative characteristics and business performance indicators (financial and non-financial). Second, testing the impact of the role of the quality of financial reporting as a mediating factor between the reliability of AIS and business performance measures (financial and non-financial) considered another contribution for the current study. Furthermore, the SysTrust's framework implementation as an internal control system for assuring the reliability of AIS could be considered as the critical intangible resources for any business organization seeks for a reliable and effective accounting system in the long run. In this study, financial reporting quality justified as the mediator from contingency theory perspective where good quality and effective of information system is an integral component of a strong internal control system.

Declaration

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed..... (Candidate)

Date.....

ACKNOWLEDGMENTS

First, all praise and thanks are to ALLAH, the Almighty, for the grace and strength He has given me to complete my PhD research; all His blessings, mercies and guidance have enabled me to achieve this work.

I would like to start with the person who made the biggest difference in my life, my mentor, my greatest appreciation goes to the best dad, Professor Hani Al-Dmour, He has been motivating and inspiring every bit of me towards new possibilities in life. Without him I would not be where I am today.

I would like to express my greatest and warmest thanks and gratitude to my first supervisor, Dr Maysam Abbod who has been my real guru since the beginning of my academic journey. He has always kept me on the right direction during all stages of my PhD study, and his patience, unlimited help, collaboration, kindness, enthusiasm, guidance, support, constructive comments and continuous encouragement are highly appreciated. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my PhD study.

I would like to acknowledge the people who mean world to me, my lovely parents, my brothers (Mohammad and Yazeed) and my sister Dr Rand. I extend my respect to my parents, my paternal and maternal grandparents and all elders to me in the family. I don't imagine a life without their love and blessings. Thanks to my great mom, dad, uncle and aunty for showing faith in me and giving me liberty to choose what I desired. I consider myself the luckiest in the world to have such a supportive family, standing behind me with their love and support.

Last but by no means least, I offer my regards and blessings to all my colleagues and friends who have supported me during the completion of my PhD journey

Dedications

I dedicate this work to God almighty, to whom all glory shall always be, for his grace and strength that helped me to accomplish this work. I also dedicate this work to my parents, for making me who I am today.

To my dad for all the things he has done for me since day one. Thank you for being my Dad, my Teacher, and my friend Prof. Hani Aldmour

AUTHOR'S PUBLICATIONS

Papers Published

1. Al-Dmour, A. Mofawiz K Al-Fawaz, Al-Dmour, R, Allozi, N (2017) "Accounting Information System and Its Role on Business Performance: A Theoretical Study", Journal of Management and Strategy Vol. 8, No. 4. Pp.79-89.
2. Al-Dmour, A. and Abbod, M, "Qualitative Characteristics of Financial Reporting and Non-Financial Business Performance", International Journal of Corporate Finance and Accounting (IJCFA), Vol. 4, Issue 2 pp. 1-20.
3. Al-Dmour, A. Abbod, M and Al-Dmour, R, (2018) "The Impact of the Implementations of the Sysrust' Framework upon the Quality of Financial Reporting: Structural Equation Modelling Approach", Accounting and Management Information Systems, Vol. 17, No. 1, pp. 69-99.
4. Al-Dmour, A. Abbod, M, (2018) "The Impact of the Quality of Financial Reporting on Non-Financial Business Performance and the Role of Organizations Demographic' Attributes (type, size and experience)" Academy of Accounting and Financial Studies Journal. Vol. 22, No 18. PP.1-18.
5. Al-Dmour "The Impact of The Reliability of The Accounting Information System Upon the Business Performance via The Mediating Role of The Quality of Financial Reporting" International Journal of Accounting and Business Society. Vol 26, No 1.PP.56-88.

Accepted Papers

6. Al-Dmour, A. Abbod, M and Al-Dmour, H, "The Implementation of SysTrust Principles and Criteria for Assuring Reliability of AIS: Empirical Study", International Journal of Accounting and Information Management, Forthcoming issues 2019.
7. Al-Dmour, A. Abbod, M' The SysTrust's Framework Implementation as an Internal Control for Assuring Reliability of AIS and Business Performance: An Integrated Approach, International Journal of Accounting and Finance.

TABLE OF CONTENTS

THE IMPACT OF THE SYSTRUST'S FRAMEWORK AS AN INTERNAL CONTROL OF AIS PROCESS UPON BUSINESS PERFORMANCE VIA THE MEDIATING ROLE OF FINANCIAL QUALITY REPORTING: AN INTEGRATED MODEL	I
<i>ABSTRACT</i>	II
<i>Declaration</i>	III
<i>ACKNOWLEDGMENTS</i>	IV
<i>Dedications</i>	V
<i>AUTHOR'S PUBLICATIONS</i>	VI
<i>TABLE OF CONTENTS</i>	VII
<i>LIST OF FIGURES</i>	XI
<i>LIST OF TABLES</i>	XII
<i>List of Abbreviations</i>	XV
CHAPTER ONE	1
INTRODUCTION.....	1
1.1 <i>Research Background</i>	1
1.2 <i>Problem Statement</i>	6
1.3. <i>Research Aim, Objectives and Questions</i>	8
1.4 <i>Significance of the Study</i>	10
1.5 <i>Thesis Structure</i>	11
CHAPTER TWO	12
THEORETICAL BACKGROUND & LITERATURE REVIEW.....	12
2.1 INTRODUCTION.....	12
2.2 THEORETICAL BACKGROUND	13
2.2.1 <i>Accounting Information System</i>	13
2.2.2 <i>Internal Control System</i>	17
2.2.3 <i>Types of Accounting Internal Control Frameworks</i>	21
2.2.4 <i>Literature Review on Reliability of AIS</i>	43
2.2.5 <i>Quality of Financial Reporting</i>	51
2.3 THE LIMITATIONS OF THE PREVIOUS STUDIES. RESEARCH GAPS.....	58
2.4 SUMMARY	60
CHAPTER THREE	61
THE PRELIMINARY INTERVIEWS AND ACCOUNTING INTERNAL CONTROL SYSTEM IN JORDAN	61
3.1 INTRODUCTION	61

3.2 OBJECTIVES OF THE PRELIMINARY INTERVIEWS.....	61
3.3 THE STRUCTURE OF THE PRELIMINARY INTERVIEWS.....	62
3.4 PLANNING FOR THE PRELIMINARY INTERVIEWS.....	62
3.5 DATA GATHERED THROUGH THE PRELIMINARY INTERVIEWS	63
3.5.1 <i>Jordan's Statutory Framework for Accounting and Auditing</i>	63
3.5.2 <i>Audit Profession Development in Jordan</i>	65
3.5.3 <i>Practicing Auditing Development in Jordan</i>	65
3.5.4 <i>Financial Reporting by Public Companies in Jordan</i>	68
3.5.5 <i>Financial Reporting in Jordan and its Effect on the Accounting and Auditing Profession</i>	70
3.5.6 <i>Internal Control System Assessment</i>	71
3.6 THE RESULTS OF INITIAL INTERVIEW	72
3.7 SUMMARY	73
CHAPTER FOUR.....	74
THE STUDY'S CONCEPTUAL FRAMEWORK	74
4.1 THE NATURE OF THE CONCEPTUAL FRAMEWORK.....	74
4.2 MAIN CONSTRUCTS OF THE STUDY'S CONCEPTUAL FRAMEWORK	76
4.2.1 <i>The Quality of Financial Reporting</i>	76
4.2.2 <i>The Business Performance</i>	83
4.2.3 <i>Major Components /Constructs of SysTrust's Framework</i>	85
4.3 RESEARCH HYPOTHESES	103
4.4 SUMMARY	104
CHAPTER FIVE	106
RESEARCH METHODOLOGY	106
5.1 INTRODUCTION	106
5.2 RESEARCH DESIGN	106
5.3 RESEARCH APPROACHES	109
5.4 RESEARCH PARADIGMS	110
5.5 RESEARCH DESIGN PROCESS.....	111
5.6 DATA COLLECTION METHODS.....	113
5.7 TYPES OF QUESTIONING METHODS.....	113
5.8 STRUCTURE OF THE INTERVIEW	114
5.9 THE DOMAIN OF RESPONDENTS.....	115
5.10 KEY INFORMANT APPROACH	115
5.11 SCALE OF MEASUREMENT	116
5.12 PILOT STUDY: METHODOLOGY.....	117
5.13 DEVELOPMENT OF QUESTIONNAIRE ITEMS	118

5.14 ETHICAL CONSIDERATIONS	118
5.15 PREPARING FOR DATA ANALYSIS	119
5.16 CLASSIFICATION OF STATISTICAL TECHNIQUES	120
5.17 STATISTICAL METHODS USED FOR RESEARCH OBJECTIVES	121
5.17.1 Factor Analysis	121
5.17.2 Multiple Regression Analysis.....	122
5.17.3 Artificial Neural Networks Model.....	124
5.17.4 Structural Equation Modelling	126
5.18 STATISTICAL METHODS USED FOR TESTING RESEARCH HYPOTHESES.....	131
5.19 SUMMARY	133
CHAPTER SIX	134
DATA ANALYSIS AND TESTING HYPOTHESES	134
6.1 INTRODUCTION	134
6.2 FIRST SECTION: THE FINDINGS OF THE FACTOR ANALYSIS	135
6.3 THE INTERPRETATION OF THE FINAL FACTOR ANALYSIS	135
6.3.1 Main Constructs of the SysTrust Service Conceptual Framework	135
6.4 VALIDITY ASSESSMENT	150
6.5 SUMMARY OF THE FACTOR ANALYSIS	152
6.6 SECTION TWO: DATA ANALYSIS AND TESTING HYPOTHESIS	153
6.7 THE EXTENT OF THE RELIABILITY OF AIS PROCESS IN THE CONTEXT OF THE IMPLEMENTATION OF THE SYSTRUST'S FRAMEWORK REQUIREMENTS (PRINCIPLES AND CRITERIA).....	154
6.8 RELATIONSHIP BETWEEN THE RELIABILITY OF AIS AND THE QUALITY OF FINANCIAL REPORTING	158
6.9 THE RELATIONSHIP BETWEEN THE RELATIONSHIP BETWEEN THE RELIABILITY OF AIS AND BUSINESS PERFORMANCE DIMENSIONS (FINANCIAL AND NON-FINANCIAL); TAKEN TOGETHER OR SEPARATELY	161
6.9.1 Multiple Regression Findings	161
6.9.2 Stepwise Multiple Regressions: Non- Financial Performance Dimension (As a Dependent Variable; taken alone).	163
6.9.3 Stepwise Multiple Regressions. Financial Performance Dimension as a Dependent; taken alone... 163	
6.9.4 Stepwise Multiple Regressions. Financial and Non-Financial Performance Factors; taken Together.	164
6.10 THE RELATIONSHIP BETWEEN THE RELIABILITY OF AIS AND BUSINESS PERFORMANCE VIA THE QUALITY OF FINANCIAL REPORTING AS A MEDIATING	166
6.11 NEURAL NETWORKS ANALYSIS AND COMPARISON	170
6.12 STRUCTURAL EQUATION MODELLING. THE VALIDATION OF THE STUDY'S CONCEPTUAL MODEL.....	174
6.12.1 Measurement Model: Confirmatory Factor Analysis	174
6.12.2 Structural Model	181
6.13 SUMMARY	183

CHAPTER SEVEN.....	185
CONCLUSION, CONTRIBUTIONS AND FUTURE STUDIES.....	185
7.1 CONCLUSION.....	185
7.2 MAIN CONCLUSIONS OF THE RESEARCH FINDINGS	186
7.2.1 <i>The Extent of the Implementation of the SysTrust's Framework. The Finding of the First objective</i>	188
7.2.2 <i>The Relationship between the Implementation of SysTrust's Framework and the Quality of Financial Reporting. The Findings of the Second objective.....</i>	190
7.2.3 <i>The Relationship between the Implementation of SysTrust's Framework and the Business Performance. The Findings of the third objective</i>	190
7.2.4 <i>The Role of the Quality of Financial Reporting as a Mediator between the Implementation of SysTrust's Framework and Business Performance. The Findings of the Fourth Objective</i>	192
7.2.5 <i>Comparison between the Performance of ANN and MRA Tests</i>	192
7.2.6 <i>The Validation of the Study's Conceptual Model: The Findings of the Fifth Objective</i>	193
7.3 RESEARCH CONTRIBUTIONS.....	194
7.3.1 <i>Theoretical and Methodological Contributions.....</i>	195
7.4 RESEARCH LIMITATIONS	199
7.5 AREAS FOR FURTHER RESEARCH.....	200
REFERENCES.....	202
APPENDIX A	221
APPENDIX B	226
APPENDIX C	244

LIST OF FIGURES

Fig. 4.1 Study's Conceptual Framework.	75
Fig. 4.2 Relationships among principles of the system reliability.	86
Fig. 4.3 Requirements of Information Integrity.	99
Fig. 4.4 A Summary of Conceptual Framework Relationships.	105
Fig. 5.1 Simple Neural Network Topology	125
Fig. 5.2 A classification of Fit Measures.	128
Fig. 6.1 The Study's Conceptual Framework.	154
Fig. 6.2 The Relative Importance of the Predictors of Business performance indicators (combined) based on ANN.	172
Fig. 6.3 The Relative Importance of the Predictors of Financial Performance based on ANN.	172
Fig. 6.4 The Relative Importance of the Predictors of Non-Financial Performance based on ANN.	173
Fig. 6.5 Second-order Factor analysis of quality reporting.	177
Fig. 6.6 Path Diagram of the Study's Structural Model	182

LIST OF TABLES

Table 2.1 Types of Assessing Accounting Information System. COSO vs. COBIT.	27
Table 2.2 The Structure of the SysTrust Services Framework.	29
Table 2.3 The Differences between SAS 70 Audit and SysTrust Engagement.	42
Table 2.4 Qualitative Characteristics of the Quality of Financial Reporting.	53
Table 3.1 List of the Interview Questions.	62
Table 3.2 The Objectives of Each Stage of the Preliminary Interviews.	63
Table 4.1 The Characteristics of the Quality of Financial Reporting.	77
Table 4.2 The SysTrust's Framework. Principles and Criteria.	87
Table 4.3 Types of Security Control.	89
Table 4.4 Research Hypotheses.	103
Table 5.1 The Domain of the Study's Respondents.	115
Table 5.2 Research Objectives and Techniques of Data Analysis.	131
Table 5.3 Summary Research Design and Data Collection techniques	133
Table 6.1 Factors Underlying the Main Principles Systrust's Model.	135
Table 6.2 KMO and Bartlett's Test.	136
Table 6.3 Total Variance Explained.	136
Table 6.4 Main Factors Underlying the Availability of AIS Measures.	136
Table 6.5 KMO and Bartlett's Test.	138
Table 6.6 Total Variance Explained.	139
Table 6.7 The Main Factors Underlying the Security of AIS Measures.	139
Table 6.8 KMO and Bartlett's Test.	140
Table 6.9 Total Variance Explained.	141
Table 6.10 The Main Factors Underlying the Integrity Processing of AIS Measures.	141
Table 6.11 KMO and Bartlett's Test.	143
Table 6.12 Total Variance Explained.	143
Table 6.13 The Main Factors Underlying the Confidentiality of AIS Measures.	143
Table 6.14 KMO and Bartlett's Test.	145
Table 6.15 Total Variance Explained.	145
Table 6.16 The Main Factors Underlying the Privacy of AIS Measures.	145
Table 6.17 KMO and Bartlett's Test.	146

Table 6.18 Total Variance Explained.	147
Table 6.19 The Main Factors Underlying the Quality of Financial Reporting Measures.	147
Table 6.20 KMO and Bartlett's Test.	149
Table 6.21 Total Variance Explained.	149
Table 6.22 The Main Factors Underlying the Business Performance Measures.	150
Table 6.23 Survey of Average Explained Variance and Reliability Estimations of all Measures of SysTrust constructs.	151
Table 6.24 Summary of the Factors underlying the major constructs SysTrust.	153
Table 6.25 Factors underlying the Quality of Financial Reporting Measures.	153
Table 6.26 Summary of the Factors underlying Business Performance Measures.	153
Table 6.27 The level of Reliability of AIS in Business Organizations.	155
Table 6.28 The level of significance of the SysTrust's Framework Implementation among Groups of Organizations based on the type of Business industrial vs. Services.	156
Table 6.29 The level of significance of the SysTrust's Framework Implementation among groups of Organizations based on the Size of Business.	157
Table 6.30 The level of significance of the SysTrust's Framework Implementation among groups of Organizations based on the Experience in Business	158
Table 6.31 A Summary Result of the Multiple Regressions. The Relationship between the Reliability of AIS based upon the Implementation of the Principles of the SysTrust's framework and the quality of Financial Data Reporting.	159
Table 6.32 Collinearity Diagnostics.	160
Table 6.33 The Stepwise Regression Analysis. Factors of the SysTrust; Taken Together.	160
Table 6.34 A Summary Result of the Multiple Regressions. The Relationship between the reliability of AIS and Business Performance Dimensions; separately and together.	162
Table 6.35 The Stepwise Regression Analysis. Financial Performance.	163
Table 6.36 The Stepwise Regression Analysis. Non- Financial Performance.	164
Table 6.37 The Stepwise Regression Analysis. Combined Financial and Non-Financial Dimensions Together.	165
Table 6.38 A summary of the Stepwise Regression Analysis. The Importance of the	166

SysTrust Factors Related to Business Performance.	
Table 6.39 Steps for testing mediation.	167
Table 6.40 Regression Analysis for Mediation of Quality of Financial Reporting on Business Performance through the Implementation of SysTrust Principles.	168
Table 6.41 The Sobel Test Value	170
Table 6.42 Performance Comparison between ANN and MRA Model Using Statistical Criterion.	171
Table 6.43 The Relative Importance of SysTrust Factors Related to Business Performance Indicators based on ANN Analysis.	174
Table 6.44 Results of Measurement Model-second order Factor. Quality of Financial Reporting.	175
Table 6.45 Results of Measurement Model-second order Factor. Business Performance.	177
Table 6.46 Results of Measurement Model all constructs.	178
Table 6.47 Composite Reliability and Average Variance Extracted.	179
Table 6.48 Standardised Regression Weights.	180
Table 6.49 Discriminate Validity.	180
Table 6.50 Fit Indices of Structural Model.	181
Table 7.1 The Most Important Factors of SysTrust Principles that Influence the Quality of Financial Reporting and Business Performance in terms of the order of importance.	187
Table 7.2 A summary Comparison between the Influence of SysTrust and Quality of Financial Reporting upon the Business Performance.	188
Table 7.3 The level of Reliability of SysTrust Principle in Business Organizations.	189
Table 7.4 The Relative Importance of Factors that Related to each type Business Performance.	191
Table 7.5 The Important of SysTrust Principles that directly Associated with the Quality of Financial Reporting and Business Performance.	194

List of Abbreviations

AGFI	Adjusted Goodness-of-Fit Index.
AICPA	American Institute of Certified Public Accountants
AIS	Accounting Information System.
AMOS	Analysis Moment of Structures Software.
ANCOVA	Analysis of Covariance
ANN	Artificial Neural Network
ANOVA	Analysis Of Variance
ASEC	Assurance Services Executive Committee
AVE	Average Variance Extracted
CA	Cronbach's Alpha.
CBJ	Central Bank of Jordan
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CICA	Canadian Institute of Chartered Accountants
CMIN/DF	Normed Chi-Square
COBIT	Control Objectives for Information and Related Technology
COCO	Criteria of Control
COSO	Committee of Sponsoring Organizations
CPA	Certified Public Accountants
CR	Composite Reliability
CRC	Computing Resource Centre.
DF	Degree of Freedom.
DRP	Disaster Recovery Plan
EBI	Egyptian Banking Industry
EC	Electronic Commerce
EDI	Electronic Data Interchange
EMP	Electromagnetic Pulse
EPS	Earnings per Share
ERP	Enterprise Recourse Planning
EU	European Union
EVA	Economic Value Added
EVC	Error of Variance for Each Latent Construct.
FASB	Financial Accounting Standards Board
FMS	Financial Management Service
GAAP	Generally Accepted Accounting Principles
GAO	General Accounting Office
GAPP	Generally Accepted Privacy Principles
GFI	Goodness-of-Fit Index
H0	Null Hypothesis.
H1	Theoretical Hypothesis Proposed.
IASB	International Accounting Standards Board
ICS	Internal Control System
IFRS	International Financial Reporting Standards
IS	Information System
ISACA	Information Systems Audit and Control Association
ISACF	Information Systems Audit and Control Foundation
IT	Information Technology
ITP	Information Transformation Process

JACPA	Jordanian Association of Certified Public Accountants
JIC	Jordanian Insurance Commission
JIT	Just-In-Time
JSC	Jordan Securities Commission
LDS	Less-Developed-Countries
MAE	Mean Absolute Error
MENA	Middle East & North Africa
MIS	Management Information System
MLEs	Maximum Likelihood Estimators
MRA	Multi Regression Analysis
MSE	Mean Square Error
NFI	Normed-fit Index
PCA	Principal Component Analysis
PDA	Personal Digital Assistants.
RA	Regression Analysis
RMSE	Root Mean Squared Error
RMSEA	Root Mean Square Error of Approximation
ROA	Return on Assets
ROE	Return on Equity
ROI	Return on Investment
ROSC	Report on the Observance of Standards and Codes
RTA	Real-Time-Accounting
SEM	Structural Equation Modelling
SPSS	Statistical Package for the Social Sciences.
TAM	Technology Acceptance Model
VIF	Variance Inflation Factor
Z-Value	Critical Value

CHAPTER ONE

INTRODUCTION

1.1 Research Background

This chapter presents the research background and boundaries, the study rationale and locations. It introduces the reader to the research problem, research questions, objectives and the significance of the study, whilst outlining the structure of the thesis.

With the aim of enhancing and improving their business performance and operations, business companies use a set of accounting information systems, techniques and tools. The application of such information systems (IS) is mainly justified by the need to improve and bring efficiency into being; a fact evidenced by most researchers. At the scale of importance, the performance of accounting information systems is highly prioritised and this is mainly led by increased competition and revolution of business environment at various levels, especially on the level of decision making, since such systems are adopted in such a way that is designed for aiding in decision making and enhancing an organization's competitive status. Hall (2010) identified the needs of accounting information systems by organizations as follows: (a) Provision of data on the used organizational resources (b) provision of management decision making relevant data, (c) provision of data that enhances more efficiency by employed personnel. There is much research providing evidence that accounting information benefits the decision-making of firms' managers and investors (Taiwo, 2016, Appelbaum et. al., 2017).

The ultimate aim of building data information systems, as indicated by Alnajjar MIM (2016) and Susanto (2008) is to avoid risks at levels of decision-making. Thus, such systems are devoted to processing data and transforming it into accounting information according to users' needs. Financial and accounting processes at organizations, which include advanced levels of using information technology, leads to more research and greater concerns related to risks, control and audit of Accounting Information Systems (AIS). Material misstatements in financial reporting might be brought about by risks and vulnerabilities of Accounting Information Systems. Such risks, according to Klamm and Watson (2009), have mostly negative effects on integrity, accuracy, reality and availability of financial reports. Irrespective of their size, businesses companies today must consider the reliability and

security of systems more than ever before. It is noteworthy to mention that limitations that restrain the achievement of the overall objectives of the business and the public and private corporations are the result of globalization and the advancement of technology around the world. This includes the mission and visions that are also affected by other factors such as fraud, money laundering and terrorism activities. In order to avoid such limitations caused by advances in technology, companies tend to design their strategies whereby dealing with customers, provision of service, corporate social responsibilities and successful procedure of control system are embedded therein (Douglas, 2011).

The adoption of information technology as a pillar in the business world renders it critical in terms of reliability and security. System assurance, as a core part of management, is required to ensure that the accounting system and information initiated is reliable. Information technology in business is essential as long as it is reliable and secure. System reliability in administration primarily guarantees the solidity of data and accounting framework. However, unreliable system can exhibit a number of side effects, as mentioned below (Boritz et al., 1999; McPhie, 2000; Romney and Steinbart, 2017).

- Regular system disappointments and accidents that deny inner and outside clients' access to key system administrations;
- Failure to prevent unauthorised access to the system, making it vulnerable to viruses, hackers and loss of data confidentiality;
- Loss of data integrity, including defiled, inadequate and invented information, and genuine support issues bringing about unintended negative reactions from system changes, such as loss of access to system administrations, loss of information privacy or loss of information trustworthiness.
- Maintenance problems. The required maintenance could not be done, or resulted in a system outage or other failure, resulting in a reliable system.

In light of worries about an unreliable system, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) established a new assurance service called SysTrust, whereby a public accountant can write about the adequacy of controls over the reliability of a system. According to Boritz (2002), although the reliability of a system is examined theoretically in the system engineering discipline (as in Lyu, 1996; Denton - 2002) and in the quality assurance literature (Kehoe and

Jarvis, 1996; Donald, 2005), there have been no current standards for measuring business system reliability. Consequently, a joint Systems Reliability Team of the AICPA and CICA set up a procedure for building criteria that can be utilised to assess the reliability of business systems. The team formulated a definition of system reliability as "*A system that operates without material error, fault or failure in system availability, privacy, integrity, and maintainability during a specified time in a specified environment*", (Saitio, 2012). Depending on that assessment of the reliability of a system, a set of principles and criteria exist which are classified into five categories that are mainly relevant to systems reliability and the reliability of an organization's financial statements as follows.

1. Availability: Agreed and committed system and information thereof that are used for operations (legal obligation).
2. Security: Protected systems against unauthorised access- physically and logically.
3. Confidentiality: Confidential information that is protected as committed to or agreed.
4. Processing Integrity: Processing data accurately, fully, in due timing and exclusively with proper authorization.
5. Privacy: Gathering, usage, disclosure, maintenance of personal information and its protection from unauthorised disclosure in accordance with internal policies and external regulatory requirements.

These principles can be used individually or in combination in order to provide the relevant stakeholders who have an interest on the reliability of AIS process (top management, auditors, suppliers, governments, customers, and business partners) and in levels to ensure that the system actually works objectively and mechanically to ensure less risky levels. The core benefits of a reliable computing system are specifically identified by the developers of the SysTrust project. *The computing system – are running business, producing products and services and dealing with consumers and business partners... As business dependencies on information technology increases, tolerance decreases for systems that are unsecured, unenviable when needed, and unable to produce accurate information on an instant basis. Like the weak link in a fence, the unreliable system can cause a chain of events that negatively affect the company and its customers, suppliers and business partners* (ACICPA/CICA, 2013. 8). In fact, SysTrust acquires its importance because of the following factors. (1) It reengineers the internal control system of AIS depending on technological basis (2) It re-conceptualizes AIS-invisible-control-mechanism. (3) It enhances standards of

operations and security that are designed for increasing efficiency of AIS and (4) it grants a guide on a solid ground that helps in measuring AIS reliability and associated risks. A reliable system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. Therefore, any company must have the reliability of the software and database. Romney and Steinbart (2017), describes the software and databases are not reliable can harm not only the company and the employees who use them, but also the company's supply chain.

According to Danelies (2013) and Dien (2014), the reliability of internal controls system of accounting information system has a positive relationship with the quality of financial statements. Potentiality of error in reporting is related to weaknesses of internal control, namely the supervision of accounting information system (Ricchiute, 2006). Further, the need of internal control is to produce reliable financial statements through supervision of the relevant accounting system (Konrath, 2002). In terms of "quality", Toposh (2014) argues that maintaining characteristics of any "Accounting Information System" relies on a well-designed internal control system which is applied to realize operational goals and performance. Computerised accounting information systems can face a range of potential threats, and this entails protection of data from abuse and physical and moral loss where ministrations of business companies tend to design a rigid control system that is reliable and guarantees protection from both internal and external threats. This maintains the quality of outputs of the systems and aids in the efficient achievement of the organization's objectives. The quality or characteristics of useful financial information should be considered in order to increase the added value for the firm. Research Doyle, et. al. (2007) found that generally weakness in company's internal control system over financial reporting will weaken the quality of accounting. According to International Public Sector Accounting Standards (IPSAS, 2010), the qualitative characteristics of quality financial data reporting can be viewed by the following: (1) Relevance (2) Understandable, (3) Faith representation, (4) Comparability and (5) Timeliness. However, empirical studies examining the influence of previous US GAAP and IFRS to quality of financial report shows positive, not significant, and negative influence (Barth, et. al., 2008; Meulen, et. al., 2007; Bartov, et. al., 2005).

Furthermore, Woodroof and Searchy (2001) argued that for web-based continuous auditing to work effectively, particular criteria must be met. They indicated that the underlying systems of a continuous audit environment must be reliable and secure, that there must be security,

authenticity and confidentiality of data transmission between parties and that there must be an agreement on the degree of noncompliance and amount of downtime that will be tolerated. According to their perspectives, unless these criteria are met, a continuous audit will not be feasible. According to Bailey (2001), the reliability of the system is a prerequisite for continuous auditing; illustrating that the reliability of a system can be defined as the likelihood that the system will continue to function effectively over a given period of time and under specified conditions. In his study, Coderra (2006) suggested that organizations are continually exposed to errors, frauds or inefficiencies that can result in continual financial loss and an increased level of risk. Coderra (2006) also claimed that timely and continuous assessments of risk levels and control systems of firms play an important role in ensuring that the financial data is continuously reliable. Application of CA necessitates the existence of particular technological conditions (Web Server and Reliable System). Interrelated and authorised to access Web Servers for communication among continuous auditing partners (client, auditor and third parties) are clearly required. This gives the auditor authorization for access to its own database, as a result of which the auditor has direct access to required data while the server of the auditor acts as a moderator by providing the third parties (that are engaged in the continuous auditing process) with restricted access to business information (Brown, et. al., 2007; Barr-Pulliam, 2017). A reliable system is also required as continuous auditing is conducted under the supervision of real-time accounting systems. The expected benefits from web-based continuous auditing depend on the reliability of real-time accounting systems.

Recognizing the critical impact of the quality of financial reporting upon investment decision, developing countries and countries with economies experiencing significant change are attaching greater significance to transparency and reliability in corporate accounting and reporting. They are making efforts to strengthen the different components of accounting infrastructure in their respective jurisdictions so that financial resources can be assembled and utilised more effectively (IFRS 2008.VI). Financial reporting practices are more of a result of "different sources of accounting influence" and the various legal requirements (Goitom 2003, Bukenya, 2014). Thus, in line with International Financial Reporting Standards (IFRS, 2010) and according to the Companies Law No. 22 (1997), public shareholding companies in Jordan are obligated to present a reliable internal control of accounting information system and adequate annual financial reporting. Probably the toughest regulations are in the USA where the Sarbnes–Oxly Act since 2002, especially section 404 requires public companies to

include in their annual reports an assessment by management of their internal controls over financial reporting. This incorporates a statement of management's obligation for submitting and maintaining an adequate internal control, an appraisal of the adequacy of those controls as of the end of the most recent fiscal year, a statement identifying the framework that was utilised to assess those controls and a statement that the external auditor issued an authentication report on management's internal control evaluation. The rules don't mandate the utilization of a specific framework yet say an appropriate one must. Be free of predisposition, allow sensibly reliable subjective and quantitative assessment, incorporate all relevant factors that might adjust a decision about the effectiveness of the internal controls and be relevant to an evaluation of internal control over financial reporting (Sawyer, 2003; Rubino et al., 2014). Therefore, any company's management should apply an adequate and strong internal control framework for assuring the reliability of AIS process over the quality of financial data reporting and other reports. According to Daneila (2013), the weak internal controls AIS will cause error misstatements in the financial data that cannot be anticipated and potential investors will trust and invest into a company if it is business's practice are not transparent. Based upon the above discussion, the implementation of SysTrust principles, either individually or collectively are expected to have an affect over the quality of financial reporting and business performance.

1.2 Problem Statement

Over the past two decades, there have been extensive studies conducted on the adoption and effectiveness of AIS applications. While some have examined the necessary antecedents for the successful implementation of AIS (Collier and Sutton, 2011, Toposh, 2014), others have investigated the quality of the accounting information system, and its efficiency and effectiveness (Perez, et. al., 2011; Danelies, 2013; Dien, 2014) and the management of internal controls, design of an accounting information system and auditing (Bedard, et. al., 2005; Sutton, 2006; Greenberg, et al., 2012). Studies that emphasize the necessity and importance of the internal control system for assuring the quality of accounting system are increasingly being acknowledged. However, articles on the SysTrust service engagement as an internal control method for assessing reliability in the professional accounting literature are primarily devoted to explaining the background and purpose of this service and its potential demand (Boritz and Hunton, 2002; Sutton, 2006). Furthermore, assessment of the reliability of accounting information system remains under-researched as the majority of such studies have focused on the status of AIS use and its applications (Iceman and Hilson, 2012).

Specifically, the effect of reliability of AIS on the quality of financial reporting is noticeably under-researched.

There has been relatively little business-oriented research on the reliability of AIS in non-western countries. Accounting information systems (AIS) researchers can and should employ their knowledge of both technology and business to fill this void. Moreover, there is no clear empirical evidence on the extent of the effect of reliability of AIS on financial reporting quality and business performance in developing countries' environments. Thus, whether the reliability of internal control leads to systematic improvements in quality of financial data reporting and business performance remains an open question. Given that most articles of internal control system of assuring the reliability AIS process have been based on cases in Europe and the US, cultural and legislation challenges, although complex, show some inconsistency. However, relatively few studies have been implemented outside of the most developing countries, such as in Jordan, which is a beachhead for new technologies and business practices in the Middle East and North Africa (MENA). Several authors state that within organizations, attention must be given to the accounting standards and laws of each country because they affect accounting management (Davila, et. al, 2004; Romney and Steinbart, 2017). Also, Bailey (2000) indicated that the choice of a particular suite of control to meet the SysTrust criteria is a function of management style, philosophy, firm size or industry. Therefore, there has been a call for research to examine these issues within different contexts (Greenberg, et. al., 2012; Bedard, et. al., 2005; Sutton, 2006). In response to the call, the present study is taking a significant step to examine the reliability of AIS based on the implementation of SysTrust model as an internal control approach in a new environment context (see Chapter 2 ,section 2.5). System assurance, as a core part of management, is required to ensure that the accounting system and information initiated is reliable. However, the level of reliability of accounting information system largely depends on the extent of how much the internal control system in public listed companies are fully implemented and meet the requirements of SysTrust principles. In fact, over the Jordanian context, the extent of implementation of the requirements of SysTrust principles as internal control method for assuring the reliability of AIS process by public shareholdings companies is needed to be empirically examined, since there was no any clear evidence about its status quo and its relationship with quality of financial data reporting and business performance in a systematic integrated approach. With reference to AICPA and CICA, the purpose of designing SysTrust is to boost trust of management, the board of directors, customers and business partners in

terms of reliability of information systems (AICPA/CICA, 2017; Bedard, et. al., 2005). In addition, Jordan is currently committed to financial reporting standards and international auditing standards (see Chapter 3, section 3.6). Therefore, it is worthy to highlight the fact that in order to guarantee a higher percentage of success of the AIS implementation, it is essential to consider the constituents of SysTrust that are related to the quality of financial data reporting and business performance. Better perception of constituents that have an effect on data quality reporting of AIS would contribute to the improvement of AIS data quality at organizations. Furthermore, based on the general insights offered, accounting professionals, auditors and users in Jordan should not only be well-informed about the status of the reliability of the AIS process based on the context of SysTrust, but also its implementation and its influence on their business performance and quality of financial reporting. This might help them to take the right actions to enhance the effectiveness and reliability of the AIS process in line with requirements of international financial standards.

1.3. Research Aim, Objectives and Questions

This thesis aims to examine and validate the impact of the implementation of SysTrust's framework (principles and criteria) as an internal control method for assuring reliability of Accounting Information System (AIS) on the business performance via the mediating role of the quality of financial reporting among Jordanian public listed companies. Specifically, the core objectives of the present study are as follows:

1. To review the existing literature on the implementation of SysTrust principles, quality of financial data reporting and business performance in order to identify research gaps and to formulate a better understanding of the relationships among these three constructs This objective will be accomplished by comprehensively and critically reviewing the relevant studies so as to build a clear picture of the most important aspects pertaining to these components (see Chapter 3).
2. To develop a conceptual framework through the integration of several relevant studies in the field assessing the reliability of internal control accounting information system, quality of financial reporting and business performance. This framework consists of independent variables (the SysTrust's framework), the dependent variables (qualitative features of quality of financial data reporting and business performance) and the correspondence hypotheses (see Chapter 4).
3. To identify the extent to which SysTrust's framework requirements (principles and criteria) for assuring the reliability of the AIS process as internal control system are

achieved or implemented by the public listed companies in Jordan. This involves examining the content and context of internal control of AIS in Jordan. Several researchers argue that, within organizations, attention must be given to the accounting standards and laws of each country because they impact on accounting management (Davila, et al., 2004; Romney and Steinbart, 2017).

4. To establish any similarities or differences among business organizations in respect of the level of reliability of AIS process based on their type of business sector, size and experiences.
5. To identify which key component of the SysTrust's framework (principles and criteria) is highly and positively associated with the quality of financial reporting and business performance.
6. To empirically examine, validate and predict the viability of the proposed conceptual framework. This objective will be accomplished by conducting an analysis of data that are obtained from the public listed companies in Jordan.
7. To provide the decision makers with recommendations those aid the account management units in these companies to enhance the performance and reliability of AIS process (see Chapter 9).

The specific **questions** to be examined are:

1. To which extent are the existing AIS processes and applications in the Jordanian public listed companies reliable and secure in terms of providing the requirements of the five principles of the SysTrust's framework (availability, security, confidentiality, processing integrity and privacy)?
2. Is the level of implementation of SysTrust's framework (principles criteria) for assuring the reliability of AIS differ/similar according to the demographic characteristics of Jordanian shareholding companies i.e., (types of sectors, number of employees and business experiences).
3. What are the main patterns of factors that underlie each major constructs of the study's conceptual framework: SysTrust's model, quality of financial reporting and business performance?
4. Does the quality of financial reporting have any significant role in mediating the relationship between the reliability of accounting information system and business performance?
5. To what extent the reliability of AIS control process can improve the quality of financial data reporting as well as business performance (financial vs. non-financial)?

6. To which extent the study's proposed conceptual framework is valid and reliable for the predication of dependent variables (quality of financial reporting and business performance).

For these purposes, a descriptive correlational survey design approach is used in this study used as it sought to describe and establish the relationships among the study variables and it employs quantitative method to test the hypotheses first, and then to answer the research questions (Chapter five).

1.4 Significance of the Study

The most salient potential contributions of the present study can be summarised in the following points.

1. An integrated conceptual framework has developed and empirically tested and validated for the main constructs of the SysTrust's framework as an internal control method for assuring the reliability of AIS process ties together with quality of financial data reporting and business performance for the first time by using structural equation modelling approach and Neural Network..
2. The existing body of the research on assessing the internal control of AIS and its reliability is heavily oriented towards organizations in developed countries. The present research has extended this scope to include less-developed countries (LDS) such as Jordan.
3. Evidence deduced from investigating AIS practice and its quality in a developing country as Jordan, and from utilizing generally acceptable measures of assessing the reliability of AIS and its relationship with quality of financial data reporting should advance knowledge of AIS applications in a global environment. Furthermore, such evidence is further expected to provide account managers with insights in to how they can enhance the reliability of AIS process in their organizations.
4. Non-transferability of findings from research in developed countries is not the sole reason necessitating the present study, but rather it is the current limited understanding of the status of readability of AIS process among businesses in developing countries. In turn, this calls for more research to raise awareness of the status of the reliability of AIS in developing countries. Gathering empirical evidence from different environments will render it possible to generalize on the reliability and quality of AIS.
5. By examining the relationships among the implementation of SysTrust's framework requirements (i.e., availability, security, integrity process, confidentiality, and privacy), quality of financial data reporting, and business performance, professional and decision-

makers in business organizations could benefit from this study by taking the right actions within their organizations to enhance their accounting information systems (AIS) to become more effective and reliable.

1.5 Thesis Structure

This thesis is composed of nine chapters. The content of these chapters is briefly outlined as follows:

- **Chapter One.** Provides an introduction to the thesis, starting the research problem, research objectives, and the significance of the thesis.
- **Chapter Two.** Primarily focuses on the existing literature related to accounting internal control method, SysTrust model, quality financial reporting. The main findings and limitations of the previous research are presented.
- **Chapter Three.** Deals with the preliminary in – depth interview. It gives an explanation of its main purposes, structure and planning. It provides some background information about the internal control system and continues auditing in Jordan.
- **Chapter Four.** Presents the research conceptual framework. It details the main constructs of the study’s framework and the study hypotheses.
- **Chapter Five.** Explains the research design and data collection. This chapter evaluates the alternative methods of data collection and provides the basis and rationale for selecting an appropriate method. The selection of the scale of measurement, the key respondent approach, the domain of the study’s population and questionnaire development are also presented
- **Chapter Six.** Presents the methodology of analysis. The chapter starts with a review of the alternative statistical techniques available, the epistemological assumptions behind these methods and the basis for the selection of the appropriate statistical techniques. The chapter gives a description of this analysis and the justification of the use in the research
- **Chapters Seven.** Presents the research findings related to the main pattern of factors that underlie each construct of firms’ internal and external environmental dimensions
- **Chapter Eight.** Discusses the research findings
- **Chapter Nine.** Gives a summary review of the entire study and presents the main conclusions of the research and its implications for business decision-makers. The research contributions in terms of theory and practice also presented. Research limitation and area for further information are discussed.

CHAPTER TWO

THEORETICAL BACKGROUND & LITERATURE REVIEW

2.1 Introduction

This chapter presents and discusses empirical studies relating to the reliability of AIS process, and quality of financial reporting as well as business performance by means of a content analysis of the findings of previous studies. The literature review is then used in an attempt to develop a conceptual framework with which to conduct this study. This framework consists of integrated literature and SysTrust service model as an internal control system for assessing the reliability of accounting information system process. To find research that has been published on the reliability of AIS, the quality of financial reporting and business performance, full-text searches in numerous online databases (EBSCO Host, ABI Inform, and Web of Knowledge) were performed using multiple keywords, such as ‘AIS reliability,’ ‘AIS performance,’ ‘SysTrust service,’ and so on.

Greater understanding of the empirical literature on accounting information reliability should assist standard setters and regulators in establishing financial reporting standards, preparers and auditors in implementing standards, and financial statement users in evaluating accounting information reliability. Greater understanding of reliability should also assist academics in conducting research to produce new insights on reliability. Facilitating theory development and identifying over- and under-researched areas are essentially based on relevant literature reviews (Levy and Ellis, 2006). Levy and Ellis, 2006 state “that the foundations for advancing knowledge and facilitating theory development are created by literature review”. They further support the idea that literature reviews are being used to identify areas needed for research. In addition, literature review work is for the main purpose of surveying previous studies pertinent to knowledge sharing and intranets in order to scope out the requirements of key data collection to conduct the primary research. Hence, it constitutes a part of the emergent research design process.

Rationale or based reasoning of research problems to provide answers to is a part of research process that includes theoretical study. Moreover, according to Nur Indriantoro, et. al., (2011) a theoretical study in the research process develops hypotheses that aim to test a theory or hypothesis (hypotheses testing). Prior to collecting their own data, it is now acceptable for researchers to be acquainted with existing research since this is in line with grounded research work currently in practice (Levy and Ellis, 2006). Three further purposes are served as an appreciation of previous work in this area: First, the risk of overload at the primary data collection stages of the project is reduced through providing direction in the construction of data collection tools. Second, working the findings from existing literature into a formal review helped maintain a sense of the topic's perspective throughout the study. Finally, when the data analysis stages of the research were reached, the opportunities for articulating a critical analysis of the actual "meaning" of the data collected were raised through this activity.

2.2 Theoretical Background

This research has started with defining key concepts in the study framework :Accounting information system, internal control system, quality of financial reporting and business performance. The definition guides the development of a theoretical framework, the literature review and the identification of research questions of the thesis.

2.2.1 Accounting Information System

While accounting is a business function that aims to provide specific users with quantitative accounting information, the AIS is an information system that is designed and implemented within an organization to enable the accomplishment of accounting functions (Ghasemi, et. al. 2011, Al-dmour, et. al., 2016). There are various definitions of AIS. This system is simply defined as 'a unified structure within an entity, such as a business firm, that employs physical resources and other components to transform economic data into accounting information, with the objective of satisfying the information needs to a variety of users' (Agbejule, 2011). AIS consists of four major sub-systems:(1) The transaction processing system, (2) The general ledger/financial reporting system, (3) The fixed asset system and (4) The management reporting system. The AIS is a subsystem of organizational management information systems (MIS), whose goal is to measure business financial performance and perform organizational accounting functions. Accounting information is required not only by management in managing the financial activities of the companies but also by shareholders, who need regular financial statement in order to evaluate business performance. It is required by a government

to ensure the effective utilization the country's resources; therefore, it plays a significant role in all economic and social aspects. It assists in auditing and examining irregularities and misappropriations. Accounting information is the cornerstone of any organization, without it, it is likely to stay inactive or unworkable (Rom and Rohde, 2007; Kabir, 2012).

AIS are a tool that organizations can use to achieve stronger, more flexible corporate culture to face continual changes in the environment. One of the major reasons why business enterprise takes advantage of accounting information technology is to receive support for their business decisions. The benefits of accounting information systems can be measured by its impact on improvement of the decision-making process, quality of accounting information performance evaluation, internal control, and facilitating company's transactions. Accounting information systems assist companies to gauge the risk of some operations or predict future warnings using sophisticated statistical software applications (Alsharayri, 2011). Accounting systems are responsible for analysing and monitoring the financial condition of companies, preparing documents necessary for tax purposes, providing information to support many of the other organizational functions such as production, marketing, human resource management, and strategic planning. Without such a system it will be very difficult for business companies to determine performance, identify customer and supplier account balances and forecast future performance of the organization (Amidu, et. al., 2011; Saira, et. al., 2010). Using standardised guidelines, the transactions are recorded, summarised, and presented in a financial report or financial statement such as an income statement or a balance sheet. Here, using AISs is viewed as a system that helps management in planning and controlling processes by providing relevant and reliable information for decision making (Gordon and Miller, 1976). It suggests that AIS's functions are not solely for the purpose of producing financial reports. Its role goes beyond this traditional perspective.

Prior researches have shown that information system adoption did increase companies' performances and operations efficiency, especially in big companies (Saira, et. al., 2010). An AIS is a tool which, when incorporated into the field of Information and Technology systems (IT), were designed to help in the management and control of topics related to companies' economic-financial area (Salehi, et. al., 2010). AISs also provide information on both actual and budget data, which would help company to establish, plan, and control operation (Grande, et. al., 2011). Good management of resources and better control of expenditure, budgeting and forecasting enhance the well-being of company (Saira, et. al., 2010). The main function of

AIS is to assign quantitative value of the past, present and future economic events. The system will process the data and transform them into accounting information during input, processing and output stages that will be used by a wide variety of users such as internal and external users (Akanfe, et. al., 2014). They indicate that an effective AIS performs several key functions throughout these three stages, such as data collection, data maintenance, data AIS, knowledge management, data control (including security), and information generation. In general terms, business entities use three types of information systems, namely manual system, computer-based transaction systems and database systems (Ballada and Ballada, 2011).

- 1. Manual System.** This is the first type of accounting systems. It utilizes paper-based journals and ledgers. Nowadays, computer-based transaction systems have replaced some paper records into computer records. A manual system is labour intensive for this system and relies on human processing. Because manual systems rely on human processing, they may be prone to errors.
- 2. Computer-Based Transaction System.** Organizations employ multiple forms of information technology in their accounting information systems [Shanker, 2013, Amidu, et. al., 2011]. Because of the advancements in information technology, computer-based transaction systems were created. In this system, accounting data are kept separately from other operating data. At this point, there is a greater degree of compartmentalization of work in order to preserve the integrity of accounting information system. Treatment of information is the same as that of the manual system. The only difference is that the user here is simply filing in a computer screen that looks and often times acts as the source document of the transaction. The following are the advantages of computer-based transaction system as described by Ballada (2011). Transactions can be quickly posted to the appropriate accounts, by passing the journalizing process; detailed listings of transactions can be printed for review anytime; internal controls and edit checks can be used to prevent and detect errors, and a wide variety of reports can be prepared. Accounting packages are available in the market. This consists of modules that deal with the business accounting systems. A simple accounting package might also contain one module or also referred to as a stand-alone module. But most of the time, it will consist of several modules. Examples of this are the QickBooks and Peachtree.
- 3. Database System.** This system reduces inefficiencies and information redundancies. Relational database systems, such as enterprise resource planning (ERP), depart from the accounting equation method of organizing data. Such a system captures both financial and

non-financial data, and then it stores that information in the data warehouse. The advantages of this system include the recognition of business rather than just accounting events; the support in the reduction in operating inefficiencies; and the elimination of data redundancy.

The four basic steps involved are analysis transactions, recording the effects of transaction, summarizing the effects of transactions, and preparing records. This procedure is neutral; the steps involved can be applied both in manual and technology-based. The first step is the analysis of transactions, the transaction must be known to be financial in nature, recordable and non-recordable transactions are separated. In this step, the transaction is being analysed on how it affects the accounting equation. Source documents, such as invoices, orders, and checks are helpful in this stage. The second step is to record the effect of the transactions. Transactions are recorded using journal entries. These journal entries are the accountant's way of recording the effect of both simple and complex business transactions. Journals provide a chronological record of all transactions of a business. They show the dates of the transactions, the amounts involved, and the particular accounts affected by the transactions. Sometimes a detailed description of the transaction is also included. It is also known as the books of original entries.

The third step is to summarize the effects of transaction. Under this step, the journal entries will be posted to the ledger and a trial balance will then be prepared. Once transactions have been analysed and recorded in a journal, it is necessary to classify and group all similar items. This is accomplished by the book-keeping procedure of posting all the journal entries to appropriate accounts. All accounts are maintained in an accounting record called a ledger. A ledger is also referred to as the book of accounts. The next step is to determine the total balance of each account. After the account balances have been determined, a trial balance is usually prepared. A trial balance lists each account with its debit or credit balance. The fourth step is the preparation of the reports. This encompasses adjusting entries, preparation of financial statements and closing the books. There will be recording and posting of some adjusting entries that is applicable for the period. Then, the trial balance will again be recomputed. From the data in the trial balance, the financial statements are then prepared. This includes the statement of financial position, income statement, cash-flow statement and the notes. The last procedure will be the closing of the books.

In manual systems, journals and ledgers are paper-based. Today, most business entities use computers and electronic technology as an integral part of their accounting systems. Computers helped business to make millions of calculations per second. The time spent in manually accomplishing the steps is far compared to the time spent in computerised systems. The four processes involved are actually still the same. The only difference is that in manual systems, the accountant is manually computing and preparing the papers while in computerised system, you only enter and analyse the data and the computer automatically calculates the balances. Some software even has the automatic update of financial statements. You can immediately track the progress of the business. The fact still remains that computers cannot think and that is the accountant's job (Shanker, 2013). In the computerised system, the accountant's job is just the first two steps in the accounting process. The accountant just needs to analyse the transactions, record their effects and adjust entries. Major computations are left to the computer.

2.2.2 Internal Control System

The definition of internal control was presented for the first time in 1949 by the American Institute of Certified Public Accountants (AICPA). It defines internal control as a plan and other coordinated means and ways by the enterprise to keep safe its assets, to check the coherency and reliability of data, to increase its effectiveness, and to ensure the settled management politics. Nevertheless, due to continuous improvement of the given definition of control concept, in modern times most conceptions signify the internal control system as one of the ways of leadership to guarantee the safety of enterprise assets and its constant improvement. Presently, the concept of internal control incorporates a new approach that could identify the fields of control management and processes and stimulate improvement of their detailed analysis as well as acknowledge errors and find ways of preventing them. The internal control can be described as a system or processes designed to give reasonable assurance of achievement of objectives in certain categories, like efficiency and effectiveness of operations, ensuring reliable accounting reports, and strengthening loyalty to company policy. The board of directors, management and other personnel carries out the system.

According to Arens, et. al. (2008), it is necessary for companies to develop an internal control that is designed to give a reasonable assurance that their financial statements have been presented fairly. Insufficient internal control over financial statements can cause a financial statement to disagree possibly with accounting standards (GAAP). The results of study by

Doyle and McVay (2007) show that the weakness of internal control has an effect on the low quality of accruals, which supports the observation that internal control influences the quality of accounting information. Internal control efficiency is considered as one of the main components of accounting information system effectiveness. Hoitash et. al. (2009) states that the value of internal control influences operational performance through information reliability operational effectiveness. Computerised internal controls have effects on the value of internal controls and performance of operations. Although there are different definitions of internal control, in a complete analysis of internal control the results show that it still has general purposes that focus on making sure information is reliable and complete, protecting documents and property, making sure the economic performance is effective, reviewing accounting principles and presenting trustworthy financial records, and conforming to laws, executive acts, enterprise rules, and efficient control of risk. When analysing control, there are many different interpretations that prove control as an expansive concept because control involves many different factors and can be interpreted differently according to the situation. Bodnar and Hoopwood (2010) state an internal control is a process that designed to provide reasonable assurance regarding the achievement of objectivities in the following categories: (i) reliability of financial reporting, (ii) effectiveness and efficiency of operations, (ii) compliance with applicable laws and regulations. Elder, et. al. (2010) state that a system of Internal Control consists of policies and procedures designed to provide management with reasonable assurance that it achieves company's objectives and goals. Reviews these policies and procedures are often called controls, and collectively they comprise the entity's internal Control.

In their research, Wright, et. al. (2012) show that the controls' strength is expected to affect the likelihood and nature of financial statement errors. The internal control objectives according to Romney, et. al. (2012), namely: i) safeguarding assets, including preventing or detecting, on a timely basis, the unauthorised acquisition, use, or disposition of material assets company, ii) Maintaining records in sufficient detail to accurately and fairly reflect company assets, iii) Providing accurate and reliable information, iv) Providing reasonable assurance that the financial reporting is prepared in accordance with GAAP, v) Promoting and improving operational efficiency, including making sure the company receipts and expenditures are made in accordance with management and directors' authorizations, vi) Encouraging adherence to prescribed managerial policies, and vii) Complying with applicable laws and regulations.

Azhar (2013) explains that the purposes of the control are to. (i) Provide assurance that the goal of every business activity is achieved, (ii) Reduce the risk that would be faced by the company due to crime, danger, or losses caused by fraud, misappropriation and embezzlement, and (iii) Provide convincing and trustworthy assurance that all legal responsibilities are met. An internal control system involves safeguarding assets by policies and procedures applied by managers in order to guarantee reliable accounting and promote efficient operations. Topash (2014) asserts that the qualitative characteristics of accounting information can also be maintained if there is sound internal control system in an organization. Internal controls are procedures set up to protect assets, ensure reliable accounting reports, promote efficiency and encourage adherence to company policies. Internal controls are essential to achieve some objectives like efficient and orderly conduct of accounting transactions, safeguarding the assets in adherence to management policy, prevention and detection of error and fraud, and ensuring accuracy, completeness, reliability and timely preparation of accounting data. If good internal control exists in any organization, management can use information with greater reliance to maintain their business activities properly which provide AIS. Marshal and Romney (2015) allege that developing an internal control system requires a thorough understanding of information technology (IT) capabilities and risks as well as how to use IT to achieve some organizational control objectives. Accountant and system developers help management achieve their control objectives by (i) designing effective control systems that take a proactive approach to eliminating systems and detecting, correcting, and recovering from threats when they occur, (ii) making it easier to build controls into systems at the initial design stage than to add them after the facts. They also allege that internal control performs the following important functions (Marshal and Romney, 2015):

1. **Preventive control.** Which deter problems before they arise. Examples include hiring qualified personnel, segregating employee duties, and controlling physical access to assets and information.
2. **Detective control.** Which discovers problems that are not prevented? Examples are duplicate checking of calculations, preparing bank reconciliations, and monthly trial balances.

3. **Corrective control.** Which identifies and correct problems as well as recover from the resulting errors? Examples include maintaining backup's copies of files, correcting data entry errors and resubmitting transactions for subsequent processing.
4. **General control.** Controls designed to make sure an organization's information system is stable and well-managed. Examples include security infrastructure, software acquisition, development and maintenance control.
5. **Application controls.** Controls that prevent, detect, and correct transaction errors and fraud in application programs. They are concerned with accuracy and authorization of data captured, entered, processed, stored, transmitted to other systems and reported.

Any effective control system consists of some basic components that guarantee its efficiency and effectiveness. The major components of any control system consist of control environment, the entities in risk assessment process, the information system, control activities and the monitoring of control. Here, each of these components is explained as follows (Gelinias, et. al., 2014).

1. **Control Environment.** According to Gelinias, et. al. (2014) control environment relates to the process of operationalizing the organization culture of the company from one side, and the managerial actions and attitudes as regards internal control role and importance for the company. In this regard, management can get use of incentives power to prevent personnel from engaging in dishonest, illegal, or unethical acts. However, ISA UK and Ireland 315 states that any control environment should take into account some critical elements, such as integrity and ethical values above system and people. This element ensures and guarantees the effectiveness of the internal control design, administration, and monitoring of other components of the internal control system. Hence, the company should take into account carefully the communication and enforcement of integrity and ethical values of control environment.
2. **Entity's Risk Assessment Process.** Any business encounters risks that could threaten its success. In this regard, Szylar (2013) explains that risk is everywhere and surrounds our personal activities and a professional life, so preventing risks is impossible, but we can use risk assessment processes in order to minimize these risks. Thus, any internal control system should take into account this element, which helps the company to identify the business risks in order to respond to them.

- 3. Information System.** Information system is the third important element for internal control system, which highly depends on using information technology (IT). (Dhunna and Dixit, 2010) define IT as the process of merging computing with high speed communications links carrying data, sound and video depending on technology. Thus, an effective IT should consist of some basic elements, such as physical and hardware components (infrastructure), software, people, procedures, and data.
- 4. Information Processing Controls.** This is considered as an important element since it is concerned with data and information protection. However, it also guarantees the accuracy, completeness, and authorization of transactions. There are many types of information processing controls, but application controls and general IT controls are the most common controls.
- 5. Physical Monitoring Controls.** This kind of controls deal with the physical assets and the needed activities for securing it, like authorization to access files, programs and data files, security and inventory counts with accounting records. Thus, this kind of control helps in discovering all frauds and inventory losses, preventing theft of assets, and enhancing the reliability of financial statement preparation. The physical security control is also important for the auditing. Stealing of assets as commented on by (Abu Musa, 2004) can range from shoplifting an accessory, diskettes and software from a store to taking a whole large asset.

2.2.3 Types of Accounting Internal Control Frameworks

A number of frameworks have been developed to assist businesses in establishing and assessing their operational and financial controls. This section presents a primer of the leading frameworks that businesses can employ to establish and assess internal controls, along with a discussion of pros and cons of each framework.

2.2.3.1 COSO and COBIT Frameworks

The theory of internal control has undergone major reappraisals and changes during the last decade. These changes began in 1988, when the AICPA issued SAS No. 55, which describes internal control in terms of its three major components, control environments, accounting systems, and control procedures. Four years later, the Committee of Sponsoring Organizations (COSO) issued the Internal Control Integrated Framework. The COSO report defines internal control as a process affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (i) Effectiveness and efficiency of operations, (ii)

reliability of financial reporting, and (iii) compliance with applicable laws and regulations. This definition reflects certain fundamental concepts. Internal control is:

- Geared to the achievement of objectives in one or more categories- operations, reporting, and compliance.
- A process consisting of ongoing tasks and activities- a means to an end, not an end in itself
- Affected by people- not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to affect internal control.
- Able to provide reasonable assurance- but not absolute assurance to an entity's senior management and board of directors.
- Adaptable to the entity structure- flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process.

The purpose of internal control in accordance with COSO is divided into three parts. The first is the operational objective that requires the effectiveness and efficiency of the company's operations, including financial performance, and protecting the assets of the company is the purpose of reporting losses. The second objective is that both financial and non-financial reporting is allocated to internal parties, and external parties want that reporting to be reliable, timely, transparent and in accordance with the applicable rules and policies of the company. The third objective is obedience to the laws and regulations, which the company complies with in carrying out its business. Then, the COSO internal control divides elements into five sections, namely environmental control, risk assessment, control activities, information and communication and control. These five elements are integrated with each other. Environmental control consists of actions, policies, procedures portrait attitude of high-level management, board of directors, and business owners in applying the entity's internal control environment (Arens, et. al., 2014).

- **Environmental Control.** Environmental monitoring aimed at ensuring that internal controls have been implemented throughout the organization ranks of companies that contain integrity and ethical values of the organization.
- **.Risk Assessment.** The organization must identify, analyse, and manage its risks. Managing risk is a dynamic process. Management must consider changes in the external environment and within the business that may constitute obstacles to its objective. (i)

Specifying objectives clearly enough for risk to be identified and assessed, (ii) Identifying and analysing risks to determine how they should be managed, (iii) Considering the potential of fraud, and (iv) Identifying and assessing changes that could significantly impact the system of internal control.

- **Control Activities.** Control policies and procedures help ensure that the actions identified by management to address risks and achieve the organization's objectives are effectively carried out. Control activities are performed at all levels and at various stages within the business process and over technology. (i) Selecting and developing controls that might help mitigate risk to an acceptable level, (ii) Selecting and developing general control activities over technology, and (iii) Deploying control activities as specified in policies and relevant procedures.
- **Information and Communication.** Information and communication systems capture and exchange the information needed to conduct, manage, and control the organization's operations. Communication must occur internally and externally to provide information needed to carry out day to day internal control activities, and all personnel must understand their responsibilities. (i) Obtaining or generating relevant, high-quality information to support internal control, (ii) Internally communicating information, including objectives and responsibilities necessary to support the other components of internal control, and (iii) Communicating relevant internal control matters to external parties.
- **Monitoring.** The entire process must be monitored, and necessary modification is made so that the system can change as conditions warrant. Evaluations ascertain whether each component of internal control is present and functioning. Deficiencies are communicated in a timely manner, with serious matters reported to senior management and the board. (i) Selecting, developing and performing on-going or separate evaluation of the components of internal control, and (ii) Evaluating and communicating deficiencies to those responsible for a corrective action, including senior management and the board of directors, when appropriate (Marshal and Paul, 2015).

In the meantime, the concept of internal control evolved from a "structure" into a "process," making it both broader and more dynamic. However, some users of the COSO report have found it difficult to read and understand. A model that some believe to be able to overcome this difficulty is found in a report from the Canadian Institute of Chartered Accountants, which was issued in 1995. The report, *Guidance on Control*, presents a control model

referred to as Criteria of Control (CoCo). The CoCo model, which relies upon COSO, is thought to be more concrete and user-friendly. The CoCo describes internal control as actions that foster the best result for an organization. These actions, which contribute to the achievement of the organization's objectives, centre on:

- Effectiveness and efficiency of operations.
- Reliability of internal and external reporting.
- Compliance with applicable laws and regulations and internal policies.

The COSO framework indicates that a secure control environment is the basis of an effective internal control system, where the system is characterised as having management and where there is dedication to proficiency, integrity, and valuing the task of responsibility, over internal control, by the company's governing body. In layman's terms, the control environment is often described as the "tone at the top," which simply refers to how much the people at the top of the organization care about the entity's internal controls. CoCo indicates that control comprises those elements of an organization (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organization's objectives. COSO model recognizes four interrelated elements of internal control, including purpose, capability, commitment, and monitoring and learning. An organization that performs a task is guided by an understanding of the purpose (the objective to be achieved) of the task and supported by capability (information, resources, supplies, and skills). To perform the task well over time, the organization needs a sense of commitment. Finally, the organization must monitor task performance to improve the task process. These elements of control, which include twenty specific control criteria, are seen as the steps an organization takes to foster the right action.

In 2000, ISACF (The information Systems Audit and Control Foundation) developed the COBIT (Control Objectives for Information and related Technology), which is a framework of generally applicable IS security and control practices of information technology control. This framework allows management to benchmark the security and control practices of IT environment. Additionally, it ensures that adequate security and controls exist. However, control objectives under COBIT are defined in a process-oriented manner following the principle of business reengineering. This type of control is exercised at the domain and process level. CobiT focuses primarily on efficiently and effectively monitoring information

systems. This control model can be used by management to develop clear policy and good practice for control of IT. The COBIT IT domain consists of four parts: Planning & organization, acquisition and implementation, delivery, support and monitoring. The COSO Internal Control Framework recognizes the importance of the quality, timeliness and effectiveness of information and communications in ensuring that all significant risks have been identified, the appropriate controls have been established, and those assigned to monitoring can execute their responsibilities effectively.

The COSO framework is very extensive and is used by both operational and financial reporting controls for effectiveness and efficiency. Understanding the framework is reasonably easy and can be adapted to both start-up and mature business operations, although it may be harder to apply it to more complex businesses (e.g., businesses with diverse operations and complex data systems) due to the framework being extensive. To correctly use the COSO framework, there must be a secure, recognised control environment. Unfortunately, the framework does not provide much guidance on how to apply it, which can make it difficult or overwhelming to carry out for start-up businesses. COSO Internal Control Framework could be seen as too extensive or awkward by department managers of businesses to implement to their specific operations.

COBIT specifies 210 detailed control objectives for these 34 processes to enable effective management of an organization's information resources. It also describes specific audit procedures for assessing the effectiveness of those controls and suggests metrics that management can use to evaluate performance (IT Governance Institute, 2017). An advantage of the COBIT framework is that it is very understandable, and it is, therefore, increasingly accepted internationally to manage and control information systems. External auditors, however, may be concerned only with a subset of the issues covered by COBIT, specifically those that most directly pertain to the accuracy of an organization's financial statements and compliance with the Sarbanes-Oxley (SOX) Act. Consequently, ISACA issued a document entitled "IT Control Objectives for Sarbanes-Oxley, 2nd Edition" that discusses the portions of COBIT most directly relevant for compliance with SOX and provides guidance for assessing the adequacy of those controls.

The COBIT framework shows that achieving the organization's business and governance objectives requires adequate controls over IT resources to ensure that information provided to

management satisfies seven key criteria. (i) Effectiveness-the information must be relevant and timely, (ii) Efficiency-the information must be produced in a cost-effective manner, (iii) Confidentiality-sensitive information must be protected from unauthorised disclosure, (iv) Integrity-the information must be accurate, complete, and valid, (v) Availability-the information must be available whenever needed, (vi) Compliance-controls must ensure compliance with internal policies and with external legal and regulatory requirements, and (vii) Reliability-management must have access to appropriate information needed to conduct daily activities and to exercise its fiduciary and governance responsibilities. COBIT provides for controls across a domain and process framework. The framework consists of a large set of IT processes (e.g., point of sale systems, accounts payable), grouped into four primary domains (Khther and Othman, 2013). Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. Supporting these IT processes are more multiple detailed control activities necessary for effective implementation. The CoBIT framework also addresses specific information objectives, such as the quality and security of information, as well as its alignment with the entity's business strategy (i.e., fiduciary role).

The COBIT framework is usually not employed by start-up or individual businesses because it is usually used by companies with complex information technology systems where there is a greater risk, from the failure of these systems to management not being able to achieve their business strategies and financial reporting objectives. While the specific definition of internal control differs across the various models, a number of concepts are very similar across these models. In particular, the models emphasize that internal control is not only policies and procedures that help an organization accomplish its objectives, but also a process or system impacted by people. In these models, people are perceived to be central to adequate internal control. These frameworks emphasize the concept of reasonable assurance, as it is relevant to internal control. Internal control can only provide reasonable assurance that a company will perform its objectives and cannot guarantee it. The ability and loyalty of the people of the company create the effectiveness of internal control. There are restrictions to internal control, like imperfect human judgment, misinterpreting instructions, errors, management taking precedence over controls and conspiracy. Also, due to reasons of financial costs, not all available controls will be implemented (Ribeiro and Gomes, 2009).

These restrictions make that internal control not able to guarantee that a business will perform its objectives. Furthermore, there are clear linkages between the CobiT information criteria

and COSO's objectives related to effectiveness and efficiency of operations, compliance with laws and regulations, and reliability of information. Achieving the CobiT information criteria, therefore, has important implications for financial statement assertions as well as broader implications for the efficiency and effectiveness of operations.

Table 2.1 Types of Assessing Accounting Information System: COSO vs. COBIT

Types of Assessing IT Control	Issued by	Objectives	Components
COSO (the Committee of Sponsoring Organizations)	This framework was used by the Committee of Sponsoring Organization of the Tredway Commission satisfies the SEC criteria.	Companies may use it to meet management's annual internal control evaluation & disclosure requirements. However, it does not provide specific criteria for IT control.	Control elements: 1) Control environment. 2) Identifying control objectives, risks and Priorities. 3) Control activities. 4) Monitoring and corrective measures.
COBIT (Information Systems Audit and Control Association (ISACA) and IT Governance Institute, 1996)	The Information Audit and Control Foundation developed the control objective for information and related technology	The objective is a generally applicable and accepted standard for IT security and control practice that provides a references framework for management, users, auditors, and security practitioners.	Control areas: 1) Control environment. 2) Planning and Organizing. 3) Acquisition and implementation 4) Delivery and Service. 5) Monitoring and Evaluation. 6) Control processes. 7) Control activities.

*Source: Developed by the researcher

2.2.3.2 Web Trust and System Trust Service Framework

2.2.3.2.1 Web Trust Service

Web Trust is a Web assurance service developed together by AICPA and CICA for Business to Consumer ("B to C") electronic commerce. Web Trust is a professional service where an independent auditor receives payment from a business, which administers B to C electronic commerce ("EC Businesses") and provides assurances regarding the reliability of the B to C electronic commerce administered by the EC business. Assurance services, from within the framework of financial audit, is what Web Trust provides. The Web Trust features of assurance methods are. (i) "Assertions" that an EC business works in order for the B to C electronic commerce, which the EC business operates, to be trusted.

The assertions are the topic of the assurance, and (ii) "Established criteria", which are established by the AICPA and CICA are the Web Trust principles and serve as the standards for the assurance provider. The assurance provider assesses the "level of correspondence" between the "assertions" and the "criteria" and if the assertions are in agreement with the criteria for a fixed term, the assurance provider "relates" to the customers of the EC business that the B to C electronic commerce concerned is trustworthy shown by placing an assurance seal (Web Trust Seal) on the EC business Web site. As a reference, in financial audit, "assertions" are the financial statements, and "established criteria" are the Generally Accepted Accounting Principles, and an independent auditor "communicates" through the Independent Auditor's Report. Listed below are three principles that are the evaluation points used for assurance under Web Trust.

Principle 1: The EC business completes transactions in accordance with its disclosed business practices that it discloses for B to C electronic commerce transactions (Business Practices Disclosure).

Principle 2: By managing effective controls, the EC business provides sound assurance that customers' transactions using B to C electronic commerce are executed and billed as agreed (Transaction Integrity).

Principle 3: By managing effective controls, the EC business provides sound assurance that personal customer information attained as a result of B to C electronic commerce is protected from uses not associated with the EC business's business (Information Protection).

A series of interviews with managers, accountants, government representatives and representatives of the CICA has indicated that Web Trust has suffered from low market penetration due to stringent requirements and extensive work (and cost) in obtaining the seal (Gendron and Barrett, 2004). Another investigation by Fogarty, Radcliffe and Campbell (2006) has deemed Web Trust to be a failed attempt at broadening the range of services offered by public accountants by pursuing non-traditional assurance engagement. Regardless of the reasons for the lack of immediate adoption of Web Trust, it is evident that the pursuit of a specific seal is directly related to its influence on users in terms of perceived trust in the seal and the ultimate transfer of audit costs.

2.2.3.2.2 SysTrust Service Framework: Definition and Importance

The SysTrust service is an assurance service that was jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered

Accountants (CICA). It is designed to increase the comfort of management, customers, and business partners with systems that support a business or particular activity. SysTrust is a type of assurance service performed by a licensed CPA or CA to independently test an organization’s system and to offer assurance on the system's reliability. The intent is to enable those who use or rely on the system including the company itself, its partners, and customers to gain trust and confidence in the system (AICPA/CICA, 2017). Unlike COCO and COBIT, Trust Services framework was specifically designed for independent auditors to give an audit opinion as to whether the controls around the system were sufficiently effective to deem the system as “reliable”. SysTrust initially began as a distinct standard (separate From Web Trust). In 2003, the two standards, SysTrust and Web Trust, were amalgamated into a single standard. However, practitioners can now draw on the relevant principles and criteria from the Trust Services Principles and Criteria framework and give a SysTrust opinion. The standard in its entirety consists of 5 principles, 4 control layers, and 139 criteria in total. Table 2.2 illustrates the structure of the Trust Services framework and the distribution of the criteria.

Table 2.2 The Structure of the SysTrust Services Framework

Control Layers	Security	Availability	Processing Integrity	Online Privacy	Confidentiality	Totals
Policy	3	3	3	3	3	15
Communication	5	5	5	10	5	30
Procedures	12	15	19	18	15	70
Monitoring	3	3	3	3	3	15
Total	23	26	30	24	26	139

- Source: Boritz, J. Efrim, (2003) 12.28.

The greatest difference between COBIT and SysTrust can be understood by examining the deliverable that is produced by each framework. COBIT envisions a “Maturity Model”, where a firm moves from a low level of maturity (the lowest being 0) to the highest level of maturity. The idea behind assessing the organizations level of maturity is that management will “grade itself” (Martin, 2005). In contrast, SysTrust is designed specifically with the idea that independent auditors will render opinions on the state of control that exists over a system. According to Irving Tyler CIO of Quaker Chemical "Cobit is great from a management point of view, but not all of that applies to Sarbanes-Oxley. There's lots of good advice and guidance in there that shouldn't be a part of a Sarbanes-Oxley audit" (Martin, 2005). In contrast, the SysTrust framework identifies the specific controls that are necessary to ensure that the system is reliable. According to the AICPA, SysTrust is an assurance

service that independently tests and verifies a system's reliability. The AICPA succinctly describes the overall purpose of SysTrust in the following way. "Developments in information technology provide far greater power to companies at far lower costs. As business dependence on information technology increases, tolerance decreases for systems that are not secure, and these systems become unavailable when needed and unable to produce accurate information on a consistent basis". An unreliable system can cause a chain of events that negatively affect a company and its customers, suppliers, and business partners (Hunton, 2002).

Although COBIT and SysTrust share common foundational frameworks (e.g., COSO), the terminology used to describe information quality is slightly different in each document. Using the definitions contained in each document, the AICPA information qualities (listed previously) have been mapped into the seven COBIT information qualities of efficiency, integrity, effectiveness, availability, confidentiality, reliability and compliance. Five of the COBIT information qualities map directly into the SysTrust principles. Efficiency and reliability are not directly represented (Hunton, 2002). An IT control objective is defined by COBIT as "[a] statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity." The objective of a SysTrust engagement is to determine whether management has maintained effective controls over its system to enable the system to function reliably. First, management provides assertions regarding the availability, security, integrity and maintainability of the system. Then, the auditor determines the existence of system controls and performs tests to assess the extent to which such controls were operating effectively during the period covered by the assurance report.

The objective of a SysTrust engagement is to enable the practitioner to issue an attestation/assurance report on whether management maintains appropriate reliability controls over its system(s). Potential users of a SysTrust report include the entity itself as well as its shareholders, creditors, customers, suppliers, third-party users, including those who outsource to other entities and any other party who in some fashion relies on an information system. The term was intended to include auditing as a subcategory, as indicated in the following quote, which refers to the Special Committee's conceptual framework for assurance services. "The framework's primary objective is to provide a consistent view of assurance services. It provides guidelines that will enhance consistency and quality in the performance of services. (AICPA, 2013). The SysTrust assurance service is distinct from reporting on internal control

over financial reporting, which was established in 1993 by the AICPA and is described in SSAE No. 6.5 The latter service is limited to internal controls related to financial reporting and typically uses the criteria established in COSO, *Internal Control. Integrated Framework*. As such, it does not address the reliability of information systems designed for the broader decision needs of management and external users, who may need online access to real-time, updated and accurate information. In contrast, the new SysTrust assurance service relates directly to the overall reliability of a system, regardless of the type of information processed by the system. As such, the system may include financial and nonfinancial information that is critical to management and external users.

Martin (2005) also found the Trust Services framework to be a much more focused framework to work within the context of a SOX engagement and due the Trust Services “focus on the controls that are in place to ensure the company's systems carry out business processes reliably”. He also found that the “Trust Services' illustrative controls are detailed enough to help management identify the controls that exist and those that are missing.” A reliable system is the one that works without material errors, fault, or failure during a specified time in a specified environment. As for the symptoms of unreliable systems, they include frequent system failures and accidents that prevent users from accessing essential services, failure to prevent unauthorised access to the system, which makes it vulnerable to viruses, hackers and loss of data confidentiality, loss of data integrity, including corrupted, incomplete and fictitious data, and serious maintenance problems resulting in unintended negative side effects (Boritz, et. al., 2000). This assurance service has the potential to provide a twofold benefit. (i) Enhancing the confidence of a broad audience (management, boards of directors, customers, and business partners) regarding the reliability of information systems (Pugliese and Halse, 2000), (ii) Providing accounting professionals with the ability to leverage their existing skills to fulfil the needs of the systems assurance marketplace (Pugliese and Halse, 2000). Based on these potential benefits and the increasing dependence of companies on information technology, the profession expects that SysTrust engagements will contribute to the demand for trust services, as well as other assurance services, as predicted by Elliott (1995). Through the WebTrust and SysTrust services, companies have the ability to establish their credibility and build confidence with important end users.

SysTrust can benefit a business's day-to-day operations in the following scenarios. (i) A company is trying to win a major contract as a supplier to a corporation that uses just-in-time

(JIT) inventory management. A SysTrust report that demonstrates the reliability of the company's systems and shows its capacity to be a dependable partner in the JIT environment enables the company to differentiate itself from its competitors, (ii) a company decides to outsource its human resources, payroll, and other employee-related systems. To ensure smooth operations, it insists that any successful bidder maintain unqualified SysTrust reports on the outsourced systems, (iii) A retailer qualifies for a discount on business interruption insurance because its SysTrust report attests to the reliability of its inventory management systems, and (iv) When technology problems at foreign subsidiaries cause trouble for an international company, its audit committee decides to adopt the SysTrust principles and criteria as a minimum standard for key subsidiaries (Anthony and Ronald, 2003). Users of SysTrust would be interested in a systems assurance examination for some of the following reasons. (i) Internal and external users can lose access to essential services because of system failures and crashes, (ii) Systems can be vulnerable to viruses and hackers because of unauthorised system access, (iii) System failure can result in loss of access to system services or loss of data confidentiality or integrity, and (iv) Negative publicity in the wake of high-profile system failures can undermine customer and investor confidence.

Elliot and Pallais (1997) define assurance services related to information systems reliability as the "assurance that systems are designed and operate in a manner that provides reliable information or operate according to accepted criteria". The market for assurance services stems from the decision makers' desire to receive an independent expert's assurance that information used for decision evaluation is accurate (Kinney, 2000). Regarding the factors and drivers that are behind the demand on this service, (Boritz, et. al., 2000) pointed out that the demand on this service resulted from companies' search for new markets, reduced costs, and faster change which forced companies to rely on third parties' systems through different ventures. This assurance service profits internal and external parties of the entities that are engaged in information-based commercial activity, such as system users, outsourcing service providers, system developers and consultants, management and board of directors, and internal auditors and system owners (Boritz and Hunton, 2002).

Furthermore, as computer systems can be isolated, it is necessary to observe and verify their performance through a capable assurance provider, and also as an IT is a complex field, it requires special expertise. System unreliability can pose a risk due to making incorrect decisions for system users, or when there are major consequences related to unreliability, like

unnecessary costs, poor revenue, loss of investors' trust due to system failure; therefore, assurance on system reliability is greatly valued (Boritz and Hunton, 2002; Aly, et. al., 2010). Due to the increasing demand on system reliability, the system reliability task force, which is instantiated by a joint venture of the AICPA assurance services executive committee and the CICA assurance services development board, has developed a new assurance service, which is "SysTrust". In this type of engagement, assurance providers report on the availability, security, integrity and maintainability. A SysTrust engagement includes system description that identifies the boundaries of the system covered by the engagement, management's assertions about the system's underlying controls and an attestation report by a CPA that evaluates the system against specific criteria (Boritz, et. al., 1999). Boritz, et. al. (1999) and McPhie (2000) have documented several examples of unreliable systems. These include. (i) Denial of service, where users cannot use the system because it fails or crashes, or there are capacity issues, (ii) Unauthorised access, where the system is working, but viruses or hackers invade the system, or confidentiality is lost, and (iii) Loss of data integrity, where information is corrupted, incomplete or fictitious. In a SysTrust service, the management of a company prepares a description that defines the aspects of the system that will be covered, so that the scope is clear to users of the report. Then, a licensed practitioner (CPA or CA) performs audit procedures to examine and test the five key components of the system (infrastructure, software, people, procedures, and data), as well as their relationships. Finally, the practitioner assesses whether the whole system meets the SysTrust principles and the related criteria. If the system satisfactorily meets all the principles and the related criteria, it achieves the reliability defined by SysTrust. The practitioner will issue a written SysTrust assurance report with an unqualified opinion, independently verifying that the company has effective system controls and safeguards enabling the system to function reliably. The company may use the SysTrust assurance report in its marketing of documents, agreements and contract with customers, business partners or others system users to enhance trust in its system.

Concerning the participating parties in the assurance services, Bedard, et. al. (2005) notes that there are three parties involved in systems assurance services: (i) the users of the assurance services, (ii) the entity hiring the assurator (assurance provider), and (iii) the assurator or "provider". Assurance providers play a crucial role in the assurance service engagement, and they should have certain attributes. Knechel, et. al. (2006) discusses the required attributes of assurance service providers by using a sample of Dutch senior accounting and financial officers, and suggests certain attributes, confidentiality, expertise, professional reputation,

independence, objectivity, integrity, and costliness. They also conclude that overall expertise and objectivity are perceived to be the most important attributes for selecting an assurance service provider. Cost is perceived as the least important attribute for assurance services in general. Most respondents (97.6%) agree that expertise is important in the assessment of systems reliability. In addition, the provider of system trust service should have skills related to information technology; however, the degree of complexity depends on the system being examined (Boritz, et. al., 1999). Additionally, the expert should be able to observe internal control effectively. Also, it is necessary for the auditor, who takes up the task to be able to meet the general standards of attestation services, specifically the specialised professional proficiency standard in the system field. The auditor must also be able to perform the service as a combined process that results in a positive assurance and prepare a report on testing the system that complies with specific formal and substantive factors (Aly, et. al., 2010).

The AICPA Assurance Services Executive Committee (ASEC) has developed a set of principles and criteria (trust services principles and criteria) to be used in evaluating controls relevant to the security, availability, and processing integrity of a system, and the confidentiality and privacy of the information processed by the system. In this document, a *system* is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) in accordance with management specified requirements. System components can be classified into the following five categories.

- *Infrastructure.* The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
- *Software.* The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- *Processes.* The automated and manual procedures.
- *Data.* The information used or processed by a system (transaction streams, files, databases, and tables).

A SysTrust engagement includes a system description that delineates the boundaries of the system covered by the engagement, management's assertion about the system's underlying

controls, and an attestation report by a CPA that evaluates the system against specific criteria. To earn an unqualified opinion, a system must meet all of the SysTrust principles and criteria. A reliable system is one that operates without a material error, a fault, or failure during a specified time in a specified environment. SysTrust standards include 58 underlying criteria that establish the specific control objectives a system must meet to be considered reliable. The AICPA and the Canadian Institute of Chartered Accountants (CICA) have developed the following principles and related criteria for use by practitioners in the performance of trust services engagements (AICPA, 2013; 2017).

1. Availability. The system is available for operation and use as committed or agreed. The *availability principle* refers to access to the system, products, or services that contract, service-level, or other agreements advertise or agree. To note, the principle itself does not set a minimum acceptable performance level for system availability. The minimum performance level is confirmed through a mutual agreement (contract) agreed upon between parties. The *availability principle* does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems), but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance. In assuring availability, the SysTrust provider attests that accessibility to the system, products or services is available as committed to, or agreed upon, by the entity. Consistent system availability is difficult to achieve. Modern computer networks are composed of hundreds of different parts from hundreds of different companies. In these complex environments, network managers often lack the resources needed to do the preventive maintenance necessary to keep systems running on a continuous basis.

2. Security. The system is safeguarded against unauthorised access (both physical and logical). The *security principle* applies to safeguarding the system, both logical and physical, from an unauthorised access. When the system has restricted access, it helps in preventing possible exploitation; resource theft and software misuse of the system, and inappropriate use, or access to, modification, damage or disclosure of information. To protect the system, the main factors are to allow authorised access to the system according to necessity and deny unauthorised access in all other cases.

The *security principle* refers to the protection of the system resources through logical and physical access control measures in order to support the achievement of management's commitments and requirements related to security, availability, processing integrity, and

confidentiality. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or unauthorised removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information. Assurance of system security implies that access is restricted to the physical components of the system, the logical functions the system performs, and the information stored in the system. System security is the number one issue identified by the AICPA's (2003). Top Technologies Task Force Security breaches may result in errors that can have a far-reaching effect on planning and operations of a business and its partners. Possible losses from security breaches increase with the increased use and dependence on IS and the information processed by them. While noting the importance of system security, the Task Force also notes the difficulty of securing even the most carefully planned systems. The primary causes of system security failures are not related to design flaws, but to creative hackers and/or lax employees.

- 3. Processing Integrity.** The *processing integrity principle* refers to the completeness, accuracy, validity, timeliness, and authorization of system processing. Processing integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorised or inadvertent manipulation. Completeness generally indicates that all transactions are processed or all services are performed without exception. Validity refers to processing transactions and services no more than once and with compliance to business principles and expectations. Accuracy refers to keeping important information, concerning the submitted transaction, accurate while the transaction is being processed and that the transaction or service is processed as planned. The agreement context made for the provision of services or delivery of goods shows their eligibility. Authorization means that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing. Processing integrity addresses whether the system achieves its aim or the purpose for which it exists, and whether it performs its intended function in an unimpaired manner, free from unauthorised or inadvertent manipulation. Processing integrity does not automatically imply that the information received and stored by the system is complete, valid, accurate, current, and authorised. System control usually cannot address the risk that data contain errors introduced prior to its input in the system, and the unit is not usually liable to identify these types of errors. In the same way, users from outside the system boundary may be accountable for starting processing.

The data may become invalid, imprecise, or unsuitable if actions like these are not taken. System processing integrity refers to the completeness, accuracy, timeliness, and authorization of system processing (i.e., all phases of processing, including input, transmission, processing, storage, and output). If processing integrity is not present, even a system that is secure and available is of little benefit to users. While the number of audit failures directly attributed to inaccurate assessment of controls is relatively small, there have been a significant number of system failures that have caused users untold grief. System processing integrity addresses all system components and all phases of processing (input, transmission, processing, storage, and output) that are the subject of the SysTrust engagement. If a system processes information inputs from sources outside the system's boundaries, an entity can establish only limited controls over the completeness, accuracy, authorization, and timeliness of the information submitted for processing because, for the most part, procedures at external sites are beyond the entity's control. Thus, when the information source is explicitly excluded from the boundaries of the system that define the SysTrust engagement, it is important to describe that exclusion in the system description. In other cases, the data source may be an inherent part of the system being examined, and controls over the completeness, accuracy, authorization, and timeliness of information submitted for processing would be included in the system description.

System integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorised or inadvertent manipulation of the system. In this document, system integrity refers to the completeness, accuracy, timeliness, and authorization of system processing. Data integrity exists if information and programs only can be changed in a specified and authorised manner. In this document, data integrity refers to the completeness, accuracy, currency, and authorization of data. Data integrity depends on system integrity, and system integrity depends on controls over system components and the risks affecting those components in the system's business context. Although system and data integrity are obviously related, the focus of a SysTrust engagement is system integrity. Because SysTrust is a controls-based engagement, ordinarily it would not provide sufficient evidence to enable a practitioner to provide examination level assurance about data integrity. This is due to the following inherent limitations of controls. The possibility of circumvention, either by employee collusion or management override, when it is difficult to prevent or detect such circumvention.

- The trade-off between operating efficiency and complex controls that may reduce exposure.
- The practical materiality limits, below which it is impractical to implement controls.
- Changing conditions in entities that may lead controls to deteriorate or to become inappropriate.
- The reliance on human judgment in the design, implementation, and monitoring of controls, any of which may lead to control breakdowns.

Because of the inherent limitations of controls, evidence about the effectiveness of controls over system integrity ordinarily would not provide sufficient evidence about data integrity to reduce attestation risk to the low level required. Thus, although evidence about the effectiveness of controls over system integrity may be very persuasive, procedures beyond those performed in a SysTrust examination would be required to reduce attestation risk about data integrity to a level required by examination-level attestation standards. It is also important to recognize that system integrity does not automatically imply that the information stored by the system is complete, accurate, current, and authorised. This is because errors may have been introduced into system data at some previous time (for example, at initial data conversion) and those errors could still be present in the data, even though current system processing may be complete, accurate, timely, and authorised.

4. Confidentiality. The confidentiality principle refers to the system's ability to protect the information designated as confidential, as committed or agreed. Unlike personal information, which is defined by regulation in a number of countries worldwide and is subject to the privacy principles, there is no widely reorganised definition of what constitutes confidential information. Partners usually exchange information that need to be kept confidential, at the time of communicating and transacting business. Often the request of respective parties is that they be assured that the information they give is only accessible for those individuals who need access to it, to complete the transaction or to clarify any questions that may arise. To enhance business partner confidence, it is important that the business partner be informed about the entity's system and information confidentiality policies, procedures, and practices. The entity needs to disclose its system and information confidentiality policies, procedures, and practices relating to the manner in which it provides for an authorised access to its system and uses and shares information designated as confidential. The need for information to be confidential may arise for many different reasons. For example, the information is proprietary

information, information intended only for company personnel, personal information, or merely embarrassing information. Confidentiality is distinguished from privacy in that (i) privacy deals with personal information, whereas confidentiality refers to a broader range of information that is not restricted to personal information, and (ii) privacy addresses requirements for the treatment, processing, and handling of personal information.

5. Privacy. Privacy can be defined as “the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information” (GAPP, 2009). Distributed by the AICPA and CICA, criteria set forth in Generally Accepted Privacy Principles (GAPP) indicate that personal information is collected, used, maintained, disclosed, and destroyed. This is also in compliance with the agreements in the entity's privacy notice. *Personal Information* refers to information relative to an identifiable individual and includes any information that can be directly or indirectly used to identify an individual, and any information that can be connected to an individual. Any information, gathered by an organization, which can be linked to an individual, is most often considered personal information. Organizations are trying to strike a balance between the proper collection and use of their customers' personal information. Governments are trying to protect the public interest and, at the same time, manage their cache of personal information gathered from citizens. Consumers are very concerned about their personal information, and many believe they have lost control of it. Furthermore, the public has a significant concern about identity theft and inappropriate access to personal information, especially financial and medical records and information about children. Individuals expect their privacy to be respected and their personal information to be protected by the organizations with which they do business. They are no longer willing to overlook an organization's failure to protect their privacy. Therefore, all businesses need to effectively address privacy as a risk management issue. The following are specific risks of having inadequate privacy policies and procedures: (1) Damage to the organization's reputation, brand, or business relationships. (2) Legal liability and industry or regulatory sanctions. (3) Charges of deceptive business practices. (4) Customer or employee distrust. (5) Denial of consent by individuals to have their personal information used for business purpose (6) Lost business and consequential reduction in revenue and market share. (7) Disruption of international business operations, and (8) Liability resulting from identity theft” (GAPP, 2009).

For organizations operating in more than one country, the management of their privacy risk can be a significant challenge. For example, the global nature of the Internet and business means regulatory actions in one country may affect the rights and obligations of individual users and customers around the world. Many countries have laws regulating trans-border data flow, including the European Union's (EU) directives on data protection and privacy, with which an organization must comply if it wants to do business in those countries. Therefore, organizations need to comply with changing privacy requirements around the world. Further, different jurisdictions have different privacy philosophies, making international compliance a complex task. To illustrate this, some countries view personal information as belonging to the individual and take the position that the enterprise has a fiduciary-like relationship when collecting and maintaining such information. Alternatively, other countries view personal information as belonging to the enterprise that collects it. In addition, organizations are challenged to try and stay up-to-date with the requirements for each country in which they do business. By adhering to a high global standard, such as those set out in this document, compliance with many regulations will be facilitated. Even organizations with limited international exposure often face issues of compliance with privacy requirements in other countries. Many of these organisations are unsure how to address often stricter overseas regulations. This increases the risk that an organization inadvertently could commit a breach that becomes an example to be publicised by the offended host country. Furthermore, many local jurisdictions (such as states or provinces) and certain industries, such as healthcare or banking, have specific requirements related to privacy. The trust services framework identifies four essential criteria for successfully implementing each of the five principles that contribute to systems reliability (APICA, 2013).

1. *Developing and documenting Policies.* The entity has defined and documented its policies relevant to the particular principle. (The term *policies* as used here refer to written statements that communicate management's intent, objectives, requirements, responsibilities, and standards for a particular subject.) Management needs to develop a comprehensive set of security polices before designing and implementing specific control procedures. Developing a comprehensive set of security policies begins by taking an inventory of information system resources. This includes not only hardware but also software and database.
2. *Effectively Communicating policies to all authorised users.* The entity has communicated its defined policies to responsible parties and authorised users of the system. To be effective, this communication must involve more than just handling

people written documents and asking them to sign an acknowledgment that they received and read them. Instead, users must receive regular, periodic reminders about security and training in how to employ them.

3. *Designing and employing appropriate control Procedures to implement.* The entity places in operation procedures to achieve its objectives in accordance with its defined policies.
4. *Monitoring the system and taking a corrective action to maintain compliance with policies.* The entity monitors the system and takes action to maintain compliance with its defined policies. Effective control system involves a continuous cycle of developing policies to address identified threats, communicating those policies to all employees, implementing specific control procedures to mitigate risks, monitoring performance and taking a corrective action in response to identified problems. The necessary corrective action often involves the modification of the existing policies and the development of new ones. A SAS 70 audit engagement is created to give information and assurance to the user organizations and their auditors about the service organization's controls. The service auditor gives an opinion on whether the controls were correctly designed, positioned in operation, and are operating efficiently. The independent auditor's opinion, a description of the service organization's controls, and the results of the service auditor's processes (as in a Type II audit) are contained in the SAS 70 service auditor's report. How is a SysTrust engagement differentiated from services already available, like a service auditor's engagement performed through SAS No. 70, the Service Organizations (in the United States), and S 5900 "Views on Control Procedures at Service Organizations" (in Canada)? When an entity acquires services from another organization (a service organization) and an auditor audits the financial statements of that entity, SAS No. 70 applies.

It is created to give information and assurance to the user organization's auditor about controls at the service organization that may influence the user organization's financial statements. A SysTrust engagement is created to give report-users assurance concerning whether the entity has maintained effective controls on the reliability of a system, and unlike a service auditor's engagement, users do not attain a comprehensive description of the system, the processes the practitioner performs and the results of those processes. There may be questions about the differences between the SysTrust service and two other assurance services, WebTrust and ISPTTrust (a new assurance service being designed by the electronic

commerce task force that aims to evaluate Internet service providers). There are differences in both the type of the systems being addressed and the type of the assurance being provided. Both WebTrust SM and ISPTrust SM only target Internet-based systems.

Table 2.3 The Differences between SAS 70 Audits and SysTrust Engagement

	SAS 70 audit engagement	SysTrust engagement
Type of engagement	It gives a report on a service organization's controls regarding financial statement assertions of user organizations	It gives a report on system reliability using standard principles and criteria for all engagements.
Are there pre-established control objectives or criteria	No	Yes
Objective of the engagement	Information sharing and assurance. It gives detailed information on the design of the system and controls, an opinion on the system description and controls, and the results of the auditor's procedures	Assurance on a system. No detail on the underlying control procedures is given
Types of systems addressed by the engagement	The Systems that process transactions or data for the user organization	Any system
Distribution of report	Generally restricted to the service organization, user organizations, and prospective user organizations.	No restriction
Audience for the report	Service organizations, user organizations (i.e. customers), and auditors of the user organizations.	Stakeholders of the system for example, management, customers, and business partners

**The information in the above table is taken from version 2.0 of the "AICPA/CICA SysTrust Principles and Criteria for Systems Reliability".*

However, SysTrust applies to various types of systems and while WebTrust and ISPTrust target mainly controls over Internet-based transactions, SysTrust targets particularly the reliability of systems themselves. Whereas it is possible to have a qualified SysTrust report, that is not possible for a WebTrust report. WebTrust provides the trust in the websites containing the information, and the SysTrust service provides the trust in the systems producing the information (Pathak and Lind, 2002; Amin and Mohamed, 2016).

Some of the specific differences between a SAS 70 audit engagement and a SysTrust engagement are illustrated in Table 2.3. An information system must satisfy all of the SysTrust criteria to be deemed reliable. A SysTrust practitioner examines system controls related to the criteria to collect evidence that the criteria have been met (Boritz, et. al., 1999; Bortiz, 2002). The SysTrust guidance materials provide practitioners with several necessary illustrative controls. Ultimately, it is an organization's responsibility to implement controls that address risks relating to security, privacy, processing integrity, availability and confidentiality. The intention of the Trust Service Framework is not to list specific controls necessary to address these risks, but rather to provide an appropriate basis for benchmarking (system development) and assessment (audit and evaluation).

2.2.4 Literature Review on Reliability of AIS

In order to survey empirical studies pertinent to the reliability of AIS as the main focus, a scholarly internet search engine (scholar.google.com), in addition to several online databases, was used. The databases cover all leading journals, not only in the fields of internal control of AIS process, but also in the accounting of information systems in general and the recently developing field of trust service in e-commerce and accounting. AIS is embedded within IS journals. The majority are conceptual or non-empirical, where the empirical previous studies that discuss the same topic apply one of the two approaches, either qualitative or quantitative. Recently, researchers have been more in depth to study the AIS in enterprises. However, the majority of previous studies focus in their work on testing the effect of accounting information systems on business performance. The theory of demand for trust services is based on some innate hardships related to electronic commerce. While all business transactions carry a risk factor that intended transactions will not be processed as planned, the risk factor is greater in electronic commerce because of the loss of human mediators that are at hand in physical markets, indicating a reliance on electronic systems to avert, or identify and correct, errors (Westland, 2000). In addition, as information irregularity between parties to transactions is higher in electronic commerce, they are usually geologically distributed (Papazoglou and Tsalgatidou, 2000; Tan and Theon, 2002, Al-Dmour, et. al., 2018).

Henry (1997) carries out a survey on 261 companies in the US in order to determine the nature of their accounting systems and security in use. Seven basic security methods were presented in his study. These methods were encryption, password access, backup of the data, viruses' protection, and authorization for system changes, physical system security and

periodic audit. Henry's study results indicate that 80.3% of the companies' backup their accounting systems, 74.4% of the companies secure their accounting systems with passwords, where only 42.7% use antivirus in their systems. The results also reveal that less than 6% of the companies use data encryption, lastly 45% of companies undergo some sort of periodic audit for their accounting information systems. Another study, carried out by Qurashi & Siegel (1997), assures the accountant's responsibility to check the security of the computer system. The researchers carried out a theoretical study to develop a security checklist. This list covers the following four security controls groups: Client policy, Software security, Hardware security and Data security. Cerullo and Michael (1999) conducted a survey using a questionnaire of twenty potential security and control mechanisms, which was circulated among audit directors of two hundred fortune companies in the US. These mechanisms were placed by Cerullo study in four categories, namely Client-based, Network-based, Server-based and Application-based. The researches, Tan and Theon (2012), conclude that parties would not use an electronic transaction unless the degree of transaction trust is higher than the threshold value, which relies on features of the party and of the transaction itself. The possibility to resist taking part in electronic transactions develops the requirement for a service that will strengthen trust to the level that it exceeds the user's threshold.

WebTrust and SysTrust deal with this requirement through assuring observance of standards of control. Together, the attributes of the particular assurances made (e.g., reliability, privacy, etc.), and the attributes of the assuring party (e.g., a CPA; Kaplan and Nieschwietz, 2003) are theorised to result in the trust-enhancing value of these services. From amongst trust services literature, the researchers Kovar and Mauldin (2003) give a theoretical model that targets its focus on the natural prospective need for assurance services, resulting together from circumstantial business setting features and sources of information risk within that setting and from a precedent of the market demand for third-party assurance services. Because SysTrust was created after WebTrust, there is a lack of experimental research available in that perspective. In their study of electronic data interchange (EDI), Khazanchi and Sutton (2001) give evidence of the requirement for systems assurance, illustrating that numerous companies enforcing these systems do not use them to full benefit. This shows that entities authorizing EDI for their clients or customers should require assurance of suitable functioning. Results of these studies recommend a demand for trust services. Consequently, it follows that there should be a positive effect on the business of clients that meet approved trust services standards. Moreover, a study from Havelka, et. al. (1998) argues that expression of agreement

on measurement criteria for assurance services among providers and users will enable a more effective and efficient production of those services. They created measurement criteria for assurance services generally and made a comparison of the views of IT consultants and system users on the related significance of those criteria in performing systems assurance.

SysTrust is one of the models to update Internal Control Systems (ICS) of AIS through frame working the technological variables which affect designing AIS. Due to such nature, much of the practical studies have been implemented using the principles and criteria of SysTrust to examine quality and performance of AIS. The term ICS has been used by COSO (1992) to refer to the risks associated with ineffectiveness management of public companies, both large and small. Integrated framework of COSO has long served as a blueprint for establishing internal controls that promote efficiency, minimize risks, and help check the reliability of financial statements, and comply with laws and regulations. According to COSO's study, ICS is no longer accounting concept. COSO's report has outlined 26 fundamental principles associated with the five key components of ICS: (I) Control environment. (II) Risk assessment. (III) Control activities (IV) Information and communication and (V) Monitoring. ISACF (2001) considers the control objectives associated with use of IT. The study is widely known as COBIT. COBIT consists of three control groups, business objectives, IT resources, and IT-based process. The key feature of COBIT is coming from the fact that it has developed 36 standards of control related to security of IT-based AIS. The impact of IT formed an accounting process on the operational variables of cost and productivity, and profitability has been addressed by Casolaro and Gobbi (2004). The study was conducted on more than 600 banks belonging to the Italian banking industry. The study concludes with the facts that intensive use of IT-based AIS has reasonable impact on. (I) Reduction of banking services cost, (II) Expansion of banking services package, and (III) Increasing banking profit. Another study was conducted by Raupeliene and Stabingis (2003) has considered the effectiveness of IT based AIS. The study has developed a quantitative model based on set of technological, economics, and social parameters. According to the study of Raupeliene and Stabingis (2003), the effectiveness of IT-based AIS varies according to the superiority level of IT infrastructure of AIS and the environmental development of AIS.

Proposed benefits of the use of SysTrust service include improved confidence in the systems of both business partners' and one's own internal systems, avoiding problems of system development (McPhie, 2000) and reducing the cost of business interruption insurance (Pugliese and Halse, 2000). The literature also suggests that SysTrust provides a good

framework for auditing internal systems (Boritz and Kearns, 1999) and restructuring systems controls and procedures (Trabert and Mackler, 2001). It also sets a standard for structuring information technology outsourcing agreements (Trabert and Mackler, 2001). While recognizing the potential benefits of trust services, Gray (2002) warns customers to investigate the relative value of the benefits against the associated cost before hiring a third party assurance provider. Accordingly, it is clear that system assurance has a positive impact on system users and their reliance and in turn on their decisions, especially when this assurance is provided on continuous basis, which is more suitable to the current changing environment. SysTrust developers also expect that the SysTrust report would be seen in the market as a sign of quality. According to this viewpoint, Trabert and Mackler (2001) imply that SysTrust opinions will function as a marketing tool and add value for the client. In the most recent version of the trust services guidelines, electronic seals or reports can be used with SysTrust engagements. Users may recognize that displaying the electronic seals or reports will help in their marketing efforts through improving their skill to distinguish themselves from other entities. This contention is supported by the results of the study of Arnold, et. al. (2000), which indicate that good-quality dealers are willing to pay for reports that differentiate along quality lines.

Moreover, Boritz and Honton (2002) report that SysTrust assurance significantly increases user comfort levels with the reliability of the information technology of a service provider, as well as the possibility that users would recommend contracting with the service providers. Even though the possible benefits of trust services to clients have been focused on in the literature, there is a lack of experimental evidence to support the belief that the existence of a trust service assurance report gives a precise sign of systems quality. A study by Jamal, et. al. (2002) focuses on this aspect and examines the link between the existence of web seals and actual company practices with regard to information privacy. The results indicate that, on overall, clients comply reasonably well with privacy policies concerning notification, disclosure, and privately identifiable information choice options. While compliance with acknowledged privacy policies is not perfect, Jamal, et. al. (2002) find that disclosure for web sites with privacy seals is better than those without seals. However, performing SysTrust engagements is not without potential risks. There are two potential issues inherent in such engagements, some of which present exposures to the provider of assurance services. For example, users might not recognize that trust services cannot provide continuous assurance

regarding system, and further performance might not be predictable based on past performance and test (Bedard, et. al., 2005).

A study by Warren (2002) entitled "Security Practices" attempts to study the difficulties facing the information system using a sample consisting of Australian, English and American companies. The results of the study show that the limitation of technological security procedures and intentional incorrect entry of financial data in the American companies is a noticeable limitation facing information system. Previous literature discussed the effect of assurance on its beneficiaries. Boritz and Hunton (2002) tried to evaluate the amount that auditor-provided systems reliability assurance affects prospective service recipients' through (i) the probability of recommending that their company enter into a contractual agreement with the service provider, and (ii) the comfort level with the reliability of the service provider's information systems. Abu Musa (2004) performs an empirical study to investigate the adequacy of Security Controls implemented in the Egyptian banking industry (EBI), where the respondents were restricted to the head of the computer department and the head of internal audit department. Abu Musa tried to check whether the applied Security Controls in the EBI are adequate to protect against the perceived security threats through self-administrated checklist. The CAIS security checklist included eighty security procedures which were categorised under the following ten groups. (1) Organizational information security controls. (2) Hardware and physical access security controls. (3) Software and electronic access security controls. (4) Data and data integrity security controls. (5) Off-line programs and data security controls. (6) Utility security Controls. (7) Bypassing of normal access security controls. (8) User programming security controls. (9) Division of duties. (10) Output security control. Also, from a security perspective, Siponen and Oinas-Kukkonen (2007) reconcile prior security research literature and emphasize the distinct importance of accessibility and availability as it relates to communication issues, like user authentication and appropriate maintenance of data retention. Likewise, Nelson, et. al. (2005) argue that accessibility represents a system attribute that is distinct but similar in importance to the system's ability to produce reliable data, although they argue that this impact of accessibility is second in order of influence to the system's processing reliability

Boritz (2005) conducts an extensive review of the literature to identify the key attributes of information integrity and related issues. He brought two focus groups of experienced practitioners to discuss the documented findings extracted from the literature review through

questionnaire examining the core concepts of information integrity and its elements. Boritz (2005) considers information security (distinct from confidentiality) as one of the core attributes for information integrity. This security should cover the following areas: Physical access controls and Logical access controls. The results indicate that security has a lower impairment severity score than other severe practical aspects, such as availability and verifiability. Boritz's such findings refer to the effective use of security controls in the organizations represented. In his study, Coe (2005) focuses on the fulfilment of Sarbanes-Oxley act 2002 that requires public companies to report about the effectiveness of their internal control systems. Coe. In this study, it is explained that American companies are using COBIT for Sarbanes-Oxley act 2002 compliance, and this is because its objectives have been mapped to COSO in a publication entitled IT Control Objectives for Sarbanes-Oxley. COBIT also has been mapped to popular enterprise resource planning (ERP) systems, like SAP, Oracle and PeopleSoft.

This mapping and related guidance provides COBIT with framework references and methodologies for auditing and testing the major ERP systems. But it is decided later to use SysTrust service to ensure the company's systems carry-out business processes reliably. Herein, Coe establishes five-step processes showing how CPAs can use the trust service framework to evaluate a company's IT controls when the entity primarily uses the COSO approach. These steps are: (I) Use COSO framework to identify the risks in each business cycle and the controls that mitigate them, (II) Gather initial IT information, (III) Identify all information systems that relate to financial reporting, (IV) Be used to trust services framework to create one overall IT matrix, (V) Assess the controls identified in the matrices created above. Martin (2005) mentions the same steps in his study, in which he tries to explain how information system auditor can use the AICPA/CICA trust services framework to evaluate internal controls, particularly controls over information technology. The participants in the experiment were 481 middle and upper-level managers from a wide range of functional areas. The study concludes that auditor-provided assurances on information systems availability, security, integrity and maintainability will show significant key effects with respect to the probability of the participant entering into a contractual agreement with the ASP organization. In addition, the comfort level of the participant with the reliability of the ASP organization's ERP system will increase.

Also, Meharia (2011) aims to study the effects of assurance services and the trust in the mobile payment system on how users' use the system. To demonstrate this matter, the study depends on the Technology Acceptance Model (TAM). The study finds that the users' intention to use their attitude towards the system determines their real use. Their attitude towards the system is decided by the apparent usefulness of the system and the simplicity of use. However, the study adds that the assurance on the security, availability, confidentiality, privacy, and process integrity of the system will have a positive influence on the users' attitude towards the system, in combination with the apparent usefulness and simplicity of use.

In the same manner, Zhou (2011) intends to evaluate the influence of initial trust on user adoption of mobile banking. The study supposes that initial trust decides the intent to use the mobile banking system, as well as the apparent usefulness of the system. The initial trust is decided by the structural assurance (such as third party certifications), information quality, and system quality. The apparent usefulness is decided by the information quality and system quality. Information quality indicates the relevance, adequacy, precision and timeliness of the information whereas system quality indicates the speed of access, simplicity of use, navigation and look of the mobile banking system (Kim, et. al., 2004 as cited in Zhou, 2011). The study finds that structural assurance, information quality, and system quality have an influence on initial trust. Users need to depend on structural assurance to trust mobile banking because mobile banking relies on wireless networks and includes great risk and doubt. Information quality and system quality have an influence on the apparent usefulness of the mobile banking system. Users may feel that the providers of these types of system will not provide quality services to them if the quality of information is low. Furthermore, if mobile banking has a slow access speed or if users experience service unavailability or interruption, because of system unreliability, users' observation towards mobile banking will have a negative effect. In the same context, Greenberg, et. al., (2012) aim to investigate the influence of SysTrust criteria (availability, integrity and security) on users' intent to use reliability on an online accounting system (of Oracle Small Business Suite). According to the TAM, the study supposes that the intention to take up online systems depends on the apparent usefulness of the system, apparent ease of use, trust in system reliability, and trust in the internet. The study finds that users' intention to take up the online accounting system is greater when users' trust in system reliability and trust in the internet are greater. The results of the study indicate that the reliability of a system, as measured by SysTrust criteria, is related to the decisions relevant to the intention to take up online accounting systems.

Consequently, it is apparent that system assurance has a positive influence on system users, their reliance and, therefore, on their decisions, particularly when this assurance is provided constantly, which is more suitable according to the present changing environment. In reviewing the literature, it can be seen that Certified Public Accountants (CPAs) can provide assurance on RTA Information Systems. CPAs are accepted as independent parties that provide assurance concerning the accuracy and fairness of financial information. Also, CPAs are well-informed about the subject matter to be assured and the assurance matters, recognised for their independence, objectivity and reliability, and acquire advanced technical competencies (Burton, et. al., 2012). Boritz and Hunton (2012, p. 69) aim to assess the extent to which auditor-provided systems reliability assurance affects potential service recipients' (I) likelihood of recommending that their company should enter into a contractual agreement with the service provider, and (II) comfort level with the reliability of the service provider's information systems. Based on an experiment on 481 middle- and upper-level managers from a broad spectrum of functional areas participating in the study, the conclusion is that auditor-provided assurances on information systems availability security, integrity and maintainability will exhibit significant main effects with respect to the participants' likelihood of entering into a contractual agreement with the ASP firm and the participants' comfort level with the reliability of the ASP firm's ERP system will increase. Similarly, Greenberg, et. al., (2012) have attempted to investigate the impact of SysTrust criteria on users' intention to use online accounting systems and their reliability. Based on the TAM, the study posits that the intention to adopt online systems depend on the perceived usefulness of the system, perceived ease of use, trust in system reliability, and trust in the internet. The study finds that users' intention to adopt the online accounting system is higher when users' trust in system reliability and trust in the internet are higher. The results of the study suggest that the reliability of a system, as measured by SysTrust criteria, is relevant to the decisions related to the intention to adopt online accounting systems.

After reviewing the previous studies, in this specific area of research, relating to reliability and security of the evaluation of CAIS control systems, it can be observed that there are not enough studies available, and this could be due to the fact that this area of research is reasonably new. In addition, many of the studies in this subject are administered on a small level and connected with combined studies from the fields of business management, computer science, and at times engineering. They are often in the form of reports or descriptive studies, and rarely experimental. To summarise, there is a lack of academic

literature on the issues of trust services. As there is a lack of research on the assessing of the reliability and security of AIS process and its influence on the quality of financial reporting as well as business performance, it would be a prospective area for research. The above discussion of the literature on trust services could be summarized in several important points:

- Limited research on user demand for trust services is set in the framework of web seals.
- Research is required in the specific context of systems assurance.
- Most research is required on user issues in trust services (e.g., demand for these services, and their effect on decisions) employs behavioural experiments, and uses archival research and field studies to supplement behavioural and survey studies of user demand and the effects of systems assurance services on users' decisions.
- Existing research tends to consider either user expectations about trust services or the effect of these services on management decisions.

2.2.5 Quality of Financial Reporting

2.2.5.1 Definition and Importance

Kieso, et al (2015, 25) defines financial reporting as the process of presenting business financial statements in the form of financial report for both internal and external parties related to the company. Merriam-Webster in Lam and Lau (2009) proposes the same concept by adding that it also includes initially recording and rating all business activities, especially financial transactions, then comes the reporting phase of these activities in order to present them for the related parties. Elliot and Elliot (2011) implies that financial reporting relates to the process of providing the current situation of business financial status represented by financial information to the related parties, such as (internal and external parties) from onside and to the current and potential investors from the other side, who can depend on this information to asses' business performance, and, then, make appropriate decisions. The main objective of financial reporting is to provide information concerning economic entity, primarily financial in nature, useful for economic decision making (IASB, 2008; Cao, Myers and Omer, 2012). Financial reporting provides information about the management's stewardship; the entity's assets, liabilities, equity, income and expenses (including gains and losses), contributions by and distributions to owners as well as cash flows (Van Beest, *et al.*, 2009). This information is usually in the form of annual financial statements such as the statement of financial position; the income statement or statement of comprehensive income; statement of cash flows and statement of changes in equity as well as notes to the accounts (IASB, 2008, 2010). To enhance reliability and confidence in the minds of the users, these

reports are subjected to scrutiny by external auditors. However, the spate of financial scandals in recent times has casted serious doubt on the quality of audited financial reports circulating in our corporate environment.

Thus, the concept of quality financial reporting has commanded considerable research interest around the world. However, researchers, practitioners or regulators are in disagreement as to a clear definition of what constitutes 'quality financial reporting' (Pomeroy and Thomson, 2008; cited in Miettinen, 2008). SOX (2002), for instance, require audit committees and auditors to discuss the quality of the financial reporting methods of the company, and not just their acceptability. But the Act did not define what constitutes 'quality' in financial reporting. The IASB (2008) has however provided a working definition of quality financial reporting. The Board in its conceptual framework defines quality financial reporting as that which meets the objectives and the qualitative characteristics of financial reporting (IASB, 2008; Van Beest, et. al., 2009). Meanwhile, Kieso, et. al. (2015) stress that in order to have quality financial report, the information should be relevant, by having the ability to make different decisions, valid through producing a predictive value, which is the input for investors in predicting future conditions, and have a value of confirmation, which helps the user to confirm or correct information of previous expectations. Honest presentation or faithful representation of information is also considered to be an important variable for ensuring quality financial report, which means the complete presentation of all necessary information. The next requirement is neutrality, which means that the information presented by the company not only caters to certain parties over the interests of other parties. The last condition is presented in an honest accounting, which means that information is error free

Evidence from previous literature ensure that the judgment of the quality of financial report is not easy and a complex activity, because it is connected with the perceptions and decisions of individual users. Therefore, various types of measurement methods have been developed to assess and evaluate the quality of financial reporting (e.g., Clor-ProellProell, and Warfield 2014; Müller, Riedl, and Sellhorn, 2015). However, most of researchers depend on quantitative measures and indicators, such as earnings quality and value relevance proxies, for assessing information quality, because these measures focus on specific attributes of financial reporting information Barth, Jagolinzer and Riedl (2010), Ogneva (2010), and Ahmed, Neel, and Wang (2013). They prefer this method because it concentrates on the decision usefulness of the information given in financial report, and the quality metrics used at this method are generally more reliable than other methods. Other researchers; such as Jonas and Tasios and Bekiaris (2012), Yurisandi and Puspitasari (2015), Mbodo and Ekp

(2016), P̄aşcan and Ţurcaş (2016) also stress on the importance of qualitative characteristics for assessing information quality provided by financial reports, as well as the recommendations of CF (IASB, 2010). In addition to the evidence from other researches, which discovered that, qualitative characteristics can indeed be operationalised.

Developing high-quality accounting standards has been investigated commonly and internationally by many works and researches. One of these issues, presented in May 2008 by FASB and the IASB, involves an exposure draft called "An improved Conceptual Framework for Financial Reporting"[ED] (IASB, 2010; FASB, 2008a). This implies that the company should give more importance and focus on qualitative characteristics objectives, beside the accounting principles in order to enhance the effectiveness and the quality of financial reporting process, which is also appropriate for decision makers, and leads to accurate, useful and constitute decisions (FASB, 1999; IASB, 2008). According to Mbodo and Ekp (2016) "Qualitative Characteristics Model" for measuring is the most recent model for assessing the quality of financial reporting. This model examines the level of decision usefulness of financial reporting information by operationalizing the qualitative characteristics of financial reports. Jonas and Blanchet (2000) pioneered the use of this model in assessing the quality of financial reporting. They develop questions that were germane to the separate qualitative characteristics of financial reporting as stipulated by the FASB (1980) and IASB (1989). The model was adopted many by researchers (Gaynor, et. al., 2016 and Mbobo and Ekpo, 2016). The major advantage of this model is that it provides a direct measure of financial reporting quality and covers all aspects of financial reports, including both financial and non-financial information.

Table 2.4 Qualitative Characteristics of the Quality of Financial Reporting

Characteristics of the QFR	Examples of Previous Studies
Relevance	FASB, (2013), Mamic, Sacar and Oluic (2013); Samukri (2015). Gaynor, et al., (2016) and Mbobo and Ekpo (2016).
Faithful Representation	FASB (2013,2018); Hu, Feng (2005); Sajady, et. al., (2008); Beest, et. al., (2009); Mamic Sacar and Oluic (2013). Mbobo and Ekpo (2016)
Understandability	Beest , et al., (2009; Samukri, (2015), Gaynor, et al., (2016); Mbobo and Ekpo (2016).
Comparability	FASB (2013); Mamic Sacar and Oluic (2013); Samukri, (2015); Gaynor, et al., (2016) and Mbobo and Ekpo (2016).
Timeliness	Beest, et. al., (2009). Nobes - (2014) Mbobo and Ekpo (2016)

*Source: Developed by the Researcher

2.2.5.2 Literature Review on the Quality of Financial Reporting.

Previous literature emphasizes that the accurate and qualified financial report is considered to be an effective tool for conducting financial analysis, feasibility analysis, and interpretation. For example, Mbodo and Ekp, (2016) clarifies that the good financial report stresses on financial elements and exchanged relations among them, so that the user can easily conduct comparisons among them and then make appropriate decisions. It also highlights at the company past and current financial performance, so that the user can make predictions about the needed future financial performance of the company. Many studies have been conducted to study and examine the extent of financial reporting quality, its dimensions, and the effecting variables (e.g.; Tasios, and Bekiaris, 2012; P̃aşcan and Țurcaș, 2016; Mbodo and Ekp, 2016).

The fundamental principal of any financial report relies on its understandability, relevance, reliability and comparability. However, there are two main qualities that should characterize information provided by financial report in order to rely and get benefit of them from user's relevance and reliability. Relevance relates to the value and difference added from the financial decision depending on this information. It is also connected to the speediness of this decision, and it is affected by its predictive value, confirmatory value, materiality and timeliness, while reliability refers to accounting information neutrality, faithfulness, representational, and verifiability, and being free of bias and error. Other secondary qualities that should characterize information provided by financial report are comparability and consistency, where comparability refers to measuring and reporting accounting information for different companies and organizations in a similar way, and consistency refers to applying the same accounting tools and treatments for similar events and operations from period to period (Mbodo and Ekp, 2016; Tasios and Bekiaris, 2012).

The research literature explained the benefits of IFRS adoption, related to the increase comparability and transparency of financial reporting (Haverals, 2007; Mbodo and Ekp, 2016), the decrease of information asymmetry (Djatej et al., 2009) or to the improvement of the functioning of capital markets (Schleicher, et. al., 2010) and to the decrease of the variation financial reporting regulations between countries, reduction of the cost of multinational company financial reporting and reduction on the cost of financial reporting analysis (Yurisandi and Puspitasari, 2015). On the other hand, the limits of IFRS adoption are also revealed in the research literature. Many researchers suggest that IFRSs are too complex,

costly and burdensome (Guerreiro, et. al., 2008; Callao, et. al., 2007); or that IFRS have affected negatively the relevance of financial reporting (Callao et al., 2010; Hung and Subramanyam, 2007; Knechel and Vanstraelen; 2015; Barth, et. al., 2008). Over this discussion, it was concluded that because of lack of direct measurement over the quality of financial reporting, the results were conflicting and misleading (Yurisandi and Puspitasari, 2015). Furthermore, some researchers have concluded that factors unique to a certain country, such as the economy, politics, laws, regulations and culture, may influence the adoption and implementation of IFRS in that country, with effects on the comparability between countries (Yurisandi and Puspitasari, 2015; Holm, et. al., 2009).

Hall (2011), Ewert and Wagenhoff (2013), Yurisandi and Puspitasari (2015) performed the financial reporting quality study by measuring the quality using the following characteristics: Relevancy, timeliness, accuracy, completeness and summarizing. Petreski (2006) found that management could improve the company business performance, could have higher accountability and could enhance the financial reporting creditability. Ewert and Wagenhoff (2013) revealed that more unbending accounting standard could increase the quality of financial reporting. Besides, Azhar Susanto (2004) mentions that in order to have qualified information for financial reporting, the information provided should be accurate, through reflecting the actual situation for the event. Then, it should be timely provided and available or existing on when the information is required. Other important characteristics are relevancy in accordance with the required action, and completeness of the information without any shortage, which affects the quality of financial report. As indicated by Xu, et. al., (2009), inaccurate and incomplete data may harm competitiveness of firms. They also found out that that input control and competent employees are important to data quality of accounting information system.

In summary, it can be concluded that the quality of financial reports depends on the ability of this report in providing appropriate, relevant, reliable and accurate financial information system that can meet and fulfil users' needs. Other research stresses on the other side of financial reporting process, which is the data used for preparing and presenting the financial statements. IASB and FASB (2010), in this regard, imply that qualitative characteristics should also take into account qualitative characteristics of the financial information. This means the quality attributes that financial information should have. They contribute in making financial information useful and accurate. Some of the fundamental and important

qualitative characteristics are comparability, verifiability, timeliness, relevancy, faithful representation and understandability. Qualitative characteristics are “the attributes that make the financial information useful and are distinguished as fundamental or enhancing depending on the way they affect the usefulness of the information” (IASB, 2008). International Accounting Standards Board (IASB) stresses that the usefulness of financial information is enhanced if it is comparable, verifiable, timely and understandable. FASB (2008) has issued “Qualitative Characteristics of Accounting Information” in 1980 and amended in 2008. In the pronouncement, besides relevancy, faithful representation, comparability, verifiability, timeliness and understandability, consistency is highlighted as important qualitative characteristics of accounting information. When compared with Wang and Strong’s IQ attributes, IASB and FASB’s reports share most of the attributes in common.

2.2.5.3 Reliability of Internal Control of AIS, Business Performance Studies and Quality of Financial Reporting

Explaining variation in firm performance is the central focus of much of the business literature. A large part of literature and previous studies try to examine quality of financial reporting and its effects on the subsequent performance of a company. For example, Garcia-Lara, et. al. (2010), Ahmed and Duellmand (2011), in their study found that there was a positive effect for the quality of financial reporting on the overall higher performance of the company. Due to the fact that quality of financial report guarantees and enforces the company to present good and accurate information, which in turn reduces the mystery and the conflict in information provided for both shareholders and stakeholders and other market participants interested in this report. The integrity and reliability of data produced by organizational information systems are critical, not just for the production of reliable financial reports, but also for overall business success (Krishnan, et. al., 2005).

Other benefits of having high-quality information from financial reporting are mentioned in Lambert, et. al., (2007). He clarifies that the high-quality information guarantees the reduction of information risk and liquidity. Other opinions are mentioned in Chen, et. al. (2011). It reduces the managers authority and power in making decisions for their own interests and guides them to make appropriate and efficient investment decisions. Rajgopal and Venkatachalam (2011) add that the high-quality financial reporting reduces the lack of equivalence and the asymmetric information that arises from conflicting agency. It also helps market agents to get full understanding about all company operations and activities by

reducing the ambiguity that surround some events (Jo and Kim, 2007). Lambert, et. al. (2007) mention that quality of accounting information has critical effects on market participants' perceptions about the distribution and decisions related to the company future cash flow. On the other hand, Chen, et. al. (2011) find both banks and government can get benefits of having the high- quality financial reporting, because it has a positive effect on private firm's investment efficiency and financial performance, which in turn increases tax payment and lending from banks. Visser and Erasmus (2008) put it that an ICS contains certain control activities, including policies and procedures with regard to approval, authorisation, verification, reconciliation, review of operational activities, safeguarding of assets, and segregation of duties. Muraleetharan (2013) in his study on control activities and performance of organisations established a positive relationship between control activities and performance. However, Ejoh and Ejom (2014) in their study revealed that there is no significant relationship between internal control activities and financial performance.

Toposh (2014) suggested that other qualitative characteristics of accounting information can likewise be kept up if there is sound internal control framework in an organization. Internal controls are methods set up to secure assets, guarantee reliable accounting reports, urge efficiency and encourage adherence to organization policies. Internal controls are fundamental to accomplish a few objectives like proficient and efficient direct of accounting exchanges, protecting the assets in adherence to management policy, prevention of error and detection of error, prevention of fraud, avoidance of misrepresentation and location of extortion and guaranteeing exactness, fulfilment, and detection of fraud and ensuring accuracy, completeness, reliability and timely preparation of accounting data. If good internal control exists in any organization, management can use information with greater reliance to maintain their business activities properly which provide AIS. But if internal control is not strong, management cannot achieve its goal. The study by Topash (2014) likewise found that the accompanying criteria or indicators should be available in any accounting information system for it to be productive in any organization which is, cost effectiveness, great documentation, presence of legitimate safety efforts, free inward and outside review, separation of other operation from accounting, and effective internal control. In smellier vain, Daneila (2013), state that accounting information systems and internal controls have a positive relationship to the financial reporting to produce reliable financial statements. Furthermore, Ricchiute (2006) indicated that internal control weaknesses in overseeing the accounting information system will affect the likelihood that a material error in reporting.

Internal control is needed to oversee the accounting system that can produce reliable financial statements (Konrath, 2002) AIS and internal control an integral part in generating quality financial reports that can be used as a foundation for management decision making and the parties concerned. Research conducted by Costello and Wittenberg (2011), revealed that if the company's internal control AIS is not reliable then the investors will not use the financial statements generated by the company in its decision making. Also, Kim, et. al. (2011) claim that internal control weakness which lead to lower internal control quality will increase the cost of financing in bank loans. Li, (2017), states that the higher internal control quality can reduce the cost of finance, detect and prevent fraud and errors, safeguard assets, encourage employees to follow policy, comply with legal regulation and other benefits for the firms (Li, 2017).

2.3 The limitations of the Previous Studies. Research gaps

There are many studies which emphasize the necessity and importance of internal control system for accounting system. An inadequate internal control accounting system often causes an inability to detect fraudulent activities and a decrease in the performance of business (e.g., Amudo, et. al. 2009; Daneila, 2013). Accounting information system implementation and success have been comprehensively researched but the contemporary literature shows slight evidences of the relationship between the quality of accounting information system (AIS) and business performance measures (Hla and Teru, 2015). As shown by a review of previous studies, the assessment of the reliability of accounting information system remains under-researched as the majority of such studies have focused on the status of AIS use and its applications (e.g., Iceman and Hilson, 2012; Choe, 2015). Specifically, the effect of reliability of AIS process on the quality of financial reporting has not been before examined empirically in a systematic way. Studies on SysTrust service engagement as an internal control method for assuring the reliability of AIS in the professional accounting literature are primarily devoted to explaining the background and purpose of this service and its potential demand (e.g., Boritz, et. al., 1999, 2000; Pugliese and Halse, 2000). Thus, it is still an open question whether reliability of internal control of accounting information system leads to systematic improvements in financial reporting quality and business performance as well.

The proposed interaction among the main components of SysTrust's framework (i.e., availability, security, processing integrity, confidentiality and privacy), which were not ever examined statistically before, can be either potentiating or mitigating, and the relative weight

of each component may change according to the environment circumstances characterizing the accounting internal control system and its regulations. Previous studies did not give any empirical evidence whether the interaction of these five components could enhance the quality of financial reporting or business performance (i.e., none of previous studies have articulated the differences or the strength and the direction of relationship of assessing the level of reliability of internal control in AIS, the level of quality of financial reporting and business performance). This means that an integrated approach (model) to examine these components (five principles) with other dependent variables; either taken separately or together, is needed. Previous researchers have tried to examine the relationship between the adoption of accounting information systems and business performance (e.g., Karruddin, et al., 2010; Grande, et al., 2011; Choe, 2015). While these studies contribute rigorously to the accounting literature, they do not use models from the IS literature to explain if there is a systematic relationship between the reliability of AIS and business performance.

Given that most studies of AIS have been based on cases in Europe and the US, cultural and legislation challenges, although complex, show some consistency. However, relatively few studies have been investigated outside of the most developed countries, such as in Jordan, which is a beachhead for new technologies and business practices in the Middle East and North Africa (MENA). Several authors state that within organizations, there must be attention given to the accounting standards and laws of each country, because they affect accounting management functions (Davila and Foster, 2007; Romney and Steinbart, 2017). This study, therefore, has come to bridge this gap by assessing the reliability of internal control in AIS based on the implementation of SysTrust principles (either taken separately or together) and their influence on the quality of financial reporting and business performance through an integrated approach. Also, this study aims to overcome the above limitations of the previous studies and to improve the understandings of the importance of the reliability AIS process in the environmental context of Jordanian organizational culture as a developing country.

2.4 Summary

In this Chapter, a brief review of accounting information system, its definitions, and importance are presented. Also, a review of internal control frameworks. COSO and COBIT Frameworks; Web trust and SysTrust, were presented and discussed as a basis of theoretical background for the purpose of the study. A discussion of empirical studies on SysTrust framework, the quality of financial reporting and business performance was given. The chapter has ended up with a section about the limitations of the previous studies.

Chapter Three is dedicated to the presentation and discussion the main purposes of the preliminary interview, its structure and results are presented. Furthermore, some background information about the type of internal control system and statutory framework for accounting and auditing in Jordan.

CHAPTER THREE

THE PRELIMINARY INTERVIEWS AND ACCOUNTING INTERNAL CONTROL SYSTEM IN JORDAN

3.1 Introduction

In this chapter, the main purposes of the preliminary interview, its structure and results are presented. Furthermore, some background information about the type of internal control system and statutory framework for accounting and auditing in Jordan. The researcher has conducted several interviews with relevant persons in auditing accounting licensed offices, as well as with a number of initial respondents of shareholdings companies. The purpose of these interviews is to get more insight about current situation of internal accounting system, in particular, Jordan's statutory framework for accounting and auditing, and to formulate specific hypotheses that were relevant to the reliability of AIS.

3.2 Objectives of the Preliminary Interviews

The objectives of the preliminary interviews are.

1. To get more insight into the study problem under investigation,
2. To formulate specific hypotheses in respect of the objectives of the study,
3. To shed light into the accounting internal control situation in Jordan from the point view of the internal and external auditors.
4. To be able to prepare and design an appropriate questionnaire that will handle the study's main questions.

This approach was viewed as the most appropriate way to obtain the in-depth views and experiences of knowledgeable individuals who are intricately involved in the evaluation and testing of internal control systems in accounting process.

3.3 The Structure of the Preliminary Interviews

The preliminary interviews consisted of free discussion with the financial/accounting managers and external auditors of large business organizations in Jordan. The general form of these interviews free open structured interviews. No statistical analysis was attempted at this stage of the present study. The selection of these companies was mainly based on. (1) Issue awareness: The companies had to have focus on the quality of financial reporting and internal controls. (2) Size: The companies had to be of a size sufficient for internal controls system to be formalised processes (five large sized shareholding companies). The list of questions is summarised in Table 3.1.

Table 3.1 List of the Interview Questions

List of Questions
1. What are the most important new developments in the field of internal control systems on accounting information systems in Jordan
2. What criteria does your company use to assess the reliability of internal control system?
3. Which type of the internal control systems for AIS is implemented at your company? Why?
4. How can you be sure a company of reliability of accounting information system?
5. Who is responsible for checking the requirements for reliable company accounting system?
6. Is there professional electronic audit legislation on accounting information systems in Jordan?
7. What principles of reliability requirements that you think are most important in accounting information system? Why?
8. Does your company organize any training sessions for verifying the reliability of accounting information systems?
9. Do external auditors possess the ability to evaluate the reliability of AIS in accordance with the principles set out in the Canadian joint US project (protection, system availability, processing integrity, online privacy, and confidentiality)?

*Source. Developed by the Researcher

3.4 Planning for the Preliminary Interviews

The in-depth interviews were conducted in two stages. At the first stage, a convenience sample of five of financial managers/accounting in public shareholding companies were contacted by telephone and their cooperation were sought*. The prior arrangements for the meeting were well scheduled in terms of the name of the persons to be interviewed. At the second stage, a convenience sample of six of external auditors of licensed offices were telephoned and their cooperation was sought. The interviews were held separately at the organization's premises. The main objectives of each stage are given in Table 3.2.

3.5 Data Gathered Through the Preliminary Interviews

The data collected through the preliminary interviews are presented under the following headings.

1. The statutory framework for accounting and auditing in Jordan
2. Audit profession development in Jordan
3. Internal control system assessment
4. The results of the initial interviews

Table 3.2 The Objectives of Each Stage of the Preliminary Interviews

Stages of Interview	Objectives
<p>Stage 1. Six financial managers in shareholdings companies were interviewed</p>	<p>(1) To get more specific information about the types of control system in accounting information system implemented in Jordan.</p> <p>(2) To acquire more information about how companies, evaluate the reliability of accounting information system.</p> <p>(3) To get their point view about the principles of SysTrust requirements in AIS.</p>
<p>Stage 2. Conduct Free discussion with six external auditors.</p>	<p>(1)To get their point view in respects of the regulations or technological applications of electronic audit and control of accounting system in Jordan</p> <p>(2)To find out if the auditors possess the ability to evaluate the reliability of AIS in accordance with SysTrust requirements (protection, system availability, processing integrity, online privacy, and confidentiality).</p>

**Taking into consideration the confidentiality of details with regard to the interviewees (i.e., names, position, companies, etc.) cannot be enclosed in the thesis, the researcher possesses documents in this respect.*

3.5.1 Jordan's Statutory Framework for Accounting and Auditing

According to the participants' opinions, the Companies Law 22/1997 in Jordan requires public shareholding companies, general partnerships, limited partnerships, limited liability companies, private shareholding companies, and foreign companies operating in Jordan to prepare annual audited financial statements. All companies registered under the Companies Law should maintain sound accounting records and present annual audited financial statements in accordance with “internationally recognised accounting and auditing principles.” Auditors are elected for one year with the possibility of renewal. An auditor’s performance is evaluated by company shareholders, who at their annual general meeting decide whether to appoint a new auditor or renew the appointment of the existing auditor.

The Companies Law also requires the auditor's report to address the following at the annual general meeting.

- All data and explanations for satisfactory fulfilment of duties have been obtained.
- The company maintains satisfactory accounting records and documents.
- The company's financial statements (balance sheet, income statement, and statement of cash flows) are prepared in accordance with internationally recognised accounting and auditing principles.
- Audit procedures have been sufficiently followed.
- Financial statements, which are included in the Board of Director's report addressed to the General Assembly, comply with the company's records.
- All relevant legal requirements have been reflected in the accounts.

They also indicated that the Jordanian Securities Commission (JSC) Law (23/1997) and Directives of disclosures, auditing, and accounting standards (1/1998), all entities subject to JSC's supervision are required to apply International Financial Reporting Standards (IFRS). However, the explanation included in the directives states that if there is a conflict between international standards and local legislation, the latter shall supersede. The entity should then disclose this decision along with its impact on the financial statements (balance sheet, income statement, statement of cash flows, changes in shareholders' equity, and notes to financial statements). The JSC requires all listed companies to file annual audited financial statements (within 90 days from fiscal year-end) and mid-year reviewed financial statements (within 30 days from mid-year-end). The JSC Law also requires entities under its jurisdiction to form an audit committee of three nonexecutive members. The committee should meet at least four times a year to examine and discuss matters arising from work of external and/or internal auditors. The JSC Directives also require listed companies to publish their financial statements in Arabic in a widely circulated newspaper. This requirement could be counterproductive to users of financial information if only undetailed financial statement summaries are published (The World Bank's Report on the Observance of Standards and Codes (ROSC) – Accounting and Auditing for Jordan as of 10 June 2004).

3.5.2 Audit Profession Development in Jordan

The development of accounting profession in Jordan has played a considerable role in the development of audit profession. In fact, the audit profession is relatively new in Jordan. However, several legislations have worked together to organize the audit profession in Jordan. For example, Jordanian Companies Law No. 22 of 1997 and its amendments put much emphasis in its different articles on the audit profession in Jordan. For example, it organised the process of electing the licensed auditors and how to determine their fees. It also obligated companies to present the comparative annual financial statements accompanied with their clarifications, all certified by licensed auditors. Jordanian Companies Law No. 22 of 1997 and its amendments also asked companies to keep their accounts in accordance with the recognised international accounting and auditing standards. More important, the law determined in details the auditors' duties in monitoring, revising and auditing the operations of company and its internal control system in accordance with recognised auditing rules, auditing profession principals and scientific and technical standards. The Interim Income Tax Law No. 28 of 2009 and the Interim General Sales Tax Law No. 29 of 2009 have obligated the taxpayer to keep all the necessary books and records necessary to determine the tax liability amount. Tax laws accept only those statements that prepared in accordance with international accounting standards and audited and certified by a licensed auditor.

3.5.3 Practicing Auditing Development in Jordan

In 2003, a new auditing law was issued in Jordan - the "Law of Organizing the Practice of the Public Accounting Profession. Law No. 73 (2003)". This law addresses a contemporary basis for practicing the public accounting profession in Jordan in such a way as to guarantee the reliability of the financial statements presented by companies and other institutions. In this regard Law No. 73 (2003) aims to achieve the following:

1. Organizing the practice of the auditing profession; ensuring compliance by Jordanian companies with International Accounting and Auditing Standards.
2. Developing the technical and educational abilities of Jordanian auditors.
3. Ensuring compliance of the auditors with the code of professional ethics to achieve the above, a high council for accounting and auditing was established. Consistent with the composition of the past committees, the composition of the auditing high council is dominated by governmental members, with only 25% being practitioner auditors. Law No. 73 (2003), requires that the applicants for entry into Jordan's public accounting profession complete a training period at a certified public accountant office, in addition to passing the audit examination prerequisite. It is reasonable to expect that this new

arrangement should enhance the quality of the auditing profession, ensure that public accountants are trained at a well-known office, and that they obtain the necessary practical skills to enter the profession. Applicants are required to hold one of the following qualifications in order to be entitled to sit for the audit professional examination. Bachelor's degree with a major in accounting; a Diploma in accounting; a related bachelor's degree, not in accounting, but with accounting courses meeting a minimum threshold; or a Professional Certificate from an acceptable professional body. To enhance the quality of the auditing profession under the new law, eligibility to sit the auditing examination is granted only to those holding an accounting degree or who have studied a specified minimum of accounting courses. It is expected that the holders of an accounting degree will be more efficient and appropriate auditors than others without that credential.

Concerning whether current accounting professionals maintain the competencies to perform continuous auditing in Jordan, preliminary indications are somewhat mixed. While some view that the present generation of accountants has the requisite skill set to sufficiently provide these services, others contend that the desired expertise is not available to perform such task. However, the competencies identified by interviewees' participants include the following.

- Knowledge of business processes, controls, and inherent risks
- Internal audit experience
- Familiarity with audit planning, audit processes, and forensic accounting
- An understanding of data extraction tools (IDEA, ACL)
- Data analytics background (regression, ANOVA, data mining, SQL, probabilities)
- Knowledge in statistics
- Technical skills (ERP, programming)
- Professional scepticism and judgment.

Some participants explained that to report on a continuous basis, an organization must have strong controls. Many of these controls exist within and around IT systems. The special skills and knowledge that IS auditors have been essential to the assessment of these controls and to the performance of these engagements. It should be noted that in order to perform a SysTrust engagement, practitioners should have a number of competencies, including information technology (IT)-related skills. The participants added that many practitioners in Jordan

already have most of the essential skills needed to conduct an effective evaluation of internal control. With modest additional training, practitioners can enhance these skills to enable those with internal control evaluation skills to provide valuable SysTrust services to their clients.

When explicitly asked what types of financial auditors reporting, interviewees reported and agreed that there are two types of service auditor reports. A **Type I** service auditor's report includes the service auditor's opinion on the fairness of the presentation of the service organization's description of controls that had been placed in operation and the suitability of the design of the controls to achieve the specified control objectives. A **Type II** service auditor's report includes the information contained in a Type I service auditor's report and includes the service auditor's opinion on whether the specific controls were operating effectively during the period under review. The preliminary indications also show that the auditors companies in Jordan to some extent are familiar with the AICPA (SOC 2 and 3) reporting frameworks, both of which are based on the Trust Services Principles, to allow for reports focused on areas other than financial controls. Specifically, SOC 2 and 3 reports concentrate on the controls that are related to the security, availability and processing integrity of an organization's system; the confidentiality of the information that an organization's system processes or maintains for user entities; and the privacy of personal information that the organization collects, uses, retains, discloses and disposes of for user organizations.

All the participants in the interview have agreed that there are some obstacles that may prevent of business to perform the process of continues auditing according to the AICPA requirements. The most important of these obstacles could be. 1. The high cost of auditing this type of service and 2. Inadequate legislation to govern professional electronic auditing. However, it should be noted that a company isn't required to address all these principles, the reviews can be limited only to the principles that are relevant to the outsourced service being performed. The auditors can report on all five SysTrust principles or each principle separately. Because the SysTrust principles and criteria are established and available to any user, the auditor's report does not have to be restricted to specific parties. The service auditor renders an opinion on whether the controls were suitably designed, placed in operation, and operating effectively. The SAS 70 service auditor's report includes the independent auditor's opinion, a description of the service organization's controls, and the results of the service auditor's procedures (in the case of a Type II audit). Concerning the practicing of auditing of

the reliability of internal control system of accounting information, the auditors in Jordan usually use their professional judgment based upon the requirements of business. In fact, there are many frameworks have been developed for this purpose. According to the participants' experiences, the SysTrust model is the most recommended one by Jordanian Association of Certified Public Accountants (JACPA) because of its compliance with laws and regulations. The judgment on the reliability is based on five key components. (1) Infrastructure facilities, equipment and networks, (2) Software (systems, applications and utilities, (3) People developers, operators, users and managers, (4) Procedures (automated and manual and (5) Data (transaction streams, files, databases and tables. Also, a reliable information system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. When an information system meets the five principles security, availability, processing integrity, confidentiality, and privacy

3.5.4 Financial Reporting by Public Companies in Jordan

The participants further explained that the financial reporting in Jordan is regulated through the commercial laws. The Companies Law regulates all types of companies; the Banking Law regulates the banks, while the Insurance Law regulates the insurance companies. In the same context, the Securities Law regulates all companies regarding listing and trading matters in the financial markets.

1. Financial Reporting in the Companies Law No. 22 (1997). According to the Companies Law No. 22 (1997), Jordanian companies are divided into General Partnership, Limited Partnership, Limited Liability Company, Limited Partnership in Shares, Public Shareholding Company. The securities of public shareholding companies can be listed and traded in the capital market and their minimum paid-in capital is 500,000 Jordanian Dinars (JD). According to the Companies Law No. 22 (1997), public shareholding companies are obligated to appoint an auditor. Duties are assigned to the Jordanian auditor according to the Companies Law - the major responsibility being to audit companies' accounts in accordance with the recognised auditing rules, the auditing profession's principles and its scientific and technical standards. Moreover, an auditor is to review the financial and administrative by-laws of the company and its internal financial controls, to ensure their suitability for the company's business and the safeguarding of its assets. Accordingly, auditors in Jordan are responsible for assessment

of companies' internal controls, in addition to undertaking the appropriate substantive tests. In accordance with Companies Law No. 22 (1997), all public shareholding companies are required to prepare and issue their annual audited financial statements - their balance sheets, income statements, and cash flows statements - within three months from the end of the company's fiscal year. Further, each public company is to prepare and issue its semi-annual financial statements, certified by the company auditors within 60 days from the end of the half-year period.

2. Financial Reporting in the Securities Law No. 76 (2002). The Securities Law in Jordan (No. 76/2002) also requires all public shareholding companies to prepare and issue their annual audited financial statements, within a period not exceeding three months from the end of its fiscal year. Semi-annual financial statements with comparisons to the same period of the preceding fiscal year are to be prepared within a period not exceeding one month from the end of the half-year period. Moreover, each company shall declare their primary results upon a primary revision by its auditor, within no more than 45 days from the end of its fiscal year. In addition to the above, the Directives for listing securities on the Amman Stock Exchange, issued by virtue of the provision of article (72) of the Securities Law No. 76 (2002), require the listed companies on the first market (one of the stock exchange markets governed by strict conditions) to issue quarterly reviewed financial statements, within one month of the end of the relevant quarter. All the financial statements shall be prepared consistently with the IFRSs, and the ISAs shall be adopted in auditing them.
3. Financial Reporting in the Banks Law No. 28 (2000). The Central Bank of Jordan (CBJ) is considered the main surveillance authority, besides the Ministry of Industry and Trade and the Jordanian Securities Commission, scrutinizing and regulating the banks. The CBJ has issued laws and regulations, the most important of which is the Banks Law No. 28 (2000). According to the Banks Law, the auditors' main duties are. (i) To assist the bank to maintain correct records and accounts, (ii) To review and scrutinize the adequacy of the internal auditing and the internal control procedures and provide recommendations thereon, (iii) To submit an annual report on the results of auditing the accounts of the bank showing its actual financial position, and attaching to the report an opinion on such accounts, and (iv) To furnish the Central Bank with a certificate stating an audit opinion on the adequacy of the bank's doubtful debt provisions and any deficit in the provisions

required for the bank's assets, pursuant to the orders issued by the Central Bank for the purpose.

4. Financial Reporting in the Insurance Regulatory Law No. 33 (1999). The Jordanian Insurance Commission (JIC) was established in 1999 to regulate and scrutinize insurance companies' operations, in addition to the inspections undertaken by the Ministry of Industry and Trade and the Jordanian Securities Commission. The JIC issued Insurance Regulatory Law No. 33 (1999) regulating the financial reporting and the implementation of IFRS and ISAs in the insurance sector. In compliance with Insurance Regulatory Law No. 33 (1999), all insurance companies in Jordan are to prepare and issue annual audited financial statements compliant with the IFRSs within two months of the end of the fiscal year, and reviewed semi-annual financial statements within one month of the end of the half-year. Furthermore, on a quarterly basis insurance companies are required to submit the financial reports and statements forms for supervisory purposes to the Insurance Commission within one month from the end of the related quarter, except for the fourth quarter, when it is to be within two months from the end of that quarter. These reports are to be certified by the company auditor indicating their consistency with the records of the company.

3.5.5 Financial Reporting in Jordan and its Effect on the Accounting and Auditing Profession

Based upon the participants' experience and knowledge, the importance of financial reporting in Jordan is indicated by the extent to which each of the commercial laws addresses different articles in relation to it. The public shareholding companies listed on the Amman Stock Exchange in Jordan are divided into four main sectors, the banking, insurance, services, and industrial sectors. The above discussion of the financial reporting requirements of the different laws clearly shows that the number of financial statements required from public shareholding companies in different commercial sectors is substantial, and has increased over time. Accordingly, Jordanian commercial laws have obliged public companies to present audited quarterly, semi-annual, annual financial statements, and other financial reports. Auditors are required to assess companies' internal control structures. The large number of mandatory financial statements to be prepared by the companies has caused a dramatic increase in the demand for accountants as well as for members of the auditing profession.

3.5.6 Internal Control System Assessment

As it was presented in the previous sections, according to the Company Law 1997, public companies in Jordan require to include in their annual reports an assessment by management of their internal controls over financial reporting. This includes a statement of management's responsibility for establishing and maintaining adequate internal control, an assessment of the effectiveness of those controls as of the end of the most recent fiscal year, a statement identifying the framework that was used to evaluate those controls and a statement that the external auditor issued an attestation report on management's internal control assessment. The rules imply companies must base its internal control evaluation on a suitable, recognised control framework established by a body or group that followed due-process procedures. The rules do not mandate the use of a particular framework but say a suitable one must. (1) Be free of bias, (2) Permit reasonably consistent and quantitative measurements, (3) Include all relevant factors that might alter a conclusion about the effectiveness of the internal control and (4) Be relevant to an evaluation of internal control over financial reporting. Because public companies rely today heavily on technology, the criteria they use to assess the effectiveness of their IT-related controls are particularly important. While COSO addresses the topic of IT general controls, it does not dictate requirements for control objectives and related activities. Indeed, the audit standards highlight the importance of IT general controls but do not specify which in particular a company must include. Thus, to meet the requirements of company law, IT management and auditors need a specific IT control framework

When participants are asked which framework (COSO, COBIT or SYSTRUST) is highly used by public companies in Jordan. They said COBIT is accepted in Jordan as good practice for control over IT and related risks because of its comprehensive approach for managing risk and control of IT and explaining how IT processes deliver the information a business needs to achieve its objectives. However, other interviewees said some of companies turn to use Trust Services because of its focus on the controls that are in place to ensure the company's systems carry out business processes reliably and because its principles define a reliable system as one capable of operating without material error, fault or failure during a specified period in a specified environment.

They also mentioned that the use of COSO as an internal control framework does not provide specific criteria for IT controls, this why many companies to turn to a supplemental framework such as the AICPA/CICA Trust Services framework to ensure that the systems a

company uses are reliable. However, some of the interviewee indicated that the cost of applying for such service is considered high and few companies might not have fully documenters their internal control procedures in line with SysTrust requirements. However, according to the participant's point view, there is no one de facto or generally accepted standard to assess and audit IT control system. The main reason behind that is that IT controls are dependent on the business type and supporting IT infrastructure. Each company has its own unique control system based on its IT assets, people, processes, and technology. Each framework has its strengths and weaknesses. Executives need to decide on what is the best framework for their company, or they might need a combination of frameworks in the course of assessing their IT control reliability and effectiveness. They indicate the SysTrust seal of assurance suggest that company's IT processes have adequate controls as per internationally accepted best security practices.

It should also be noted that for companies to conclude its system of internal control is reliable and effective, all principles of SysTrust must be present and functioning. Being present implies a given principle assists within design and implementation of the entity's system of internal control. Functioning implies the principle continues to exist in the operation and conduct of the control system. A reliable control system also requires that all five principles operate together in an integrated manner. When the participants are asked whether public companies have adequate and qualified persons to assess the reliability of internal control system according to the requirements of SysTrust principles, they claimed that the public companies have well-qualified staff in auditing and many of them possess CPA license to perform such service.

3.6 The Results of Initial Interview

In the previous sections, the information required and gathered by the interview method are presented and discussed. In this section, the main results of the initial interview can be summarised as follows.

1. All companies registered under the Companies Law should maintain sound accounting records and present annual audited financial statements in accordance with “internationally recognised accounting and auditing principles.”
2. Several legislations have worked together to organize the audit profession in Jordan. According to the Jordanian Securities Commission (JSC) Law (23/1997) and Directives of disclosures, auditing, and accounting standards (1/1998), all entities subject to JSC’s supervision are required to apply International Financial Reporting Standards (IFRS).

3. Accounting professionals maintain the competencies to perform continuous auditing in Jordan.
4. The preliminary indications show that the auditors companies in Jordan to some extent are familiar with the AICPA (SOC 2 and 3) reporting frameworks
5. All the participants in the interview have agreed that there are some obstacles that may prevent them to perform the process of continues auditing according to the AICPA requirements.
6. According to Company Law 1997, public companies in Jordan require to include in their annual reports an assessment by management of their internal controls over financial reporting.
7. The company Law in Jordan allows public companies to use any suitable available framework to its IT policies, but it should. (1) Be free of bias (2) permit reasonably consistent and quantitative measurements, and (3) include all relevant factors that might alter a conclusion about the effectiveness of the internal control and (4) Be relevant to an evaluation of internal control over financial reporting.
8. Many public companies in Jordan prefer to use the AICPA/CICA Trust Services framework to ensure that the systems a company uses are reliable rather than other framework such as COSO and COBIT
9. Public companies have adequate and qualified persons to assess the reliability of internal control system effectively in line with the principles of SysTrust.

3.7 Summary

The purpose of this chapter is twofold. (1) To present the main purpose of the preliminary in-depth interview and its structure, and (2) to present some background information about the type of internal control system and statutory framework for accounting and auditing in Jordan. The variables which were generated from the preliminary interview will be integrated in the conceptual framework of this study.

CHAPTER FOUR

THE STUDY'S CONCEPTUAL FRAMEWORK

This chapter discusses the conceptual framework for this study, its main constructs and the expected relationship among them as well as it presents the proposed hypotheses.

4.1 The Nature of the Conceptual Framework

In Chapter Two, theoretical background and empirical studies on the SysTrust's framework as an internal control for assuring the reliability of AIS as well as the relevant theoretical literature on business performance and the quality of financial reporting were reviewed and integrated to develop a conceptual framework to guide this study. The proposed framework has tied together the components of SysTrust's service framework (i.e., principles and criteria) which are postulated to assess the reliability of AIS process and its influence on the business performance. These major components are mainly derived from five principles of SysTrust's framework, availability, processing integrity, privacy, security and confidentiality.

According to the existing frameworks on IS and accounting management (Dehning and Richardson 2002; DeLone and McLean 2003; Gable, et. al., 2008), business performance as well as the quality of financial reporting could be as a function of the quality of internal control of accounting information system. In this issue, Contingency theory also has been used to describe the relationships between the context and structure of internal control effectiveness and business performance, especially quality of financial reporting (Cadez and Guilding, 2008; Islam and Hui, 2012). Contingency theory is usually applicable in the context of effectiveness achievement, for example, Nicolaou (2000) and Chenhall (2003, 2007) have used contingency theory to determine the effectiveness of accounting information system. Therefore, understanding the critical components of SysTrust framework as an internal control for assuring reliability of AIS process which influence the quality of financial reporting could assist organizations to improve their operational business performance. Inadequate financial reporting quality might cause a lot of business operations run inefficiently and less in accordance with the demands and needs of the stakeholders. Supposedly, in order to anticipate these conditions, businesses must have reliable system in generating quality information.

The integrated framework proposed is used here to investigate whether the business performance (i.e. financial and non-financial indicators) is a function of the implementation of SysTrust's framework as an internal control system of accounting (i.e., availability, security, processing integrity, confidentiality and privacy) through the mediating role of quality of financial reporting. The quality of financial reporting was conceptualised by the IASB's framework fundamental qualitative characteristics (relevance, faithful representation, comparability, understandability and timelines). The expected relationships among these constructs are illustrated in Figure 1 and further elaborated in the following sections. Some of the components of SysTrust framework are expected to be more important than others (either individually or together) in explaining the variation in the quality of financial reporting or the business performance.

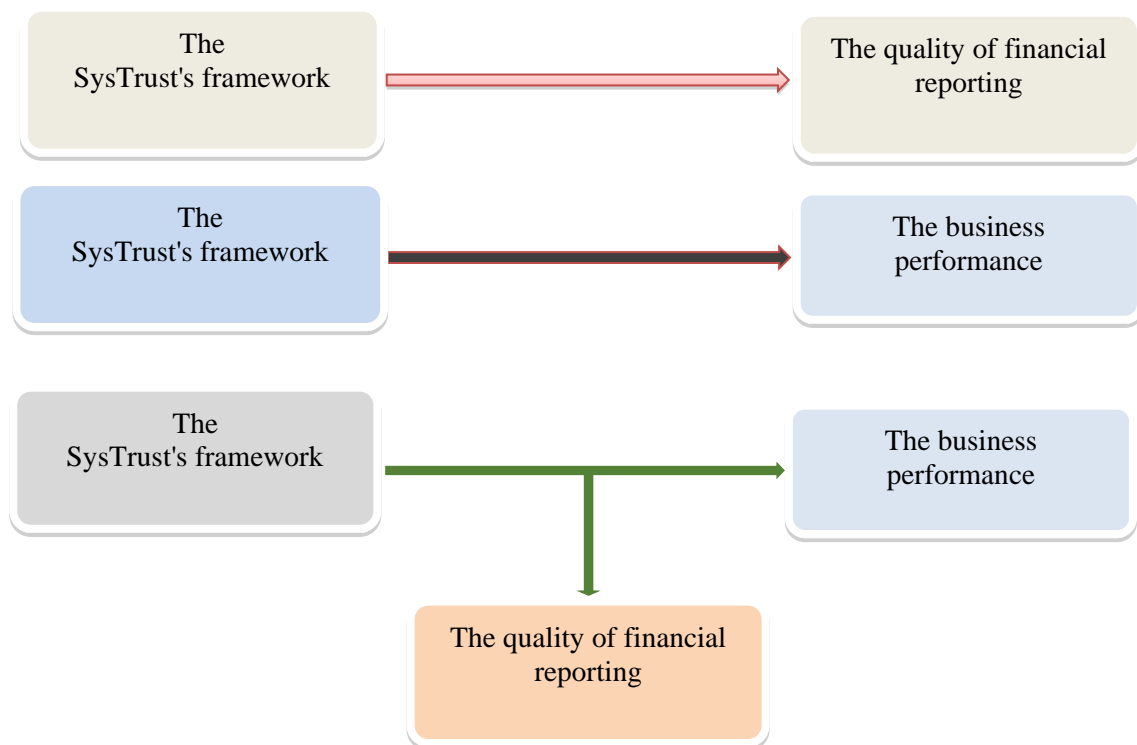


Figure 4.1 Study's Conceptual Framework

*Source: Developed by the Researcher

According to the AICPA, SysTrust is an assurance service that independently tests and verifies a system's reliability. It is assumed expect that any system that satisfies the SysTrust principles should be viewed as being more reliable and thus be trusted more than one that does not. In other words, trust in the system of specific provider is influenced by the extent to which the system meets the SysTrust principles. It is referred to as trust in system reliability in the present study.

It should be noted that some of these constructs may be more important than others on the influencing on the quality of financial reporting in comparing with business performance. On the other hand, some constructs may be important in both the quality of financial reporting and the business performance. The conceptual framework here suggests that the quality of financial reporting and business performance are thought to be here as a function of the level of reliability of the accounting information system. For example, the extent of the security of AIS as a one construct of the SysTrust model (i.e., it is assumed to have influence on the quality of financial reporting as well as business performance). This construct is expected to interact with other constructs of SysTrust model such as availability, integrity, privacy, and confidentiality which results in an overall assessment of the level of reliability of accounting information system. The classification of the components /constructs is illustrated in and further elaborated in the following sections.

4.2 Main Constructs of the Study's Conceptual Framework

The major constructs of the study's model are presented below with brief discussion of studies which were concerned with them. Furthermore, the expected relationship among these constructs are clearly defined and discussed throughout the presentation of each constructs.

The Quality of Financial Reporting and Business Performance

There are two indicators (mediation and dependent variables) used here separately to achieve the study's objectives: The quality of financial reporting and the financial business performance.

4.2.1 The Quality of Financial Reporting

In light of the requirement for improvement in the current financial reporting system, the International Accounting Standards Board (IASB) discharged a conceptual framework for financial reporting following the exposure drafts issued in 2008 and 2010. The key issues brought up in the framework are the objectives of financial reporting and the characteristics of quality financial reporting. It showed that a key essential for accomplishing quality financial reporting is the adherence to the objectives and the qualitative characteristics of financial reporting information. According to the framework, qualitative characteristics are the attributes that meet the decision usefulness of financial information. The framework listed these attributes as; relevance, faithful representation, comparability, understandability, verifiability and timeliness. It has been argued that the model which uses the qualitative characteristics approach in measuring quality financial reporting provides a direct and better measure of financial reporting quality (Tasios and Bekiaris 2012; Mbodo and Ekp, 2016). In spite of the obvious merits of this model, especially the fact that it aligns strongly with the

International Financial Reporting Standards (IFRS), many researchers in recent studies still prefer to use the indirect method, especially discretionally accrual (earnings management) as a proxy for financial reporting quality.

Table 4.1 The Characteristics of the Quality of Financial Reporting

Quality of Financial Reporting Characteristics	Influencing Variables	
1. Relevance	<ul style="list-style-type: none"> - The extent presence of the forward-looking statement helps forming expectations and predictions concerning the future of the company. - The extent of the presence of non-financial information in terms of business opportunities and risks complement the financial information. - The extent of company uses fair value instead of historical cost. - The extent of reported results provide feedback to users of the annual report as to how various market events and significant transactions affected the company 	<p>Cole et al., (2007); FASB, (2013); Sajady et al., (2008) Beest , et al., (2009), Mamic Sacar & Oluic (2013); Samukri, (2015).</p>
2. Faithful Representation.	<ul style="list-style-type: none"> - The extent of valid argument provided to support the decision for certain assumptions and estimates in the annual report. - The extent of the company bases its choice for certain accounting principles on valid arguments. - discussion of the annual result, highlight the positive events as well as the negative events. - Type of auditor's report is included in the annual report. - The extent of the company provides information on corporate governance. 	<p>- Beuselinck and Manigart, (2007) ; FASB, 2013;; Beest , et al., (2009); Mamic Sacar & Oluic (2013)</p>
3. Understandability	<ul style="list-style-type: none"> - The extent of the annual report presented in a well-organised manner - The extent of notes is to the balance sheet and the income statement sufficiently clear. - The presence of graphs and tables clarifies the presented information. - The extent of the use of language and technical jargon in the annual report easy to follow. - The size of the glossary. 	<p>- Jonas & Blanchet, (2000); Maines and wahlen, (2004); Beest, et al., (2009), Samukri, (2015).</p>
4. Comparability	<p>The extent of notes to changes in accounting policies explains the implications of the change?</p> <p>The extent of notes to revisions in accounting estimates and judgments explain the implications of the revision.</p> <p>The extent of a company adjusts previous accounting period's figures, for the effect of the implementation of a change in accounting policy or revisions in accounting estimates.</p> <p>The extent of a company provides a comparison of the result of current accounting period with previous accounting periods.</p> <p>The extent of information in the annual report comparable to information provided by other organizations.</p>	<p>Willekens,(2008); Sajady et al., (2008) ; Beest , et al., (2009); FASB, (2013); Mamic Sacar & Oluic (2013); Samukri, (2015).</p>
5. Timeliness	<p>The amount of days between year-end and the signature on the auditors' report after year end is calculated.</p>	<p>Beest , et al., (2009); FASB, (2013);</p>

This, perhaps, is due to the difficulty in operationalising the qualitative characteristics (Van Beest, et. al., 2009). Indeed, studies which attempt to operationalize the qualitative characteristics in financial reporting are very few in Jordan. This study therefore contributes towards filling this gap. Based on these facts the current study will depend on the seven-point rating scales of qualitative characteristics mentioned on ED (IASB, 2008) to assess financial reporting quality. To assure the internal validity of these items, the quality measures are based on prior empirical literature (Tasios and Bekiaris 2012; Mbodo and Ekp, 2016) Table 4.1 provides an overview of the 26 measured items used to operationalize the fundamental and enhancing qualitative characteristic. These measures are employed here in order to facilitate the comparison between the findings of using it and the findings of previous works in this field, for example, prior studies (e.g. Van Beest, et. al., 2009; Tasios and Bekiaris, 2012) provide a model for operationalising the qualitative characteristics, based on the IASB conceptual framework.

1- Relevance

IASB (2008) defines relevance as the capability of making a difference in the decisions made by users in their capacity as capital providers. Relevance is usually operationalised in terms of predictive and confirmatory value (McDaniel, et. al., 2002; Van Beest, et. al. 2009). Predictive value generally refers to information on the firm's ability to generate future cash flows. Many previous literatures stressed on the importance of relevancy of information related to financial reporting, regard its role in making differences in user's decisions, it enhances their capabilities and innovations in making decisions (Tasios and Bekiaris 2012, Mbodo & Ekp, 2016 IASB, 2008). Nichols & Wahlen, (2004) define relevance as the level of earnings quality, predictive and confirmatory value of financial reporting, in this definition we note that the concentration is only made upon the past and current financial information, while neglecting the company non-financial information, and the future transactions. Predictive value has attained attention from many researchers, it refers according to (Francis, et. al., 2004 Schipper and Vincent, 2003) point of view the ability of past earnings to predict future earnings, (IASB, 2008. 36) in this regard stated that Predictive value is related to the ability of the company financial information to generate future cash flows, for example the economic phenomenon that surround the company, which the capital providers take into account for predicting the future operations and strategic expectations. Thus, in this study predictive value was considered as the most important indicator of information relevancy and decision usefulness, it was measured by using the following three items.

- The extent of providing forward-looking statements especially managers expectations for the company future at the company annual reports, (Bartov & Mohanram, 2004) stated that the information provided at the annual reports will be relevant when the company managers has an access to all information, besides their ability to evaluate and make forecasts to other stakeholders, capital providers and other users.
- The extent of the company disclosures in annual reports information in terms of business opportunities and risks. In this regard Jonas and Blanchet (2000) stated that business opportunities and risks help capital providers to have a clear vision about all company future scenarios, they also stressed that in order to have a predictive value of information, complementation must have made between both financial information and non-financial information.
- The extent of using fair value by the company, for many years' fair value versus historical cost have been used by many researchers in order to examine financial information predictive value. Many companies started considering new standards to allow more fair value accounting to increase the relevance of financial reporting information. For example, and in this regard, FASB and IASB are currently, stated that fair value is one of most important tools used to increase financial information relevance (Barth et al., 2001). Other researchers such as (Hirst, et. al., 2004; Schipper and Vincent, 2003; Schipper, 2003) prefer fair value upon historical cost because it represents the real current value of assets instead of purchase price.

2- Faithful Representation

Faithful representation is the second fundamental qualitative characteristic as elaborated in the ED, it means that all information listed in financial report must be represented faithfully, (IASB, 2006. 48) stated that in order to accomplish this all information and Economic Phenomena Listed in annual reports must be complete, accurate, neutral, and free from bias and errors. The reason why should take care of this is related to the fact that all of these phenomena and transactions are changeable among time, so the annual report must document every events and transaction carefully and accurately (IASB, 2006). Previous literature such as (Cohen, et. al., 2004; Maines and Wahlen, 2006; Gaeremynck and Willekens, 2003; Kim et al., 2007; Willekens, 2008) indicated that Faithful representation could be measured by using five main items which are completeness, freedom from material error, neutrality, verifiability, and finally relevance and predictive value which was presented by Jonas and Blanchet (2000). However, ED in its definition to verifiability characteristic and its role in enhancing qualitative characteristic, stated that it is one of the most important characteristics

that the financial information should have, in order to convince users of financial report that the information are faithfully represented, according to Maines and Wahlen (2006), all estimations and assumptions that closely correspond with the underlying economic phenomenon can enhance faithful representation. Meanwhile Botosan (2004) stated that measuring faithful representation directly is a complex and not easy process, especially when depending only on annual reports, which not take all current economic phenomenon into account, which is the most important things for guaranteeing faithful representation. This in turn indicate the importance of annual reports, which is also used as a tool to enhance the probability of information faithful representation, in addition to that US GAAP or IFRS, have stated that annual reports can also provide an indirect proxy of faithful representation of financial reporting information prepared in accordance with certain accounting standards. For example, the information provided in annual reports never derived completely free from bias because all economic phenomena are surrounded with uncertainty, for this (IASB, 2008) clarified that it is important to examine the opinions and point of views included and listed in the annual report (Jonas and Blanchet, 2000). If valid arguments are provided for the assumptions and estimates made, they are likely to represent the economic phenomena without bias.

Another important variable should be taken into account, providing a well-grounded and valid arguments for the accounting principles in order to fully understand the measurement method and minimize financial report errors and in objectivity, which in turn help in reaching for consensus and minimize misstatements for both capital providers and auditors (Jonas and Blanchet, 2000; Maines and Wahlen; 2006). Neutrality is another important character that guarantee information faithful representation, (IASB, 2008) in this regard define Neutrality as having financial information without any bias, and authority in particular opinion and behaviour. As Jonas and Blanchet (2000) state; “Neutrality is about objectivity and balance”. It refers to the intent of the preparer; the preparer should strive for an objective presentation of events rather than focusing solely on the positive events that occur without mentioning negative events

3- Understandability

Understandability is the third fundamental qualitative characteristic as elaborated in the ED, it referred to the process of classifying, characterizing, categorizing, then presenting the financial information clearly and concisely, for (IASB, 2008) Understandability provide the users and capital providers with the ability of comprehending their meaning, according to previous literature as mentioned in (Iu and Clowes, 2004; Courtis, 2005; IASB, 2006) It means assuring financial information transparency and clearness, this process needs relating to some financial measures. However, there are five major financial variables or items used internationally within different context, to measure information Understandability, the first one is the process of revising classification and characterization of financial information listed in annual report, here the most will organise the information in annual report, the most is the information searchable, and untestable (Jonas and Blanchet, 2000).

The second item is financial information disclosure, in this regard (Beretta and Bozzolan, 2004) states that in order to achieve that both balance sheet and income statement should explain in depth the earning figures from one side and providing narrative explanations that help in increasing the information understandability according to (IASB, 2006; Iu and Clowes, 2004). The third item for enhancing understandability of information as stated in (IASB, 2006) is the process of adding graphic formats or tabular, that explain some numbers at the annual reports, especially the exchanged relationships between some variables. Moreover, the fourth item based on the process of combining some words and sentences listed at the annual report in order to facilitate the understandability of some complex transactions and numbers (Courtis, 2005). If technical jargon is unavoidable, for instance industry related jargon, an explanation in a glossary may increase the understandability of the information

4- Comparability

Comparability is the fourth fundamental qualitative characteristic as elaborated in the ED, however, during the process of preparing financial report the user may find similar situations which are presented the same, and in some cases different situations which are presented differently. Thus comparability means the ability that the information has in explaining and identifying similarities in and differences between two common sets or transactions of economic phenomena (IASB, 2008). According to the ED, comparability could be arrived by attaining consistent information by companies, this could happen by enforcing the company to use the same accounting policies and procedures, either from period to period within an

entity or in a single period across entities (IASB, 2008). Comparability refers to the users' ability to make comparisons over time between different financial statements of a certain entity and those of other entities (Alfredson, et. al., 2007). The widespread use of the Internet in financial reporting has resulted in a demand for summarised information to be provided to users in a standardised form and Internet reported financial information to be reported at certain intervals of time (Khan, et. al., 2006).

Previous literature expressed that there are six items used to measure comparability and consistency, according to (Beuselinck and Manigart, 2007; Cole, et. al., 2007) four items from them focus on the consistency of the company ability in using of the same accounting policies and procedures from period to period, while the rest two items according to Cleary, Cole, et. al., (2007); Beuselick and Manigart (2007), IASB (2008) focus on measuring the comparability in a single period across companies. In general companies deal with a very changing environment full of doubt and uncertainty or rules and government regulations, which in turn underline the concept of consistency, thus the company in such circumstances should change their estimates, judgments, and accounting policies to cope with that (Jonas and Blanchet (2000). In addition to that (IASB, 2006; Cole, et. al., 2007) stated that company should also evaluate the earning figures comparability, because it's an important item for measuring and evaluating the company performance over time. Any change of the company judgments, estimates, or accounting policies, then it should modify the earning figures of previous years' in order to visualize the impact of the change on previous results.

Additionally, and according to consistency definition which imply using the same accounting procedures within the same period, IASB (2008) states that company should provide an overview in which they compare the results of different years. For example, the company should compare earning figures, change in estimates, judgments, or accounting policies occurred for both periods (current and previous year) in order to improve the comparability of financial reporting information. IASB (2008) also clarified that comparability in not limited for single company; it also referred within different companies. For example; one company can benefit from comparability of other company annual reports, its structure of the annual report, its used accounting policy, and its transaction and other events (Jonas and Blanchet, 2000) and ratios and index numbers during the process of comparing companies' performance.

5- Timeliness

The last enhancing qualitative characteristic discussed in the IASB (2010) conceptual framework is timeliness. The framework defines timeliness as having information available to decision makers before it loses its capacity to influence decisions (IASB, 2010). In specific terms, timeliness relates to the decision usefulness of financial reports. It refers to the time it takes to reveal the information in annual reports. It is usually measured in terms of the number of days it takes for the auditor to sign the accounts after book-year end.

4.2.2 The Business Performance

Organisations today are struggling aggressively to cope with all the changes surrounding them by enhancing their business performance through the competitive advantage they develop (Kagaari, 2011; Masa'deh, et. al., 2015). Researchers have always looked at business performance as the ultimate goal concerned with almost every area in management. This is because business performance allows researchers to evaluate organisations, their actions, and environments and compare them to those of their competitors (Richard et al., 2009; Santos and Brito, 2012). Most literature suggests that when it comes to business performance, researchers find it difficult to define, conceptualise and measure this concept (Alrowwad, 2017; Taghian et al., 2015). Some authors (Chow and Steve, 2006; Marie et al., 2014) indicated that although financial measures are important, they are not sufficient for a good performance evaluation system. The system should further include non-financial measures of performance. According to Dossi and Pateli (2010), appropriate performance measures are those which enable organizations to direct their actions towards achieving their strategic objectives to the opportunities and threats in the environment. Despite the dearth of research available on separate performance dimensions, the choice of adequate performance measures is likely to be influenced by several contextual factors identified in the contingency-based research (Chenhall, 2005; Henri, et. al., 2014). In response to the debate relating to the advantages and disadvantages of considering financial or non-financial performance measures and the appropriate choice of measures, some empirical evidence indicates that financial and non-financial measures are not substitutes, but that non-financial measures are used as supplements to financial measures (Al-Thuneibat, et. al., 2015; Kinyua, et. al., 2015).

Yet effective frameworks of performance measures that integrate both financial and non-financial measures have been developed. Such frameworks are based on the fact that

management accounting information systems cannot solely be based on financial information. A combination of financial and non-financial information is needed to give a more balanced representation of the overall performance of the organisation. An examination of the performance measurement systems in the literature demonstrates that many management accounting scholars (Harrison et al., 2012; Hla and Teru, 2015; Taiwo and Edwin, 2016) incorporated non-financial performance measures as an essential part of the management information system.

As far as operationalization of business performance measures is concerned, apart from the dimensionality, another challenge is the selection of the kind of measure, i.e. objectives subjective measures. Several scholars have argued the necessity to use subjective performance measures as a substitute for objective measure (Sandeep and Bedi, 2016; Masa'deh, et. al., 2015; Wall, et. al., 2004; Kim, et. al., 2004). The use of subjective measurements for business performance is made more necessary by the relative difficulty of gathering objective financial data. Either these types of data are unavailable, or they are obscured or manipulated by managers eager to protect their firms' reputations or avoid personal or corporate taxes. In addition, subjective measures would allow comparison across firms and contexts, such as industry types, time horizons, cultures or economic condition (Vij and Bdi, 2016). Indeed, it could be a good alternative if the measures focus on the firm's current condition and the objective data may not be compatible with the intended level of analysis (Wall, et. al., 2004). Furthermore, subjective scale measures have been commonly featured in the business literature and supported it as a valid and reliable method (Vij and Badi, 2016 Masa'deh, 2015). Therefore, these results maintain that subjective measures can be used to assess the firm's performance and probably lead to convergent results of different magnitudes. In the validation issue, for example, Dess and Robinson (1984) state that subjective measurements are strongly correlated with objective measurements in terms of the absolute changes in return on assets and sales, over the same time period. For example, the result of the correlation (r) between objective and subjective measures to total sales gives a value for r of .80, and to ROA gives a value for r of 0.79. This supports the validity of the performance evaluation through subjective measures.

Based upon these above arguments, this study will use subjective measures for both dimensions of business performance (financial and non-financial) and the respondents will be asked to point out the degree of their business performance relative to industry /service sector average using a seven-point Likert scale with anchors 'very low' to 'very high. Seven-point

scale provides a wide range of flexibility to respondents for comparing the business performance with major competitor ranging from 1 to 7 (Vij and Badi 2016). Comparing the firm's performance relative to its industry (competitors) or service average is considered reasonable and preferable when researchers interested in measuring firm performance across industries with subjective indicators (Santos and Brito, 2012). Sandeep and Bedi, (2016) emphasised that subjective measures may be more appropriate than objective measures for comparing profit performance in cross-industry studies. This is because profit levels can vary considerably across industries, obscuring any relationship between the independent variables and company performance. Subjective measures might be more appropriate in this situation because managers can take the relative performance of their industry into account when providing a response. The items making up this scale were divided into two subscales: Financial performance (e.g. return on assets (ROA), return on equity (ROE), sales growth, market value, and profitability growth), and non-financial performance (customer satisfaction, employees satisfaction, shareholder satisfaction, environmental performance, and social performance etc.). These most common measures were selected in order to facilitate the comparison with the findings of prior studies in this field (see Appendix A for more details).

4.2.3 Major Components /Constructs of SysTrust's Framework

Trust service is an attestation services guide established by the Assurance Services Executive Committee of the AICPA. Trust Services are consisted from Web Trust and SysTrust and defined as a set of professional services and advisory services based on a common framework (that is a core set of principles and criteria) to address the risks and opportunities associated with IT based accounting process (AICPA and CICA, 2006). SysTrust by its principles, criteria, and illustrative controls is the key guide for the current study to examine business performance and quality of financial reporting in terms of AIS availability, security, maintainability, integrity and privacy.

According to the AICPA, SysTrust is an assurance service that independently tests and verifies a system's reliability. It is assumed expect that any system that satisfies the SysTrust principles should be viewed as being more reliable and thus be trusted more than one that does not. In other words, trust in the system of specific provider is influenced by the extent to which the system meets the SysTrust principles. It is referred to as trust in system reliability in the present study. Figure 4.2 shows five fundamental components (principles) that

contribute to the overall objective of the system reliability. These components are presented as follows.

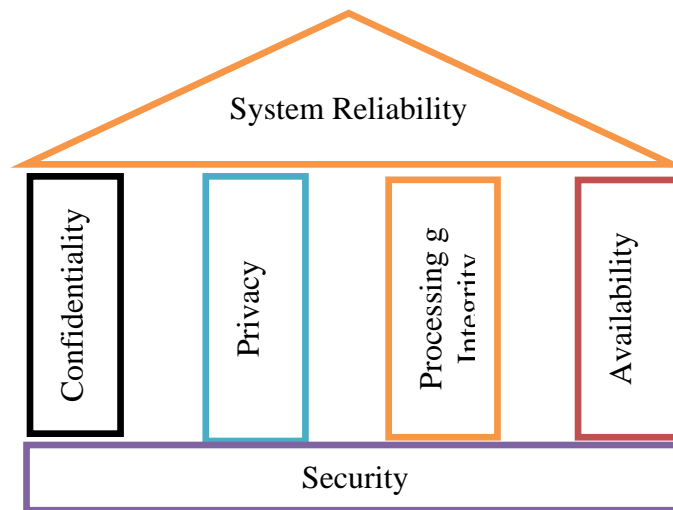


Figure 4.2 Relationships among Principles of the System Reliability

***Source:** Boritz, et al., (1999), 75-83.

1- Availability of AIS.

Availability is an operation of accessibility characterised by the end-client capacity to utilize AIS in adaptation with schedules and agenda of business organizations, and whenever it is required. Utilizing AIS implies performing flawless and quality inputting, upgrading storing, and re-establishing process in the time chosen. There are various conceivable sorts of threats to the availability of AIS including: Failures of hardware and software, natural and man-made disasters, human mistake, viruses and worms, and attacks of rejection-of-services and other acts of harm. SysTrust has created a set of criteria, operational policies, illustrative controls and producers to diminish; however, it has not wiped out threats to AIS availability and they are disaster recovery plan and business continuity plan. Availability is best guaranteed by thoroughly keeping up all hardware, performing equipment repairs instantly when required and keeping up an accurate working framework environment that is free of software conflicts. It is additionally critical to keep updated with all important framework overhauls. Giving sufficient correspondence data transfer, capacity and keeping the event of bottlenecks are similarly vital. Excess, Fail over, RAID even high-availability groups can alleviate genuine results when hardware issues do happen.

Table 4.2 The SysTrust's Framework. Principles and Criteria

The Main principles	Selected Items measures	References
1. Availability	<ul style="list-style-type: none"> • Policies for minimizing risk system downtime; • Data Backup, and restoration • Incremental backup and differential backup • Disaster plan recovery • Business continuity planning 	AICPA, (2013; 2017); Greenberg, et al., (2012) Satio, (2012) Bedard, et. al., (2005).
2. Security	<ul style="list-style-type: none"> • IT security policy and producers • Security awareness, and communication • Logical access; Physical access • Security monitoring • User authentication; Incident management • Systems development, and maintenance • Personnel security; Configuration management; Monitoring, and compliance 	AICPA, (2013; 2017); Abu-Musa, (2010); Satio, (2012).
3. Confidentiality	<ul style="list-style-type: none"> • Confidentiality policy; Confidentiality of inputs; Confidentiality of data processing • Confidentiality of outputs • Information disclosures (including third parties) • Confidentiality of information in systems development 	AICPA, (2013); Satio, (2012); Boritz, (2005).
4. Integrity processing	<ul style="list-style-type: none"> • System processing integrity policies • Completeness, accuracy, timeliness, and authorization of inputs, • System processing, and outputs. • Information tracing from source to disposition 	AICPA, (2013, 2017); Greenberg, et al., (2012), Satio, (2012); Bedard, et. al., (2005).
5. Privacy	<ul style="list-style-type: none"> • It defines documents, communicates, and assigns accountability for its privacy policies and procedures. • It provides notice about its privacy policies and procedures • It describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information. • It collects personal information only for the purposes identified in the notice. • It limits the use of personal information to the purposes identified in the notice. • It provides individuals with access to their personal information for review and update. • It discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual. • It maintains accurate, complete, and relevant personal information for the purposes identified in the notice. 	AICPA, (2013; 2017); Greenberg, et. al., (2012); Boritz, (2005).

Source developed by the researcher based mainly on ACPA (2013) and previous studies*

Fast and adaptive disaster recovery is crucial for the most pessimistic scenario situations. That limit is dependent on the presence of an exhaustive disaster recovery plan (DRP). Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To keep data misfortune from such events, a backup

copy might be stored in a topographically secluded area, maybe even in a fireproof, waterproof safe. Extra security equipment or software, for example, firewalls and proxy servers, can make preparations for downtime and inaccessible data because of malicious actions such as denial-of-service (DoS) attacks and network intrusion. System users must have the capacity to include new or amended data into a system. In the event that system unavailability disables users from doing this, the system preparing may contain blunders.

Thus, users who access data from the system for decision-making purposes will be hampered by a system that is distracted when required. Another part of availability includes system accessibility by support staffs that monitor system performance and roll out improvement to the system when required. In spite of the fact that there is a relationship between the concepts of system availability, functionality, and usability, the SysTrust availability principle does not imply to address the particular functions the system performs or the ability of users to apply system functions to specific tasks or issues. The availability principle addresses whether the information stored in the system is accessible for routine processing, monitoring, and maintenance. These principles imply that stakeholders expect to be able to access or send emails and to place orders when convenient for them, and the Internet connection is expected to be functional without disruption. These are examples of availability. Thus, availability is the property that the system has always honoured any legitimate requests by authorised principals or entities. Availability ensures that information assets are accessible whenever needed. Availability compromises could also be classified as technical, human or natural phenomena, such flood, and earthquake or power outage.

2- Security of AIS

The definition of security is the protection of AIS against unauthorised physical and logical access. To guarantee the ethical use of the accounting data is part of AIS security. It is necessary to build an IT infrastructure to ensure the reliability of AIS against security risks and improve the internal control system of AIS. To ensure AIS security needs the developing of operational and physical procedures pertaining to the use of hardware, software, and accounting data. Also, AIS security requires developing physical and logical access controls such as user identification controls, physical possession identification, and compatibility tests. However, security of extended AIS requires developing Internet and e-commerce and e-business applications. The objective of security is to ensure resources against specific undesired results coming about because of intentioned acts or 'Acts of God'. Most authors agree that security objective apply to an overall information system and there are plentiful

cases of blunder or abuse to exhibit that safety mechanisms in a computer system are not adequate to give insurance alone. This infers that secure is not a property of a computer system, it is a property of the overall information environment of which the computer system is a part. Furthermore, security is a relative rather than an absolute measure. A protected information system is one that decreases the risks of undesired results to a satisfactory level. Access to a system must be confined to authorised users. The access restriction applies to the physical components of the system as well as the logic functions the system performs. Confining access to a system avoids potential misuse of system components, burglary of system assets, abuse of system software, and improper access to, use, alteration, destruction, or disclosure of information. The terms security and privacy are sometimes used interchangeably, yet they may have altogether different definitions implications relying upon the definitions utilised.

Table 4.3 Types of Security Control

Types of Security Control	Measures
Administrative Controls	<ul style="list-style-type: none"> • Developing and publishing of policies, standards, procedures, and guidelines. • Screening of personnel. • Conducting security-awareness training and • Implementing change control procedures
Technical or Logical Controls	<ul style="list-style-type: none"> • Implementing and maintaining access control mechanisms. • Password and resource management. • Identification and authentication methods • Security devices and • Configuration of the infrastructure
Physical Controls	<ul style="list-style-type: none"> • Controlling individual access into the facility and different departments • Locking systems and removing unnecessary floppy or CD-ROM drives • Protecting the perimeter of the facility • Monitoring for intrusion and • Environmental controls

➤ **Source.** **Source.** These variables have been selected from several empirical studies on the Security (see Chapter 2)

As characterised in this report, the privacy guideline addresses access to the framework and the techniques used to ensure access to the data that is accumulated, put away, and scattered by an element. Protection concerns identified with limiting access and utilizing confidential data are in this manner tended to by the SysTrust privacy guidelines. At the point when there are laws and regulation governing such matters, a framework should conform to them. As characterised in this section, the security principle addresses access to the system and the techniques used to ensure access to the information that is accumulated, stored, and disseminated by an entity. Protection concerns identified with restricting access and the use

of confidential information are in this manner tended to by the SysTrust security principle. At the point when there are laws and regulation governing such matters, a framework should conform to them.

Looking into the previous studies concerned with assessing the security of computerised information systems uncover the scarcity of available studies in that particular area of research. One reason is that the security of CAIS is generally new research area. The main objectives of these studies were to list the security threats that might threaten computerised information systems in an organization; to investigate the importance of such perceived security threats in the reality; and to explore their events and potential losses in various organizations. Loch, et. al. (1992) performed a standout amongst the most critical studies and overviewed the impressions of management information systems executives concerning the security threats in microcomputer, mainframe computer, and network environments.

A list of twelve security threats was created by the researchers to be analysed scientifically in that study. The findings of the study indicate the top security threats were natural disasters, accidental actions by employee (entry of corrupt data and destruction of data), poor control over media, and the unauthorised access to systems by hackers. Davis (1996) utilised the questionnaire developed by Loch, et. al. (1992), to find out the current situation of IS security practice in reproduction of their work. The findings of Davis's (1996) survey indicated that information systems auditors identified that different computing environments have different relative levels of security risks. The findings, likewise, pointed out that the three top security threats in a microcomputer environment were employees' accidental entry of "corrupt" data, the accidental destruction of data, and the introduction of computer viruses. All in all, unauthorised access to data and systems (or both) by employees, accidental entry of "corrupt" data by employees, and poor separation of information system duties were considered as the primary threats to the midrange computing environment. As needs be, Whitman (2004) focused on that protecting information system from these workers was more troublesome and confounded, as it originated from inside the organization.

With respect to the mainframe computer environment, accidental entry of "corrupt" data by employees, natural disaster, and unauthorised access to data and system (or both) by employees are assumed the main threats. The most imperative threats in network computer environments were unauthorised access to data and systems (or both) by outsiders (hackers) and insiders (employees) alike, and the advancement of technology faster than control

practices. The research of Ryan and Bordoloi's (1997) explained how companies that transfer from a mainframe to a client or server environment observed and took security measures to protect against potential security threats. The results of Ryan and Bordoloi's (1997) study outline that the most foremost security threats were accidental destruction of data by employees, accidental entry of invalid data by employees, deliberate destruction of data by employees, intentional entry of invalid data by employees, loss due to insufficient backups or log files, natural disaster including fire, flood, loss of power, etc., and single point of failure.

Hood and Yang (1998) examined the banking information systems security in China where the findings indicate that all participants perceive that management knows about security matters; however, they did not trust that their banks had had made adequate move to diminish the risks and losses because of conflicting financial and human resources. Moreover, the four banks overviewed demanded that they had a security policy, however, it was just officially expressed in one of them. In China, managing an account industry human security threats were seen as the most critical security threats, especially, hateful attack from outsiders. These distinctions demonstrate that developing countries perceive security differently. Dhillon (1999) studied the nature of security breaches that have occurred in different areas of the world. He argued that if organizations embrace a more practical approach in managing security breaches many of the security losses as a consequence of computer related fraud could be counteracted. The findings of Dhillon's (1999) study show that doing controls, as distinguished in a security policy, would anticipates computer abuse. Selecting an adjusted approach of security controls, that place equal importance on technical, formal, and informal interventions to CAIS would prevent committing computer fraud.

Hermanson, et. al. (2000) conducted a preliminary survey to acknowledge how organizations concentrate on their IT risk and to audit assessments of IT risk performed by the internal auditors. The findings of the survey show that the essential focus of the internal auditors is on conventional IT risks and controls, for example, the protecting IT assets, application processing, and data integrity, privacy and security. Coffin and Patilis (2001) examined the role of internal auditors in assessing the security controls to safeguard sensitive data in CAIS in financial organizations such as banks, security companies and insurance companies. They argue that internal audit can enormously help organizations to distinguish and assess security controls identified with gathering, utilize, and access to customer information, and consistence with appropriate regulatory. White and Pearson (2001) looked into more than 200 organizations in the U.S, where they examined the security controls concerning individual

utilization of computers, monitoring email accounts, and security of organization data. The results of the study highlight the need to improve security control in a large number of companies surveyed. Likewise, the findings show that many companies do not execute proper safeguards before they start to use computer technology. Furthermore, in the most organizations there was an absence of safeguards. Warren (2002) performed a survey in three countries: Australia, the UK, and the US to evaluate the security methods of computerised information systems. The paper attempted to review security methods from different aspects and to investigate whether security practices differ from one country to another. The results of the survey reveal that.

- In Australia, there was a lack of computer security found among Australian companies. Poor security methods used were among the security problems identified. The results also show that almost fifty per cent of companies do not financially plan for computer security.
- In the UK, 42% of organizations did not have an information security policy. The results also show that almost half of the organizations listed insufficient funds as being an issue in implementing computer security.
- In the US, information theft and financial fraud are the reasons for the majority of financial damage. However, differences in the levels of CAIS exploitation implemented by internal and external individuals were not of importance. The paper suggests that the security practices of the United States seem to be more effective than those of Australia or the UK. Wright and Wright (2002) conducted an exploratory study, using a semi-structured interview approach, to gain an understanding of distinctive risks linked to the implementation and operation of Enterprise Resource Planning (ERP) systems.

The findings of the examinations indicate that inadequate user training increases the likelihood for financial statement errors and business risks. The findings also show that proceeding with risks differ across applications and across vendor packages. Finally, the findings demonstrate that major corporations, when hired to provide assurance on the risks for an ERP system, use process audit techniques, rather than validation testing (i.e., they do not depend upon tests of output). In recent times, the National Institute of Standards and Technology (2003) in the U.S. distributed its first publication draft titled *Standards for Security Categorization of Federal Information and Information Systems*. This publication exhibits three security goals (confidentiality, integrity, and availability) identified with securing computerised information systems and the possible levels of risk (low, moderate, and high) for each of the security objectives. The proposed levels of risk are more likely to affect the impact of risk on the security of CAIS and the possible amount of damage that the

loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image, or reputation), agency assets, or individuals (data privacy).

Recent evidence from a survey by the Computer Security Institute (Richmond, 2003) shows genuinely extreme issues with corporate system security. For example, 82% of respondents experienced virus attacks, 45% had unauthorised access, 42% experienced denial of service, and 36 percent had system penetration. If a SysTrust review had recognised the risks associated with their systems failure and management had implemented controls to relieve those risks, it might just have been justified regardless of the expense of the engagement to these companies. For all intents and purposes, all organizations with overwhelming dependence on systems face similar risks, prompting a potential interest for assurance services such as SysTrust, which verify that controls have adequately operated within the systems. From October 2002 to June 2003, the United States General Accounting Office (GAO) (2003) did an audit at the Financial Management Service (FMS) to assess whether FMS. (1) Administered a complete security risk assessment, and (2) Documented and performed suitable security measures and controls for the system's security. The findings of the GAO (2003) survey recognised that in spite of the fact that FMS and the Federal Reserve had performed many security controls to protect their computing resources, risks were not adequately assessed, and a majority of security control shortcomings were identified. Therefore, it was highly prescribed that quick actions to remedy the shortcomings and to immediately address new security threats and risks as they rise to CAIS were taken.

Abu Musa, (2004) conducted an empirical study to examine the adequacy of Security Controls implemented in the Egyptian banking industry (EBI). He attempted to examine whether the applied Security Controls in the EBI are sufficient enough to protect against the perceived security threats through self-administrated questionnaire. The CAIS security checklist consists of eighty security procedures which were classified under the following ten groups. (1) Organizational information security controls. (2) Hardware and physical access security controls. (3) Software and electronic access security controls. (4) Data and data integrity security controls. (5) Off-line programs and data security controls. (6) Utility security Controls. (7) Bypassing of normal access security controls. (8) User programming security controls. (9) Division of duties. (10) Output security controls. He revealed that the head of computer departments paid relatively more attention to the technical problems of CAIS security controls, where the head of internal audit departments emphasised behavioural

and organizational security controls rather than the technical problems of the CAIS security controls.

Boritz (2005) identified information security as one of major characteristics for information integrity; this security should include the following points. Physical access controls and Logical access controls. The findings showed that the security had a lower impairment severity score than several other practical aspects such as availability and verifiability. Boritz refer such findings to the effective use of security controls in the organizations represented. Coe (2005) in his study focused on the fulfilment of Sarbanes-Oxley act 2002 that requires public companies to report about the effectiveness of their internal control systems. The aforementioned studies of the information security were undertaken in developing countries. However, there are no sufficient studies exploring CAIS security issues in developing countries. Hence, it can be presumed that the vast majority of the previous studies (e.g., Loch, et. al. 1992; Davis, 1997; Ryan and Bordoloi, 1997) do not differentiate between security threats clearly (i.e., possible negative events) and security weaknesses (i.e., inadequate security controls). There are numerous security threats, for instances, the inadequacy of some security controls (such as inadequate control over media-disks and tapes), poor control over manual handling on input/output, inadequate separation of information systems duties, and poor separation of accounting duties are treated as security threats. Notwithstanding, deficient control over storage media, poor audit trail, inadequate or non-existent log-on procedures, loss due to lack of backups or log files, uncontrolled read, and update access (or both), uncontrolled user privilege, and weak/ineffective or insufficient physical controls are also regarded as security threats.

3- The Confidentiality

This principle focuses on information designated as confidential. Unlike personal information, which is being defined by regulation in a number of countries worldwide and is subject to the privacy principles, there is no widely recognised definition of confidential information. In the course of communicating and transacting business, partners often exchange information they require to be maintained on a confidential basis. In most instances, the respective parties wish to ensure that the information they provide is available only to those individuals who need access to complete the transaction or resolution on any questions that arise. To enhance business partner confidence, it is important that the business partner is informed about the entity's confidentiality practices. The entity needs to disclose its practices relating to the manner in which it provides for authorised access to and uses and

shares information designated as confidential. Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. Access must be restricted to those authorised to view the data in question. It is common, as well, for data to be categorised according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories. Sometimes safeguarding data confidentiality may involve special training for those privacy to such documents. Such training would typically include security risks that could threaten this information.

GAPP (2009), explained “unlike personal information, rights of access to confidential information to ensure its accuracy and completeness are not clearly defined. As a result, interpretations of what is considered to be confidential information can vary significantly from organization to organization and, in most cases, are driven by contractual arrangements. A good example of methods used to ensure confidentiality is an account number or routing number when banking online. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm. Other options include biometric verification and security tokens, key fobs or soft tokens. In addition, users can take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a required transaction. Extra measures might be taken in the case of extremely sensitive documents, precautions such as storing only on air gapped computers, disconnected storage devices or, for highly sensitive information, in hard copy. Confidentiality is the property that information is not made available or disclosed to unauthorised individuals, entities or processes. Confidentiality protects data in storage and in transmission. Confidentiality is compromised whenever information can be viewed or read by unauthorised entities or disclosed out of the ‘need to know’ group or community. This compromise could be either physical or electronic”.

The electronic confidentiality compromises include end-users or entities accessing information, data or resources that are not meant for them. For instance, if someone can access one’s email messages without the express authorization from the account owner, confidentiality property is said to be breached. The physical confidential compromises include reading printouts marked ‘confidential’ or verbal disclosure of confidential information outside the ‘need to know’ group. Confidentiality ensures that information is

accessed by and disclosed to authorized users only. Confidentiality encompasses the concepts of data privacy, encryption and cipher or cryptography. Furthermore, confidentiality implies that stakeholders expect that the privacy of their correspondences, their passwords, phone numbers, and any other information shared during email interactions will be secured. These are examples of confidentiality. Thus, Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes, either in storage or in transmission (ACPA, 2013).

4- Processing Integrity

Integrity of AIS is known as completeness, accurateness, timeliness, and the authorization of AIS process. It is defined by AICPA (2013) as accuracy or the degree to which applications are error-free. According to SysTrust, AIS has reliability, if the accounting process is accomplished in a sound manner and free from unauthorized misuse. To improve reliability of AIS, the application and general controls have to be inherited in the creation of ICS. There are many examples of application control among them; source data controls, on-line data entry controls, input validation practices, data processing and storage controls, output controls, and data transmission controls. AICPA (2013) provides four important concepts of (a) assertions, (b) error classes, (c) information transformation processes and (d) control procedures for assessing Accounting Information System (AIS)'s reliability. A reliable AIS is most likely to have output (accounting information) that have integrity. Therefore, these four concepts are further evaluated thus.

- **Assertions.** An assertion is a statement about the absence of a particular class of error in the ledger accounts (Krishnan, Peters, Padman and Kaplan, 2005). The degree of reliance on an assertion depends on the trust and confidence stakeholders have on the person making the assertion. If the person is considered to be one having integrity, they will have trust that the assertion made is correct and therefore has integrity. If otherwise the assertion will not be relied on because it is coming from some who cannot be trusted to provide information with integrity
- **Errors.** AICPA (2013) identifies five classes of errors namely completeness, existence, valuation, rights and obligations, and presentation and disclosure. They are.
(I) **Completeness errors.** These are errors that occur when a valid transaction that should have been included in financial report is missing as a result of human error of either failing to record it or deleted incorrectly (Krishnan, et. al., 2005). The act of failing to record or delete is subject to the integrity of the person involved. It could be intentional if the person involved lacks integrity and otherwise may be due to

carelessness or ineffective internal control system that does not provide for checks and balances. Checks and balances system will ensure that the acts of one person are checked when the next person in the chain of process is carrying out the assigned responsibilities. (2) Existence errors. According to Krishnan, et. al. (2005), these are errors occurring where an invalid transaction is included in the financial report. This may be due to the incompetence of the personnel if the act is not deliberately committed but if deliberate, then it is an integrity issue. A person of integrity will not deliberately include a transaction that did not take place in the financial data in process because he knows that will misrepresent the actual facts which the information presented represents. (3) Valuation errors. These occur when the data included in financial reports do not accurately reflect the economic results of the transactions that created the data (Krishnan, et. al., 2005). This is a type of error associated with the personnel involved in data recognition in an organization. A competent and an integrity minded person will record economic events at their right values. A person lacking in integrity can falsify values involved in transactions with a viewing to benefiting personally from the transactions at the expense of the organization. This can be deliberate reduction of revenue items or inflation of expense items. Either way the difference will be excluded from the organizations data processing.

- Rights and obligations. Every financial transaction bestows on the parties involve rights and obligations. The rights translate into assets while the obligations translate into liabilities in accounting. An error associated with rights and obligations is where wrong persons are bestowed with rights and obligations. A person lacking in integrity can deliberately transfer the rights of one person to other with a view to personally benefitting through sharing with the person to whom the right is transferred. An obligation can also be transferred to a person who originally was not involved in a transaction either mistakenly or deliberately.
- Information transformation processes (ITPs). Captured data flows through a series of ITPs until they reach the general ledger and an error could be introduced at any stage in these processes. Again, such errors could be deliberate and if so they become personal integrity issue which may have negative effect on the accounting information provided.
- Control procedures. According to Krishnan, et. al. (2005), these are procedures designed to prevent or detect one or more of the errors listed above. From the point of view of integrity, these procedures can be strengthened if a person of high integrity is

charged with the responsibility of designing, assessing and review the procedures from time to time but a person lacking in integrity can create loopholes in the system to be exploited for personal interest. Such loopholes if exploited will have negative impact on the output of the system. In other words, the information provided by the system will be lacking in integrity.

According to the IT Governance Institute (ITGI, 2004), integrity refers to good or intact condition. When applied to information, 'integrity is the represented authenticity of the information to the situation or subject matter of which that information represents. The figure graphically illustrates the process of how information integrity is achieved. This demonstrates that to have information integrity both the data and the system (including IT infrastructure and operating system) need to have integrity. Boritz (2005) define information integrity as representational faithfulness. Information integrity involves both accuracy and completeness and therefore timeliness too, as well as the validity with respect to applicable rules and regulations. Information integrity requires data integrity. "The state that exists when data are unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed" (Boritz, 2005). Integrity is closely related to the notion of reliability. It is specifically interested in information systems to be used to control and account for an organization's assets. In such systems, the primary goal is prevention of fraud and errors. The meaning of improper modification in this context has been given by Clark and Wilson [CLAR87] as follows: No user of the system, even if authorised, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted.

As mentioned previously, the raw material data is used to produce the finished product, information, ready for use. It is significant to note that other than data, information integrity depends on system integrity. In other words, information integrity must be as good as the integrity of the system processing the data or information, although, it can be as bad (ITGI, 2004; Woodroof and Searcy, 2001). A system establishes processing integrity if 'its outputs are a complete reflection of its inputs, and its processes are comprehensive, timely, authorised and precise (ITGI, 2004). To highlight the two elements, a system may have integrity, but if there is a lack of integrity of the data being processed at the time the system receives it, then the lack of integrity of the data can continue until it is transferred to its target or transformed into information. Therefore, Transmission integrity is a part of system integrity and not a separate element. "Integrity involves maintaining the consistency, accuracy, and

trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorised people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version control maybe used to prevent erroneous changes or accidental deletion by authorised users becoming a problem. In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. Some data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state” (AICPA, 2013).

Integrity goals may apply to both data and software, and have a range of possible interpretations, maintain consistency, prevent inappropriate modification, detect modification or allow recovery. The consistency requirement is concerned with maintaining correspondence between representations of information (e.g. system data) and reality, and so can only be implemented by a suitably constrained business process. The parallel between distributed workflows and existing paper workflow systems provides an important model for integrity in collaborating systems and suggests that provenance will become as important a concern as consistency. Grid data, web documents and relational database share a graph structure where relational consistency properties may be required. Finally, there is a requirement in a range of emerging systems to ensure the integrity of execution environments independent of any applications that they may run. Integrity also implies that stakeholders expect that content of the emails are not altered and stock counts received are accurate and any attachments downloaded are authentic and complete. These are examples of integrity. Thus, integrity is the property that data has not been altered in an unauthorised manner during transmission or storage.

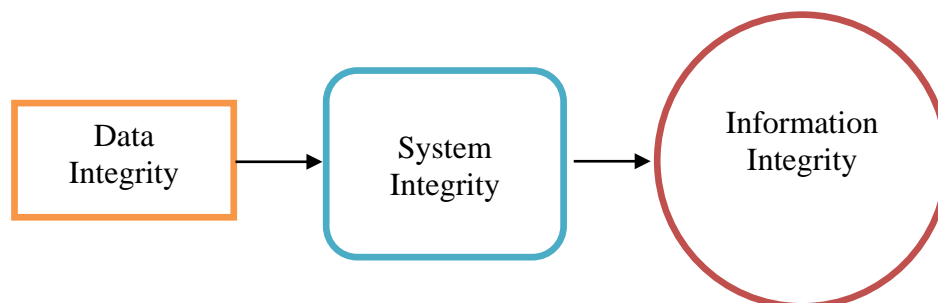


Figure 4.3 Requirements of Information Integrity

*Source: Boritz J. Efrim., (2005) pp. 260-279

5- Privacy

The privacy principle addresses the system's collection, use, retention, disclosure, and disposal of personal information in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and Canadian Institute of Chartered. Privacy can be defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information. According to Solove (2006), privacy can be threatened by three main information-related activities, information collection, processing, and dissemination. Information collection refers to the process of gathering and storing data about an individual. Information processing refers to the use or transformation of data that has been already collected. Information dissemination refers to the transfer of collected (and possibly processed) data to other third parties (or making it public knowledge). The information-related activities described above can represent a chance to breach the privacy of an agent's principal. GAPP have been developed from a business perspective, referencing significant domestic and international privacy regulations. GAPP operationalizes complex privacy requirements into a single privacy objective that is supported by 10 privacy principles. The privacy principles are essential to the proper protection and management of personal information. They are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognised good privacy practices. GAPP is a management framework that includes the measurement criteria for the trust services privacy principle. GAPP consists of 10 sub principles.

1. *Management.* The entity defines documents, communicates, and assigns accountability for its privacy policies and procedures.
2. *Notice.* The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. *Choice and consent.* The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. *Collection.* The entity collects personal information only for the purposes identified in the notice.
5. *Use and retention.* The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfil the

stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.

6. *Access.* The entity provides individuals with access to their personal information for review and update.
7. *Disclosure to third parties.* The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. *Security for privacy.* The entity protects personal information against unauthorised access (both physical and logical).
9. *Quality.* The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. *Monitoring and enforcement.* The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

For each of the 10 privacy principles, relevant, objective, complete, and measurable criteria have been specified to guide the development and evaluation of an entity's privacy policies, communications, and procedures and controls. *Privacy policies* are written statements that convey management's intent, objectives, requirements, responsibilities, and standards. *Communications* refers to the organization's communication to individuals, internal personnel, and third parties about its privacy notice and its commitments therein and other relevant information. *Procedures and controls* are the other actions the organization takes to achieve the criteria. For each of the five principles, criteria have been established against which a system can be evaluated. The criteria address the following features that contribute to system reliability:

1. The definition and documentation of an entity's performance objectives, policies, and standards as they relate to system performance expectations and service level commitments, and their communication to applicable personnel. Performance objectives, policies, and standards represent management's awareness and commitment to a level of performance and control at the entity. Performance objectives are the overall goals that an entity wishes to achieve. Policies are rules that provide a formal direction for achieving the objectives and that enable enforcement. Standards are the required procedures that are implemented to meet the policies. In some entities, policies and standards represent separate items and in other entities they are terms that are used interchangeably.

2. The procedures an entity implements for all system components to achieve its performance objectives in accordance with its established policies and standards.
3. System monitoring activities and monitoring of the surrounding environment to enable an entity to identify potential impairments to system reliability and to take appropriate action to achieve compliance with objectives, policies, and standards.

Privacy is related to the degree of intrusiveness systems impose on people and the nature and extent of personal information those systems request, store, and use in providing services. Other privacy concerns pertain to the nature and extent of the information gathered and stored by an entity about its customers and other system users. Some privacy concerns may be related to local customs or legislative initiatives, as when some jurisdictions regulate the kinds of personal information that may be sent across borders. The SysTrust criteria are designed to be complete, relevant, objective, and measurable and to address all of the system components and the relationships among them. In some cases, for evidence-gathering purposes, the criteria may need to be broken down, for example, by system component, to address infrastructure, software, people, procedures, and data or by system development phase, which includes investigation, acquisition, implementation, operation, and maintenance.

Based upon review of literature, it can be concluded the relationship between the constructs of the study's model either separately or together are not yet examined. Therefore, this study aims to explore. (1) The effect of the interaction of this study's model upon the quality of financial reporting; and (2) To explore the effect of the extent of the existing relationship between the implementation of SysTrust model's requirements and the business performance either taken separately or together.

4.3 Research Hypotheses

Based upon the study's conceptual framework and the results of the initial of in-depth – interview, the study hypotheses are formulated and proposed as summarised in Table 4.4.

Table 4.4 Research Hypotheses

Hypotheses	
H1.	The overall reliability of the accounting information system of shareholding companies based on the SysTrust's framework (i.e. the five main principles. availability, security, integrity data processing, confidentiality, and privacy) are significantly implemented by their internal control system.
H1_n.	The overall reliability of the accounting information system of shareholding companies based on the SysTrust's framework (i.e. five main principles. availability, security, integrity data processing, confidentiality, and privacy) are significantly not implemented by their internal control system.
H2.	The overall reliability of accounting information system of shareholding companies based on the implementation of the SysTrust's framework (i.e. the five main principles. availability, security, integrity data processing, confidentiality, and privacy) are significantly differ according to their demographic characteristics (type of business sectors, number of employees, business experience, the type of control system).
H2_n.	The overall reliability of accounting information system of shareholding companies based on the implementation of SysTrust's framework (i.e. the five main principles. availability, security, integrity data processing, confidentiality, and privacy) are not significantly differ according to their demographic characteristics (type of business sectors, number of employees, business experience, the type of control system).
H3.	There is a significant relationship between reliability of AIS based upon the implementation of SysTrust's framework (i.e., availability, security, integrity data processing, confidentiality, and privacy) and the quality of financial data reporting.
H3_n	There is no a significant relationship between reliability of AIS based upon the implementation of SysTrust's framework (i.e., availability, security, integrity data processing, confidentiality, and privacy) and the quality of financial data reporting.
H4	There is a significant relationship between reliability of AIS based upon the implementation of SysTrust's framework (i.e., availability, security, integrity data processing, confidentiality, and privacy) and the financial business performance
H4_n	There is no a significant relationship between reliability of AIS based upon the implementation of SysTrust's framework (i.e., availability, security, integrity data processing, confidentiality, and privacy) and the financial business performance.
H5.	There is a significant relationship between reliability of AIS based upon the implementation of SysTrust's framework (i.e., availability, security, integrity data processing, confidentiality, and privacy) and the non- financial business performance.
H5_n	There is no a significant relationship between reliability of AIS based upon the

	implementation of SysTrust's framework (i.e., availability, security, integrity data processing, confidentiality, and privacy) and the non- financial business performance.
H6	There is a significant relationship between reliability of AIS based upon the implementation of SysTrust's framework (i.e., availability, security, integrity data processing, confidentiality, and privacy) and the financial and non- financial business performance, taken together.
H6_n	There is no a significant relationship between reliability of AIS based upon the implementation of SysTrust's framework (i.e., availability, security, integrity data processing, confidentiality, and privacy) and the financial and non- financial business performance, taken together.
H7.	The quality of financial reporting is significantly mediating the relationship between the implementation of SysTrust's framework and business performance.
H7	The quality of financial reporting is not significantly mediating the relationship between the implementation of SysTrust's framework and business performance

4.4 Summary

In this Chapter, the conceptual framework for this study has been developed through the integration of the components of the SysTrust's model (availability, integrity, confidentiality, security, and privacy) with the characteristics of the quality of financial reporting and business performance, Figure (4.4) represents a summary of the expected relationships proposed in this study. The generalised relationship stipulates that the quality of financial reporting is an assumed to be influenced by the implementation or meeting the requirements of the SysTrust model. The relationship is also applied to the firm's business performance. The combination of these relationships represents the present **study's framework, they are.**

1. The level of quality of financial reporting is assumed to be as a function of the implementation or meeting the requirements of the SysTrust model.
2. The firm's business performance is assumed to be as a function of the interaction of the level of the quality of financial reporting as well as the level of the implementation the requirements of the SysTrust model.

The main dimensions of the study's framework:

1. The characteristics of the quality of financial reporting are relevance, faithful representation; understandability, comparability and comparability.
2. The main five components of SysTrust's model are availability, security, integrity processing, confidentiality and privacy.
3. The two firm's business performances dimensions are financial and non-financial performance.

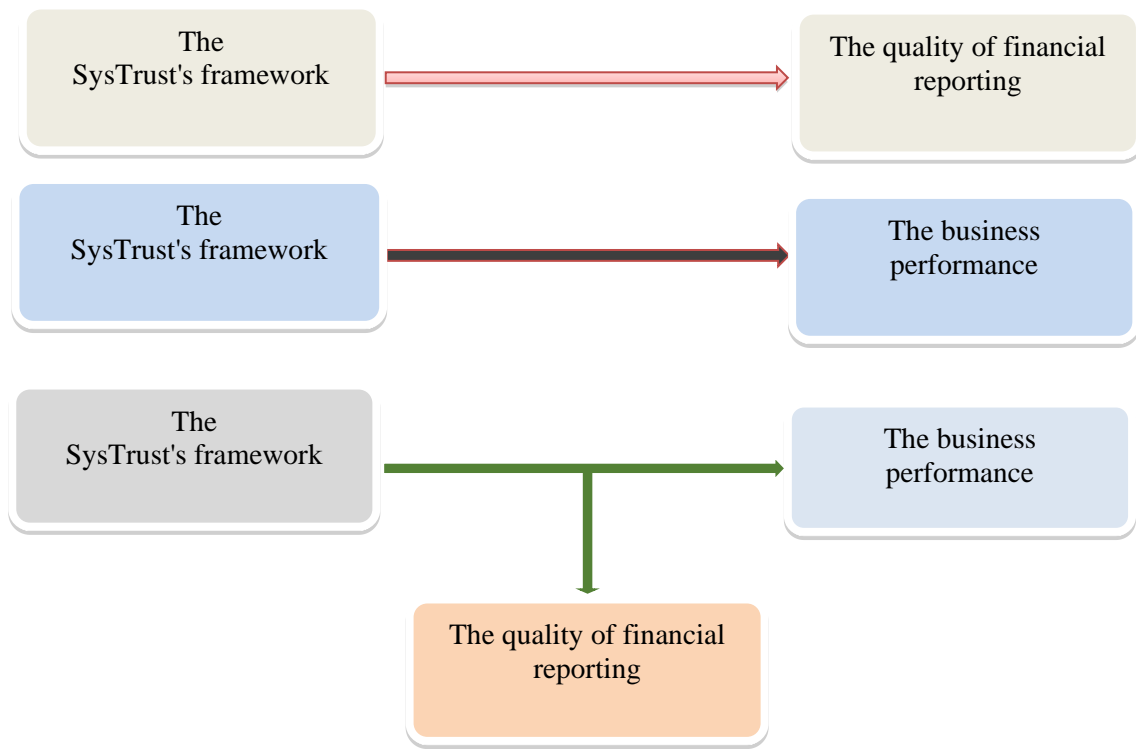


Figure 4.4 A Summary of Conceptual Framework Relationships

Source: Developed by the Researcher

CHAPTER FIVE

RESEARCH METHODOLOGY

5.1 Introduction

In the previous chapter, the conceptual model and hypotheses of the study were presented. This chapter presents a description of the methodology that was employed in carrying out the study. In this chapter, the types of research approaches (quantitative and qualitative) research followed by research paradigms are discussed. Next the research design in terms of its definition, concepts and approaches are presented. Special emphasis is placed upon the data types and source, data collection methods, questionnaire design, scale of measurement and the domains of the study. The chapter spells out the research design, the study population and area, the sampling method, size and procedure, data collection, processing and analysis procedures and techniques, the process of data collection, questionnaire design, and data preparation for the final stage of analysis were fully presented. The aim for this is to provide a brief explanation of the statistical analysis techniques that are used to achieve the research objectives and test its hypotheses. The main goal of this study is to examine the relationship among implementation of the SysTrust principles, quality of financial performance and business performance in the Jordanian shareholding's companies. To successfully accomplish this goal and arrive to credible results, a number of considerations need to be taken into account in the process of doing the research (Bryman and Bell, 2015). These considerations include the research philosophy, approach, and strategy that will be adopted.

5.2 Research Design

Blumberg, et. al. (2014) stated that number of researchers conduct research without knowledge of the basic assumptions of philosophical considerations; however, it is important to understand research philosophies as they help in recognizing and choosing the appropriate research design. Research design is viewed as a protocol determining and influencing the ground rules for data collection and analysis. It acts as the glue that holds the research project together. A design is used to structure the research to show how all of the major parts of the research project. The samples or groups, measures, treatments or programs, and methods of assignment work together in an attempt to address the questions of central research. Research methodology is "a structured set of guidelines or activities to assist in generating valid and reliable research results", according to Sekaran and Bougie (2010). Thus, this

chapter explains the selection of an appropriate research methodology and design for examining the model of this study to measure the constructs and empirically test the hypotheses that have been derived from the research model. A methodology is defined by Irny and Rose (2005) as a guideline system for problem-solving, with specific components such as phases, tasks, methods, techniques and tools. From the definition, it should be noted that the method is a branch of the methodology. As such a methodology can be considered to include multiple methods, each with different facets of the whole scope of the methodology.

Methodology considers the method, in addition to other factors such as the rationale for using the particular method. The methodology explains how, by following the steps defined, someone else can evaluate the result of the research work. In addition to the methodology, the term method should be clearly understood in the context of this study. When defined in scientific terms, the method is actually a body of techniques for investigating phenomena, acquiring new knowledge, or correcting and integrating previous knowledge. To be termed scientific, empirical and measurable evidence subject to specific principles of reasoning must be the basis of a method of inquiry (Goldhaber et. al, 2010). Sugiyono (2010) defined the research method as a scientific way to acquire data for a specific purpose and function. For the research to achieve its objectives, it uses methods or certain procedures that are well regulated. Knowledge of research method logy that examines contains provisions concerning the methods used in the study. According to the research have now (2009) put forward as the investigation of organised, systematic, based on the data, critical, objective and scientific to the specific problems that require solutions. Research by Indriantoro, et. al., (2011), basically is the operationalization of the method used to acquire scientific knowledge known as the scientific method. Because this study aimed to find out what and how much the factors thought to affect a variable (Kuncoro, 2007 in Meiryani, 2014). The main reason for using the scientific method according Sekaran (2009) is that the result will be fewer errors and confidence in the findings will be greater due to higher accuracy in the application of design detail. Meanwhile, according to Sugiyono (2010), the scientific method means that research activities are based on the characteristics of science, namely the rational, empirical and systematic. Characteristics of the scientific method according to Kuncoro (2009) were a critical and analytical, logical, objective, conceptual and theoretical, empirical, and systematic. Descriptive correlational survey design is used in this study used as it sought to describe and establish the relationships among the study variables. A research design is the arrangement of conditions for collection, measurement and analysis of data that aims to combine relevance to the research purpose Kothari (2010). Correlational survey design also

allows a researcher to measure the research variables by asking questions to the respondents and then examining their relationship (O'Connon, 2011). After the philosophy of the research is chosen, another factor should be considered regarding the relationship between theory and research, which is whether to adopt a deductive or inductive approach (Bryman and Bell, 2015). The deductive approach refers to "the logical process of deriving a conclusion about a specific instance based on a known general premise or something known to be true" (Zikmund, et. al., 2013). Here the researcher deduces hypotheses, based on what is known in a particular field and the theoretical consideration in relation to that field, that are then subjected to empirical scrutiny (Bryman, et. al., 2014). Six steps are generally included in the deductive approach, theory, hypothesis, data collection, findings, hypotheses confirmed or rejected, and revision of theory.

At the other end of the spectrum lies the inductive approach, which refers to the process of establishing a general theory based on observing particular events (Zikmund, et. al., 2013). Thus, in this approach, the researcher observes certain phenomena; and on this basis; arrives at a conclusion (Sekaran and Bougie, 2013). Deduction has several characteristics that distinguish it from the inductive approach. These include hypotheses development, collection of quantitative data, controls to allow the testing of hypotheses, structured methodology, independence of the researcher from what is being observed, Operationalization of concepts, and generalization of the results (Saunders, et. al, 2015).

According to Collis and Hussy (2014) the research approach adopted needs to support the achievement of the research aim and objectives. This research develops a theoretical model and hypotheses based on the existing literature in order to measure and provide evidence of their validity. Given that the characteristics of the deductive approach mentioned earlier fit with the objective and other conditions of this study, it can be asserted that the deductive approach is the appropriate approach for this thesis. Once the philosophy and approach for conducting this study have been chosen, the next step is to determine the strategy that will be adopted in this research. A research strategy is a common orientation to the accomplishment of business research (Bryman and Bell, 2015). Nevertheless, it is often challenging for most research work to decide on which research methodology to adopt. A decision should be made regarding the adoption of a qualitative or a quantitative research methodology, with individual strengths and weaknesses for each of them or to perhaps adopt a mixed-methodology which utilizes aspects of both methodologies (Gerhardt, 2004). Rational or based reasoning of research problems to provide answers is part of a research process that

includes theoretical study. Moreover, according to Indriantoro, et. al., (2011) a theoretical study in the research process develops hypotheses that aim to test a theory or hypothesis (hypotheses testing). Through the process of testing this fact, hypothesis testing is the process of developing a science or theory using the deductive approach. This type of research is known as hypothetic-deductive approach. As for quantitative methods, they can be interpreted as a research method that is based on the philosophy of positivism which is used to examine the population or a particular sample, data collection using research instruments, quantitative data analysis/statistics, with the aim to test the hypothesis that has been set (Sugiyono, 2011).

5.3 Research Approaches

Careful attention was paid to the research methodology and approaches used in this study in order to successfully achieve its objectives. In general, two research approaches are used in social science research studies including information systems (IS). Quantitative and qualitative approaches. Although quantitative and qualitative research methodologies have their own distinctive approach, they also share some similarities and areas of mixed approaches and can be brought together in various ways. Based on the problem definition and the nature of information sought, researchers usually choose one of these two approaches, or a combination of both (Punch, 1998). Quantitative research is generally considered more formalised and structured when compared to qualitative research (Crestwill, et al, 2009).

Numerical representation and manipulation of observations are part of quantitative methods for the purpose of describing, explaining, and testing hypotheses (Crestwill, et al, 2009). As for qualitative research, it involves non-numerical examination and interpretation of observations for the purpose of discovering the underlying meanings and patterns of relationships (Creswell et al., 2009). It emphasizes the processes and meanings which are not rigorously examined or measured in terms of quantity, amount, intensity or frequency. This can be achieved through in-depth interviews, focus groups, participant observations and case studies (Cavana and Sekran 2011). However, the results generated by using the qualitative approach can vary from one research to another, and this can be problematic, especially when researchers become fixated on exploratory research and do not progress beyond this to the hypothesis testing stage. According to Biga and Neuman (2006), at the heart of quantitative research lie variables and relationships which are useful in terms of providing the necessary detailed planning prior to data collection and analysis, as well as the tools needed for measuring concepts, planning design stages, and dealing with population or sampling issues.

Furthermore, a deductive mode is utilised by this approach to test the relationship between variables in order to provide evidence, whether for or against pre-specified hypotheses (Biga and Neuman, 2011). As discussed in Chapter 1, this study attempts to investigate the between the level of reliability of AIS and the quality of financial reporting and business performance context by testing the proposed hypotheses. Drawing on the existing literature of internal control system for assessing the reliability of accounting system based on SysTrust's model, this study developed a theoretical model to test the research questions and the hypotheses. Punch (2013) maintained that to be in line with research questions, the method used to conduct the research should be targeting this objective. Thus, this thesis employs quantitative method to test the hypotheses first, and then to answer the research questions. i.e. the research is quantitative and action based to validate the proposed integrated model.

5.4 Research Paradigms

It is of importance to consider the paradigm that is most suitable to the study prior to discussing the method applied in the current research. In all areas of the study, the research process vitally depends on selecting the appropriate research paradigm (Mangan, et. al., 2004) due to its important role in understanding the phenomenon in question, especially if it is related to human and social sciences (Crestwill, et al, 2009). As indicated by (Weaver and Olson, 2006). Paradigms are "patterns of beliefs and practices that regulate inquiry within a discipline by providing lenses, frames and processes through which investigation is accomplished. A number of purposes are served by a paradigm; namely. (1) Guiding professionals by indicating important issues that challenge any discipline; (2) Developing models and theories for practitioners to solve these issues; (3) Establishing criteria for tools such as methodology, instruments, and data collection that would enable solving these issues; (4) Providing the principles, procedures, and methods to be considered when similar issues (phenomena) appear again" (Sekaran and Bougie, 2010). According to Neuman (2006), positivist social science is widely used and the positivism paradigm forms the basis of natural science and has influenced scholars as a rational system. Within this paradigm, the focus of researchers is mainly on facts and direct cause and effect, while remaining external to the events being examined. Formulated hypotheses are involved in this paradigm as a process of problem solving. However, they are subject to empirical testing through a quantitative approach. The quantitative approach provides objective, value-free and unambiguous interpretation of reality (Guba and Lincoln, 2005). Accordingly, as long as there is evidence of formal propositions, quantifiable measures of variances, hypothesis testing, and the

drawing of inferences about a phenomenon from the population sample, information system research has been classified as positivist (Walshem, 2006).

As discussed by the underpinning of the positivism paradigm and based on the idea that interaction should be made between research questions and the conducted research methods, the study seeks to measure underlying variables, as the “measurement of the variables in the theoretical framework is an integral part of research and an important aspect of quantitative research design” (Sekaran and Bougie, 2010). The aim of research in positivism is to explain in order to predict and finally control the researched phenomena. From this point of view, positivism in this research applies a quantitative method to test hypothetical deductive generalizations of the theory. Regardless of the criticism in terms of its ability to produce theory and generate in-depth explanations of qualitative enquiry, the quantitative approach is able to verify the hypotheses and provide strong validity and reliability (Sekaran and Bougie, 2010). Prior studies have applied this methodology which has been successfully used in similar studies (Buonanno, et. al., 2005). Consequently, this methodology was mainly seen as suitable given that the objective of the research is to empirically investigate causal relationships among the underlying constructs. Based on the above, this study is best classified as using a positivism paradigm and, therefore, for this study, the researcher decided to choose a quantitative rather than qualitative approach. The research objectives and questions are summarised in Chapter 1.

5.5 Research Design Process

As it sought to describe and establish the relationships among the study variables, this study used descriptive correlational survey design. A research design is the arrangement of conditions for the purpose of data collection, measurement and analysis to combine relevance to the research purpose Kothari (2010). Moreover, a researcher is allowed through the correlational survey design to measure the research variables by asking questions to the respondents and then examining their relationship (O’Connon, 2011). Given that the quantitative method is considered appropriate for this research, the research design involves a series of rational decision-making alternatives which suggested by Sekaran (2013), are generally related to the purpose of the study (exploratory, descriptive, hypothesis testing), its location (i.e., the study setting), the type of investigation, the extent of researcher interference, time horizon, and the level to which the data will be analysed (unit of analysis). In addition, decisions have to be made regarding the sampling design, how data is to be collected (data collection methods), and how variables will be measured and analysed to test the hypotheses (data analysis). Research design is another

critical element for enhancing conducting a good scientific research, many researchers concentrate about the importance of research design. Bryman and Bell (2007), for example, stated that research design provide the researcher with data collection methods such as self-completed questionnaires or structured interviews and the needed data analysis tools from one side, it also determines research process dimensions priorities from the other side, while De Vaus (2001), clarified that research design guaranteed that the research instruments and tools and analysis can answer the study questions and test its hypotheses. Bryman and Bell (2007) argued that a framework for data collection and analysis is provided by research design, which reflects decisions about the priority in the research process for a range of dimensions. According to them, research methods are considered as the techniques for data collection, including specific instruments such as self-completed questionnaires or structured interviews. De Vaus (2001) argued that “the function of a research design is to ensure that the evidence obtained enables us to answer the initial question as unambiguously as possible”.

According to Sekaran (2013), the methods are part of the design; thus, she supports the view of Bryman and Bell (2007) that data collection is meant to be described by methods. Based on Sekaran’s definition of research design, this study is conducted for the purpose of testing the hypotheses derived from the conceptual framework presented. Studies employing hypotheses testing purpose are believed to tend usually to explain the nature of certain relationships or establish the differences among groups or the independence of two factors or more in a situation. Hypotheses testing offers enhanced understanding of the relationships existing among variables. With respect to the type of investigation, a correlation study is chosen for the purpose of delineating the variables associated with the research objectives and identifying the most important (strengths and direction) components of the SysTrust model in assessing the reliability of AIS in Jordanian business organisations. In terms of the settings, this study is conducted in a non-contrived setting. It is considered a field study with minimal interference from the researcher. The study’s horizon refers to conducting a longitudinal versus cross-sectional study. This study is a cross-sectional survey in which data is collected at one point in time from the population to determine relationships between variables at the time of the study. Even though the researcher acknowledges the limitations of this type of investigation, it is beyond the timeframe of this research project to make use of a longitudinal study. In conclusion, a research design is a connection between what has been established (the research problem and objectives) and what is to be done in the conduct of the study. Without explicit design, the researcher would be left with only foggy notions about what to do. Based upon the research objectives and hypotheses, the research design for this study involves the following process.

5.6 Data Collection Methods

The data required for this study is categorised into two main types: Secondary and primary data. Secondary data is defined as “data that have already been collected for purposes other than the problem at hand “(Hair, et al., 2017). Secondary data offer several advantages over primary data. Secondary data are easily accessible, relatively inexpensive and quickly obtained besides time and cost saving, secondary data has other advantages over primary data. The secondary data used in this study is related to the existing literature concerned with the research problem. The purpose of using those sources of information was to have a better understanding of the problem, and to determine the required data as well as the suitable method for data collection. However, because secondary data have been collected for purpose other than problem at hand as mentioned above, their usefulness to the current problem may be limited in several important ways, including relevance and accuracy. Therefore, and despite time and cost, there was no alternative but to conduct a field study to collect the primary data required for this study.

Primary data can be obtained through experimentation, analogies and (questioning) survey method. The experimentation and analogous tools were inappropriate because of the limits of time and budget. Therefore, the survey method was selected. Primary data collection methods are classified into two major categories: survey and observation. In the survey approach respondents play an active role, while in the observing approach respondents do not directly interact or communicate with the research (Cooper and Schindler, 2008). The survey approach was considered more appropriate for this study because of time limitations along with the numbers of and types of variables that needed to be measured.

5.7 Types of Questioning Methods

According to Sekaran and Bougie (2010), different methods for data collection are employed through AIS research. In addition to focus groups and depth interviews, surveys are also common and popular. Surveys range between the use of non-internet survey forms and Internet survey methods. The administration of the first type of surveys can be made through a number of techniques. Door-to-door interviews (rarely used today) and the equivalent “executive interviews” when the sample consists of managers, mall intercept interviews, telephone interviews, self-administered questionnaires, ad hoc mail surveys, and mail panels. Sekaran and Bougie (2010) adds observing people and phenomena as means to survey data collection methods, stating that each method has its advantages and disadvantages. In this research,

personally administered were preferred to the postal interview alternative. The reasons for section the questionnaire survey are:

1. The questionnaire survey is an effective and efficient research tool for measuring respondents' thoughts and is associated with both positivistic and phenomenological methodology.
2. The survey questionnaire allows us to ask a relatively larger number of questions. Clarification and follow up remarks were also possible to supplement the information collected.
3. One of the objective of this tool is s to collect information that could be confidential by some business companies such as the type of internal control accounting system, company IT resources, IT budget, and so forth. This type of information is difficult to be granted by the postal questionnaire.
4. The appointments were pre-organized by telephone calls directly with the persons concerned. Thus, and by personal interview, a relatively higher percentage of response can be gained by this method
5. Identity of the respondents could be confirmed and general information about the respondents could be collected.
6. It was expected that business employees would be more forthcoming in personal interviews. In fact, the researcher's prior experience in Jordan indicates that Jordanian business employees would feel more comfortable with personal contact than indirect approaches.

The disadvantages of a personal interview using direct questionnaires are relatively limited. The most important disadvantage can be overcome by presenting the respondent with the questionnaire and asking them to complete it by themselves.

5.8 Structure of the Interview

Structured and unstructured, or standardised and unstandardized are two major types' interviews. Sekaren and Bougie (2010) defined the structure as "the degree of standardization imposed on the questionnaire". Directness is the amount of information about the purpose of a study communicated to a respondent. In this study, the structured-direct technique is used, with the necessity in this tool to present the questions to all respondents with exactly the same wording and order. The reason for standardization is to ensure that all the respondents are replying to the same questions. Besides, the other major advantages of using the standardised - direct interview are: simplicity of administration and ease of tabulation.

5.9 The Domain of Respondents

As discussed in the previous section, it is decided that a field study is necessary for the current study's objectives. Because this study is mainly concerned with the investigation of the reliability of AIS in shareholding companies, other non-shareholding companies were not included. Because of the limitation of the statistical population, sampling was not done and the whole population was selected as research sample. This population was selected because their information was more accessible from the database of Amman Stock Market. The survey units in this study are the individual business firms which were chosen in light of the nature and the objectives of the study. In other words, the investigation was conducted at the micro level. Recognizing the individual business firms in the country (Jordan) could be done by obtaining names of all firms, as well as their addresses, from a variety of private and public sources in order to identify the type of the business sector, and the number of firms in each sector. Since time and financial resources restrictions made the inclusion of all business organizations impossible, the target population is limited only to the shareholding companies listed in the Amman Stock Exchange Market database in 2016. Table 5.1 demonstrates the domain of the study's population and the number of respondents.

Table 5.1 The Domain of the Study's Respondents.

Type of Sector/company	Number of Companies	Number of Respondents*	Percentages
Services	202	162	0.80
Industries	126	77	0.61
Total	328	239	0.73

Sources: ase.com.jo 2016

5.10 Key Informant Approach

Being the major source of data, careful attention should be paid in the selection process to individuals to whom the self-administered questionnaire is subsequently directed. As suggested by Campbell (2009), the informants would be chosen because they possess special qualities, but not for statistical representativeness. Such informants should occupy a role that guarantees more knowledge about the issues under the study, and more capability of "speaking the language of the researcher" (Campbell, 2009). Sekaran (2013) is with the view that a single key informant is to be used, where most of the informants occupy top executive or ownership positions. He argued that directors of financial accounting at the higher level of management are the key figures in dealing with the accounting and financial issues are

suitably qualified to speak on behalf of the firm. However, these views have faced some criticism (Wagner, et al., 2010) with the point of view that a single or a few informants lack the capability of providing reliable data. Although there is still some argument regarding the particular reliability of the key informant, the target respondents for this study should be essentially the chief executive managers, Heads of Internal Audit or financial managers rather than lower level users of the system. This is because the type of information sought necessitates that the respondent is a person occupying a position that makes him knowledgeable of AIS applications and their reliability, in addition to being a firm's policymaker whose decision will have a strong influence on the direction the firm will pursue. Financial managers are also the persons who influence on the AIS decision making. Compared to their counterparts in the Western countries, shareholding companies in Jordan are relatively small (in terms of the number of employees and capital assets). Furthermore, due to the relatively long time and high cost associated with the use of the multiple informant approach, it is essential to rely upon a single informant for collecting data for this study. In addition, this notion was supported by previous works on the adoption of AIS by claiming that the directors or managers of financial managers should be the key informant in this type of study (Campbell, 2009). This selection is also based on the fact that they are supposed to be well-informed about the questions under investigation. As a result, an effort was made to access the person at the higher level of management of the individual firm, i.e., the general manager or the director of financial management.

5.11 Scale of Measurement

Measurement is defined as "the rules for assigning of numbers to objects in such a way as to represent quantities of attribute" (Churchill Jr and Iacobucci, 2009). There are four general levels of measurement, nominal, ordinal, interval and ratio. However, the selection of the appropriate level of measurement is difficult. This arises mainly from disagreement over the statistics that can legitimately be used at the different levels of measurement. Churchill and Iacobucci (2009) suggested that the empirical evidence indicated that, "None of the scaling devices is superior in all instances; each one does not have its place nor is there one single optimum number of scale positions or single optimum conditions for other measured characteristics". The nature of the problem, the characteristics of the respondent and the planned mode of administration will and should affect the choice as to which technique should be used in a particular instance and what features the scale should possess".

In the first part of the questionnaire, the nominal scale was employed to cover the firm's parameters. Though this scale is the simplest amongst those available, it is appropriate for such data category (e.g., the type of business, business experience, etc.). The questions in the nominal scale cannot be used for normal arithmetic calculating, adding, subtracting, multiplying or dividing. The 7-point rating scale is used in the second, third and fourth parts of the questionnaire. The justification for using this type of scale was as follows: (1) it is relatively easy to construct and administer, and (2) subjects generally find it easy to respond to because the response categories allow sufficient expression of intensity of feeling (Aaker, 2011). Furthermore, the selection of the 7 point rating scale is based on the fact that empirical studies, such as the one conducted by Aaker (2011), have suggested that scales with three or more points can, and do, provide a valid measure. Furthermore, in discussing the validity and reliability of different scales, (Sekaran and Bougie, 2010) concluded that the reliability of different scale as well as the number of the scale points increased. On the one hand, any rating fewer than seven points would reduce the scale's ability to discriminate, since the respondent would be less able to express refined gradations. Conversely, more than a seven-point scale would be less than the optimum, because of the limited increase in information gathered. Lehmann and Hulbert (1972) commented. “. Increasing the number of scale points reduces the rounding error as benefit, but may also increase the cost of administration, non-respondent bias and respondent fatigue, since averaging tends to reduce the rounding error. When scale points aim to be averaged, the cost of increasing the number of scale points will usually out-weight the benefit". A large amount of researchers use this methodology, because it is relatively easy for respondents to use, and responses from such a scale are likely to be reliable (Balzan and Baldacchino, 2007; Lam and Kolic, 2008).

5.12 Pilot Study: Methodology

As indicated in the previous section, the content of the study's questionnaire is based on a review of related literature on accounting internal control and SysTrust's model. In the first stage, the first copy of the questionnaire which was developed, designed and translated into English, was reviewed by the researcher's supervisor. The questionnaire was then redesigned in the light of their suggestions and comments. At the second stage of the pre-test, six professors of accounting in public and private universities in Jordan, who are knowledgeable in AS in questionnaire design, reviewed the questionnaire and commented on its clarity and relevance. After incorporating their comments in a revised questionnaire, stage three of the pre-test was carried out on few responding firms. A convenience sample of 10 accounting managers of shareholdings companies were contacted, and only 7 of them were able and

willing to participate in the interview (five from services companies and two from industrial companies). The Feedback from all the responses unanimously showed that participants agreed on the clarity of the instructions of the questionnaire, simplicity of the questions and finally the attractiveness of the questionnaire layout. The validity and the content of the questionnaire were investigated through open-ended interviews. This procedure allowed the researcher to check for possible misunderstandings, and to assess the subjects' willingness and ability to respond to the questions. As a result of this stage, the questionnaire was re-edited for the final stage.

5.13 Development of Questionnaire Items

To draw up appropriate questions for the questionnaires in this study, key variables from the literature review on accounting internal control, quality of financial reporting and business performance as well as the components of SysTrust model (See Chapter 2 and Chapter 3). The constructs, measurement variables, items code, item descriptions and measurement scale of the questionnaire are summarised with references in Appendix A. Variables used in the identification the level of reliability of AIS which affect the quality of financial accounting and business performance by target organizations consisted of independent, mediating and dependent variables.

5.14 Ethical Considerations

This section describes why maintaining ethical standards must be ensured to achieve moral research (Neuman, 2006) and make the right or most appropriate decision (McMurray, et. al., 2004). To achieve these outcomes, the current research followed the ethical guidelines of the research conducted by Brunel University. Essentially, the study obtained the committee's ethical approval prior to the data collection process being assumed (see Appendix B). Participants will be provided with detailed information about the research themes and objectives. They were also informed that the collected data and findings will not be used for any reasons other than the research as specified. For ethical issues, all questionnaires were distributed and gathered without name and identification of participants. The data gathered was used only in forms of statistical information and all participants were informed about it. The research will be conducted with integrity and will not undertake for personal gain. The research has no negative effect on the respondents. The researcher will not abuse the trust of the subjects by using the data collected to get somebody into trouble or to stigmatize them. Researchers are highly recommended to pay attention to disclosure as an important ethical standard in conducting scientific researches (Bhattacharjee, 2012). Disclosure normally

requires the researchers to provide the respondents with sufficient information explaining to them the nature and the aim of study which is targeted by the data collection process. In line with Bhattacharjee's remarkable, such information is important as it has to be provided to potential respondents prior to the collecting of data so as to enable them to make a decision whether to be a part or not be a part in the research. In the current study, the researcher explained to the respondents that the current survey is part of a PhD study examining the relationship between the implementation of SysTrust principles, quality of financial reporting and business performance. Such information included the researcher's e-mail, phone number, and the name of the institution (i.e. Brunel University) where this study was being conducted and such information was provided on the questionnaire's cover page.

5.15 Preparing for Data Analysis

Before beginning data analysis process, it was important to undertake the preliminary steps of editing, coding, and tabulating the data (Al-Dmour, R., 2014). Editing refers to the process of inspecting completed questionnaires and making whatever corrective action needed to ensure that the data is of a high quality. Editing is frequently done in two stages, field editing and central – office editing. Field editing is a preliminary check intended to identify and handle the most clear omissions, obscurities, and mistakes. In this study, effort has been made to keep the data accurate. Office editing encompasses a more complete and exacting scrutiny and correction of the completed and returned. There are five issues with which the editing function should be concerned. These include legibility, completeness, consistency, accuracy, and response classification (Bryman and Bell, 2007) .

In this study, a large of editing work was conducted by the researcher himself. All the surveys were examined to guarantee that they were appropriately filled in, and that no noteworthy omissions were made. Questionnaires that appeared to be hastily filled in (for example, by assigning number 7 for all the variables) or partially filled out by leaving any questions unanswered were excluded from analysis. However, if the left out questions in a partially-completed questionnaire were few, the questionnaire was used in the final analysis and the unanswered questions were assigned a missing value. Coding and entering the data. coding means translating answers into both class membership and a symbolic representation of this membership usually by means of a column and position designation on a punch card used for machine tabulation (occasionally, coding is used in manual tabulation, but this is more of a type of shorthand of a truly symbolic code). In this research, the coding was done manually. There was little difficulty in coding the questionnaire, since most of the questions were to be

rated on a scale of seven points, but the other questions related to the firm's parameters were categorically measured. Each edited and coded question was transferred to a coding sheet. Every completed and edited coding sheet was sent directly to the computer and copied onto computer diskettes on a mainframe.

5.16 Classification of Statistical Techniques

As suggested by business research literature, there are different statistical methods for data analysis which can be grouped into three techniques according to the type of data and number of variables (e.g., Sekaran and Bougie, 2010); namely, univariate, bivariate, and multivariate. As for the Univariate technique, it is used in the case of a single measurement of each of the sample objects or if there are several measurements of each of the observations. The central tendency measures (mean, median and mode) and the measures of dispersion (standard deviation, relative and absolute frequencies), as well as the T-test, F-test, are among the suggested techniques are used. With respect to the multivariate analysis technique, it is concerned with the investigation of interaction among a set of variables. The multivariate technique can be classified as either dependent or independent method. For the first method, it implies that one or more variables are specified as being predicted by a set of independent variables. It might include analysis of variance (ANOVA), analysis of variance and covariance (ANCOVA), and stepwise multiple regressions.

The dependent method might include analysis of variance (ANOVA), analysis of variance and covariance (ANCOVA), and stepwise multiple regressions. In this research, the decision was made to use a combination of the above data analysis techniques. The chi-square test and T-test were used from the univariate statistical methods, while the factor analysis and regression analysis were used from the multivariate techniques. For the selection of these statistical techniques, the following criteria were used as stated by Blumberg, Cooper and Schindler (2008) for the selection of the appropriate technique depends on:(1) The type of data (nominal, ordinal, interval and ratio), (2) The research design (dependency of the observation, number of observations per object, number of groups being analysed) and (3) The assumptions underlying the test statistics. This research focuses on the investigation of the effect of the reliability of AIS, the quality of financial reporting and business performance. A seven-point scale which was assumed to have an interval property was used to measure the variables, with the necessity to use various statistical techniques suitable for each level.

5.17 Statistical Methods Used for Research Objectives

5.17.1 Factor Analysis

Factor analysis is an interference multivariate technique, which can be defined as a procedure entailing a large number of variables or objects to see if they contain a small number of factors in common that account for their inter-correlation. The common factor analysis assumes that each variable is a function of the same set of underlying common factors plus a factor unique to that variable. However, there is a different set of weights associated with the factor analysis for each variable (Sekaran and Bougie, 2010). The interest in applying factor analysis is to examine the strength of the overall association among the variables in terms of a smaller set of linear composites of the original variables that preserve most of the information in the full data (Hair, et. al., 2014).

The input of factor analysis is usually a set of variables values for each individual or object in the sample. In this present research, the input is a set of attributes that relate to search construct alone. In other words, the variables which express each construct of the SysTrust (principles and criteria) were used as inputs for factor analysis. Factor analysis uses a derived matrix of correlation, the components of which provide a measure of similarity between variables. Factor analysis has value only when correlation amongst a subset of variables really exists. The higher these inter correlations are, the better defined are the resulting factor dimensions. The most important outputs are factor loading, factor scores and variance explained percentages. Each of the original variables has a factor loading on each factor. The factor loading is the correlation between the factors and the variables. These are used to interpret the factors. Furthermore, the nearer to one the factor loading is, the stronger the association between the variable and the factor (Blumberg and Schindler, 2008; Cooper & Schindler 2008). Normally, factor loadings are crystallised by using a rotation procedure, the most commonly used one is the Varimax orthogonal rotation which attempts to produce some high loading and some near zero loading on each factor. The Varimax orthogonal rotation method is preferred when the objective is to utilize the factors results in a subsequent statistical analysis (Hair et al.2010). This is because the factors are orthogonal (uncorrelated) and therefore eliminate the collinearity.

Factor analysis was conducted to assess how well each of the questions measured the independent variables. According to Rea and Parker (1992), “the main applications of factor analytic techniques are: (1) To reduce the number of variables and (2) To detect structure in the relationships between variables, that is to classify variables. Therefore, factor analysis is

applied as a data reduction or structure detection method” (StatSoft, 2010). Combining two (or more) correlated variables into one factor, illustrates the basic idea of factor analysis, or of principal components analysis to be precise (Statsoft, 2010,). Principle components analysis (PCA) is a common technique for finding patterns in data of high dimension (Leedy and Ormund, 2005). Thus, for each of the independent variables, the items on the survey were assessed with PCA to determine if they are measuring the same factor or component. Factor analysis was used in this study for the following objectives.

1. To find out the main factors that underlie each construct (principle) of the SysTrust’s model as well as the main the factors that underline the quality of financial reporting measures and business performance measures.
2. To use the output of factor analysis as an intermediate step for further analysis by regression. It is decided that the cut-off point for the factor loadings should not be less than .30. The rationale for this is that those variables which load above or equal .30. On any factor are considered significant (Hair, et. al., 2010).
3. To overcome the potential problem of Inter-correlation among independent variables, i.e., the multicollinearity problems.

5.17.2 Multiple Regression Analysis

Multiple regressions are a multivariate statistical technique through which one can analyse the relationship between a dependent or criterion variable, and a set of independent or predictor variables. Multiple regressions can be viewed either as a descriptive technique by which the linear dependence of one variable on another is summarised and decomposed, or as an inferential tool by which the relationship is the population evaluated from the examination of sample data.. Multiple regression is the appropriate method of analysis when the researcher has a single dependent variable which is presumed to be a function of other independent variables. Usually, the dependent variable is predicted or explained by a group of independent variables Bryman and Bell (2007) have suggested two different concepts of independent variable on the basis of the study’s goal. Firstly, the independent variables (explanatory), sometimes, called the predictor variable when prediction is the goal. They help to predict the value of dependent variable (criterion). Secondly, they are called explanatory variables because they explain variation in the dependent variable. When constructing the model, the analyst must include all relevant variables. If an important variable is omitted, the power of the model is reduced.

As for variables, the larger of the beta coefficient, the stronger is the impact of that variable upon the criterion variable. In addition, the Beta weight enables the analyst to see how well a set of explanatory variables explain the criterion variable, and to determine the most influential explanatory variables. The simple R^2 (the coefficient of multiple determination) through which one can measure the proportion of the variation in the dependent variable, tends to overestimate the population value of R^2 . Therefore, adjusted R^2 attempts to correct the optimistic bias of the simple R^2 . Adjusted R^2 does not necessarily increase as additional variables are added to an equation and is the preferred measure of goodness of fit because it is not subject to the inflationary bias of unadjusted R^2 . In summary, multiple regression is often used to gain an understanding of the relationship between variables by (1) Finding a function or formula by which one can estimate the value of the criterion variable from the predictor variable (Hair, et. al., 2010), and (2) Determining which of the independent variables has the greatest influence upon the dependent variable (Hair, et. al., 2010).

However, the use of multiple regression analysis is not without disadvantages: One of the most common problems in applying regression analysis is the multicollinearity. Multicollinearity refers to the situation in which some or all of the independent variables are very highly correlated. In other words, when independent variables are related to each other and not truly independent of each other, multicollinearity is said to exist. Such correlation between the explanatory variables in the regression equation makes the identification of structural relationship difficult or impossible. Bryman and Bell (2007) distinguished between two forms of multicollinearity. The first form is perfect Collinearity in which some independent variables regressed against the other independent variables in the model yield an R^2 of precisely 1.00. This arises from very small data sets (i.e., small samples). The second is less extreme multicollinearity in which the independent variables in a regression equation are inter correlated but not perfectly. The study of multicollinearity in data analysis revolves around two major problems. (1) How it can be deleted, and (2) What can be done about it. These problems are particular to business research where one often faces the dilemma of needing a number of variables to achieve accuracy of explanatory variables (Bryman and Bell, 2007). Multicollinearity can be dealt with by different approaches. Hair et al, (2010) suggested several ways for dealing with such situations. First, it can be ignored, particularly when multicollinearity may be prominent in only a subset of the explanatory variables and when this subset does not account for a large proportion of the variance in the data. The second approach is to omit one or more of the highly correlated predictor variables. This one is recommended when two variables are clearly measuring the same thing. Thirdly, the

correlated variables can be combined or otherwise transformed, to produce unrelated variables that can be summarised in a set of explanatory factors using factor analysis. Furthermore, Bryman and Bell (2007) add that another way to avoid multicollinearity is by increasing the sample size. In this research, the use of the principal components analysis technique was the only possible way to overcome the potential problem of multicollinearity. The regression analysis techniques (stepwise regression method) was preferred here since it fulfils the requirements of the study objectives as shown in Table 5.1 The primary purposes behind using this technique are:

1. To find out statistically whether there is a significant relationship between the level of reliability of AIS (i.e., sets of SysTrust factors/**independent variables**) and the **dependent variable** the quality of financial reporting.
2. To find out statistically whether there is a significant relationship between the level of reliability of AIS (i.e., sets of SysTrust factors/ **independent variables**)) and the **dependent variable** business performance (financial and non-financial).
3. To conclude whether these explanatory variables (taken together) are strongly relevant to the business performance or quality of financial data reporting.
4. To determine the most important independent variables (sets of SysTrust factors) explaining the variation of each dependent variable (business performance or quality of financial data reporting).

5.17.3 Artificial Neural Networks Model

An artificial neural network (ANN) is mathematical model representing a massively parallel, distributed processing systems inspired by the neural network of the human brain (Haykin and Network, 2004, Greenwood, 1991). Learning in biological systems involves adjustments to the synaptic connections that exist between the neurones. The neural network approach was originally proposed to solve problems in the same way that a human brain would. The key feature of such a approach is the novel way of processing information (Greenwood, 1991). An ANN model is composed of a large number of highly interconnected processing elements (neurones) working in parallel to solve complicated problems (Haykin and Network, 2004). According to computer-based learning model, there are three models namely, supervised learning, unsupervised learning and reinforcement learning. The ANN model is considered as a supervised-based learning model, where the learning is done based on pre-existed examples called training data. An ANN can be configured for a specific application, such as pattern recognition or data classification, through training or learning processes. An ANN is often applied to model complex relationships between inputs and

outputs or to find patterns in data. An ANN model is normally divided into three layers, namely, input layers, hidden layers, and an output layer. The nodes in each layer are assigned weights (synaptic weight), and a layer or a node has an associated linear or non-linear activation function (Chong 2013; Sharma, Govindaluri, and Al Balushi 2015). The activation function used in the ANN model is often a sigmoid function such as a hyperbolic tangent (Bakar and Tahir, 2009, Murtagh and Heck, 2012). These weights will be transferred to the hidden layers which consist of several hidden node. A hidden layer is utilized by ANN as feed-forward process with x_1, x_2, \dots, x_n as inputs and y_k as the output. The weights are assigned to each input node and are transferred to the hidden layer that are made of a number of hidden nodes.

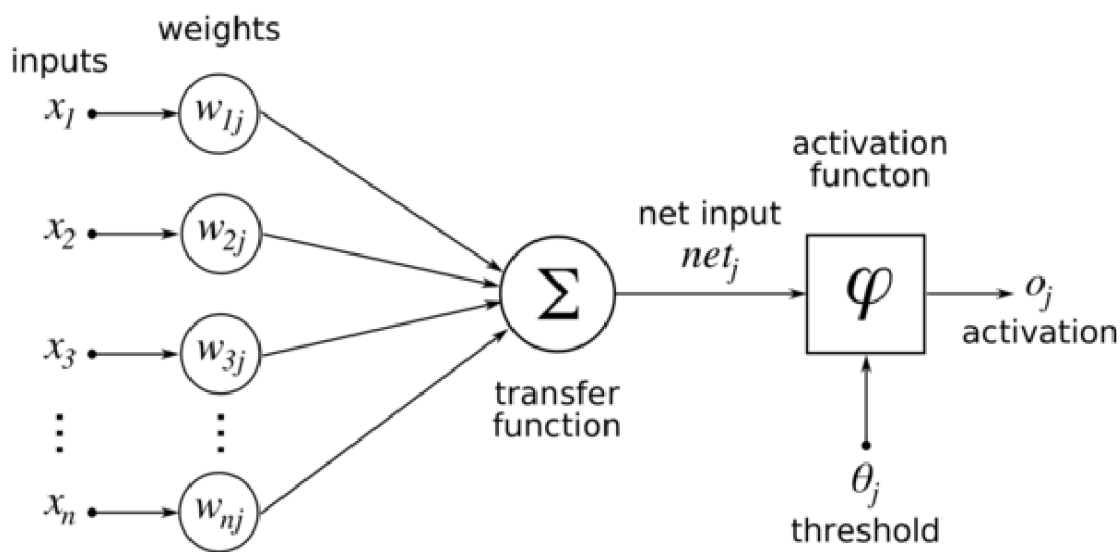


Figure 5.1 Simple Neural Network Topology.

*Source; Mousavi, et. al., (2008), p.134

The output of ANN is estimated based on the weighted sum of inputs and the nonlinear activation function of hidden layer(s) and is given as follows:

$$f(x) = \vartheta \left(\sum w_{xi} g_i(x) \right),$$

*Where $\vartheta(v)$ is predefined function that commonly referred to as activation function, w_{xi} is the synaptic weight between output of node x and input of node i .

The ANN model is employed in different information systems fields including e-commerce and e-learning domains because of its computational power and the ability to handle various type of data (Chong, 2013, Shmueli and Koppius, 2011, Doherty et al., 2015, Scott and Walczak, 2009). Furthermore, the ANN models offer various advantages over traditional statistical models, they are considered as non-parametric based models, as there are no

predefined assumption regarding the distribution of the input data is given and able to capture linear and nonlinear relationships. In contrast, traditional statistical models, such as regression model, are regarded as parametric based models where the assumption of a predefined distribution of the data is given (Hair et al., 2010, Chong, 2013). This study employs neural network to predict the factors (SysTrust) that influence business performance. The results from the neural network will then be compared to the ones obtained from multiple regression analysis in order to determine which one offers better predictive power.

5.17.4 Structural Equation Modelling

The study is applying the Structural Equation Modelling (SEM) technique to test the proposed theoretical relationships among the constructs in the model. This technique is considered to be an appropriate statistical technique for validating the conceptual model and for testing the research hypotheses. Malhotra, et. al. (2013) have defined the SEM as a. *"...is a procedure for estimating a series of dependence relationships among set of concepts or constructs represented by multiple measured variables and incorporated into an integrated model."* The rationale for considering SEM as the most appropriate statistical technique is explained here. Basically, the SEM is able to perform the following functions;

1. Examine several inter-related associations between observed variables (indicators) and non-observed variables (latent constructs) simultaneously (Hair, et. al., 2010). Such of these examinations could be conducted using the confirmatory factor analysis (CFA) (Byrne, 2010).
2. Verifying the causal relationships between the latent constructs using the structural model analyses; this is useful for testing the hypotheses and validating the conceptual model proposed (Byrne, 2010; Kline, 2005).
3. Examining the unidimensionality, reliability and validity of each construct individually
4. Evaluating how closely a model fits the observed data, as well as being able to evaluate both measurement error and error variance parameters.

Complex models which include a number of causal relationships can be readily administrated using the rigorous statistical techniques found in SEM (Hair, et. al., 2017). SEM is a more suitable analyses method in the case of confirmatory studies, Byrne (2010) also sees SEM as "a statistical confirmatory method testing hypotheses and analysing a structural theory that is related to a particular problem. According to Hair, et. al. (2017), SEM is used to test theoretical models. A structural equation model normally consists of two types

of approaches, the one-stage approach or the two-stage approach. For the one-stage approach, both the measurement model and the structural model are concurrently assessed. For the two-stage approach, the initial step is to calculate and identify (if required) the measurement model estimates; this is followed by examining the structural model in the second stage (structural model). In this study, the two-stage approach has been adopted. This is because the two-stage approach is abler to provide further accuracy in estimating the validity and reliability of each construct rather than the one-stage approach (Hair, et. al., 2017). Further, analysing of the causal relationships in the structural model requires examining the measurement model first, since the measurement model represents a condition that must be satisfied as a matter of logical necessity. In the first stage of the two-stage approach, the constructs' reliability, validity and model fitness were inspected; this is also referred to the confirmatory factor analysis (CFA) (Hair, et. al., 2017). In the next stage, the structural model was to be assessed by examining causal hypothesised paths between the main independent (exogenous) and dependent factors (endogenous). As discussed in Chapter Four entitled 'The Stusy's Conceptual Framework', the main exogenous constructs are the main five components of the SysTrust model (Availability of AIS, Security, Integrity processing, Confidentiality and Privacy) the endogenous constructs are the quality of financial reporting and business performance.

(1) Measurement Model (Confirmatory Factor Analysis): The confirmatory factor analysis (CFA) is employed to evaluate the model fitness, and then to measure the constructs' reliability and validity. If the statistical results indicate that the measurement model does not adequately fit the observed data, further modifications and re-specification should be made on the measurement model (Hair, et. al., 2017). Noteworthy, the main aim of this study was to reach a model that is able to provide sound logic and theoretical evidence to demonstrate the causal relationships among the constructs, as well as statistically fit to the observed data. To conclude, both theoretical and statistical considerations have been taken into account when re-evaluating and respecifying the measurement model in the current study. Basically, a refinement process followed a number of criteria to enhance the model's fitness including the inspection of standardised regression weights (factor loading), modification indices, and standardised covariance matrix. The maximum likelihood estimators (MLEs) are considered to be suitable for parameter estimates, particularly for sizeable samples (Anderson and Gerbing, 1984). MLEs have been widely used for carrying out the SEM analyses on SST studies (Weijters, et. al., 2007). For the above reasons, the MLE has been adopted to conduct an SEM analyses in this study.

Assessment Model Fitness: There are three types of fit indices that have been suggested and considered to assess the model fitness in the current study; they are absolute fit indices, parsimonious fit indices, and incremental fit indices (Byrne, 2010). Further discussion regarding each criterion adopted with their cut-off values are provided below:

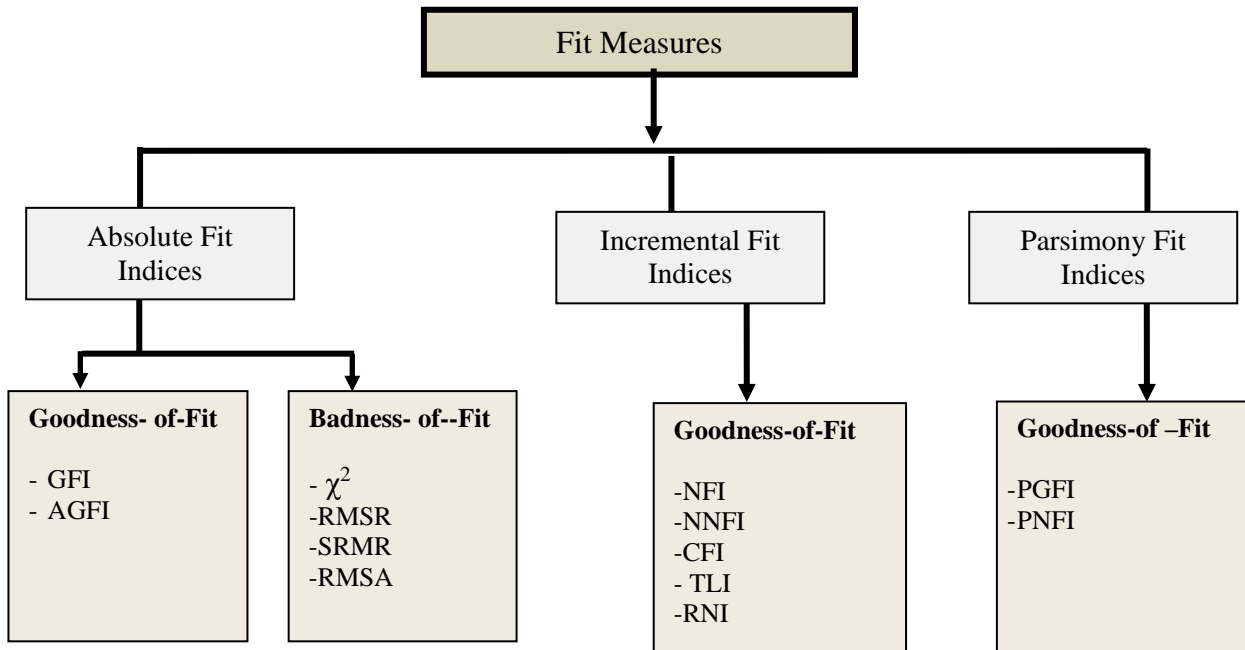


Figure 5.2 A classification of Fit Measures

**Source: Byrne, 2010, p 186*

The goodness of fit of a certain model is able to be assessed independently of any other models using absolute fit indices (Hair, et. al., 2017). Basically, the absolute fit indices allow for an indication of how well the proposed theoretical model fits the data. In contrast to the incremental fit indices, absolute fit indices can be conducted without carrying out comparisons with baseline models (Hooper, et. al., 2008). What they measure is how well the specified model fits when compared to the absence of a model. Chi-Square value (χ^2), Goodness of Fit Index (GFI), Root Mean Square Error of Approximation (RMSEA), and Adjusted Goodness of Fit Index (AGFI) are all used as the absolute fit indices in the current study:

1. Chi-Square value (χ^2) test provides a statistical test for the differences in the covariance matrices. A good fit for a model is deemed to be the case when the value of Chi-Square is insignificant; this is at a threshold of 0.05 (Barrett, 2007). Thus, the value of Chi-Square is used by researchers as one index for testing their models, and other indices are to be used alongside it to estimate the overall model fit.

2. The Goodness-of-Fit Index (GFI) is introduced as an alternative to the Chi-Square (Hooper et al., 2008). The test is used to give an estimate of the amount of variance that can be ascribed to the population covariance (Tabachnick and Fidell, 2007). The examination of the variances and covariance accounted for by the model reveals how accurately the model is able to replicate the observed covariance matrix (Diamantopoulos and Siguaw, 2000). A value of 0.90 or above has been reported as a common rule of thumb indicating a model's fitness (Hair, et. al., 2017), and accordingly, this value is adopted in the current study.
3. The Adjusted Goodness of Fit Index (AGFI) uses degrees of freedom to adjust the GFI; generally, the more degrees of freedom, the worse the model fit (Tabachnick and Fidell, 2007). An AGFI value of 0.80 was considered a cut-off value indicating a good fit model (Hair, et. al., 2017).
4. Root Mean Square Error of Approximation (RMSEA) allows for uncertainty due to estimation to be accounted for (Hair, et. al., 2017). The RMSEA value from 0.05 to 0.10 is an indication of a fair fit, with values above 0.10 indicating a poor fit (MacCallum, et. al., 1996). Values from 0.08 to 0.10 suggest a mediocre fit; while a RMSEA value below 0.08 was highly reported as a good indication of the model fitness (Hair, et. al., 2017), and therefore, a RMSEA value less than 0.08 was adopted in the current study. The next type of fit indices adopted in the current study is associated with incremental fit indices; they can also be called comparative (Miles and Shevlin, 2007) or relative fit indices (McDonald and Ho., 2002). They form a group of indices that use a baseline model for comparison with the Chi-Square value, rather than using the Chi-Square in its 'raw form' (Hooper et al., 2008). Here, the null hypothesis is that there is no correlation between any variables (McDonald and Ho, 2002).
5. A Normed-fit Index (NFI) and Comparative Fit Index (CFI) are both used as incremental fit indices in the current study (Hair, et. al., 2017). A Normed-fit Index (NFI) takes the Chi-Squared value of the model, along with the same for the null model in order to compare them (Hooper, et. al., 2008). The null model posits that all variables that are measured are uncorrelated. The statistic has a range between 0 and 1; Bentler and Bonnet (1980) suggest that values above 0.90 indicate a good fit. This value has been adopted in the current study to ensure an adequate model fit, as suggested by Byrne, (2010); Hair et al. (2006). The CFI builds on the foundation of the NFI by taking a sample size into account. Even when the sample size is small, this is still a useful index (Tabachnick and Fidell, 2007). Like the NFI, the null model indicates that there is no correlation between the measured variables, and the range of the values of the CFI is between 0 and 1; a good fit is indicated at values above 0.9

which is adopted in the current study to ensure an adequate level of model fitness (Hair, et. al., 2017).

6. A normed Chi-Square (CMIN/DF) was adopted in the current study as a form of parsimonious fit indices to ensure the model's goodness of fit along with prior indices discussed above. Traditionally, the CMIN/DF is proposed by Wheaton, et. al. (1977, cited by Byrne, 2010) to mitigate the influence of the sample size on the model Chi-Square (Hooper et al., 2008). The value of CMIN/DF less than 3 was suggested as a good indication of the model fitness (Hair, et. al., 2017), and therefore, it was adopted in the current study. Prior to conducting the second stage of the SEM analysis, the measurement model analysis (CFA) was also subjected for further assessments to confirm the constructs' reliability and validity.

According to Bhattacharjee (2012), reliability is “the degree to which the measure of a construct is consistent or dependable.” In other words, under constant circumstances, comparable findings should be reached when using the same scale for assessing the same construct. In this study, three common reliability measures (internal consistency reliability (Cronbach's alpha), composite reliability (CR), and average variance extracted (AVE)) were adopted to ensure an adequate level of the constructs' reliability (see section 6.5 in this chapter). Several items within a construct can be assessed for consistency by measuring the internal consistency reliability (Bhattacharjee, 2012). Here, Cronbach's alpha (1951) was examined using SPSS. This was used to assess the internal consistency reliability of the underlying constructs. To demonstrate an adequate level of internal consistency reliability, the value of Cronbach's alpha, for all constructs, should be higher than 0.70; this value is highly recommended by Nunnally (1978). The AVE has been defined as “the amount of variance that is captured by the construct in relation to the amount of variance due to measurement error” (Fornell and Larcker, 1981). Using Formula 6.2, the values of the AVE for all latent constructs have been estimated. A value > 0.50 demonstrates that the construct has an appropriate amount of AVE (Hair et al, 2010).

(2) Structural Model: The conceptual model and research hypotheses that are proposed in Chapter Four are to be validated in the second stage of SEM structural model analyses (Hair et al., 2017). In detail, the main fit indices adopted to assess the measurement model's goodness-of-fit were also used to evaluate how much the structural model (the hypothesised model) is able to adequately fit the sample data. In this stage, the structural model was also evaluated in the terms of its predictive power by looking at the values of R^2 that are

accounted for in the dependent (endogenous) constructs (Straub, et. al., 2004). Further, the path coefficient analyses were conducted using AMOS 21 with a view to verify the research hypotheses as well as to see the extent and the pattern of the causal relationships between the latent constructs (Hair, et. al., 2017). As a rule of thumb, the path coefficient (hypothesised path) is considered statistically significant if its critical value (Z-value) is not less than 1.96 with the *p* value no more than 0.05 (Hair, et. al., 2017). According to this basis, the decision was made to support or reject any hypothesis. A summary of the study objective and suggested statistical techniques are summarised in Table 5.2.

Table 5.2 Research Objectives and Techniques of Data Analysis

The Research Objectives		Techniques of Data Analysis
1	To develop a theoretical framework through the integration of the relevant several studies in the area assessing the reliability and security of internal control accounting information system, quality of financial reporting and business performance. This framework consists of the dependent and independent variables.	The study Framework
2	To find out the main factors (i.e., component) that underlie each construct of the study's model (i.e., SysTrust, quality of financial reporting and business performance)	Factor Analysis
3	To find out whether there are any differences or similarities among companies in respect to the level of reliability of AIS process based upon the implementation of SysTrust's principles due to their type of business sector, size and business experiences.	ANOVA
4	To identify which the key principle /component of SysTrust model that is highly associated with quality of financial reporting.	Multiple Regression
5	To identify which the key principle /component of SysTrust model that is highly associated with business performance.	Multiple Regression
6	To determine whether the quality of financial reporting is mediating the relationship between the reliability of AIS based upon the implementation of SysTrust principles and business performance	4 steps Multiple Regression
7	To empirically examine and validate the proposed conceptual model. This objective will be accomplished by conducting an analysis of data that are obtained from the shareholding companies in Jordan	Structural Equation Model

5.18 Statistical Methods Used for Testing Research Hypotheses

There are alternative statistical tests available for any given research design, and it is necessary to use some rationale for selecting among them. In hypothesis testing, we must state the hypothesised value of population parameters before we begin sampling. The

assumption we wish to test is the null hypothesis " H_n ". A statistical test is good if it has a small probability of rejecting (H_n) when it is true, but has greater probability of rejecting (H_n) when it is false. If our sample results fail to support the null hypothesis, we must conclude that something else is true. In other words, in applying a statistical test, the researcher must choose either accepting or rejecting the null hypothesis (H_n). If (H_n) is rejected, then he tends to use this as evidence in favour of (H_1) (Siegel, 1956). Siegel (1956) suggests that there are two major considerations in choosing a statistical test. Firstly, the researcher must consider the manner in which the sample was drawn and the nature of its population. Secondly, he must consider the kind of scale of measurement (i.e., nominal, Ordinal, interval or ratio) which was employed in the definition of the variables involved in the study. Hair et al., 2010 added another consideration which must be taken into account when deciding on the appropriate statistical test, such as, (1) how many samples are involved in the problem "one, two or many (K) samples?", (2) Are the samples independent or related to each other? In this study, two different statistical tests representing were used to test the research hypotheses (i.e., F- test, T- test, and test). Table 6.2 illustrates the research hypotheses and the relevant tests.

(1) T-Test. The T- Test is a parametric statistical test. It is employed for testing hypotheses (H_0) this statistical test is provided by the stepwise regression analysis computer program. It is also used to measure the significance of the relationship between each independent variable (the output of principle component analysis), and the level of quality of financial reporting as well as financial performance; taken separately.

(2) Univariate F- Test. The SPSS statistical package provides the result of the F-test with the results of some of the statistical techniques (e.g., RA regression analysis). In this research the F- test is used to test the significance of regression equations.

5.19 Summary

This chapter described the research design process and data collection methods that were used in this research. It outlined the types of research approaches, quantitative and qualitative research, as well as the research paradigms. It also discussed data types and sources, data collection methods, questionnaire design, scale of measurement, and the domains of the study. The ethical considerations and the process of data preparation for final analysis were also explained.

Table 5.3 Summary Research Design and Data Collection techniques

Research Methods	Techniques
Research Approach	Quantitative Research
Research Paradigm	Positivism
Research Design	Testing the Hypotheses
Type of Investigation	Correlation and Descriptive
Time Scope	This Study is Cross-Sectional
Data Collection Method	Face to Face /survey questionnaire
Structure of the Interview	The Structured- Direct Technique
Data Type	Primary /Secondary
Measurement	Nominal/ Likert Scale (7 point rating)

Furthermore, based upon the research objectives and hypotheses, several statistical techniques were preferred to analyse the data and to achieve the research objectives in addition to testing the research hypotheses. The statistical techniques chosen varied from the univariate, the bivariate and the multivariate, depending on the type of data and the number of variables. With regard to the multivariate techniques, the following were used factor analysis, and multiple-regression analysis and structural equation modelling. This chapter included a brief description of the alternative statistical techniques which have been used in this study, the basis for choosing the appropriate statistical techniques, and the reason for using each technique in this research. Finally, the chapter concluded with a discussion of the reliability and validity assessment of the research.

The following chapter is dedicated to the presentation and discussion of the research findings of the use of factor analysis. The purpose of these techniques is to identify the main pattern of factors that underlie the SysTrust dimensions. The validity and reliability of data are also presented.

CHAPTER SIX

DATA ANALYSIS AND TESTING HYPOTHESES

6.1 Introduction

This Chapter is divided by two sections the first one presents the main findings of the Principal Component Analysis. The main purpose behind the use of these techniques here is to reduce the large number of variables that underlie each construct of five dimensions of SysTrust (i.e., availability, integrity processing, privacy, security and confidentiality), in addition to extract the main factors underlying each construct of the quality of financial reporting into orthogonal indices for further analysis by the regression analysis. Furthermore, by employing the principal component analysis techniques, it may be possible to explore the patterns of factors that underlie each major construct. It was considered an appropriate method to overcome the potential problems of multicollinearity among the variables that pertain to each construct.

The second section will use the eleven factors that were extracted from the factor analysis in the first section to be analysed in terms of their relationships, direction, and strength; and their ability to predict the quality of financial reporting and business performance. The statistical analysis techniques used are multiple regressions and structural Equation Modelling, Test and T-test. Factors and variables are analysed and discussed in this section.

In the first section, a pre-analysis was conducted to examine the appropriateness of the data for factor analysis. Then, the results of the factor analysis were examined using multiple criteria including, eigenvalues, interpretability and internal consistency, as recommended by Hair, et. al., (2010). Therefore, items with eigenvalues more than one and factor loadings less than (0.30) were determined. This means that the items had little or no relationship with each other, hence they were discarded (Hair, et. al., 2010). Finally, Cornbach's alpha reliabilities were examined for each variable. Each coefficient greater than (0.60) for adapted and (0.70) as recommended by Streiner and Norman (2008) for existing scales was considered a reliable indicator of the constructs under study (Hair, et. al., 2010).

6.2 First Section: The Findings of the Factor Analysis

The findings of the principal component's analysis indicate that eleven factors could be extracted from the five major constructs of SysTrust's framework (availability, security integrity processing, privacy and confidentiality) are derived from the five constructs of the internal environmental dimension and four factors are extracted from the three constructs of the external environmental dimension. Table 6.1 presents the number of factors underlying each construct of both dimensions.

Table 6.1 Factors Underlying the Main Principles SysTrust's Model

Major Constructs/Principles	Number of Variables	Number of Factors
Availability of AIS	13	3
Security of AIS	18	3
Integrity Processing	17	3
Confidentiality	12	1
Privacy	10	1
Total	70	11

★ *The varimax rotation version with Kaiser Normalization was used to produce more interpretable factors. The eigenvalue (>1) criteria was used in order to determine the number of factors*

6.3 The Interpretation of the Final Factor Analysis

The main patterns of factors underlying each construct of SysTrust's model and their interpretations are presented under the following sections.

6.3.1 Main Constructs of the SysTrust Service Conceptual Framework

The SysTrust's service conceptual framework for assessing the reliability of AIS consists of five major constructs: (1) Availability of AIS, (2) Security of AIS, (3) Integrity Processing, (4) Confidentiality, and (5) Privacy. The interpretations of the results of the principal components analysis are presented for each of these constructs as follows.

6.3.1.1 Availability of AIS Construct Measures

The availability of AIS is one of the major constructs of the SysTrust's service framework. It is a function of accessibility and defined as the end-user ability to use AIS whenever is needed and according to schedules and agenda of business organization. Use of AIS refers to perfect and quality implementation of inputting, updating, storing, and retrieving process during the agreed upon time. The potential sources of threats to availability of AIS are hardware and software failures, natural and man-made disasters, human error, worms and viruses, and denial-of-services attacks and other acts of sabotage.

To minimize threats to AIS availability, SysTrust has developed set of criteria, operational policies, illustrative controls and procedures such as disaster recovery plan and business continuity plan. It is used here to measure the extent of internal control's methods over the computerised accounting information systems provide requirements of availability principal for the systems. The system's availability of operation and use in different times that includes reduction of the time of the system's downtime, the design of the plans to face disasters and working on avoiding data loss and reducing the expected loss as possible. The availability of AIS construct was measured using 13 items as presented in Table 6.4. An inspection of the correlation matrix indicated in Table 6.2 that the correlations were all above the acceptable level of .30. The subsequent KMO and Bartlett's test resulted in significant level of probability ($p > 0.000$) and high KMO statistics of 0.944 indicating the factor analysis could be proceeding as 94.0% of the variance in the data can be explained by this construct as presented in Table 6.2. MacCallum et al. (1999, 2001) advocate that all items in a factor model should have communalities of over 0.40.

Table 6.2 KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Adequacy.	Measure of Sampling	0.944
Bartlett's Test of Sphericity	Approx. Chi-Square	3078.102
	Df	78
	Sig.	0.000

Table 6.3 Total Variance Explained

Component/ Factor	Rotation Sums of Squared Loadings		
	Eigenvalue	% of Variance	Cumulative %
1	3.264	25.109	25.109
2	3.125	24.040	49.149
3	3.042	23.397	72.546

Table 6.4 Main Factors Underlying the Availability of AIS Measures

Code	Items (variables)	Loadings	Communality
Factor (1). Availability Polices			
A1	The system availability requirements of authorised users, and system availability objectives, policies, and standards, are identified and documented.	0.782	0.664
A3	A formal process exists to identify and review contractual, legal, and other service-level agreements and applicable laws and regulations that could impact system availability objectives, policies, and standards.	0.773	0.759

A2	The entity's system availability are periodically reviewed and approved by an authorised people.	0.745	0.807
A4	There are procedures to ensure that personnel responsible for the design, development, implementation, and operation of system availability features are qualified to fulfil their responsibilities.	0.644	0.782
A5	Management has assigned responsibilities for the maintenance and enforcement of the entity's availability policies to the CIO.	0.594	0.765
Factor (2). Recovery Disaster Plan			
A11	The firm adopts policies and procedures for fast dealing with computerised accounting information system's mistakes to achieve a continuous availability to the system.	0.811.	0.760
A10	The firm makes preventive maintenance to the computerised information system periodically and regularly.	0.767	0.765
A13	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, monitored, and maintained to meet availability commitments and requirements	0.738	0.756
A12	Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies	0.715	0.808
Factor (3). Availability Communication			
A8	Employees are trained on special procedures concerning reducing the time of system's stop as possible.	0.775	0.806
A7	Employees are trained to make substitute copies of the programs.	0.759	0.785
06	The entity's user training program includes modules dealing with the identification and reporting of system availability issues, security breaches, and other incidents.	0.754	0.781
A9	There is formal communication of system availability objectives, policies, and standards to authorised users through means such as memos, meetings, and manuals.	0.602	0.769

* Cronbach's Alpha level is (94.3).

The results of the principal of component analysis Table 6.3 indicate that three factors could be extracted from the variables of this construct. The first factor, which accounts for (25.11%) of the variance with loadings ranging from 0.59 to 0.78, can be identified as a "**Availability Polices**" factor. The second factor, which explains 24.04% of variance with loadings range from 0.71 to 0.81, can be labelled as "**Recovery disaster plan**" factor and the

third one, which account for 23.4% of variance can be named as "**Availability communication**" factor. The combinations of these factors account for 72.55% of the total variance in the questionnaire data as can be shown in Table 6.4. As this measure was adapted from an existing scale, the computed Cronbach's Alpha level of 0.943 indicated the items were highly reliability.

6.3.1.2 The Security of AIS Construct Measures

The construct security of AIS measured eighteen items as presented in Table 6.7. It is defined as protection of AIS against unauthorised physical and logical access. Reliability of AIS against security risks entails building IT infrastructure enhances the internal control system of AIS. Ensuring security of AIS requires developing operational and physical policies related to use of hardware, software, and accounting data. In addition, security of AIS demands developing physical and logical access controls such as user identification controls, physical possession identification, and compatibility tests. It is used here to measure the extent of internal control's methods over the computerised accounting information systems provide requirements of security principal for the systems.

Table 6.5 KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.951
Bartlett's Test of Sphericity	Approx. Chi-Square	6480.699
	Df	153
	Sig.	0.000

The initial inspection of the correlation matrix for this construct revealed the presence of correlations well above acceptable limit of 0.30. An evaluation of the correlation with the Bartlett's and KMO test indicated that significant probability levels ($p > 0.000$) and high KMO statistics of 0.951, indicating that the factor analysis could proceed around 95.1% of the variance in the data can be explained by the security construct as presented in Table 6.5. The findings of the principal component analysis reveal that three significant factors accounting for 76.224% of the total variance can be extracted from the eighteen items (measures) of the security construct as can be shown in Table 6.5. The three factors with their percentage of variance are respectively: (1) "**logical Security Access**" (28.510)", (2) "**Security Policies and Communication** (26.511)", (3) "**Physical Security Access** (21.203)". The scale demonstrated high reliability with a Cronbach's alpha level of 0.965, moreover all communalities are within the acceptable level which is over 0.40.

Table 6.6 Total Variance Explained

Component/ Factor	Rotation Sums of Squared Loadings		
	Eigenvalue	% of Variance	Cumulative %
1. Logical Security	5.132	28.510	28.510
2. Security policies	4.772	26.511	55.021
3. Physical Security	3.817	21.203	76.224

Table 6.7 The Main Factors Underlying the Security of AIS Measures

Code	Items (variables)	Loadings	Communality
Factor (1). Logical Security Access			
S17	Updating continuously the antivirus software used in the computerised systems.	0.869	0.898
S16	The firm takes special control procedures prevent transferring the computers outside	0.862	0.899
S15	Personal computers are programmed to be locked electronically after finishing work with a limited period of time.	0.826	0.786
S18	Logical access security measures have been implemented to protect against unauthorised	0.758	0.737
S14	The firm takes suitable steps to protect the main devices by keeping them away from danger and in fire resistant places	0.728	0.687
S13	The entity uses industry standard encryption technology, VPN software, or other secure communication systems (consistent with its periodic IT risk assessment) for the transmission of private or confidential information over public networks, including user IDs and passwords.	0.627	0.698
Factor (2). Security Policies and Communication			
S2	The entity's system security is periodically reviewed and compared with the defined system security policies	0.800	0.795
S3	The firm's has classified the data on the basis on its criticality and sensitivity and kept in the main devices.	0.797	0.791
S1	The firm's security policies has approved and documented the security requirements of authorised users.	0.796	0.766
S4	The firm uses appropriate procedures to separate duties, tools and functions of the system's administration from net administration	0.761	0.764
S5	A security awareness program has been implemented to communicate the entity's IT security policies to employees	0.721	0.794
S6	Personnel receive training and development in system security concepts and issues.	0.594	0.713
Factor (3). Physical Security Access			
S8	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is	0.710	0.773

	restricted to authorised individuals by card key systems and monitored by video surveillance.		
S11	Firewall events are logged and reviewed daily by the security ad-Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers...	0.666	0.763
S7	Major computers are kept in closed place and the authorised people are allowed to access in to it.	0.624	0.698
S10	Documented procedures exist for the identification and escalation of potential physical security breaches.	0.624	0.754
S12	the firm uses physical selector as fingerprints or eyes' to access into data Firewalls are used and configured to prevent unauthorised access	0.593	0.729
S9	Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations.	0.537	0.676

The Cornbach's alpha level is 0.965

6.3.1.3 Integrity Processing of AIS Construct Measures

The construct integrity processing of AIS measured seventeen items as shown in Table 6.10. It refers to completeness, accuracy, timeliness, and authorization of AIS process. According to SysTrust, AIS has integrity if the accounting process accomplished in an unimpaired manner and free from unauthorised manipulation. To improve integrity of AIS, the application and general controls have to be inherited in the designing of ICS. Source data controls, input validation routines, on-line data entry controls, data processing and storage controls, output controls, and data transmission controls are example of application controls. It is used here to measure the extent of internal control's methods over the computerised accounting information systems provide requirements of integrity processing principal for the systems. The initial inspection of the correlation matrix for this construct revealed the presence of correlations well above acceptable limit of 0.30. An evaluation of the correlation with the Bartlett's and KMO test indicated that significant probability levels ($p > 0.000$) and high KMO statistics of 0.948, indicating that the factor analysis could proceed as 95% of the variance in the data can be explained by integrity processing measures as presented in Table 6.8.

Table 6.8 KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.948
Bartlett's Test of Sphericity	Approx. Chi-Square	3990.255
	Df	136
	Sig.	0.000

The findings of the principal component analysis reveal that three significant factors accounting for 67.828% of the total variance can be extracted from the seventeen items (measures) of integrity processing of AIS. The three factors with their percentage of variance are respectively: (1) the "**Integrity Processing Policies**" (27.549)" (2) the "**Data Transfer Control**" 20.453)" (3) the "**Output Control** (19.826)". The scale demonstrated high reliability with a Cornbach's alpha level of 0.949 as can be shown in Table 6.10.

Table 6.9 Total Variance Explained

Component/ Factor	Rotation Sums of Squared Loadings		
	Eigenvalue	% of Variance	Cumulative %
1. Intergtiey policies	4.683	27.549	27.549
2 Data Transfer	3.477	20.453	48.003
3. Output Control	3.370	19.826	67.828

Table 6.10 The Main Factors Underlying the Integrity Processing of AIS Measures

Code	Items (variables)	Loadings	Communality
Factor (1) Integrity Processing policies			
Ig3	There are special tests to make sure of the integration of input data to check data validity before processing	0.800	0.766
Ig1	The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group	0.758	0.707
Ig2	Firm's' administration develops procedures to make sure f the completion and accuracy of documents that represent sources of data.	0.755	0.712
Ig6	Make sure of the computer's response to every item of the input	0.723	0.664
Ig5	Data is inserted by authorised people	0.723	0.658
Ig4	Fields' frequency and their capacity are reviewed and high and low limits are examined to check the reliability and accuracy of the inputs	0.699	0.731
Ig7	Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements	0.672	0.655
Factor (2) Data Transfer Control			

Ig15	There are control procedures for protecting information when they are transferred via nets as coding and checking of the transmission.	0.785	0.750
Ig14	Computer's reports are distributed into the appropriate users	0.773	0.718
Ig16	System output is complete, accurate, distributed, and retained in accordance with processing integrity commitments and requirements.	0.724	0.694
Ig13	The sensitive outputs are protected from unauthorised access	0.679	0.678
Ig17	Files of data are named with appropriate names	0.550	0.512
Factor (3) Output Control			
Ig9	Computerised accounting information systems includes a pointer appeared as a message whenever something wrong happened in input process	0.728	0.665
Ig11	The compatibility between inputs and outputs are reviewed daily	0.697	0.684
Ig10	All the system's outputs are revised in terms of logic and formation accuracy	0.694	0.701
Ig8	Make periodically the settlements' procedures between sub accounts computerised information systems.	0.689	0.631
Ig12	Any mistake in the outputs is corrected when it is discovered	0.574	0.604

The Cornbach's alpha level is .949

6.3.1.4 The Confidentiality of AIS Construct Measures

The Confidentiality of AIS construct was measured using 12 variables as shown in Table 6.13. It refers to the system's ability to protect the information designated as confidential, as committed or agreed. The entity needs to disclose its system and information confidentiality policies, procedures, and practices relating to the manner in which it provides for an authorised access to its system and uses and shares information designated as confidential. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. Access must be restricted to those authorised to view the data in question. It is common, as well, for data to be categorised according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories. Sometimes safeguarding data confidentiality may involve special training for that privacy to such documents. Such training would typically include security risks that could threaten this information. Training can help familiarize authorised people with risk factors and how to guard against them. Further aspects of training can include strong passwords and password-related best practices and information about

social engineering methods, to prevent them from bending data-handling rules with good intentions and potentially disastrous results. This construct is used to measure the extent of internal control's methods over the computerised accounting information systems provide requirements of confidentiality principal for the systems.

Table 6.11 KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.949
Bartlett's Test of Sphericity	Approx. Chi-Square	3101.243
	Df	66
	Sig.	0.000

The preliminary examination of the correlation matrix for this construct revealed acceptable inter-correlations well above 0.30. a further examination of the data matrix indicated the Bartlett's test was significant at ($p > 0.000$), with an acceptable KMO measure of adequacy 0.949, indicating that the factor analysis could advance as it had a high amount of variance around 95% in the data, which can be explained by this construct as presented in Table 6.11. The findings of the principal component analysis showed that twelve items (measures) of this construct can be clustered into only significant factor as shown in Table 6.12. The combination of these factors is account for 63.505% of the total variance. This significant factor with its variance (63.5050) can be labelled as "the confidentiality of AIS ". The scale demonstrated high reliability with a Cronbach's alpha level of 0.948. Communalities are within the acceptable level which is over 0.40.

Table 6.12 Total Variance Explained

Component/ Factor	Rotation Sums of Squared Loadings		
	Eigenvalue	% of Variance	Cumulative %
1.	7.621	63.505	63.505

Table 6.13 The Main Factors Underlying the Confidentiality of AIS Measures

Code	Items (variables)	Loadings	Communality
Factor (1). The confidentiality of AIS			
C8	Management has developed a reporting strategy that includes the sensitivity and confidentiality of data and appropriateness of user access to output data	0.828	0.686
C4	The security administration team has custody of and is responsible for the day-to-day maintenance of the entity's confidentiality and related security policies and recommends changes to the CIO and the IT steering committee	0.828	0.685

C9	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has been granted access.	0.821	0.674
C7	Confidentiality processes exist to restrict the capability to input information to only authorised individuals.	0.819	0.670
C5	The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorised users.	0.817	0.668
C10	. Logical access controls are in place that limit access to confidential information based on job function.	0.803	0.645
C6	Error messages are revealed to authorize personnel.	0.800	0.641
C3	The entity publishes its confidentiality and related security policies on its corporate intranet.	0.792	0.627
C11	Requests for access privileges to confidential data require the approval of the data owner. Business partners are subject to nondisclosure agreements or other contractual confidentiality provisions.	0.790	0.624
C12	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorised parties in accordance with confidentiality commitments and requirements.	0.787	0.619
C2	The system confidentiality and requirements are communicated to authorised users.	0.757	0.574
C1	The entity's system confidentiality and related requirements are established and periodically reviewed and approved by a designated individual or group.	0.714	0.510

The Cronbach's alpha level is 0.948.

6.3.1.5 The Privacy Construct Measures

The privacy construct was measured by ten items as shown in Table 6.16. Privacy can be defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information. The privacy principle addresses the system's collection, use, retention, disclosure, and disposal of personal information in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and Canadian Institute of Chartered. Privacy can be defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information. It is used here to measure the extent of internal control's

methods over the computerised accounting information systems provide requirements of privacy principal for the systems. Communalities are within the acceptable level which is over 0.40. The preliminary examination of the correlation matrix for this construct revealed the presence of inter-correlations well above the acceptable limit of 0.30. An evaluation of the correlation matrix with the Bartlett's and KMO tests indicated significant probability levels ($p > 0.000$) and high KMO statistics of 0.946, indicating that the factor analysis could proceed as 94.6% of the variance in the data can be explained by this construct as shown in Table 6.14.

Table 6.14 KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.946
Bartlett's Test of Sphericity	Approx. Chi-Square	2667.560
	Df	45
	Sig.	0.000

Table 6.15 Total Variance Explained

Component/ Factor	Rotation Sums of Squared Loadings		
	Eigenvalue	% of Variance	Cumulative %
1	6.709	67.091	67.091

Table 6.16 The Main Factors Underlying the Privacy of AIS Measures

Code	Items (variables)	Loadings	Communality
Factor (1). The Privacy of AIS			
P4	The entity collects personal information only for the purposes identified in the notice	0.852	0.726
P9	The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.	0.850	0.722
P8	The entity protects personal information against unauthorised access (both physical and logical).	0.849	0.721
P7	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual	0.837	0.700
P2	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed	0.823	0.678
P10	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes	0.822	0.676
P6	The entity provides individuals with access to their personal information for review and update.	0.816	0.666
P5	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit	0.813	0.605

	consent. The entity retains personal information for only as long as necessary to fulfil the stated purpose		
P3	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.	0.778	0.661
P1	The entity defines documents, communicates, and assigns accountability for its privacy policies and procedures.	0.743	0.653

* The Cronbach's alpha level is 0.945

As can be shown in Table 6.15, the principal component analysis of the ten items yielded a single factor structure with factor loadings ranging from 0.743 to 0.852 explaining 67.02% of the variance in the questionnaire data. The internal consistency of the items was computed with Cronbach's alpha, and the results indicated that the scale yielded very reliable with coefficient alpha levels of 0.945. all communalities are within the acceptable level which is over 0.60 or an average communality of 0.7.

6.3.2 Main Factors Underlying the Quality of Financial Reporting Measures

Comprehensive assessment of the quality of financial reports is important as it may improve users' quality of economic decision making and enhance market position efficiency (IASB, 2008; IASB, 2010), thereby, minimize the expenditure of capital for companies. The quality of financial reporting construct was measured using 26 items as shown in Table 6.19. The quality of financial information implies the attributes which financial information should have for fulfilling the information needs for the information users. As described in Chapter 4, the financial qualitative characteristics are the attributes that make financial information useful. The fundamental qualitative characteristics are expressed as relevance and faithful representation. There are also enhancing qualitative characteristics which are complementary to the fundamental qualitative characteristics. Comparability, verifiability, timeliness, and understandability are qualitative characteristics that enhance the usefulness of information that is relevant and faithfully represented.

This construct is used here to examine to which extent the quality of financial reporting can be enhanced by the implementation of the main five principles of SysTrust requirements and its influence on the business performance. The preliminary examination of the correlation matrix for this construct revealed acceptable inter-correlations well above 0.30. A further examination of the data matrix indicated the Bartlett's test was significant at ($p > 0.000$), with an acceptable KMO measure of adequacy 0.932, indicating that the factor analysis could

advance as it had a high amount of variance around 93% in the data, which can be explained by this construct as presented in Table 6.17.

Table 6.17 KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.932
Bartlett's Test of Sphericity	Approx. Chi-Square	13012.886
	Df	300
	Sig.	0.000

The results of the principal component analysis Table 6.19 indicate that four significant factors can be extracted from this construct. This construct composed of 25 items (variables) as presented in Table 6.19. The first factor, which accounts for (20.981%) of the variance with loadings ranging from 0.73 to 0.76, can be identified as an "**Understandability**" factor. The second factor, which explains 20.468% of variance with loadings range from 0.61 to 0.81, can be labelled as "**Relevance**" factor. The third factor which accounts for 19.174 can be identified as "**Comparability**" factor and the forth factor which account for 15.775 can be labelled as "**Faith Representation**". The combinations of these factors accounts for 76.398 of the total variance in the questionnaire data as can be shown in Table 6.18. As this measure was adapted from an existing scale, the computed Cronbach's Alpha level of 0.965 indicated the items were highly reliability. These results support the proposition that the compound measurement tool used in this study is a valid approach to assess the quality of financial reports and they were in consistent with previous studies such as Besst, et al., (2009), Maines and Wahlen (2006).

Table 6.18 Total Variance Explained

Component/ Factor	Rotation Sums of Squared Loadings		
	Eigenvalue	% of Variance	Cumulative %
1	5.245	20.981	20.981
2	5.117	20.468	41.449
3	4.793	19.174	60.623
4	3.944	15.775	76.398

Table 6.19 The Main Factors Underlying the Quality of Financial Reporting Measures

Code	Items (variables)	Loadings	Communality
Factor (1). Understandability			
U1	The annual report presented in a well-organised manner	0.765	0.784
U6	The use of language and technical jargon is easy to follow in the annual report	0.754	0.844
U7	The annual report included a comprehensive	0.749	0.772

	glossary		
U3	Sources and level of expenditure can easily be understood	0.745	0.788
U4	Business assets are easy to know in terms of value and nature	0.743	0.847
U5	the presence of graphs and tables clarifies the presented information	0.742	0.779
U2	The notes to the balance sheet and the income statement are sufficiently clear	0.736	0.849
Factor (2). Relevance			
R3	The company uses fair value instead of historical cost	0.808	0.837
R6	No undue delays in the presentation of financial reports.	0.806	0.833
R5	Financial reports are presented annually as required by regulatory bodies of accounting	0.718	0.777
R2	The annual report discloses information in terms of business opportunities and risks complement the financial information	0.714	0.769
R1	The annual report discloses forward-looking information help forming expectations and predictions concerning the future of the company	0.712	0.675
R4	Information helps you confirm profitability levels of the business	0.628	0.750
R7	The annual report provides feedback information on how various market events and significant transactions affected the company	0.619	0.736
Factor (3). Comparability			
C4	The results of current accounting period are compared with results in previous accounting periods	0.776	0.799
C2	The notes to revisions in accounting estimates and judgments explain the implications of the revision	0.747	0.770
C3	The company's previous accounting period's figures are adjusted for the effect of the implementation of a change in accounting policy or revisions in accounting estimates	0.713	0.732
C6	The annual report presents financial index numbers and ratios.	0.709	0.734
C5	Information in the annual report is comparable to information provided by other organizations	0.654	0.689
C1	The notes to changes in accounting policies explain the implications of the change.	0.642	0.681
T1	Natural logarithm of amount of days it took for the auditor signed the auditors' report after book-year end.*	0.632	0.64
Factor (3). Faith Representation			

F2	The annual report explains the choice of accounting principles clearly	0.747	0.791
F4	The annual report includes an unqualified auditor's report	0.686	0.734
F3	The annual report highlights the positive and negative events in a balanced way when discussing the annual results	0.678	0.736
F1	The annual report explains the assumptions and estimates made clearly; valid arguments provided to support the decision for certain assumptions and estimates in the annual report	0.676	0.694
F5	The annual report extensively discloses information on corporate governance issues	0.634	0.699

Cronbach's Alpha level is (0.965).

6.3.3 Main Factors Underlying the Business Performance Measures

The business performance construct was measured using 19 items as shown in Table 6.22. Performance measurement systems are necessary for every organization to evaluate its achievements (e.g., goals, satisfaction, resource utilization, etc.). With the increased level of globalization, strong competition, and technological changes, many companies have started to use a blend of financial and non-financial measures for their performance. As it was discussed in Chapter 4, In order to gain a complete picture of business performance, a combination of financial and non-financial measures was used in different fields such as economics, strategy, finance and accounting. This construct is used here to identify the extent of business performance is enhanced by the quality of financial reporting due to the implementation of the requirements of the principles of SysTrust. The preliminary examination of the correlation matrix revealed acceptable inter-correlations well above 0.30. A further examination of the data matrix indicated the Bartlett's test was significant at ($P > .000$), with an acceptable KMO measure of adequacy 0.958, indicating that the factor analysis could advance as it had a high amount of variance around 96% in the data, which can be explained by this construct as presented in Table 6.20.

Table 6.20 KMO and Bartlett's Test

KMO and Bartlett's Test			
Kaiser-Meyer-Olkin Adequacy.	Measure of Sampling		0.958
Bartlett's Test of Sphericity	Approx. Chi-Square		7420.925
	Df		171
	Sig.		0.000

Table 6.21 Total Variance Explained

Component/ Factor	Rotation Sums of Squared Loadings		
	Eigenvalue	% of Variance	Cumulative %
1	6.897	36.303	36.303
2	6.527	34.354	70.657

Table 6.22 The Main Factors Underlying the Business Performance Measures

Code	Items (variables)	Loadings	Communality
Factor (1). Financial Performance			
F1	Economic value added (EVA)	0.810	0.802
F3	Return on assets (ROA)	0.809	0.792
F2	Return on equity (ROE)	0.805	0.789
F7	Earnings growth	0.754	0.660
F9	Net profit	0.745	0.673
F6	Productivity of employees	0.711	0.648
F10	working capital ratio	0.703	0.649
F8	Earnings per share (EPS)	0.692	0.633
F5	Level of profitability (Net margin)	0.653	0.631
F4	Return on investment (ROI)	0.624	0.604
Factor (2). Non- Financial Performance			
Nf4	Employees satisfaction	0.825	0.773
Nf5	Customer satisfaction	0.789	0.726
Nf2	Success rate in launching new products, services or programs	0.770	0.767
Nf7	Social performance	0.767	0.739
Nf1	Environmental performance	0.758	0.718
Nf6	Level of innovation	0.753	0.724
Nf8	Business growth	0.748	0.771
Nf3	Shareholders satisfaction	0.667	0.690
Nf9	Reputation in its sector	0.627	0.637

Cornbach's alpha level = 0.969

The findings of the principal component analysis reveal that two significant factors accounting for 70.657% of the total variance can be extracted from the nineteen items (measures) of integrity processing of AIS. The two factors with their percentage of variance are respectively. (1) The **Financial Performance** (36.303) (2) The **Non-Financial Performance** (34.354). The scale demonstrated high reliability with a Cornbach's alpha level of 0.969 as can be shown in Table 6.21. These results were supported by previous studies such as Santos and Brito, (2012), Ángel Machado-Cabezas, (2015) and Sandeep and Bedi, (2016), Communalities are within the acceptable level which is over 0.40.

6.4 Validity Assessment

After measuring the results of preliminary analysis by correlations, exploratory factor analysis and reliability estimates were vital to examine that the construct measures were

appropriate and ensure the validity for further statistical analysis. It's vital to assess content, construct (convergent) and external validity. Therefore, the next three sections discuss how these types of validity were achieved in the current research.

6.4.1 Evidence of Content Validity

Content or face validity is the first type of evidence used within the thesis. Content validity is a subjective but systematic assessment of the extent to which the content of a scale measures a construct (Schaller, et al., 2015). When it is evident to experts that the measure shows adequate coverage of the concept, the measure has face validity. In order to obtain content validity, the study followed the recommended procedure which is based on identifying the existing scaled from the literature and conducting interviews with the panel of experts (including academics and practitioners from the industry) and asking them to give their comments on the instrument. The interviews were conducted as part of the pre-test methods, as discussed earlier in chapter five. Given that the content validity had a subjective nature, it was not sufficient to provide a more rigorous empirical test (Zikmund, 2003). Therefore, its validity was assured a priori to conducting the final survey, as a precursor to other measures of validity.

6.4.2 Evidence of Convergent Validity

Convergent validity refers to the extent to which a measure correlates, or converges, with other measures of the same construct (Simms and Watson, 2007) indicating that the scale is an appropriate measure of the construct and supporting the theoretical position of the construct (Crano and Brewer, 2005). To demonstrate convergent validity, the items were loaded 'highly' on one factor with a factor loading of 0.50 or greater (Hair, et. al., 2017). Evidence of convergent validity was confirmed by significant and strong correlations between the different measures of the same construct (Carlson and Herdman, 2012). Moreover, according to Hair, et. al. (2017; 1988), convergent validity is established when the Average Variance Extracted (AVE) for all focal constructs was more than 0.50, which meets the first condition of achieving convergent Explained (AVE) between the constructs is equal to, or exceeds, 0.5. The average variance explained validity.

Table 6.23 Survey of Average Explained Variance and Reliability Estimations of all Measures of SysTrust Constructs

Construct	AVE	Cronbach's Alpha
1. The Availability of AIS	0.555	0.943
2. The Security of AIS	0.694	0.965
3. The Integrity Processing	0.633	0.949
4. The Confidentiality	0.649	0.948
5. Privacy	0.688	0.945

In order to achieve the second requirement of convergent validity, it was vital to consider the reliabilities of the measurements as means of providing evidence and support for the convergent validity of the constructs (Hair, et. al., 2017). In addition, those measurements that demonstrate low reliability levels were not further investigated, as the convergent validity would not be. As presented in 6.23, all the scales demonstrated an acceptable 'high' reliabilities, with the Cronbach's coefficient alpha's exceeding the 0.70 threshold, as recommended by Nunnally and Bernstein (1994); thereby, satisfying the second requirement of convergent validity. In sum, based on the preliminary analysis, the evaluation of the data by factor analysis and reliability estimates indicated that all scale items were appropriate and valid for further statistical analysis. Additional testing of the quality of the scale was conducted via establishing the content, construct and external validity.

6.5 Summary of the factor analysis

The principal component analysis techniques were performed here for the following purposes. (1) To explore the main pattern of factors that underlies each construct of SysTrust service conceptual framework, the quality of financial reporting and business performance and, (2) To reduce the large number of variables of each construct into orthogonal indices which can be used (the output of the principal component analysis) as an intermediate step (input) for further analysis by the regression analysis techniques in the following section. The principal component analysis was considered an appropriate method to overcome the potential problems of intercorrelation among the variables. The findings of the principal component analysis revealed that 11 factors could be extracted from the five major constructs of the SysTrust, four factors could be extracted for the quality of financial reporting and two factors could be extracted for the business performance. A summary of these factors, with accounting variance and eigenvalues, are presented in Table 6.24 for SysTrust, Table 6.25 for quality financial reporting and Table 6.26 for business performance respectively.

Table 6.24 Summary of the Factors Underlying the Major SysTrust Constructs

Constructs	Factors	Eigenvalue	% of Variance
1. Availability of AIS	Availability Polices	3.264	25.109
	Recovery Disaster Plan	3.125	24.040
	Availability communication	3.042	23.397
2. Security of AIS	Logical Security Access	5.132	28.510
	Security Policies and Communication	4.772	26.511
	Physical Security Access	3.817	21.203
3. Integrity Processing	Integrity Processing policies	4.683	27.549
	Data Transfer Control	3.477	20.453
	Output Control	3.370	19.826
4. Confidentiality	Confidentiality	7.621	63.505
5. Privacy	Privacy	6.709	67.091

Table 6.25 Factors underlying the Quality of Financial Reporting Measures

Factors	Eigenvalue	% of Variance
Understandability	5.245	20.981
Relevance	5.117	20.468
Faith representation	4.793	19.174
Comparability	3.944	15.775

Table 6.26 Summary of the Factors underlying Business performance Measures

Factors	Eigenvalue	% of Variance
Financial Performance	6.897	36.303
Non-Financial Performance	6.527	34.354

6.6 Section Two: Data Analysis and Testing Hypothesis

In the previous section, research findings related to the main pattern of factors that underlie each construct of the SysTrust's service conceptual framework as well as the main pattern of factors/components underlie the quality of financial reporting were presented. In this section, the eleven factors and associated variables (e. the reliability of AIS; defined here as independent variables); are analysed in terms of their relationships, direction, and strength; and their ability to predict the quality of financial reporting and business performance. Figure (6.1) shows the main components of the study's conceptual framework; the main principles of SysTrust's framework, the quality of financial reporting and business performance. The statistical analysis techniques used are multiple regressions and structural Equation Modelling, Test and T-test. Factors and variables are analysed and discussed in this chapter.

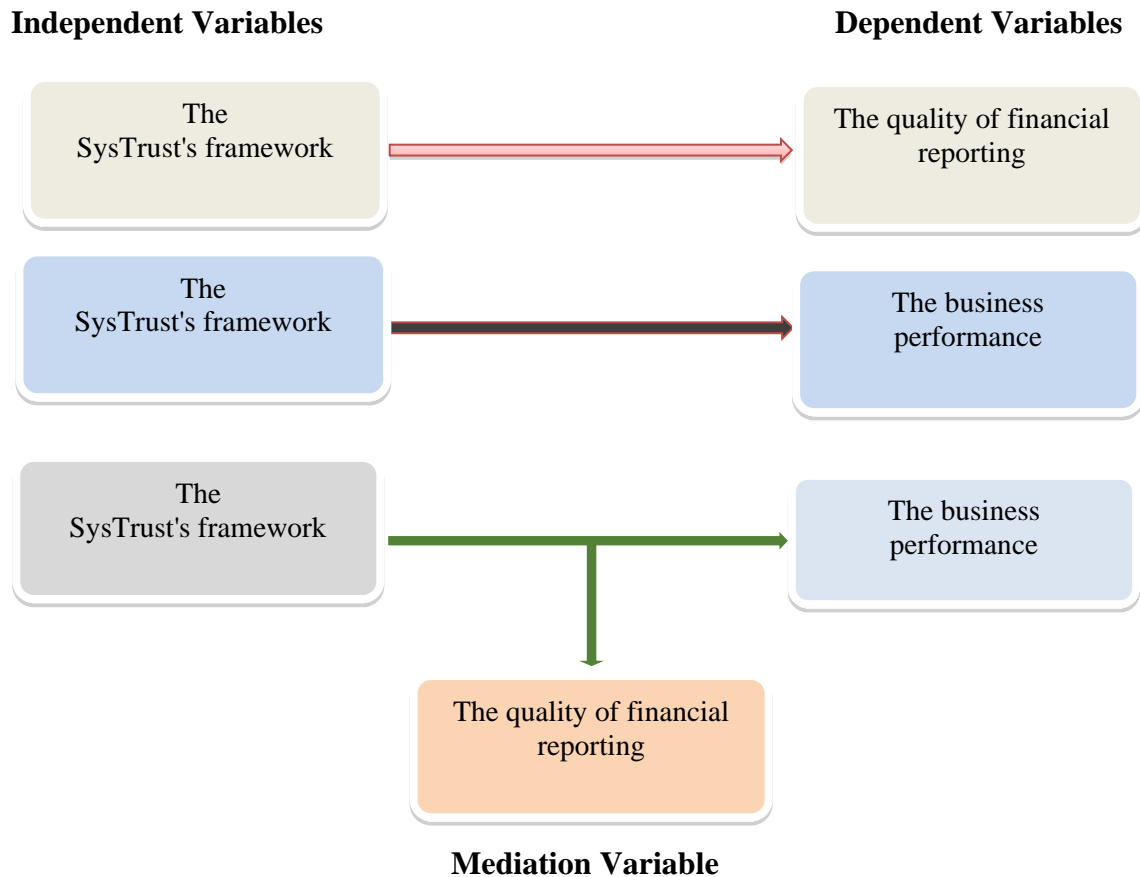


Figure 6.1 the Study's Conceptual Framework

*Source: Developed by the Researcher

6.7 The Extent of the Reliability of AIS Process in the Context of the Implementation of the SysTrust's Framework Requirements (Principles and Criteria)

The measure of extent of SysTrust's framework implementation requirements which used for assuring the reliability of AIS as an internal control method in Jordanian business organization were the main five principles and criteria (i.e., the availability, security, integrity processing, confidentiality and privacy). In this study, the extent of the implementation of these principles and criteria were identified and analysed. These were selected as they were the major constructs of the SysTrust's framework. The mean values, standard deviation and T-test are employed here to determine whether the SysTrust's framework requirements (i.e., availability, security, integrity processing, confidentiality, and privacy of AIS) are implemented and achieved in the business organizations in Jordan (see Table 8.1). Findings shown in Table 8.1 indicate that the extent of SysTrust's framework being practiced is considered to be good (i.e. 74% or 5.20%). since their mean are more than the mean of the scale, which is 4 (mean of the scale = Σ Degrees of the scale 7 =

$1+2+3+4+5+6+7 / 7 = 4$). This implies that there are some variations among shareholdings companies in terms of their level of implementations of SysTrust's framework (principles and criteria) as presented in Table (6.27) and it might be due to their type of the business and the nature of audit IT control system. The One sample t-test is used here to examine the following hypothesis.

H1 The overall reliability of the accounting information system of shareholding companies based on the implementation of SysTrust's framework (i.e. availability, security, integrity data processing, confidentiality, and privacy) are significantly achieved by their internal control system"

H1_n The overall reliability of the accounting information system of shareholding companies based on the implementation of SysTrust's framework (i.e. availability, security, integrity data processing, confidentiality, and privacy) are significantly not achieved by their internal control system

The result of one-sample T-test for the above hypothesis shows that implementation of SysTrust's framework requirements (principles and criteria) are significantly achieved as the internal control method for assuring the overall reliability of AIS in business organizations. This might indicate that internal control's methods over the computerised accounting information systems in the Jordanian business organizations provide requirements of all principals to the AIS system. Mean values have shown that the "Security" as an principle of the SysTrust's framework is the highly implemented one (79%), Assurance of system security implies that access is restricted to the physical components of the system, the logic functions the system performs, and the information stored in the system. These results are in consistent with prior studies such as Hayale and Abu Khadra, (2006), Abu Musa (2004) and Bortiz (2005).

Table 6.27 The level of Reliability of AIS in Business Organizations.

SysTrust Principles	Mean	Percentage	Standard deviation	Sig. (2-tailed)
Availability	5.1398	0.7342	0.86783	0.000
Security	5.5559	0.7937	0.91053	0.000
Integrity processing	5.2214	0.7459	0.76369	0.000
Confidentiality	5.2184	0.7454	0.87010	0.000
Privacy	5.2254	0.7464	0.91306	0000
Average practice	5.2214	0.7459	0.75279	0.000

It could be concluded that the IT infrastructure of the Jordanian business originations by its status qua is mature enough to provide the operational requirements for SysTrust's framework. Such result was supported by the results reached by Casolaro and Gobbi, (2004) and, Masour, et. al., (2009)

The ANOVA analysis technique is used here to examine a following hypothesis.

H2. The overall reliability of accounting information system of shareholding companies based on the implementation of SysTrust's framework (i.e. availability, security, integrity data processing, confidentiality, and privacy) are significantly differ according to their demographic characteristics (type of business sectors, number of employees, business experience)

H2_n. The overall reliability of accounting information system of shareholding companies based on implementation of the SysTrust's framework (i.e. Availability, security, integrity data processing, confidentiality, and privacy) are not significantly differ according to their demographic characteristics (type of business sectors, number of employees, business experience).

To assess the differences among business organizations in terms of the implementation of SysTrust's framework (principles and criteria) based on their organization's demographic characteristics such as size, type of business and business experience (age). One-way analysis of variance (ANOVA) was used to compare the means of participants' extent of the existences of the SysTrust's principles in AIS infrastructure in their business. As it is shown in Table 6.28, there are significant differences among business originations in terms of the practice of SysTrust's framework (principles and criteria) either taken separately or together due to their types of business sector (e.g., financial or non-financial service or industrial business) to which they belong. when compared, the extent of SysTrust's framework being practiced among business organizations in terms of type of business (banks, insurance, and service companies vs. industrial companies) service companies were found at a significant edge over industrial companies on all the five principles of the SysTrust's framework. This clearly indicated that the service companies apply or give more attention to the requirements of SysTrust's framework than the industrial companies. This might be due to the fact that service companies tend to be more technology-oriented and driven than industrial companies in Jordan.

Table 6.28 The level of significance of the SysTrust's Framework Implementation among Groups of Organizations based on the type of Business (industrial vs. Services)

SysTrust Principles		Sum of Squares	Mean Square	F	Sig.
Availability	Between Groups	12.125	6.063	8.395	.0000
	Within Groups	247.706	0.722		
	Total	259.832			
Security	Between Groups	9.398	4.699	5.827	0.003

	Within Groups	276.627	0.806		
	Total	286.025			
Integrity Processing	Between Groups	4.249	2.124	3.700	0.026
	Within Groups	196.964	0.574		
	Total	201.213			
Confidentiality	Between Groups	8.919	4.459	6.063	0.0003
	Within Groups	252.272	0.735		
	Total	261.190			
Privacy	Between Groups	12.383	6.192	7.716	0.001
	Within Groups	275.233	0.802		
	Total	287.616			
Total (All together)	Between Groups	8.735	4.367	8.021	0.000
	Within Groups	186.775	0.545		
	Total	195.510			

Table 6.29 The level of significance of the SysTrust's Framework Implementation among groups of Organizations based on the Size of Business.

SysTrust Principles		Sum of Squares	Mean Square	F	Sig.
Availability	Between Groups	3.804	1.268	1.694	0.168
	Within Groups	256.027	0.749		
	Total	259.832			
Security	Between Groups	4.232	1.411	1.712	0.164
	Within Groups	281.792	0.824		
	Total	286.025			
Integrity Processing	Between Groups	5.516	1.839	1.213	0.123
	Within Groups	195.697	0.572		
	Total	201.213			
Confidentiality	Between Groups	3.629	1.210	1.606	0.188
	Within Groups	257.561	0.753		
	Total	261.190			
Privacy	Between Groups	6.073	2.024	2.459	0.063
	Within Groups	281.543	0.823		
	Total	287.616			
Total (All together)	Between Groups	4.232	1.411	2.522	0.058
	Within Groups	191.279	0.559		
	Total	195.510			

Table 6.30 The level of significance of the's SysTrust's Framework Implementation among groups of Organizations based on the Experience in Business

SysTrust Principles		Sum of Squares	Mean Square	F	Sig.
Availability	Between Groups	4.413	2.471	1748	0.119
	Within Groups	242.419	0.638		
	Total	259.832			
Security	Between Groups	1.853	0.618	0.743	0.527
	Within Groups	284.172	0.831		
	Total	286.025			
Integrity Processing	Between Groups	2.407	0.802	1.380	0.249
	Within Groups	198.806	0.581		
	Total	201.213			
Confidentiality	Between Groups	4.195	1.398	1.861	0.136
	Within Groups	256.995	0.751		
	Total	261.190			
Privacy	Between Groups	2.472	0.824	0.988	0.398
	Within Groups	285.144	0.834		
	Total	287.616			
Total (All together)	Between Groups	3.379	1.126	2.005	0.113
	Within Groups	192.131	0.562		
	Total	195.510			

In their study of electronic data interchange (EDI), Khazanchi and Sutton (2001) give evidence of the requirement for systems assurance, illustrating that numerous companies enforcing these systems do not use them to full benefit. However, the results shown in Tables 6.29 and 6.30 respectively that there were no significant differences among business organizations in terms of reliability of AIS based on the implementation of the five principles of the SysTrust's framework; either taken together or separately due to their size or experience. These results suggest that irrespective of their size or experience, business organizations might aware of the importance of reliability of AIS process based on the implementation of the five principles of the SysTrust's framework.

6.8 Relationship between the Reliability of AIS and the Quality of Financial Reporting

The multiple regression analysis technique is used to examine the following hypotheses.

H (3). There is a significant relationship between the reliability of AIS based upon the implementation of the principles of SysTrust's framework (i.e., availability, security, integrity data processing, confidentiality, and privacy) and the quality of financial reporting.

H_n (3). There is no any significant relationship between the reliability of AIS based upon the implementation of the principles of SysTrust's framework (i.e., availability, security, integrity data processing, confidentiality, and privacy) and the quality of financial reporting.

Table 6.31 summarizes the results of multiple regression analysis, with the F-ratio test for the above hypothesis. The results indicate that is significant and positive relationship between the reliability of AIS based on the implementation of the principles of the SysTrust's framework. It has been empirically proved that the reliability of AIS has impact on the quality of financial data reporting on the Jordanian business organizations. The reliability of AIS and the quality of financial reporting s at 0.000 level of significant. Accordingly, it may be concluded that higher is the level of reliability of AIS based on the implementation of principles of SysTrust's framework requirements, the higher is the quality of financial data reporting. The reliability of internal control system of accounting information systems has a positive relationship to the financial reporting to produce reliable financial statements (Daneila, 2013). While Internal control weaknesses in overseeing the accounting information system will affect the likelihood that a material error in reporting (Ricchiute, 2006). Internal control is needed to oversee the accounting system that can produce reliable financial statements (Konrath, 2002; 2005).

Table 6.31 A Summary Result of the Multiple Regressions: The Relationship between the Reliability of AIS and the quality of Financial Reporting.

Hypotheses	Multiple R	R. Square	Adjusted R Square	DF	F	Sign
H3	0.822	0.676	0.665	11	63.340	0.000

According to the stepwise multiple regression method, the factors which highly correlated with the dependent variable (i.e., the level of implementation of SysTrust's framework) is expected to enter into the regression equation. The F value at 0.00 level of significance is used to determine the “goodness of fit” for the regression equation. The F value is the ratio of explained to unexplained variance accounted for by the regression equation, when the total variance accounted is low, interpretation of the individual beta coefficient has little meaning (SPSS, 2016). Therefore, when the adjusted R square is around .10 or above and the F value of the regression equation reaches to 0.05 level of significance, the individual beta weight is explained.

Also, in this study the severity or degree of multicollinearity is tested by examining the relative size of the pairwise correlation coefficient between the explanatory independent factors. An examination of the correlation matrix indicates that the correlation for each coefficient is less than about (0.50). Therefore, it is possible to interpret the findings since the multicollinearity is not severe (Hair et al., 2010). Hair, et. al. (2010) recommended assessing the tolerance and variance inflation factor (VIF). Tolerance refers to the assumption

of the variability in one independent variable that does not explain the other independent variable. The VIF reveals much of the same information as the tolerance factor. The common cut off threshold is a tolerance value of 0.10, which corresponds to VIF value above 10. Multicollinearity was indicated in a tolerance level of less than 0.10 or a VIF value above 10. The tolerance 1 value for each independent variable above the ceiling tolerance value of 0.10, is consistent with the absences of serious level of multicollinearity. This judgment was further supported by a VIF value for each independent variable above the threshold value of 1.0. For more details, as presented in Table 6.32

Table 6.32 Collinearity Diagnostics

SysTrust Principles	Independent Factors	Tolerance	VIF
1. Availability of AIS	AIS availability Polices	0.696	1.437
	Recovery Disaster Plan	0.571	1.750
	Availability communication	0.720	1.389
2. Security of AIS	Logical Security Access	0.487	2.055
	Security Policies and Communication	0.494	2.026
	Physical Security Access	0.655	1.528
3. Integrity Processing	Integrity Processing policies	0.404	2.475
	Data Transfer Control	0.420	2.383
	Output Control	0.564	1.774
4. Confidentiality	Confidentiality	0.186	5.387
5. Privacy	Privacy	0.198	5.057

The results of the stepwise regression analysis indicate that extracted factors form the main principles of the SysTrust's framework (i.e., all 11 factors, taken together) are significantly related to the quality of financial data reporting. The direction of this relationship is positive. The findings also indicate that out of those 11 explanatory independent factors, only six factors included in the regression equation. These six factors in terms of their order of importance are: (1) Privacy, (2) Confidentiality, (3) Output control, (4) AIS availability policies, (5) Security policies and communication, and (6) Physical security access, see Table 6.33.

Table 6.33 The Stepwise Regression Analysis. Factors of the SysTrust; Taken Together.

Factors	Step	R	R Square	Adjusted R Square	Beta	Sig.
Privacy*	1	0.788	0.621	0.620	0.144	0.000
Confidentiality	2	0.806	0.649	0.647	0.053	0.000
Output Control	3	0.810	0.657	0.654	0.018	0.000
Physical Security Access	4	0.813	0.662	0.658	0.012	0.000
Security Policies and Communications	5	0.817	0.667	0.662	0.010	0.000
AIS availability Polices	6	0.820	0.673	0.667	0.010	0.000

*Constant factor

The adjusted square for these six factors is 0.677 as shown in Table 6.33. This indicates that about 68% of the variations of the quality of financial data reporting can be explained by these factors. The "Privacy" factor is shown to be the first most important factor that related to the quality of financial reporting. The Adjusted R square for this factor is 0.620, which might imply that the privacy of AIS is necessary for enhancing the quality of financial reporting. The "Confidentiality" factor is the next important factor that is highly associated with the quality of financial reporting. This might imply that the availability of confidentiality principle requirement is important for companies want to improve the quality of financial reporting. The "Output control", "Physical Security Access" and "Security Policies and Communications" factors which represent the construct of "Security " are ranked at the third, fourth and fifth respectively as the most important factors associated with enhancing the quality of financial reporting. This might indicate on how much the availability of security principles are important to the quality of financial reporting. Finally, the last important factor is the "AIS availability Polices". The result indicates that there is a positive relationship between this factor and the quality of financial reporting. This might indicate that the higher importance attached to the AIS availability policies, the higher level of quality of financial reporting will be.

6.9 The Relationship between the Relationship between the Reliability of AIS and Business Performance Dimensions (Financial and non-financial); Taken Together or Separately

6.9.1 Multiple Regression Findings

Multiple regression analysis technique was used to examine the following hypotheses.

H4 There is significant relationship between the level of implementation of the SysTrust's framework and financial business performance

H4_n. There is no significant relationship between the level of implementation of the SysTrust's framework and financial business performance.

H5 There is significant relationship between the level of implementation of the SysTrust's framework and non- financial business performance.

H5_n There is no significant relationship between the level of implementation of the SysTrust's framework and non- financial business performance.

H6 There is significant relationship between the level of implementation of the SysTrust's framework and the two business performance factors. Financial and non-financial business performance; taken together.

H6_n There is no significant relationship between the level of implementation of the SysTrust's framework and the two business performance factors. Financial and non-financial business performance; taken together

The main objective of analysis here is to understand the relationship between the reliability of AIS and business performance dimensions (financial and non- financial performance (either taken separately or together. A summary of the results of multiple regression analysis, with the F-ratio test, for the above hypotheses are presented in Table 6.34. The results indicate that there are significant and positive relationship between the extent of SysTrust's framework being used for assuring the reliability of AIS and the two business performance factors (financial and no-financial) either taken separately or together at 0.000 level of significance, taken together. Thus, it can be concluded that there appears to be an important relationship between the reliability of AIS and business performance.

Table 6.34 A Summary Result of the Multiple Regressions. The Relationship between the reliability of AIS and Business Performance Dimensions; separately and together

Hypotheses	Components (types)	Multiple R	R ²	Adjusted R ²	DF	Std. Error of Estimation	F-Sign
H5	Financial	0.515	0.265	0.241	11	0.655	0.000
H6	Non-financial	0.621	0.386	0.365	11	0.642	0.000
H7	Taken together	0.751	0.564	0.550	11	0.594	0.000

Dependent Variable

The result also shows that about $R^2 = 56\%$ of variance of the two factors of business performance; (financial and non-financial factors) could be explained by the implementation of the SysTrust framework requirements, which is much higher than once each factor taken separately (financial 0.365 and non-financial 0.241). According to the stepwise multiple regression method, the factors which highly correlated with the dependent variable (i.e., the two business performance factors together) is expected to enter into the regression equation. The F value at 0.00 level of significance is used to determine the “goodness of fit” for the regression equation. The F value is the ratio of explained to unexplained variance accounted for by the regression equation, when the total variance accounted is low, interpretation of the individual beta coefficient has little meaning (SPSS, 2013). Therefore, when the adjusted R² is around 0.10 or above and the F value of the regression equation reaches to 0.05 level of significance, the individual beta weight is explained. The findings of the stepwise regression analysis are presented and discussed here under the following subsections.

6.9.2 Stepwise Multiple Regressions: Non- Financial Performance Dimension (As a Dependent Variable; taken alone).

The results of the stepwise regression analysis indicate that reliability of AIS based upon the implementation (i.e., all 11 factors which were extracted from the SysTrust's frameworks) is significantly related to the non- financial performance dimension.

Table 6.35 The Stepwise Regression Analysis. Non- Financial Performance

Factors	Step	R	R Square	Adjusted R Square	Beta	Sig.
Privacy	1	0.577	0.333	0.331	0.572	000
AIS availability Polices	2	0.595	0.354	0.350	0.168	000
Logical Security Access	3	0.607	0.369	0.363	0.131	000

*Constant factor

The Stepwise regression analysis findings also indicate that out of those 11 explanatory independent factors, only three factors included in the regression equation. These three factors in terms of their order of importance are: (1) "Privacy", (2) "Availability of AIS Policies", and (3) "Logical Security Access". The adjusted square (R^2) for these three factors is 0.363 as shown in Table 6.35. This indicates that about 36% of the variations of the non-financial performance can be explained by these three factors of SysTrust.

6.9.3 Stepwise Multiple Regressions. Financial Performance Dimension as a Dependent; taken alone.

The results of the regression analysis indicate that the reliability of AIS based on implementation of the SysTrust's framework requirements (i.e., all 11 factors; taken together) is significantly related to the financial performance dimension. The direction of this relationship is positive. The Stepwise regression analysis findings also indicate that out of those 11 explanatory independent factors, only three factors included in the regression equation. These three actors in terms of their order of importance are: (1) "Confidentiality", (2) "Availability of AIS Communication and Training", and (3) "Security Policies and Communication". The findings shown Table 8.10 indicate that only three of the explanatory independent factors are included in the regression equation.

Table 6.36 The Stepwise Regression Analysis: Financial Performance.

Factors	Step	R	R Square	Adjusted R Square	Beta	Sig.
Confidentiality*	1	0.455	0.207	0.204	0.455	0.000
Availability of AIS Communication & Training	2	0.478	0.229	0.224	0.402	0.000
Security Policies and Communication	3	0.496	0.246	0.239	0.157	0.000

*Constant factor

The adjusted square for these three factors is (R^2) 0.239 as shown in Table 6.36. This indicates that about 24% of the variations of the non-financial performance can be explained by these factors. In comparing the results shown in Table 6.36 with those of the non-financial performance, it may be concluded that the impact of the implementation of SysTrust's framework requirements upon the non-financial performance 0.36 produce slightly higher explanation of the variance than upon the financial performance 0.24.

6.9.4 Stepwise Multiple Regressions. Financial and Non-Financial Performance Factors; taken Together.

This approach is expected to provide evidence to the influence of the availability (implementation) of SysTrust's framework requirements upon business performance dimensions (i.e., combination of financial and non-financial measures), taken together when compared with their influence upon each dimension acts alone. More of the predictor factors are expected to enter in the regression equation. The findings of the multiple regression indicate that implementation of the SysTrust's framework (i.e. all 11 factors) are associated with the combination of financial and non-financial factors. The findings also indicate that out of the 11 factors extracted for the SysTrust's framework, only 7 factors are included in the regression equation. The adjusted R square for those only 7 factors together is 0.553, i.e., about 55% of the variation of combination of financial and non-financial business performance is explained by them Table 6.37. Those 7 most important factors included in the regression equation are in terms of their order of importance. "privacy", " Security policies and communication ", " Physical Security Access", " Availability of AIS communication and Training ", "AIS Availability Policies", "Confidentiality", "Employment structure", and "Integrity Processing Policies".

Table 6.37 The Stepwise Regression Analysis. Combined financial and Non-Financial dimensions, taken together

Factors	Step	R	R Square	Adjusted R Square	Beta	Sig.
Privacy*	1	0.701	0.491	0.490	0.389	0.000
Security policies and communication	2	0.715	0.511	0.508	0.151	0.000
Physical Security Access	3	0.729	0.531	0.527	0.131	0.000
Availability of AIS communication and Training	4	0.736	0.541	0.536	0.134	0.000
AIS Availability Policies	5	0.742	0.551	0.545	0.102	0.000
Confidentiality	6	0.746	0.557	0.549	0.181	0.000
Integrity Processing Policies	7	0.750	0.562	0.553	-0.081	0.000

*Constant factor

In comparing this solution with the other two solutions presented in the previous sections, it may be concluded that the influence of availability of SysTrust principles upon the combination of the two business performance dimensions (i.e., financial and non-financial) would give slightly better explanation (predictive power) than upon each factor acting alone. The rate of explanation which they account for is increased from 24% (non-financial performance) and 36% (financial performance) to about 55% as presented in Table 6.37. The importance factors of the SysTrust's framework that related to each type of business performance (i.e., financial, non-financial and combined) are summarised in Table 6.38.

This conclusion implies that a better understanding of the impact of the implementation of the SysTrust's framework requirements on business organizations upon their business performance requires that the two combinations of financial and non-financial performance dimensions should be viewed and investigated together rather than only viewing each of them alone. Furthermore, viewing financial performance alone would also give better understanding than viewing non-financial performance alone. Based upon the researcher's knowledge, this result has not investigated before. Therefore, it needs further investigation in future.

Table 6.38 A summary of the Stepwise Regression Analysis. The Importance of SysTrust Factors Related to Business Performance

SysTrust Principles	Factors		Non-Financial	Financial	Combined
1. Availability of AIS	Factor (1)	AIS availability Polices	*		*
	Factor (2)	Recovery Disaster Plan			
	Factor (3)	Availability communication & Training		*	*
2. Security of AIS	Factor (4)	Logical Security Access	*		
	Factor (5)	Security Policies and Communication		*	*
	Factor (6)	Physical Security Access			*
3. Integrity Processing	Factor (7)	Integrity Processing policies			*
	Factor (8)	Data Transfer Control			
	Factor (9)	Output Control			
4. Confidentiality	Factor (10)	Confidentiality		*	*
5. Privacy	Factor (11)	Privacy	*		*

*Important factors

6.10 The Relationship between the Reliability of AIS and Business Performance Via the Quality of Financial Reporting as a Mediating

The simple and multiple regression analysis techniques are used to examine the following hypotheses.

H7. The quality of financial reporting is significantly mediating the relationship between the implementation of SysTrust's framework requirements and business performance.

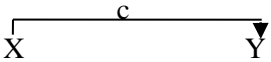

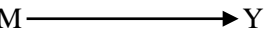
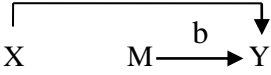
H7_n. The quality of financial reporting is not significantly mediating the relationship between the implementation of SysTrust's framework requirements and business performance

Mediation is a hypothesised causal chain in which one variable affects a second variable that, in turn, affects a third variable. The intervening variable, M, is the mediator. It mediates the relationship between a predictor, X, and an outcome (Biesanz, et. al., 2010). Graphically, mediation can be depicted in the following way (Sekaran and Bougie, 2013).



Paths (a) and (b) are called direct effects, the mediational effect, in which X leads to Y through M, is called the indirect effect. The indirect effect represents the portion of the relationship between X and Y that is mediated by M (UPA, 2015). In order to test for mediation Baron and Kenny (1986) proposed a four steps approach in which several regression analyses are conducted and the significance of the coefficients is examined at each step. Table 6.39 presents a detailed explanation of the approach proposed by Baron and Kenny (1986).

Table 6.39 Steps for testing mediation

	Analysis	Visual depiction
Step 1	Conduct a simple regression analysis with X predicting Y to test for path c alone, $Y = B_0 + B_1X + e$	
Step 2	Conduct a simple regression analysis with X predicting M to test for path a, $M = B_0 + B_1X + e$	
Step 3	Conduct a simple regression analysis with M predicting Y to test the significance of path b alone, $Y = B_0 + B_1M + e$	
Step 4	Conduct a multiple regression analysis with X and M predicting Y, $Y = B_0 + B_1X + B_2M + e$	

Steps 1-3 determine whether zero-order relationships among the variables exist. If one or more of these relationships are non-significant, researchers usually conclude that mediation is not possible or likely, however this may not always be true (MacKinnon, et. al., 2007). Assuming there are significant relationships from Steps 1 through 3, one proceeds to Step 4. In the Step 4 model, some form of mediation is supported if the effect of M (path b) remains significant after controlling for X. If X is no longer significant when M is controlled, the finding supports full mediation. If X is still significant (i.e., both X and M both significantly predict Y), the finding supports partial mediation (UPA, 2015). To test this hypothesis a combination of simple and multiple regression analyses was conducted as proposed by Baron and Kenny (1986). The results of the regression tests can be seen in Table 8.14. It is worth noting that the Baron and Kenny (1986) model of mediation focuses on the unstandardized regression coefficients, therefore, the coefficients mentioned in Table 6.40 represent the unstandardized betas.

Table 6.40 Regression Analysis for Mediation of Quality of Financial Reporting on Business Performance through the Implementation of SysTrust Principles

Variables	Step 1 Business Performance	Step 2 Quality of Financial Reporting	Step 3 Business Performance	Step 4 Business Performance
Constant	-3.479-**	-2.753**	-1.173E-016*	-1.059-**
SysTrust Principles	0.660**	0.522**		0.201**
Quality of Financial Reporting			0.558**	0.879**
R	0.702 ^a	0.786 ^a	0.790 ^a	0.801 ^a
R²	0.493	0.618	0.623	0.641
Adj. R²	0.492	0.617	0.622	0.639
F-value	335.111	557.165	569.312	305.973

** p ≤ 0.00.

In order to determine whether the quality of financial reporting acts as a mediator in the relationship between the level of implementation of SysTrust's framework requirements, (i.e., the overall reliability of AIS) and business performance, the following rule should be followed. Some form of mediation is supported if the effect of the expected mediator remains significant after controlling for the independent variable. If the independent variable is no longer significant when the expected mediator is controlled, the finding supports full mediation. If the independent variable is still significant (i.e., both the independent variable and the expected mediator both significantly predict the existence since the implementation of SysTrust's framework requirements and quality of financial reporting both significantly predict business performance (p-values = 0.000). Furthermore, the strength of the independent variable in predicting the dependent should be reduced in the presence of the mediator variable in order to support partial mediation. In this case the unstandardized beta for the implementation of SysTrust's framework requirements was reduced from 0.66 to 0.21 which supports the condition for partial mediation. According to Baron and Kenny (1986) having a partial mediation model is more realistic in most social science research because a single mediator cannot be expected to completely explain the relationship between the independent variable and the dependent variable.

Although Baron and Kenny (1986) provide an appealing approach to follow in order to determine the presence or absence of a mediation effect, it is considered necessary to conduct a formal significance test of the indirect effect if the Baron and Kenny criteria have been met (Preacher and Hayes, 2004). This is important for two reasons. First, there are shortcomings

related to the Baron and Kenny method. According to Holmbeck (2002) it is possible to observe a change from a significant $X \rightarrow Y$ path to a non-significant $X \rightarrow Y$ when adding a mediator to the model with a very small change in the absolute size of the coefficient. This result may lead a researcher to erroneously conclude that a mediation effect is present (Type I error). Conversely, it is possible to observe a large change in the $X \rightarrow Y$ path when adding a mediator to the model without observing a change in statistical significance (Type II error). This situation is likely to occur when large samples are employed as those are the conditions under which even small regression weights may remain statistically significant. Testing the hypothesis of no difference between the total effect (path c) and the direct effect (path c') more directly addresses the mediation hypothesis than does the series of regression analyses recommended by Baron and Kenny (1986). In the case of simple mediation, the indirect effect of X on Y through M is measured as the result of the $X \rightarrow M$ and $M \rightarrow Y$ path (ab), which is equivalent to $(c - c')$ in most cases. Thus, a significance test associated with (ab) should address mediation more directly than a series of separate significance tests that do not directly involve (ab) (Preacher and Hayes, 2004).

There are more statistically rigorous methods by which mediation hypotheses may be tested (Preacher and Hayes, 2004). Baron and Kenny (1986) describe a procedure developed by Sobel (1982) that assesses more directly the indirect effect of mediation. According to MacKinnon and colleagues (2002) the Sobel test is considered a superior test in terms of power and intuitive appeal. The Sobel test is performed by comparing the strength of the indirect effect of X on Y to the point null hypothesis that it equals zero. The indirect effect of X on Y in this situation is defined as the product of the $X \rightarrow M$ path (a) and the $M \rightarrow Y$ path (b), or (ab). In most situations, $ab = (c - c')$, where c is the simple (i.e., total) effect of X on Y , not controlling for M , and c' is the $X \rightarrow Y$ path coefficient after the addition of M to the model. Standard errors of a and b are represented, by s_a and s_b , respectively. The standard error of the indirect effect (s_{ab}) is given by the following equation.

$$s_{ab} = \sqrt{b^2 s_a^2 + a^2 s_b^2 + s_a^2 s_b^2}$$

In order to conduct the test, ab is divided by s_{ab} to yield a critical ratio that is compared with the critical value from the standard normal distribution appropriate for a given alpha level. One of the assumptions necessary for the Sobel test is that the sample size is large, so the rough critical value for the two-tailed version of the test, assuming that the sampling distribution of ab is normal and that $\alpha = .05$, is ± 1.96 (Preacher and Hayes, 2004). Thus, it can be concluded that a more powerful strategy for testing mediation may be to require only (1) that there exists an effect to be mediated (i.e., $c \neq 0$) and (2) that the indirect effect be

statistically significant in the direction predicted by the mediation hypothesis (Preacher and Hayes, 2004). To calculate the indirect effect according to Sobel (1982), the unstandardized regression coefficient obtained from regressing the mediator to predict the dependent variable (adjusting for the independent variable) ($\beta = 0.522$) should be multiplied by the unstandardized regression coefficient obtained from regressing the independent variable to predict the mediator ($\beta = 0.879$). Thus, the indirect effect of the implementation of the SysTrust's framework (the overall of reliability of AIS) on business performance through quality of financial reporting = $0.522 \times 0.879 = 0.458$. In order to ensure that the indirect effect is significant, it is recommended to run Sobel test (Sobel, 1982). The Sobel test requires the computation of the raw regression coefficient (unstandardized coefficients) and the standard error for this regression coefficient for the association between the independent variable and the mediator (path a), and the association between the mediator and the dependent variable (adjusting for the independent variable, path b) (Pierce, 2003). The unstandardized β for path (a) = 0.558 and the standard error = 0.023, and for path (b) unstandardized $\beta = 0.522$ and the standard error = 0.022. The data are then entered into the following program to calculate the Sobel test value.

Table 6.41 The Sobel Test Value

Input		Test Statistic		Std. Error	P-Value
A	0.558	Sobel test	16.96322406	0.01717103	0
B	0.522	Arolan test	16.95586362	0.01717848	0
Sa	0.023	Goodman test	16.9705941	0.01716357	0
Sb	0.022	Rest all	Calculate		

The results revealed that the null hypothesis (H11) should be rejected and the alternative hypothesis (H11) should be accepted since the p-value for the Sobel test (< 0.001) falls below the established alpha level of 0.05, indicating that the association between the independent variable (the level of implementation of SysTrust principles) and the dependent variable business performance) is reduced significantly by the inclusion of the mediator (quality of financial reporting) in the model; in other words, there is evidence of mediation.

6.11 Neural Networks Analysis and Comparison

The purpose of this section is to compare the results of ANN with results of regression analysis. The aim of using linear models and neural networks, multilayer perceptron in order to predict the impact of the reliability of AIS using SysTrust's framework(the five main principles and related criteria) on business performance indicators (financial and non-financial and combined). The recent upsurge in research activities into artificial neural

networks (ANNs) has proven that neural networks have powerful pattern classification and prediction capabilities. ANNs have been successfully used for a variety of tasks in many fields of business, industry, and science. Comparison of neural nets with more multiple regression analysis techniques has been the focus of many recent studies. There are several ways to check the accuracy of the study assumptions, some are printed directly in R within the summary output and others are just as easy to calculate with specific functions. For examples, Mean Absolute Error (MAE) and Root mean squared error (RMSE) are two of the most common metrics used to measure accuracy for continuous variables. Both MAE and RMSE express average model prediction error in units of the variable of interest. Performance of the two methods under study, namely multiple linear regression and artificial neural network, in predicting the business performance is measured by using R. square score, F. Ratio and Mean Square Error (MSE). The same data obtained from the regression analysis is used to determine the mentioned values.

Table 6.42 Performance Comparison between ANN and MRA Model Using Statistical Criterion.

Statistical Model	Input	Output	R. Square Score	F. Ratio Score	Mean Square Error
Multiple Regression Results (MRA)	Reliability of AIS	Business performance	0.536	0.786	0.594
	Reliability of AIS	Financial	0.463	0.673	0.642
	Reliability of AIS	Non-financial	0.523	0.747	0.655
Neural Network Results (ANN)	Reliability of AIS	Business performance	0.580	0.731	0.350
	Reliability of AIS	Financial	0.510	0.586	0.380
	Reliability of AIS	Non-Financial	0.563	0.705	0.410

Using these statistical criteria as shown in Table 6.42, the results demonstrate that the artificial neural network outperformed the multiple linear regression models. The neural network gives value of estimation mean square error (MSE) less than linear relationship in all business performance predictions models (financial, non-financial and combined). Furthermore, the predictive ability of the artificial neural network (ANN) is very high and gives a highly accurate prediction as a result of pattern recognition or generalization made by the network. The neural network shows R. square scores (R^2) is higher than linear relationship for all predictive measures used in this study. In all of these following models, 70% of the database used for training and the remaining 30% were used for testing performance to obtain cross validation results. The performance of the network during the training phase is very high for different numbers of neurons. The testing data set gives the lowest mean square error (MSE) value when the network contains five hidden neurons. For example, the testing

data gives a low R^2 value of about 0.580 for business performance. This value indicates the proportion of total variation explained by the results is about 58%. Results are said to be satisfactory if the R^2 value is more than 0.80.

Nevertheless, results obtained from the network have a higher R^2 value than the multiple linear regression mode. Based upon this comparison, it may be concluded that ANN model can be used for predicating the impact of the reliability of AIS on business performance indicators (financial and non-financial); either taken separately or together due to its better performance compared with MRA model. The results of these two tests (ANN and MRA) confirmed that the business performance indicators (financial or non-financial or together) could be predicated by the reliability of AIS. Figures 6.2, 6.3 and 6.4 and Table 6.43 show the relative importance of each predictor variables (SysTrust’s principles) for three business performance indicators (financial and non-financial and combined) based on ANN approach.

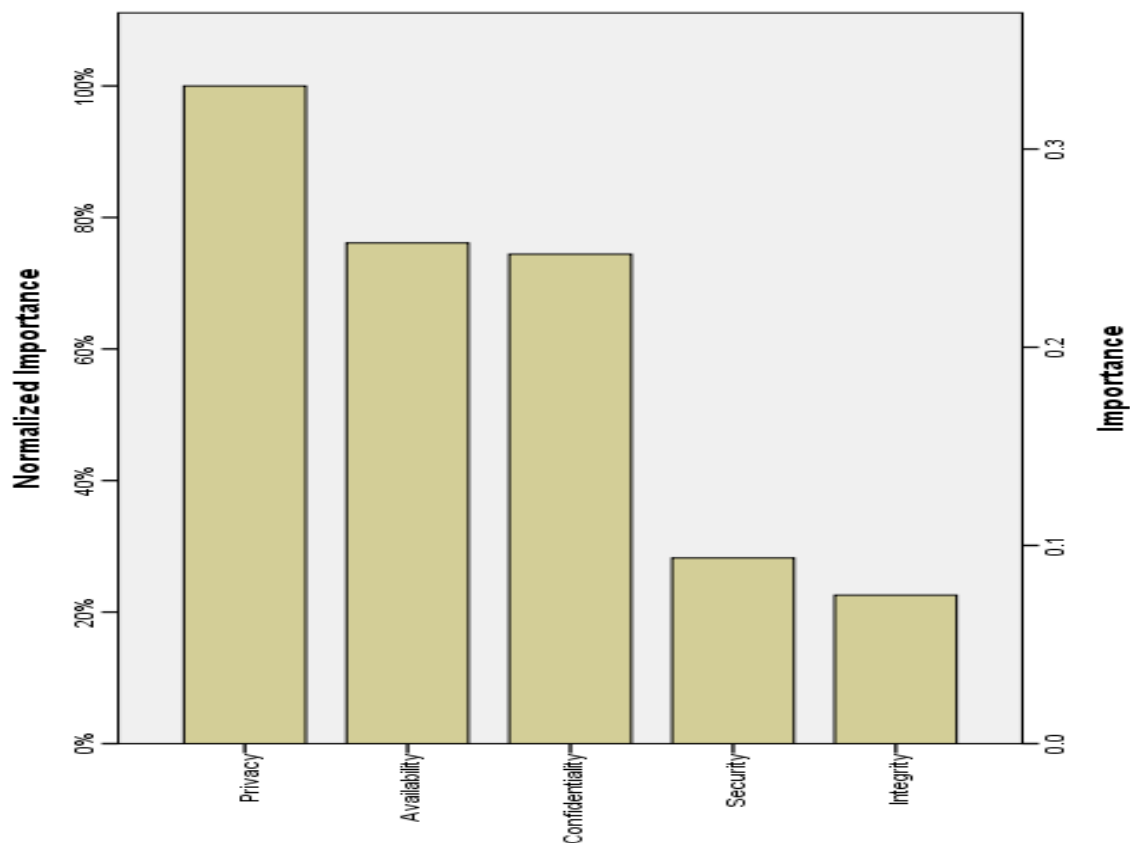


Figure 6.2 The Relative Importance of the Predictors of Business performance indicators (combined) based on ANN.

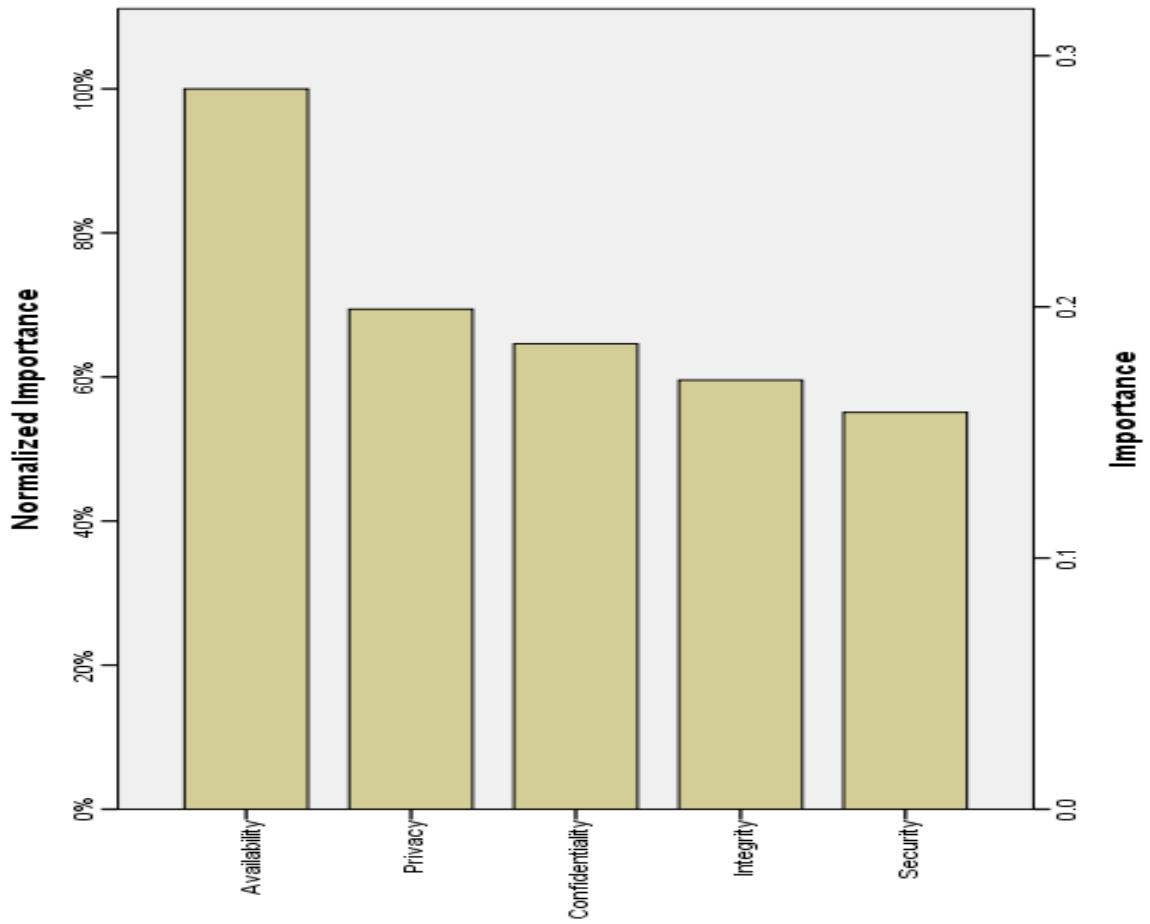


Figure 6.3 The Relative Importance of the Predictors of Financial Performance based on ANN.

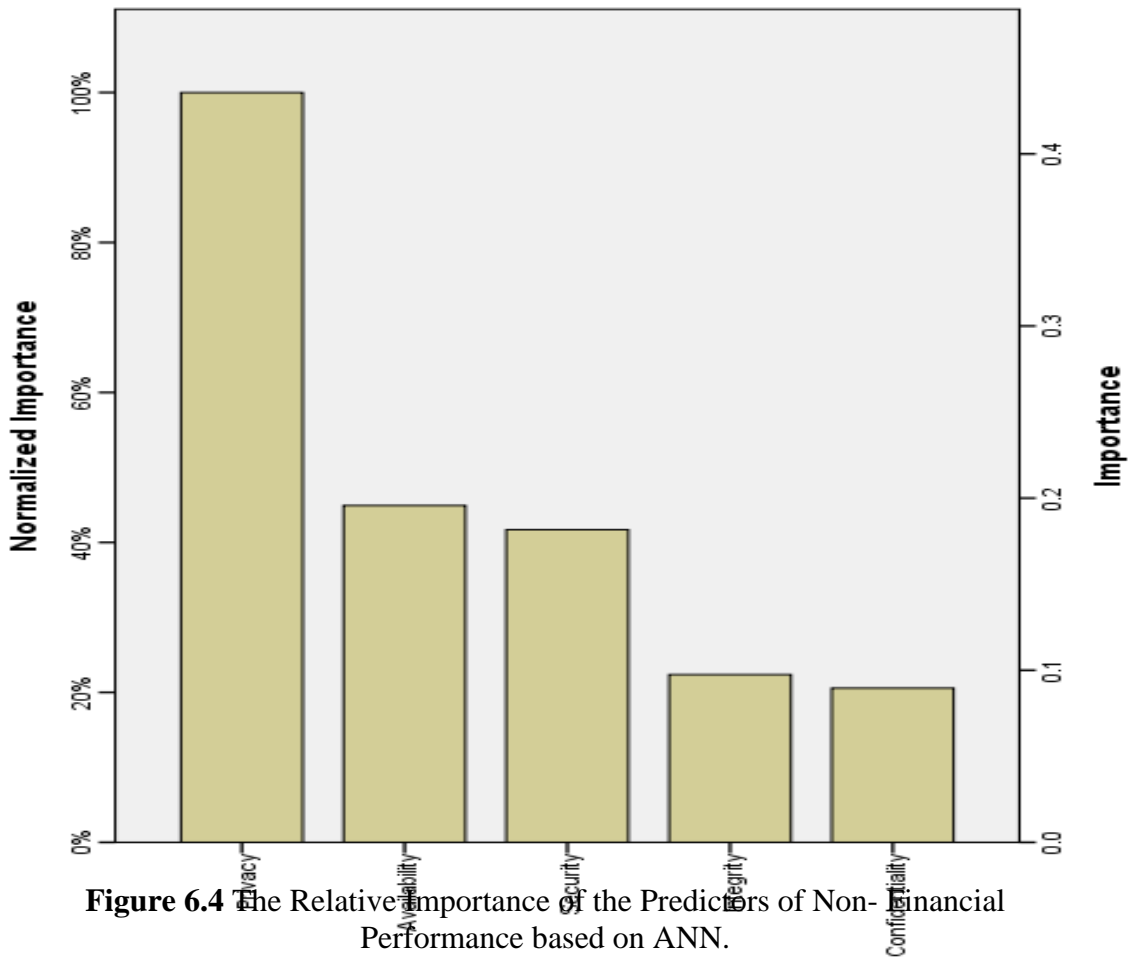


Figure 6.4 The Relative Importance of the Predictors of Non-Financial Performance based on ANN.

Table 6.43 The Relative Importance of SysTrust Factors Related to Business Performance Indicators based on ANN Analysis

Predictors	Business Performance (combined)		Financial Performance		Non-Financial Performance	
	%	Ranking	%	Ranking	%	Ranking
Availability	0.141	4	0.296	2	0.052	5
Security	0.121	5	0.168	4	0.162	3
Integrity	0.246	2	0.024	5	0.134	4
Confidentiality	0.206	3	0.317	1	0.215	2
Privacy	0.286	1	0.196	3	0.437	1

6.12 Structural Equation Modelling. The Validation of the Study's Conceptual Model

The study is applying the Structural Equation Modelling (SEM) technique to test the proposed relationships among the constructs in the study's model (Chapter Four). A two-stage approach of the SEM (measurement model and structural model) was employed to analyse the empirical data. By running AMOS21, the model fitness and constructs' reliability and validity were assessed in stage one (the measurement model) by means of the confirmatory factor analyses (CFA). This is followed by a structural model assessment which related to the validation of the conceptual model proposed and the testing of the causal paths between the main independent (exogenous) and dependent factors (endogenous). The main independent constructs (exogenous) components of SysTrust's framework are: (1) Availability of AIS, (2) Security of AIS, (3) Processing integrity of AIS, (4) Confidentiality, and (5) Privacy, while both the quality of financial reporting and business performance are all dependent (endogenous) constructs in the study's conceptual model. All of these constructs were subjected together to both measurement model and structural model analyses, and the results are presented in the following subsections.

6.12.1 Measurement Model: Confirmatory Factor Analysis

The confirmatory factor analyses (CFA) was employed to initially evaluate the measurement model's fitness (unidimensionality), and then measure the constructs' reliability and validity. It is also worth mentioning that, quality financial reporting and business performance both were considered as a second-order construct. In this regard, relevance, faithful representation, comparability, and understandability as the main dimensions for the quality financial reporting and these dimensions represent first-order factors measured through their own observed factors (items). As for the business performance, two main dimensions (financial

performance and non-financial performance) were treated as first order factor and they were measured using their observed items. The second-order of the confirmatory factor analyses (CFA) model fit was tested firstly for quality financial reporting and noticed that it does not have adequate level of model fitness due to the fact that some of indices do not capture values within their threshold levels ($\chi^2 = 2767.336$, $df = 204$; and $\chi^2/df = 13.565$), comparative fit index [CFI] = 0.756, goodness-of-fit index [GFI] = 0.678, incremental fit index [IFI] = 0.755, normed of fit indices [NFI] = 0.70 and root mean square error of approximation [RMSEA] = 0.161), AGFI= 0.601 (Hu and Bentler, 1999). Therefore, there is room for some re-specifications and purification (Byrne, 2010). Fundamentally, a refinement process followed a number of criteria to enhance the model's fitness including inspection of standardised regression weights (factor loading), modification indices, and standardised covariance matrix (Byrne, 2010; Hair, et. al., 2010; Holmes-Smith, et. al., 2006). By looking at standardised regression weights for each item, it was found that R4 (relevance), R6 (relevance), F2 (faithful representation), U3 (understandability), CC4 (Comparability) all have a value less than the cut-off value (>0.5), and accordingly, a decision was made to delete them. According to the modification indices' table, error terms of R7, U5, U7, and CC6 were found to have a higher error term value, and accordingly these items were deleted (Hooper et al., 2008).

Table 6.44 Results of Measurement Model-second order Factor. Quality of Financial Reporting

Fit indices	Cut-off point	Initial measurement model	Modified measurement model
CMIN/DF	≤ 3.000	13.565	1.808
GFI	≥ 0.90	0.868	0.918
AGFI	≥ 0.80	0.601	0.887
NFI	≥ 0.90	0.700	0.959
CFI	≥ 0.90	0.756	0.973
RMSEA	≤ 0.08	0.161	0.071

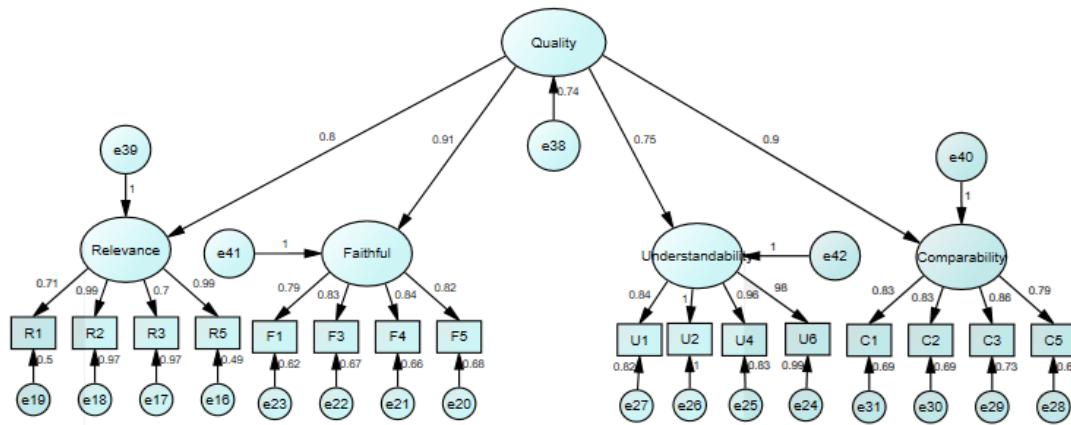


Figure 6.5 Second-order Factor analysis of quality reporting

By doing so, the CFA for the second order factor regarding the quality of financial reporting was tested again as suggested by Byrne (2010). The yielded fit indices indicated that the goodness of fit of the modified measurement model was adequately improved; all the fit indices this time were found within their recommended level as such. CMIN/DF = 1.808, GFI = 0.918, AGFI = 0.887, NFI = 0.959, CFI = 0.973 and RMSEA = 0.071 (see Table 6.44). As mentioned above, business performance was also considered as a second order factor. The initial fit indices were not found to be within their recommended level (i.e. CMIN/DF was 5.333, GFI = 0.751, AGFI = 0.701, NFI = 0.781, CFI = 0.792 and RMSEA = 0.095 (see Table 6.45). Thus, it was a need to revise the second order measurement model of business performance. According to an investigation of the standardised regression weight for each first order construct, it was identified that three items of non-financial performance (NF9; NF7; NF1) and two items of financial performance (FF4 and FF10) had a value less than 0.50; therefore, these items were removed. According to standardised residual matrix, the value of FF9 from financial performance, NF4 from non-financial performance did not exist within their acceptable scope (± 2.58) (Hair, et. al., 2017), and accordingly, they were dropped. Further, modification indices indicated that FF8, FF6, FF5, FF8, and NF2 had a higher unacceptable value, and hence, the decision was taken to eliminate these items. The CFA for the second order factor regarding the business performance was tested again as suggested by Byrne (2010). The yielded fit indices indicated that the goodness of fit of the modified measurement model was adequately improved; all the fit indices this time were found within their recommended level as such. CMIN/DF was 2.212, GFI = 0.932; AGFI = 0.891, NFI = 0.979, CFI = 0.981 and RMSEA = 0.061 (see Table 6.45).

Table 6.45 Results of Measurement Model-second order Factor. Business Performance

Fit indices	Cut-off point	Initial measurement model	Modified measurement model
CMIN/DF	≤ 3.000	5.333	2.212
GFI	≥ 0.90	0.751	0.932
AGFI	≥ 0.80	0.701	0.891
NFI	≥ 0.90	0.781	0.979
CFI	≥ 0.90	0.792	0.981
RMSEA	≤ 0.08	0.095	0.061

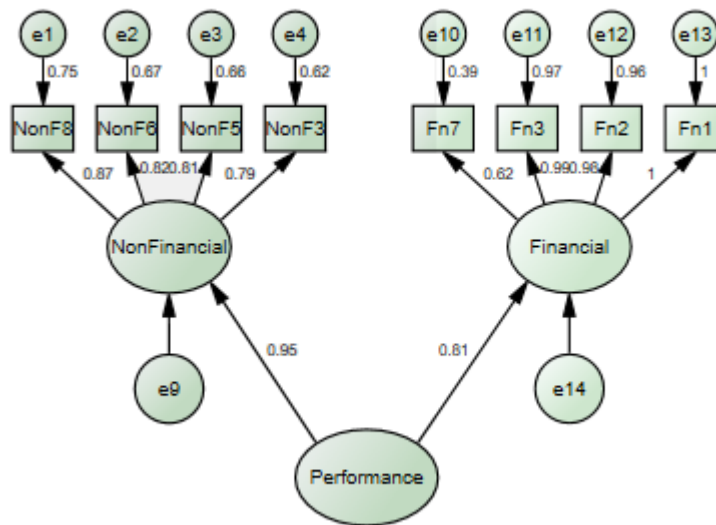


Figure 6.6 Second-order Factor analysis of business performance

Model Fitness for all Constructs

A number of fit indices (CMIN/DF; GFI; AGFI; NFI; CFI; RMSEA) have been tested to ensure an adequate level of model goodness of fit to the data (Byrne, 2010; Hooper, et. al., 2008). As seen in Figure 6.7, seven latent constructs [Availability of AIS, security of AIS, processing integrity of AIS, confidentiality, privacy, quality of financial reporting and business performance] formed the measurement model and therefore are subjected to the confirmatory factor analysis (CFA). Furthermore, 88 indicators (items) were adopted to measure these latent constructs as illustrated in the research methodology Chapters Four and Five. As shown in Table 6.46, the preliminary measurement fit indices were found as follows, chi-square (CMIN/DF = 2.323; GFI = 0.730; AGFI = 0.710, RMSEA = 0.062; NFI = 0.837; CFI = 0.900). Having a closer look at some of the fit indices (e.g. GFI, AGFI, NFI), the model does not seem to have adequate fit to data, and therefore, there is room for some re-specifications and purification (Byrne, 2010). Fundamentally, a refinement process followed a number of criteria to enhance the model’s fitness beginning with inspection of standardised

regression weights (factor loading), modification indices, and standardised covariance matrix (Byrne, 2010; Hair et al., 2017).

Table 6.46 Results of Measurement Model all constructs

Fit indices	Cut-off point	Initial measurement model	Modified measurement model
CMIN/DF	≤ 3.000	2.232	1.892
GFI	≥ 0.90	0.730	0.901
AGFI	≥ 0.80	0.710	0.818
NFI	≥ 0.90	0.837	0.903
CFI	≥ 0.90	0.900	0.953
RMSEA	≤ 0.08	0.062	0.046

By doing so, the CFA was tested again as suggested by Byrne (2010) and Kline (2005) without problematic items. The yielded fit indices indicated that the goodness of fit of the modified measurement model was adequately improved; all the fit indices this time were found within their recommended level as such. (Chi-square minimum discrepancy/degree of freedom) CMIN/DF was 1.892 (Goodness-of-Fit Index) GFI = 0.901, (Adjusted goodness-of-Fit) AGFI = 0.818, (non-normed fit index) NFI = 0.903, (comparative fit index) CFI = 0.953 and (the root mean square error of approximation) RMSEA = 0.046 (see Table 6.46). Furthermore, the rest of the estimates were found within their recommended values; for instance, all remaining items were observed to have factors loading above the threshold value (> 0.5). Standardised residual values were also found within the acceptable range of ± 2.58 (Hair, et. al., 2017). These fit indices collectively indicate that the overall fit of the measurement model is acceptable. Thus, there was no need to conduct any extra modifications or amendments in the measurement study's model (Byrne, 2010). The next sections explain the results of test for reliability and validity.

Construct Reliability

The main purpose of the measurement model is to assess and verify the measures or scale items used for each construct are both reliable and valid. A test of reliability was conducted by examining the composite reliability (CR) and average variance extracted (AVE) for each construct. The composite reliability (CR) was measured via Formula 8.1 as proposed by Fornell and Larcker (1981). As shown in Table 6.47, all latent constructs reflect an adequate composite reliability of at least 0.83. It also illustrates that quality of financial reporting had the highest value of 0.906 while the lowest value was observed regarding the availability of AIS which was 0.832. The AVE for all latent constructs was estimated and found they were above the threshold value of 0.50 as well (Hair et al, 2010). The largest value of AVE was

recorded by business performance with same value of 0.780 followed by quality of financial reporting with a value of 0.709; whereas, availability of AIS had the lowest AVE value of 0.555 (see Table 6.47). Accordingly, demonstrating that measures adopted in the study model were able to have an acceptable level of internal consistency; they also adequately satisfied the reliability criteria of CR and AVE (Hair, et. al., 2017).

Table 6.47 Composite Reliability and Average Variance Extracted

Constructs	Construct Reliability (CR)	Average Variance Extracted (AVE)
Availability	0.832	0.555
Security	0.901	0.694
Integrity Processing	0.873	0.633
Confidentiality	0.879	0.646
Privacy	0.897	0.686
Quality of Financial Reporting	0.906	0.709
Business Performance	0.875	0.780

Construct Validity

Both convergent and discriminant validity were subjected by the CFA to establish the constructs validity. As seen in Table 6.48, all remains items were found to have standardised regression weights above the cut-off value of 0.50 and were statistically significant with the p value less than 0.0001 (Hair, et. al., 2010). An inspection of the correlation table provided in the AMOS output file revealed that all inter-correlation estimates were found to be less than threshold value of 0.85 (Brown, 2006). Another important observation, as shown in Table 6.49, the squared root of AVE exhibited for each latent construct was higher than the inter-correlation estimates with other corresponding constructs.

In summary, the estimates of correlations and their standard of deviation indicated that the scales are empirically distinct from each other. Formally, the square root of the average variance extracted is larger than the correlation coefficient, including discriminant validity of the scales. Overall, the measurement model is believed to be appropriate given the evidence of good model fit, reliability, convergent validity and discriminant validity.

Table 6.48 Standardised Regression Weights

Items		Construct	Factor Loading	Items		Construct	Factor Loading
RE	<---	Quality	0.795	NF8	<---	NF	0.867
Fait	<---	Quality	0.912	FFI	<---	FF	0.999
Under	<---	Quality	0.753	FF2	<---	FF	0.981
Com	<---	Quality	0.897	FF3	<---	FF	0.986
FF	<---	Performance	0.808	A1	<---	AV	0.682
NF	<---	Performance	0.952	A2	<---	AV	0.850
R1	<---	RE	0.710	A5	<---	AV	0.764
R2	<---	RE	0.987	A9	<---	AV	0.670
R5	<---	RE	0.987	P3	<---	Privacy	0.815
R3	<---	RE	0.702	P4	<---	Privacy	0.871
F1	<---	Fait	0.786	P6	<---	Privacy	0.818
F3	<---	Fait	0.819	P7	<---	Privacy	0.807
F4	<---	Faith	0.811	IG2	<---	Integrity Processing	0.778
F5	<---	Faith	0.822	IG4	<---	Integrity Processing	0.858
U6	<---	Under	0.990	IG6	<---	Integrity Processing	0.772
U4	<---	Under	0.965	IG7	<---	Integrity	0.771
U2	<---	Under	0.998	C3	<---	Confidentiality	0.768
CC3	<---	Com	0.857	C4	<---	Confidentiality	0.863
CC2	<---	Com	0.830	C6	<---	Confidentiality	0.789
CC1	<---	Com	0.832	C7	<---	Confidentiality	0.792
CC5	<---	Com	0.796	S3	<---	Security	0.828
NF3	<---	NF	0.789	S5	<---	Security	0.874
NF5	<---	NF	0.812	S6	<---	Security	0.843
NF6	<---	NF	0.820	S7	<---	Security	0.785

Table 6.49 Discriminate Validity

	Availability	Security	Integrity	Confidentiality	Privacy	Performance	FRQ
Availability	0.745						
Security	0.696	0.833					
Integrity	0.633	0.672	0.796				
Confidentiality	0.620	0.664	0.629	0.804			
Privacy	0.566	0.568	0.660	0.789	0.828		
Performance	0.599	0.585	0.544	0.702	0.755	0.883	
FRQ	0.567	0.585	0.671	0.790	0.805	0.794	0.842

6.12.2 Structural Model

Once the validity of the measurement model fit has been established, the second stage of SEM, is the specification of the structural model. The structural model differs from the measurement model in that the emphasis shifts from the relationships between latent constructs and observed variables to the nature and magnitude of the relationships between constructs (Hair, et. al., 2017). The transition from the measurement model to the structural model implies specifying which constructs are related to each other and the nature of each relation. The structural model is used to validate the conceptual model and test the research hypotheses (Byrne, 2010; Hair, et. al., 2017). An inspection of structural model was conducted with eleven causal paths between independent factors (exogenous factors) and dependent factors (endogenous factors). As summarised in Table 6.50., the main statistical results indicated all the fit indices of the structural model were found to be within their threshold values as such CMIN/DF was 1.970, GFI = 0.903, AGFI = 0.807, NFI = 0.901, CFI = 0.954 and RMSEA = 0.053. Thus, suggesting that structural model adequately fit the data. Moreover, statistical results largely supported the conceptual model via explaining 81 per cent and 74 per cent of variance in business performance and quality of financial reporting respectively.

Table 6.50 Fit Indices of Structural Model

-Fit indices	Cut off point	Model fit
CMIN/DF	≤ 3.00	1.970
GFI	≥ 0.90	0.903
AGFI	≥ 0.80	0.807
NFI	≥ 0.90	0.900
CFI	≥ 0.90	0.954
RMSEA	≤ 0.08	0.053

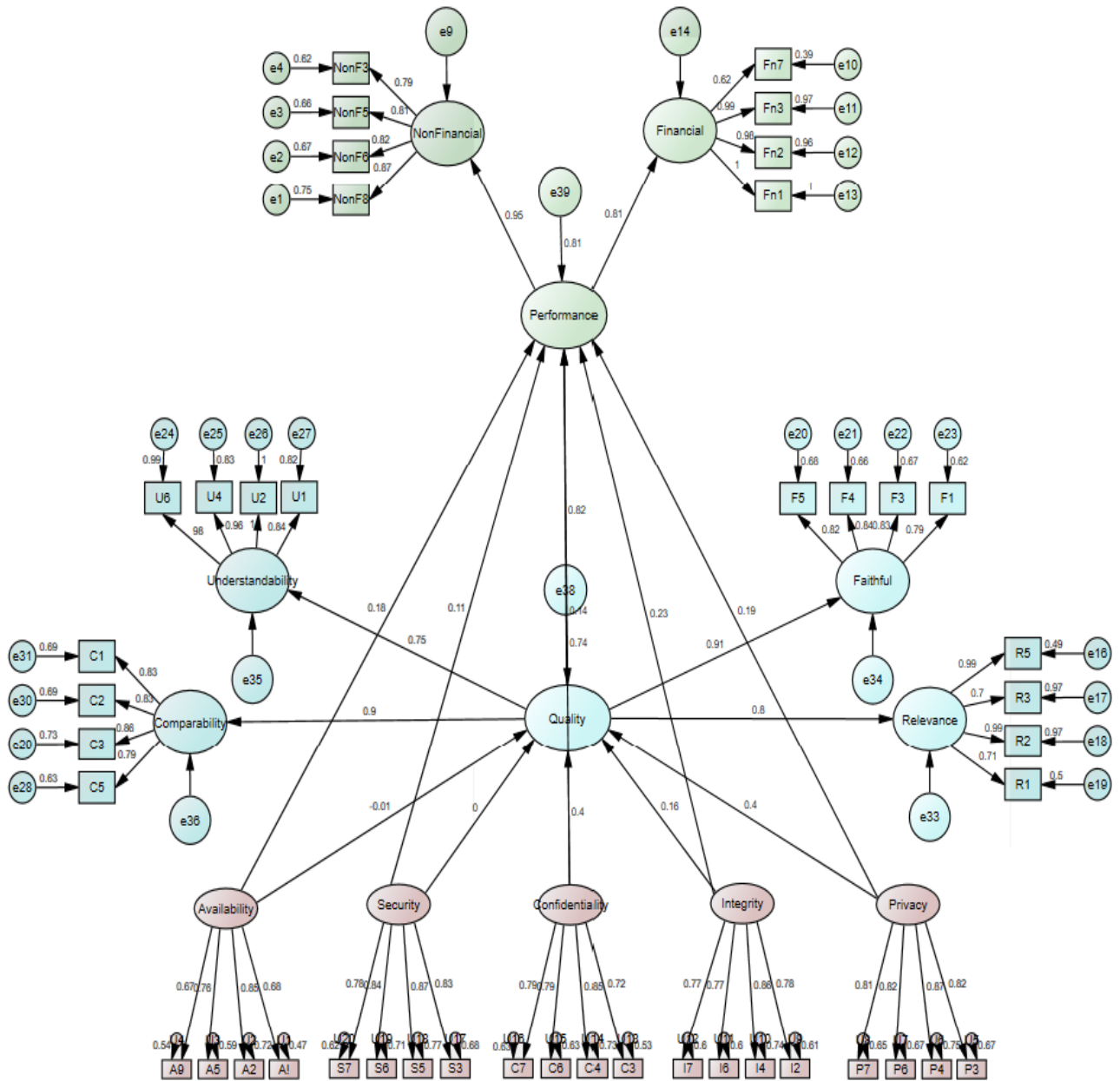


Figure 6.7 Path Diagram of the Study's Structural Model

Regarding the path coefficients analyses, the coefficient values of the paths ending to quality of financial reporting including. Processing Integrity of AIS ($\gamma = 0.29, p < 0.0159$); Confidentiality ($\gamma = 0.400, p < 0.000$); and Privacy ($\gamma = -0.397, p < 0.000$) were found to be statistically significant (see Figure 6.7). Yet, the paths between security ($\gamma = 0.005, p = 0.946$) and Availability of AIS ($\gamma = -0.0061, p < 0.930$) and quality of financial reporting were recognised as non-significant. The financial reporting quality ($\gamma = 0.81, p < 0.000$), processing integrity of AIS ($\gamma = 0.23, p < 0.000$) Availability of AIS ($\gamma = 0.185, p < 0.006$), and privacy of AIS ($\gamma = 0.19, p < 0.025$) all were found to have a significant impact on business performance. However, both security ($\gamma = 0.111, p < 0.126$); and Confidentiality ($\gamma = -0.13, p < 0.150$) did not have any significant impact on the business performance. It is also worth mentioning that the main constructs (without the quality of financial reporting) were able to predict about 61% of variance in business performance. However, R^2 values accounted for business performance were enhanced to reach 81% by the inclusion of quality of financial reporting along with other constructs in the same structural model. Accordingly, it could be concluded that the structural model seems to have more power in predicting the business performance once the quality of financial reporting is comprised in the structural model. It may be concluded that relationships with significant and meaningful estimated structural parameters are supported the study's integrated model.

In summary, the magnitude and significance of the loading estimates indicate that all of these five principles of SysTrust's framework are relevant in predicating quality financial reporting and business performance. Moreover, the reliability of AIS by the implementation of these five principles of SysTrust's framework has significant impact on both quality of financial reporting and business performances, as the structural coefficient for these paths are significant. Thus, in order to enhance the quality financial reporting as well as business performance, companies should meet fully all of these main requirements of SysTrust's framework.

6.13 Summary

This chapter presents the main findings related to the study objective and testing relevant hypotheses by using the multiple regression analysis and Pearson correlation coefficient. The results showed that the extent of the implementation of the principles of the SysTrust's framework were varied due to the type of business sectors, but were related only to the size and number of years in business (experience). This might indicate that some types of business sectors do apply. This result might indicate that the size of organizations and their number of

years in business do not play an important role on the implementation of SysTrust's framework requirements. The five main principles of the SysTrust's framework (Availability, security, integrity processing, confidentiality and privacy) was found to be significantly associated with a high quality of financial reporting. The findings also indicate that out of 11 explanatory independent factors which were extracted from the SysTrust's framework, only six factors included in the regression equation. These six factors in terms of their order of importance are: (1) Privacy (2) Confidentiality, (3) Output control, (4) AIS availability policies, (5) Security policies and communication, and (6) Physical security access". The adjusted R square result indicated that about 0.65 of the variation on the dependent variable the quality of financial reporting should be explained by above significant factor, acting together.

The results of the relationship between the variables constituting each independent factor and the quality of financial reporting were presented and discussed. The relationship between the type of business performance and the four actors extracted from quality of financial reporting (namely Understanding, relevance, comparability, and faith reorientation) are tested and analysed... The regression analysis indicates that the quality financial reporting factors are positively influences the types of business performance (financial, non-financial and combined), either taken together or separately. The results also indicate that the quality of financial performance can act as mediating variable between the implementation of SysTrust's framework requirements and business performance. In the next chapter, the conclusion, theoretical and practical contributions, and future studies are discussed and presented.

CHAPTER SEVEN

CONCLUSION, CONTRIBUTIONS AND FUTURE STUDIES

7.1 Conclusion

This study aims to examine and validate the influence of the implementation of SysTrust's framework (principles and criteria) as an internal control method for assuring reliability of AIS on the business performance via the mediating role of the quality of financial reporting among Jordanian public listed companies. The specific objectives of this study have been explicitly presented in the first chapter. In order to achieve the study objectives, and to conduct the research in a systematic approach, a conceptual framework was developed was developed to guide this study. The study's conceptual framework consists of three major constructs: The SysTrust's service framework (availability, security, integrity processing, confidentiality, and privacy), the business performance (financial and non-financial indicators) and the quality of financial reporting which was conceptualised using the IASB's framework fundamental qualitative characteristics (2010).

The research design is based upon 7 major hypotheses regarding the implementation of SysTrust's framework, the quality financial reporting (i.e., qualitative characteristics) and business performance dimensions. The data for this research were collected through structured-directed interview with 239 respondents. The target respondents were shareholding companies in Jordan, and the key respondents approach was employed. Since the issues of reliability and validity have become prerequisite to any empirical study conducted in the spirit of scientific research, it was decided to test the reliability and validity of all the variables generated for investigation. Therefore, the internal consistency reliability and content validity of the variables included in the survey were tested via the correlation alpha method.

Primary data were analysed using a variety of multivariate statistical techniques, including factor analysis, ANOVA Analysis multiple regression statistical technique Neural Network (ANN), Structural Equation Modelling, the Univariate F-ratio test, and the t-test. The findings of this study have been presented and discussed in detail in chapters 7 and 8.

Chapter 6 has outlined the main findings of a factor analysis (i.e., the factors which extracted from the main principle of the SysTrust's framework, the main qualitative characteristics of the quality of financial reporting and the business performance dimensions). Chapter 8 dealt with the influence of the implementation of SysTrust principles upon each dependent variable (i.e., quality of financial reporting and business performance). In conclusion, the author presents here how the current research objectives have been realised in light of the previous elaborated discussion of results and the extent of the implementation of SysTrust's frameworks by public listed companies in Jordan as a non-western country.

7.2 Main Conclusions of the Research Findings

Eleven factors were extracted from the five major principles of SysTrust's framework principles: Availability of AIS (3 factors), Security (3 factors), Integrity Processing (3 factors), confidentiality (1 factor) and "Privacy" (1 factor). Also, four factors were extracted from IASB's framework fundamental qualitative characteristics of the quality of financial reporting. (1) Understandability (2) Relevance (3) Comparability and (4) Faith representation and Timeliness and two factors were extracted from the business performance indicators (Financial performance and non-financial performance) factors. These 17 factors were successfully identified and labelled, and subsequently used to answer the research questions by using multiple regression analysis.

The analysis provides empirical evidence that the integration approach of the SysTrust's framework (factors) better explain not only the prediction of the quality of financial reporting but also of the prediction of the business performance. This result supports the proposition that implementation of SysTrust's framework requirements as internal method for assuring the reliability of AIS is significantly linked to the quality of financial reporting and business performance. Therefore, a better understanding of the influence of implementation of SysTrust's principles upon the quality of financial reporting and business performance should be viewed as a whole rather than isolated fragments. The study's findings show the quality of financial reporting ($R^2 = 0.665$) are explained better than business performance ($R^2 = 0.550$) by the implementation of the SysTrust's principles, when they are taken together. This result implies that the quality of financial reporting could better explained the reliability of the internal control of accounting information.

Table 7.1 The Most Important Factors of SysTrust's Framework that Influence the Quality of Financial Reporting and Business Performance in terms of their order of importance.

SysTrust Principles	Sub-Hypotheses	The Independent Factor	Quality of Financial Reporting	Business Performance
1. Availability of AIS	Factor (1)	AIS availability Polices	6**	5**
	Factor (2)	Recovery Disaster Plan		
	Factor (3)	Availability communication		4**
2. Security of AIS	Factor (4)	Logical Security Access		
	Factor (5)	Security Policies and Communication	5**	2**
	Factor (6)	Physical Security Access	4**	3**
3. Integrity Processing	Factor (7)	Integrity Processing policies		7**
	Factor (8)	Data Transfer Control		
	Factor (9)	Output Control	3**	
4. Confidentiality	Factor (10)	Confidentiality	2**	6**
5. Privacy	Factor (11)	Privacy	1**	1**
R Adjusted Square			0.665	0.550

Order of importance and significant at 0.01level

For example, while the implementation of "Output Control" factor is not shown to be importantly related to the business performance, it is regarded as one of the most important SysTrust factor associated with the quality of financial reporting. This result is of particular importance to decision-makers in business organizations who want to improve the quality of financial reporting. Similarly, while the "Availability of Communication and training" factor is important to the business performance, it was not found important to the quality of financial reporting. The moderate explanatory power of the extent of implementation of the SysTrust's framework requirements suggests that there may be other factors should be included in order to have better predication of business performance. Furthermore, the results indicate that some factors of SysTrust's framework are shown not important to both the quality of financial reporting and business performance such as "Recovery Disaster plan", Data transfer Control "and" Logical Security Access "factors". These results might indicate that there are some differences and similarities between the quality of financial reporting and business performance in terms of relative importance of these factors at the aggregate level.

Table 7.1 shows a summary of the main factors of SysTrust principles influencing the quality of financial reporting and business performance in terms of their order of importance at the aggregate level. Furthermore, the result also showed that the "privacy" factor is the most important one that highly associated with both the quality of financial reporting and business performance at the same level of order of importance.

Furthermore, in comparing between the power of the influence of the reliability of AIS upon, the quality of financial reporting and the business performance at aggregate level, the results that the variation in the quality financial reporting is slightly higher than the quality financial reporting. It could be concluded the reliability of the AIS is relatively influence on the quality of financial reporting much higher than business performance as summarised in Table 7.2.

Table 7.2 A Summary Comparison relationship between the Implementation of SysTrust’s principles, the Quality of Financial Reporting and Business Performance

Hypotheses	Multiple R	R. Square	Adjusted Square	R	DF	F	Sign
Quality of Financial Reporting	0.822 ^a	0.676	0.665		11	63.340	0.000 ^b
Business performance	0.751 ^a	0.564	0.550		11	160.317	0.000 ^b

7.2.1 The Extent of the Implementation of the SysTrust's Framework. The Finding of the First objective

The potential benefits of SysTrus's framework implementation as an internal control for any organization are enhancing the confidence of stakeholders (management, boards of directors, customers, and business partners) regarding the reliability of information systems and providing accounting professionals with the ability to leverage their existing skills to fulfil the needs of the more attention to the reliability of accounting information system and the importance role of the implementation of SysTrust's framework requirements as an internal control system.

The measure of extent of implementation of SysTrust's framework (principles) requirements for assuring the reliability of AIS in public listed companies in Jordan; These principles are: Availability of AIS, security, integrity processing, confidentiality and privacy. In this study, the implementation of these five main principles were identified and the findings indicate that the extent of these principles being implemented considered to be good either taken together or separately (i.e. 74% or 5.20%). since their mean are more than the mean of the scale, which is 4 (mean of the scale = Σ Degrees of the *scale* 7 = (1+2+3+4+5+6+7) / 7 = 4). This indicates that there are some variations among shareholdings companies in terms of their level of implementations of the SysTrust's framework requirements as presented in Table 7.3. This implies that there are some variations among public listed companies in Jordan in terms of their level of reliability of AIS. This might be due to their type of business or the nature of audit IT control system. Furthermore, the implementation of the SysTrust’s framework (five principles) is not obligatory in Jordan and public listed companies might implement one or more of these principles, partially or fully based on their needs. It could be concluded that

the IT infrastructure of the public listed companies in Jordan by its status qua is mature enough to provide the operational requirements for (SysTrust) principles and criteria and its capable and qualified to perform a continues auditing. On other word, periodically and regularly, they use the appropriate procedures and policies to assure the reliability of the internal control of accounting system. .Such result are supported by the results reached by Casolaro & Gobbi, (2004) Mansour et al., (2009, 2017), and Al Hanini, (2015). The results also showed that the Security principle was highly implemented. This could be because securities of AIS issues have been given a propriety over other principles implemented among shareholding companies It implies that public listed companies in Jordan carry out appropriate procedures to separate functions, they are also protect the system from physical and logical access (e.g. using password)from unauthorized people through keeping the major computers in indoor fire - resistant places, taking necessary procedures to prevent unauthorized employees to access into the computer, adopting strategies concerning in addition to take some control procedures regarding the employees' personal computers as using electronic lock. They also train their employees on updating antivirus continuously. This result is supported by Abu Musa (2010) and Al Hanini, (2015.)

Table 7.3 The level of Reliability of AIS

SysTrust Principles	Mean	Percentage	Standard deviation	Sig. (2-tailed)
Availability	5.1398	0.7342	0.86783	0.000
Security	5.5559	0.7937	0.91053	0.000
Integrity processing	5.2214	0.7459	0.76369	0.000
Confidentiality	5.2184	0.7454	0.87010	0.000
Privacy	5.2254	0.7464	0.91306	0.000
Level of reliability	5.2214	0.7459	0.75279	0.000

Furthermore, while the extent of the implementation of the SysTrust's framework (principles) requirements are shown significantly differ in terms of the types of business organization (service vs. industrial organizations), they found not differ in terms of their size and business experiences. When compared, the extent of SysTrust being practiced among business organizations in terms of type of business, service companies were found at a significant edge over industrial companies on all the five main principles of SysTrust. This clearly indicated that the service companies apply or give more attention to the requirements of SysTrust principles requirements than the industrial companies. This might be due to the fact that service companies tend to be more technology-oriented and driven than industrial companies in Jordan. In their study of electronic data interchange (EDI), Khazanchi and Sutton (2001)

give evidence of the requirement for systems assurance, illustrating that numerous companies enforcing these systems do not use them to full benefit.

7.2.2 The Relationship between the Implementation of SysTrust's Framework and the Quality of Financial Reporting. The Findings of the Second objective

The application of the multiple regression analysis indicates that there is a moderate relationship between the implementation of the SysTrust's framework (principles) and the quality of financial reporting at the aggregate level. The application of stepwise regression analysis also showed that some of these factors are highly associated with the quality of financial reporting. These factors in terms of their order of importance are: (1) Privacy (2) Confidentiality, (3) Output control (4) AIS availability policies (5) Security policies and communication and (6) Physical security access". The adjusted square for these six factors is 0.675 as shown in Table 7.4. This indicates that about 68% of the variations of the quality of financial reporting can be explained by these factors.

It might be conceded that in order to get clear picture for the influence of the reliability of AIS process on the context of the implementation of SysTrust principles upon the quality of financial reporting should be viewed together. This result is of central concern for business decision-makers who concern about enhancing the quality of financial reporting within their organizations to consider the importance of the implementation of SysTrust principles and criteria for this purpose, in particular, those principles which have shown highly relationship with quality of financial reporting.

7.2.3 The Relationship between the Implementation of SysTrust's Framework and the Business Performance. The Findings of the third objective

The application of the multiple regression analysis reveals that there is a moderate relationship between the implementation of the SysTrust principles and each dimension of business performance (financial, non-financial and combined) at the aggregate level. In comparing this among the type of business performance (financial, non-financial and combined), the result indicated that the influence of implementation of SysTrust principles upon the combination of the two business performance dimensions (i.e., financial and non-financial) would give slightly better explanation (predictive power) than upon each factor acting alone. The rate of explanation which they account for is increased from 24% (financial performance) and 36% (non- financial performance) to about 55% when they were taken together.

Furthermore, the application of stepwise regression analysis also showed that the relative importance of these factors is differing according to the type of business performance. In addition, there are some factors are not shown important with each type of business performance such as "Recovery Disaster plan", Data Transfer Control" and "output Control" This result needs further investigation. Table 9.6 summarises these factors in terms of their order of importance that related to each type of business performance.

Table 7.4 The Relative Importance of Factors that Related to each type Business Performance Indicators

SysTrust Principles	Factors		Non-Financial	Financial	Combined
1. Availability of AIS	Factor (1)	AIS availability Polices	2*		5*
	Factor (2)	Recovery Disaster Plan			
	Factor (3)	Availability communication & Training		2*	4*
2. Security of AIS	Factor (4)	Logical Security Access	3*		
	Factor (5)	Security Policies and Communication		3*	2*
	Factor (6)	Physical Security Access			3*
3. Integrity Processing	Factor (7)	Integrity Processing policies			7*
	Factor (8)	Data Transfer Control			
	Factor (9)	Output Control			
4. Confidentiality	Factor (10)	Confidentiality		1*	6*
5. Privacy	Factor (11)	Privacy	1*		1*

*Important factors in terms of their order of importance

.This conclusion implies that a better understanding of the impact of the implementation of SysTrust principles on the business performance requires that the two combinations of financial and non-financial performance factors should be viewed and investigated together rather than only viewing each of them alone. Furthermore, viewing financial performance alone would also give better understanding than viewing non-financial performance alone. This result is supported by Onaolapo and Odetayo (2012).

7.2.4 The Role of the Quality of Financial Reporting as a Mediator between the Implementation of SysTrust's Framework and Business Performance. The Findings of the Fourth Objective

The results of testing the mediating effect of quality of financial reporting on the relationship between the implementation of the SysTrust principles and business performance at the aggregate level indicated that it partially mediated this relationship. The Baron and Kenny (1986) mediation model does not necessarily indicate that an indirect effect exists; therefore, the researcher conducted a Sobel (1982) test for the indirect effect. The results of the Sobel test showed that an indirect effect does exist, and that the quality of financial reporting did mediate the proposed relationship. In conclusion, the current thesis has provided support that all the proposed relationships between and among the model constructs: the SysTrust principle, quality of financial reporting and business performance are significantly and positively related. Furthermore, it provided support for the ability of quality of financial performance to mediate the SysTrust principles-business performance relationship. Thus, this study and its findings have a number of contributions and managerial implications.

7.2.5 Comparison between the Performance of ANN and MRA Tests

In order to understand whether a multiple regression analysis or an ANN is making good predictions, the test data which has never been presented to the network is used and the results are checked at this stage. The statistical methods of R. square score, F. Ratio and Mean Square Error (MSE). values have been used for making comparisons. The same data obtained from the regression analysis is used to determine the mentioned values. The results demonstrate that the artificial neural network outperformed the multiple linear regression models. The neural network gives value of estimation mean square error (MSE) less than linear relationship in all business performance predictions models. Furthermore, the predictive ability of the artificial neural network (ANN) is very high and gives a highly accurate prediction as a result of pattern recognition or generalization made by the network. The neural network shows R. square scores (R^2) is higher than linear relationship for all predictive measures used in this study. It was concluded that ANN model can be used for predicating the impact of the reliability of AIS on business performance indicators (financial and non-financial); either taken separately or together due to its better performance compared with MRA model.

7.2.6 The Validation of the Study's Conceptual Model: The Findings of the Fifth Objective.

To empirically examine and validate the current study's conceptual model, an analysis of the moment structures (AMOS, version 21) was applied. It was used to assess the measurement model by means of the confirmatory factor analysis (CFA). The main aim behind conducting the measurement model is to identify the manner of how the observed variables (indicators) loaded into their latent (unobserved) construct (Arbuckle, 2005; Byrne, 2010). The main findings of structural equation modelling techniques (SEM) are presented as follow.

- Eleven causal paths were proposed among the conceptual model to demonstrate the relationships between five exogenous (independent. five System SysTrust principles) constructs (AIS availability, Security integrity processing, confidentiality and privacy) and two endogenous (dependent) constructs (Quality of financial reporting. Relevance, Understandability, Comparability and Faith Representation) and (Business performance dimensions; financial and non-financial). The magnitude and significance of the loading estimate indicate that all of these five principles of SysTrust are relevant in predicating quality financial reporting and business performance. Moreover, the reliability of AIS by implementation of these five principles of SysTrust has significant impact on both quality of financial reporting and business performances, as the structural coefficient for these paths are significant Thus, in order to enhance the quality financial reporting as well as business performance, companies should meet fully all these main requirements of SysTrust principles.
- The revised version of the structural model was able to adequately fit the observed data due to all fit indices. CMIN/DF, GFI, AGFI, NFI, CFI, and RMSEA were found within their threshold. The main statistical results indicated all the fit indices of the structural model were found to be within their threshold values as such CMIN/DF was 1.970, GFI = 0.903, AGFI = 0.807, NFI = 0.901, CFI = 0.954 and RMSEA = 0.053. Thus, suggesting that structural model adequately fit the data. Moreover, statistical results largely supported the conceptual model via explaining 81% and 74% of variance in business performance and quality of financial reporting respectively.
- While the path coefficient analyses results indicated that Processing Integrity, Confidentiality and Privacy were found to be statistically significant with the quality of financial reporting, Security and Availability of AIS were recognised as non-significant.

The financial reporting quality, processing integrity, Availability, and Privacy of AIS all were found to have a significant impact on business performance. However, both Security; and Confidentiality did not have any significant impact on the business performance. Surprisingly result security as a principle of the SysTrust model is found not important neither for the quality of financial reporting or for the business performance. This result might need further investigation in the future.

Table 7.5 The Important of SysTrust Principles that directly Associated with the Quality of Financial Reporting and Business Performance

SysTrust Principles	Quality of Financial Reporting	Business performance
Availability		X
Security		
Integrity processing	X	X
Confidentiality	X	
Privacy	X	X

X= the Significant Principles

It is also worth mentioning that the main constructs (without the quality of financial reporting) were able to predict about 61 per cent of variance in business performance. However, R^2 values accounted for business performance were enhanced to reach 81 per cent by the inclusion of quality of financial reporting along with other constructs in the same structural model. Accordingly, it could be concluded that the structural model seems to have more power in predicting the business performance once the quality of financial reporting is comprised in the structural model. These empirical results confirmed the role of quality of financial reporting as a mediating factor in enhancing and predicating the business performance by implementing the requirements of the SysTrust principles in the current study.

7.3 Research Contributions

Several contributions to existing knowledge are made in this research. These contributions are theoretical, methodological and practical implications. The theoretical contributions refer to the type of contributions that are made to enhance the conceptualization and to further enhance the understanding of the issues being studied. The methodological contributions refer to the type of conclusions that are made on the procedures employed to achieve the research objectives. The practical contributions refer to the type of contribution that can be made useful for present and future practical purposes. This research has some contributions to the relationship among the adoption of SysTrust principles (functions, policies, procedures and criteria), the quality of financial reporting and business performance.

7.3.1 Theoretical and Methodological Contributions

- (1) Extending the understanding of the practice and implementation of the main principles of SysTrust's framework (Availability, Security, Integrity processing, Confidentiality, and Privacy) as an internal control method for assuring the pliability of AIS by testing this phenomenon in a new environment. In the literature review, it was pointed out that most of the research in this area was conducted in developed countries. To the best knowledge of the researcher, the integration approach of the implementation of the SysTrust principles and its relationships with quality financial reporting and business performance as proposed in this study has never been investigated in Jordan or any other developing countries, particularly within MENA. This study contributes to the existing body of knowledge by enhancing current understanding of importance of the implementation of the SysTrust principles requirements (functions, policies, procedures and criteria) as internal control system for assessing AIS reliability, which is an under-researched area in Jordan as a developing country.
- (2) In comparison with the previous studies conducted in the same field, this study might be considered to be more comprehensive in terms of the number of variables investigated, i.e. the SysTrust's principles, qualitative of financial reporting and business performance measures. In other words, the study might be one of a few attempts to investigate 120 variables separately and together (i.e. 17 factors).
- (3) This study has been conducted in a systematic manner, guided by the conceptual framework, which was based on the integration of the SysTrust principles thought to influence the level of the quality financial reporting as well as the business performance (for more details, see Chapter 4)..
- (4) This study has also extant reliability of AIS and business performance literature by providing the following: First, it is explained the relationships between the reliability of AIS and the business performance measures (financial and non-financial). Previous research examined and linked reliability of AIS with only financial performance using MRA (Casolaro and Gobbi, 2004 Mansour et al., 2017). Second, testing the role of the reliability of AIS in the predication of business performance in a new context culture using ANN (i.e. Jordan as a developing country) considered another contribution for the current study.
- (5) The present study also has important contributions for studies aimed to understanding SysTrust implementation in developing countries. It has emphasized on the importance of contextual factors (demographic factors; type of service sector, size and experience) within organisations and its environment. By highlighting the significance of several contextual factors, this study also hopes to expand the focus of SysTrust principles. It also

provides some insights into the implementation of SysTrust by Jordanian shareholding companies, which should help accounting managers, auditors and practitioners, acquire a better understanding of the current SysTrust principles implementation status and the importance of its relationship with the quality of financial reporting and business performance.

- (6) The study provides empirical evidence regarding the impact of the qualitative characteristics of financial reporting quality using the IASB's framework and their ability to explain the prediction of the business performance measures (financial or non-financial). Factor analysis findings have indicated that relevance, understandability, faith representation, comparability and timeliness are true measures of the qualitative characteristics of financial reporting quality in that order. This result is supported by the previous studies (Beuselinck and Manigart, 2007; FASB, 2013 and Beest, et al., 2009). Furthermore, business performance measures also could be grouped into two main factors; financial and non-financial performance. This result is strongly supported by previous studies (Smith 2011, Antonio Pérez-Méndez, Ángel Machado-Cabezas, 2015, Ejoh and Ejom 2014). Regression and Structural equation Modelling analyses were conducted to determine the nature and magnitude of relationship between the qualitative characteristics of financial reporting quality and business performance dimensions. The results showed there is a positive and moderate relationship between the quality of financial reporting and business performance (financial, non-financial or combination). Furthermore, the findings provide empirical evidence that the integration approach of the qualitative attributes of financial reporting produce better explanation of variation on the combination of business performance dimensions (financial, non-financial) rather taken each dimension separately. In other words, the quality of financial reporting could enhance business performance irrespective of the type of business performance dimension (financial or non-financial or combination). Therefore, a better understanding of the influence of these qualitative attributes of financial reporting on business performance should be viewed as a whole rather than isolated. As suggested by past research, quality of financial reporting has a significant relationship on business performance (Mbodo and Ekp, 2016; Tasios and Bekiaris, 2012). This implies that business sector entities should employ highly skilled professionals that adhere to reporting requirements of the legal and regulatory framework the quality of financial reporting as a significant factor influencing financial business performance (e.g., Beuselinck and Manigart, 2007; FASB, 2013; Beest, et al., 2009).
- (7) To the researcher's knowledge, this research might be one of the few studies in this area testing the reliability and validity of the scale of measurement of data collection. (For

more details see Chapter 7). The research went a step further by not only studying the dual effect of the variables chosen, but also examining the mediating role of the quality of financial reporting for the first time; these relationships have not been previously tested empirically before. The SysTrust's framework implementation as an internal control system for assuring the reliability of AIS could be considered as the critical intangible resources for any business organization seeks for a reliable and effective accounting system in the long run. In this study, financial reporting quality justified as the mediator from contingency theory perspective where good quality and effective of information system is an integral component of a strong internal control system. Inadequate financial reporting quality might cause a lot of business operations run inefficiently and less in accordance with the demands and needs of the stakeholders. Therefore, in order to anticipate these conditions, businesses must have reliable system in generating quality information. Furthermore, the main statistical results also supported the predictive validity of the study's conceptual model by counting about 81% of variance in reliability of AIS among Jordanian shareholding companies based on the implementation of the SysTrust's framework.

The author believes that the decision-makers of business organizations could benefit from this study's findings with a better understanding of implementation of the SysTrust principles requirements for assuring the reliability of AIS (functions, policies, procedures and criteria) as well as its influence upon the level of quality of financial reporting and business performance. This might help them in implementing the required actions and important changes within their organisations. Decision-makers should also be aware of the important of each of SysTrust principles and its major requirements that either highly related to the quality of financial reporting or business performance, so that they can make the right decision and directions for any change within their organizations.

All the principles of the SysTrust are relevant and should be emphasised, in particular the privacy one. The reliability of AIS in shareholdings companies should be enhance by the implementation of SysTrust's framework (availability security, confidentiality, integrity processing and privacy). The indicators for each SysTrust principle suggest how that principle should be impacted by management action. To aware the companies' employees in general and who work in computerized accounting information systems in particular of the importance of compliance with control's procedures of system's protection and the risks facing these systems before they were trained on these systems. Companies should also keep up with the technological development concerning providing the largest amount of reliability to the internal control's systems over the accounting information systems.

Furthermore, a comparison between the results of the relationship between the SysTrust principles and the quality of financial reporting and the relationship between the SysTrust principles and business performance were also reported (see tables 7.1., 7.3, 7.4 and 7.5). This comparison will help business organizations in Jordan to implement the required changes within their organizations for the purpose(s) of either to improve the level of the quality of financial reporting or to enhance the level of business performance. This study is expected to be helpful to the financial managers in planning and implementing the appropriate strategic internal control accounting system application where extensive attention needs be given to the reliability of AIS, which must be focused on aspects required for supporting the decision-making process, rather than being limited to some IT administrative applications.

As for the role of SysTrust applications in the future for assuring the reliability of AIS, it can be argued that SysTrust is a method of internal control that can facilitate the transition from a traditional auditing to a continues auditing, enabling it to improve the quality of its financial reporting and business performance. Within this context, the implementation of SysTrust principles requirements can be facilitated through developing and using an organizational IT infrastructure, which facilitates the integration of technology in organizational processes and financial functions in addition to its role in promoting the collaboration between different departments, such as accounting, auditing departments and IT, in order to institutionalize and consolidate this change.

Financial and IT managers should also play a proactive role to support SysTrust principles implementation in their organisations. They should convince stakeholders of the importance of SysTrust applications for assuring the reliability of AIS, so that time and budget required for adoption of SysTrust applications can be allocated and justified. Stakeholders need to be convinced by the values and the strategic benefits of SysTrust principles in order to grant the required financial and non-financial support for the implementation. Wider internal organizational context factors can have a deep impact on SysTrust process success. Successful implementations are also considered to be a driver for any potential companies to fellow in the future.

In summary, the findings from this study indicate the necessity to exploit IT infrastructure for more adoption, adaptation, and integration with companies' investment applications. A challenge of AIS design is not to apply (SysTrust) principles and criteria, but how to develop

new ways to integrate these principles and criteria with parameters of the quality of financial reporting and business performance measures (financial and non-financial). In addition, there is a need to deepen the understanding of the reliability of AIS standards among the employees of these companies through the preparation and implementation of specialized training programs or through flyers and brochures.

7.4 Research Limitations

This study has some limitations that should be considered when evaluating and generalizing its conclusions. However, the limitations discussed below can give a beginning stage to future research:

(1)The study was conducted in one geographic area. . In spite of the fact that Jordan is a valid indicator of prevalent factors in the wider MENA region and developing countries, the lack of external validity of this research means that any generalizations of the research findings should be taken with these reservations. Future research can be orientated in other national and cultural settings and compared with the findings of this study.

(2) The data analysis was cross-sectional. As with all cross sectional studies, the measures tended to be static rather than dynamic. This reservation limits the generalization of the study's findings to other situations and beyond the specific population from which the data was collected. Future longitudinal studies could provide a better understanding of assuring the reliability of AIS process over time.

(3) The study used a single key informant approach for data collections. This approach might not provide an identical view about the organization. However, by using single informant approach in future research, the problem of consistent responses should be solved.

(4) Furthermore, the study has used subjective measures for the quality of financial reporting and financial performance indicators. This might determine the generalizations and the validity of the study findings.

(5)This study was confined to one type of owner business structure, i.e. The public listed companies in Jordan. Therefore, the generalization of the findings beyond this type of business structure should be taken with caution.

7.5 Areas for Further Research

Since this is the first study to address the status of the implementation of SysTrust principles in Jordan, there are many issues that could not be covered in this research that warrant further investigation. The suggested areas for further study are as follows. The external validation of the current research findings is important for future research directed towards replication of the findings of this research. It is suggested that future researchers should use the same topic. This research was conducted at a single point in time. Future work could use a longitudinal research design to fully investigate the causal effect of various factors and their relationships over time.

This research has been conducted in Jordan and further research should be carried out to investigate whether the results from this research will be consistent with findings from different countries in various business organizations. This may provide deeper insights into SysTrust principles usage in varying organizational and cultural contexts. In general, our knowledge of might be further improved by more studies in both developed and developing countries. Therefore, researchers can further look into factors influencing the extent of SysTrust principles implemented and determine if the same or a different set of factors is relevant in explaining the extent of its influence. In addition, researchers can also adopt other research methodologies such as focus group interviews or longitudinal study which may provide a richer set of data rather than the survey methodology used in this study. This research was conducted at a single point in time.

The theoretical framework tested in this research identified quality financial reporting attributes (variables) as a meditational factor between the implementation of SysTrust and business performance. As with many models, there is a risk that additional significant factors have not been included in the framework. Additional variables such as these variables which have been conducted in existing studies in AIS can be further examined in future study. Future research is required to develop multiple measures for the level of implementation of SysTrust principles and its effectiveness. The purpose would be to find out whether there are any differences of using one criterion and the results of using multiple criteria together. While this study advances the investigation of the current status of the implementation of SysTrust principles and its impact upon the quality of financial reporting as well as business performance in business organizations in Jordan, it is just a first step. Future research models could also focus on the question of whether there are constructs, or variables other than those studied here that affect the reliability of AIS in developing countries like Jordan. Also, a logical extension of this study is to focus on specific types of user involvement to determine

which types and under what conditions they have the greatest influence on the reliability of AIS and its effectiveness, especially in developing countries. A contingency approach could be very useful in understanding the true nature of user involvement and AIS systems' reliability s in Jordan and in similar settings. Additional studies of systems' reliability and its determinants in different cultures and countries are indispensable. The accumulation of such studies will enable AIS researchers to make comparisons and to integrate findings into existing or new frameworks that enhance our understanding of global information systems' reliability. Future studies should also be directed to investigate the same phenomena in other types of owner business structure.

In this research, the business performance dimensions (financial and non-financial was measured by subjective measures for the reasons explained in Chapter 4. Future research is required to use objective measures for the business performance with subjective measures. The purpose would be to find out whether there is any difference between the results of using subjective and the results of using objective measures or together with the implementation of the SysTrust as well as with the quality of financial reporting.

Future research is required to examine both qualitative and quantitative e measures of the quality of financial reporting and their relationships with the implementation of SysTrust and business performance measures. The purpose is to verify the results which were obtained in this study.

References

- A. Marie, Attiea & Ibrahim, Mohamed & Al-Nasser, Amjad., (2014) "Effects of Financial and Non-financial Performance Measures on Customers' Perceptions of Service Quality at Islamic Banks in UAE" *International Journal of Economics and Finance*, 6(10), pp. 201-215.
- Aaker, D.A., (2011). *Building Strong Brands*. 1st ed. New York: The Free Press A Division Of Simon & Schuster.
- Abu Musa, A., (2006). "Investigating the Security Controls of CAIS in an Emerging Economy: An Empirical Study on the Egyptian Banking Industry", *Managerial Auditing Journal*, 19(2).
- Agbejule, A., (2011). "Organizational culture and performance: The role of management accounting system". *Journal of Applied Accounting Research*, 12(1), pp. 74-89.
- Ahmad Abu-Musa., (2010), "Information security governance in Saudi organizations: An empirical study", *Information Management and Computer Security*, 18(4), pp. 226-276.
- Ahmed, A. S. and Duellman, S., (2011), "Evidence on the role of accounting conservatism in monitoring managers' investment decisions", *Accounting and Finance*, 51(3), pp. 6090-633.
- AICPA & CICA., (2006), "Generally Accepted Privacy Principles", 7-12.
- AICPA/CICA, (2017), Privacy frame work including the AICPA/CICA trust service privacy principles and criteria, issued by the assurance services executive committee of the AICPA and the assurance services development board of the CICA.
- AISBA/CICA., (2006). Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (Including WebTrustw and SysTrustw), American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants, available at. www.webtrust.org/principles-and-criteria/item27818.pdf
- Akande, T; Akinwumi, A.; Abegunde, T., (2015). Nutritional and economic implications of cashew reject meal in diets of laying chickens. Tropentag, Prague, Czech Republic September 17-19.
- Aldas-Manzano, J, Lassala-Navarre, C., Ruiz-Mafe, C. and Sanz-Blas, S, (2009), "The role of consumer innovativeness and perceived risk in online banking usage", *International Journal of Bank Marketing*, 27(1), pp. 53-75.
- Al-Dmour, A., Al-Dmour, R. and Masa'deh, R., (2016), "Interrelated Factors Influencing the Adoption Decision of AIS" *International Business Research*, 9, pp. 1913-9012.
- Ali A. Al-Thuneibat, Awad S. Al-Rehaily, Yousef A. Basodan., (2015), "The impact of internal control requirements on profitability of Saudi shareholding companies", *International Journal of Commerce and Management*, 25(2), pp. 196-217.
- Alnajjar MIM, (2016), Impact of Accounting Information System on Organizational Performance. A Study of Small and Mid-Sised Enterprises in UAE, *International Journal of Accounting Research*, 4.1
- Alrowwad, Alaaldin & Obeidat, Bader & Tarhini, Ali & Aqqad, Noor., (2017), "The Impact of Transformational Leadership on Organizational Performance via the Mediating Role of Corporate Social Responsibility: A Structural Equation Modeling Approach", *International Business Research*. 10, pp. 199-221.

- Alsharayri, M., (2011), "The E-commerce Impact on Improving Accounting Information Systems in Jordanian Hotels", *International Research Journal of Finance and Economics*. (75), pp. 16-17.
- Arens, A., Elder, R. and Beasley, M. (2008), *Auditing dan jasa Assurance*. 12th ed. Penerbit Erlangga Jakarta: Bahasa Indonesia language edition, pp. 371-375.
- Aly, A., S., El-Sayed, and I., Hassan., (2010), *Advanced Auditing In The Contemporary Business Environment*, Faculty of Commerce - Alexandria University (in Arabic).
- Amidu, M., Effah, J., & Abor, J., (2011), E-accounting practices among small and medium enterprises in Ghana. *Journal of Management Policy and Practice*, 12(4), pp. 146-155.
- Amin, H. and Mohamed, E., (2016), "Auditors' perceptions of the impact of continuous auditing on the quality of Internet reported financial information in Egypt", *Managerial Auditing Journal*, 31(1), pp. 111-132.
- Amudo, A. & Inanga, E.L., (2009), Evaluation of Internal Control Systems. A Case Study from Uganda, *International Research Journal of Finance and Economics*, 27, pp.124-144.
- Anderson, J. C. and Gerbing, D. W., (1982). Some methods for respecifying measurement models to obtain unidimensional construct measurement. *Journal of Marketing Research*, 19, pp. 453-460.
- Anderson, J. C. and Gerbing, D. W., (1988), Structural equation modelling in practice. A review and recommended two-step approach. *Psychological Bulletin*, 103(3), pp. 411-423.
- Arbuckle, J. L., (2005), *Amos 6.0 user's guide*, Chicago. SPSS, Inc.
- Arens, A., Elder, R. and Beasley, M. (2014). *Auditing and Assurance Services: An Integrated Approach*. 15th ed. Essex. England IFRS: Pearson Education Limited.
- Armstrong, C., Barth, M. E., Jagolinzer, A., & Riedl, E. J., (2010), "Market reaction to the adoption of IFRS in Europe", *The Accounting Review*, 85(1), pp. 31-61
- Azhar Susanto., (2004), *Management Information Systems*, 3rd Edition, Linga Jakarta, Bandung
- Azhar Susanto., (2008), *Accounting Information Systems: Developing Risk Control Structure*. 1st Edition, Lingga Jaya
- Bailey, A.D., (2000), "Discussion of AICPA/CICA SysTrust principles and criteria," *Journal of Information Systems*, 14(1), pp. 9-16.
- Bakar, N. M. A. & Tahir, I. M. (2009). Applying multiple linear regression and neural network to predict bank performance. *International Business Research*, 2, p. 176.
- Balzan, L. and Baldacchino, P.J., (2007). 'Benchmarking in Maltese internal audit units', Benchmarking", *An International Journal*, 14(6), pp. 750-767.
- Banks Law, (2000). "Law No. 28 for the Year 2000", Jordanian Official Gazette No. 4448, pp. 2950, Amman, Jordan
- Baron, R. and Kenny, D., (1986), "The moderator-mediator variable distinction in social psychological research, conceptual, strategic and statistical considerations", *Journal of Personality and Social Psychology*, 51, pp. 1173-1182.
- Barrett., (2007), *Personality and Individual Differences*, 42(5), pp. 859-67.

- Barr-Pulliam, D., (2017), "The effects of internal audit quality and earnings management option complexity on managerial discretion in financial reporting", Working Paper, University of Wisconsin-Madison.
- Barry Elliot and Jammie Elliot., (2011), *Financial Accounting and Reporting*, 14th Edition, Pearson Education. UK
- Barth, M. E , R. Kasznik and M. F. McNichols., (2001), "Analyst coverage and intangible assets", *Journal of Accounting Research* 39(1), pp. 1-34.
- Barth, M., Beaver, W. and Landsman, W., (2001), "The Relevance of the Value Relevance Literature for Financial Accounting Standard Setting: Another View", *Journal of Accounting and Economics*, 31, pp. 77-104.
- Barth, M., Landsman, W., and Lang, M., (2008), "International accounting standards and accounting quality", *Journal of Accounting Research*, 46(3), pp. 467-498.
- Bartov et al., Bartov, E., Goldberg, S.R., & Kim, M., (2005), "Comparative Value Relevance Among German, U.S., and International Accounting Standards: A German Stock Market Perspective", *Journal of Accounting, Auditing & Finance*, 20(2), pp. 95-119.
- Bartov, E. and Mohanram, P., (2004), "Private information, earnings manipulations and executive stock-option exercises", *The Accounting Review*, 79(4), pp. 889-1010.
- Bedard, J.C., Jackson, C.M. & Graham, L., (2005), "Issues and risks in performing SysTrust engagements. Implications for research and practice", *International Journal of Accounting Information Systems*, 6(1), pp. 55-79
- Bentler, P.M. and Bonnet, D.C., (1980), "Significance Tests and Goodness of Fit in the Analysis of Covariance Structures," *Psychological Bulletin*, 88(3), pp. 588-606.
- Berenson, Mark, L., David M. Levine, and T.C. Krehbiel., (2006), *Basic Business Statistics Concepts and Applications*, Tenth Edition Prentice-Hall, Inc, Englewood Cliffs, NJ, 07632.
- Beretta, S. & Bozzolan, S., (2004), "A framework for the analysis of firm risk communication. *The International Journal of Accounting*, 39, pp. 265-288.
- Beuselinck, C., & Manigart, S., (2007), "Financial reporting quality in private equity backed companies", *Small Business Economics*, 29(3), pp. 261-274.
- Bhattacharjee, A., (2012), "Social Science Research: Principles, Methods, and Practices" Textbooks Collection.
- Biesanz, J. C., Falk, C. F., & Savalei, V., (2010), "Assessing Mediation Models. Testing and Interval Estimation for Indirect Effects", *Multivariate Behavioral Research*, 45(4), pp. 661–701.
- Biga, C.F. and Neuman, W.L., (2006), *Instructor's Manual and Test Bank for Neuman, Social Research Methods and Qualitative and Quantitative Approaches*, Pearson Allyn and Bacon.
- Blumberg, B., Cooper, D.R. and Schindler, P.S., (2008), *Business research methods*, Berkshire. McGraw-Hill.
- Bryman, A. (2006), "Integrating quantitative and qualitative research; how is it done", *Qualitative Research*, 6(1), pp. 97–114.
- Blumberg, B., Cooper, D.R., Schindler, P.S., (2014). *Business Research Methods*, 4th Revised edition edition. ed. McGraw Hill Higher Education, London.

- Bodnar., George H. & William S., Hoopwood. (2010), *Accounting Information Systems*, 10th Edition. NJ. Prentice Hall
- Bollen KA., (1989). *Structural Equations with Latent Variables* (Wiley, New York).
- Boritz J. Efrim., (2005), "IS practitioners' views on core concepts of information integrity" *International Journal of Accounting Information Systems*; 6(4), pp. 260-279.
- Boritz, E., and J., Hunton., (2002), "Investigating The Impact Of Auditor-Provided Systems Reliability Assurance On Potential Service Recipients", *Journal of Information Systems, Supplement*, 16, pp. 69-88.
- Boritz, E., D., McPhie, and B., Walker., (2000), "In Systems We Trust", *CA Magazine*, Mar, 133(2), pp. 47-49.
- Boritz, E., E., Mackler, and D., McPhie, (1999), "Reporting on Systems Reliability", *Journal of Accountancy*, 188(5), pp. 75-83.
- Boritz, J. Efrim & Kearns, J. H., (2000), "Symposium in IS Assurance Panel Discussion on Systrust", *Journal of Information Systems*, 14(1), pp. 163-176.
- Botosan, C., (2004), "Discussion of a framework for the analysis of risk communication", *The International Journal of Accounting*, 39, pp. 289-295.
- Brown, C. E., J. A. Wong, and A. A. Baldwin., (2007), A review and analysis of the existing research streams in continuous auditing, *Journal of Emerging Technologies in Accounting* 4.1-28.
- Brown, T. A., (2006), *Confirmatory Factor Analysis for Applied Research*. New York, Guilford Press.
- Bryman, A. (2014). *Social Research Methods*, 4th edition, Oxford, Oxford University Press.
- Bryman, A. and Bell, A., (2007). *Business Research Methods*, 2nd edition, New York, Oxford University press.
- Bryman, A. and Bell, E., (2003), *Business research methods*. New York, Oxford University Press.
- Bukenya, Moses., (2014), "Quality of Accounting Information and Financial Performance of Uganda's Public Sector", *American Journal of Research Communications*. 2(5), pp. 183-203.
- Buonanno, G., Faverio, P., Pigni, F., Ravarini, A., Sciuto, D. and Tagliavini, M., (2005), "Factors affecting ERP system adoption: a comparative analysis between SMEs and large companies", *Journal of Enterprise Information Management*, 18(4), pp. 384-426.
- Burton, F., S., Emett, C., Simon, and D., Wood, (2012). "Corporate Managers' Reliance on Internal Auditor Recommendations", *A Journal of Practice and Theory*, 31(2), pp. 151-166.
- Byrne, B., (2010), *Structural equation modeling with AMOS: Basic concepts, applications and programming* 6th Edition, New York, USA. Taylor & Francis Group.
- Cadez S, Guilding C., (2008), "An Exploratory Investigation of an Integrated Contingency Model of Strategic Management Accounting", *Accounting, Organizations and Society*, 33(7-8), pp. 836-863.

- Callao Gastón, S (2010), IFRS adoption in Spain and the United Kingdom. Effects on accounting numbers and relevance, *Advances in Accounting, incorporating Advances in International Accounting*, pp. 1-10.
- Callao, S., Jarne, J. I., and Lainez, J., (2007), “Adoption of IFRS in Spain. Effect on the comparability and relevance of financial reporting”, *Journal of International Accounting, Auditing and Taxation*, 16, pp. 148-178.
- Cao, Y., Myers, L.A. and Omer, T.C., (2012), “Does company reputation matter for financial reporting quality, Evidence from restatements”, *Contemporary Accounting Research*, 29(3), pp. 956-990.
- Carlson, K. and Herdman, A. O., (2012), “Understanding the impact of convergent validity on research results”, *Organizational Research Methods*, 15, pp. 17–32.
- Casolaro, L. and Gobbi, G., (2004), “Information Technology & Productivity Changes in the Italian Banking Industry” Report Published by Bank of Italy Economic Research Department, pp.1-26.
- Cerullo M. and Michael J., (1999), “Client/Server Systems Security and Controls”, *Internal Auditor Journal*, 56 (5), pp. 67-89.
- Chen, F., Hope, O. K., Li, Q. and Wang, X., (2011), "Financial Reporting Quality and Investment Efficiency of Private Firms in Emerging Markets", *The Accounting Review* 86(4), pp. 1255-1288.
- Chenhall, R., (2003), “Management control systems design within its organizational context. Findings from contingency based research and directions for the future”, *Accounting, Organizations and Society*, 28(2/3), pp. 127-168.
- Chenhall, R. H., (2005), “Integrative strategic performance measurement systems, strategic alignment of manufacturing, learning and strategic outcomes; an exploratory study”, *Accounting, Organizations and Society*, 30(5), pp. 395-422.
- Choe, J., (2015), “The Relationships among Performance of Accounting Information Systems, Influence Factors, and Evolution Level of Information Systems”, *Journal of Management Information Systems*, 12(4).
- Chong, A. Y.-L. (2013). Predicting m-commerce adoption determinants: A neural network approach. *Expert Systems with Applications*, 40, pp. 523-530.
- Chow, C., & Steve, W., (2006), “The Use and Usefulness of Nonfinancial Performance Measures”, *Management Accounting Quarterly*, 7(3), pp. 1–8.
- Churchill Jr, G.A. and Iacobucci, D. (2009), *Marketing research; Methodological foundations*, Cengage Learning.
- Clor-Proell, S. M., C. A. Proell, and T. D. Warfield., (2014), “The effects of presentation salience and measurement subjectivity on nonprofessional investors' fair value judgments”, *Contemporary Accounting Research* 31(1), pp. 45-66.
- Coderre, David., (2006), “Continuous Auditing. Implications for Assurance, Monitoring, and Risk Assessment”, A Summary of The IIA’s Global Technology Audit Guide, pp. 1-10.
- Coe. Martin J., (2005), “Trust Services. A better way to evaluate IT controls”., *Journal of Accountancy*, 199(3), pp. 203-340.

- Coffin, R.G. and Patilis, C., (2001), "The internal auditor's role in privacy", *Internal Auditing*, 16(2), pp. 22-8.
- Cohen, J., Krishnamorthy, G. & Wright, A., (2004), "The corporate governance mosaic and financial reporting quality", *Journal of Accounting Literature*, 23, pp. 87-152.
- Cole, V., Branson, J. & Breesch, D., (2007). A review of the different methods developed to measure the comparability of financial statements, working paper series.
- Collis, J. & Hussey, R., (2014), *Business Research: a practical guide for undergraduate and postgraduate students*, 4th edition.
- Companies Law., (1997). "Law No. 22 for the Year 1997", Jordanian Official Gazette No. 4204, pp. 2038, A y7mman, Jordan.
- Cooper, C. R., & Schindler, P. S., (2008), *Business Research Methods* 10th Edition Boston. McGraw-Hill.
- Crano, W. D., & Brewer, M. B., (2005), *Principles and Methods of Social Research*, 3rd Edition, Mahwah, NJ. Lawrence Erlbaum Associates, Inc.
- Creswell, J., (2009), *Research Design. Qualitative, Quantitative, and Mixed Methods Approaches*, Sage Publishing.
- Creswell, J. W., (2013)., *Educational Research. Planning, conducting, and evaluating quantitative and qualitative research*, 4th Edition, Upper Saddle River, NJ, Pearson Education.
- Creswell, J., (2003)., *Research Dsign. Qualitative, Quantitative and Mixed Methods Approaches* 2nd edition, Thousand Oaks, CA. SAGE Publications.
- Cronbach, L. J., (1951, "Coefficient alpha and the internal structural of tests", *Psychometric*, 16(3), pp. 297-334.
- Daneila M., Vassen E, H.J., Dameri, R, P., (2013), *Accounting Information System for Decision Making*, Springer - Verlag, Berlin.
- Davis C. E., (1996), "Perceived security threats to today's accounting information system: A survey of CISA", *Information System Audit Control Journal*, 3, 38-41
- Daw Hla And Susan Peter Teru., (2015). 'Efficiency of Accounting Information System and Performance Measures – Literature Review ', *International Journal of Multidisciplinary and Current Research*, 3, pp. 976-984.
- Dehning, B. and Richardson, V.J., (2002), "Returns on Investments in Information Technology. A Research Synthesis", *Journal of Information Systems*, 16(1), pp. 7-30.
- DeLone, W. H. and E. R. McLean., (2003), 'The DeLone and McLean model of information systems success. A ten-year update', *Journal of Management Information Systems*, 19(4), pp. 9-30.
- Denton S., (2002), Data estimates for different maintenance options for reinforced concrete cross heads. Draft report for Highways Agency, U.K., Brinckerhoff Ltd.
- Dess, G. G. & Robinson, J. R. B., (1984). "Measuring organizational performance in the absence of objective measures.; The case of the privately-held firm and conglomerate business unit." *Strategic Management Journal*, 5(3), pp. 265-273.

- DeVellis, R. F., (2003). *Scale development. Theory and applications* 2nd ed. Thousand Oaks, CA. Sage.
- Dhillon, G., (1999). "Managing and controlling computer misuse", *Information Management & Computer Security*, 7(4), pp. 171-175.
- Dhunna, M. and J. B., D., (2010), *Information Technology in Business Management*, 1st Edition, Laxmi Publications.
- Diamantopoulos, A. and Siguaw, J. A., (2000), *Introducing LISREL*. London. Sage Publications Ltd.
- Dien, N., (2014), "The impact of internal audit function effectiveness on quality of financial reporting and its implications on good government governance research on local government Indonesia", *Research Journal of Finance and Accounting*, 5(18), pp. 64-75.
- Djatej, A., Gao, G., Sarikas, R., Senteney, D., (2009). "An investigation of the comparative impact of degree of implementation of IFRS upon the public and private information quality of East and West European firms", *Advances in Accounting, incorporating* 25, pp. 208–215.
- Doherty, I., Sharma, N. & Harbutt, D. (2015). Contemporary and future eLearning trends in medical education. *Medical teacher*, 37, pp. 1-3.
- Dossi, Andrea & Patelli, Lorenzo., (2010), "You Learn From What You Measure. Financial and Non-financial Performance Measures in Multinational Companies", *Long Range Planning* -. 43. pp. 498-526.
- Doug McPhie., (2000), "Information Systems Assurance and Advisory Services, Ernst & Young.AICPA/CICA Systems Reliability Task Force", *Journal of Information Systems* 14(s-1), pp. 1-7.
- Doyle, J., Ge W, and McVay, S., (2007), "Accrual Quality and Internal Control Over Financial Reporting", *Accounting Review*, 82(5), pp. 1141-1170.
- Eastin, M.S., (2002), "Diffusion of e-commerce. An analysis of the adoption of four e-commerce activities", *Telematics and Informatics*, 19(3), pp. 251-267.
- Ejoh, N. and Ejom, P., (2014), "The Impact of Internal Control Activities on Financial Performance of Tertiary Institutions in Nigeria", *Journal of Economics and Sustainable Development*, 5(16), pp. 133-143
- Elder, Randal J., Mark S. Beasley, and Alvin A. Arens., (2010), *Auditing and Assurance Services: An Integrated Approach*. NJ. Prentice-Hall
- Elliott, R. K., (1995), "The future of assurance services: Implications of academia", *Accounting Horizons* 9(4), pp. 118-127.
- Elliott, R., and D., Pallais., (1997). "Are You Ready For New Assurance Services?" *Journal of Accountancy*, 183(6), pp. 47-51.
- Ewart, R., and Wagenhofer, A., (2013), *Accounting Standards, Earnings Management, and Earnings Quality*, University of Graz, Working Paper.
- FASB., (2008), *Financial Accounting Series, Statement of Financial Accounting Standards No. 1570-100, Exposure Draft on an Improved Conceptual Framework for Financial Reporting*. Norwalk.

- FASB (2013), "Rules of Procedures, Amended and Restated December 11, 2013." www.fasb.org.
- Financial Accounting Standards Board [FASB], (1999), International standard setting: A vision for the future. Norwalk.
- Fogarty, T.J., Radcliffe, V.S. and Campbell, D.R., (2006). "Accountancy Before the Fall. The AICPA Vision Project and Related Professional Enterprises" *Accounting, Organizations and Society*, 31(1). pp. 125.
- Fornell, C., Larcker, D.F., (1981), Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research* 18(1), pp. 39-50.
- Francis, J., LaFond, R., Olsson, P. & Schipper, K., (2004)," Cost of Equity and Earnings Attributes, *The Accounting Review*, 79(4), pp. 967-1010.
- Fritz, M. S., & MacKinnon, D. P., (2007), "Required sample size to detect the mediated effect", *Psychological Science*, 18, pp. 233-239.
- Gable, G., Sedera, D. and Chan, T., (2008), "Reconceptualising information system success; the IS-impact measurement model", *Journal of the Association for Information Systems*, 9(7), pp. 377-408.
- Gaeremynck, A. & Willekens, M., (2003). "The Endogenous Relationship between Audit-Report Type and Business Termination: Evidence on Private Firms in a NonLitigious Environment", *Accounting and Business Research*, 33(1), pp. 65-79.
- García Lara, J. M., B. Garcia Osma, and F. Penalva., (2010). "Conditional conservatism and firm investment efficiency". Working Paper, Universidad Carlos III de Madrid, Madrid.
- Gattoufi, S., Oral, M., Kumar, A. and Reisman, A., (2004), "Content analysis of data envelopment analysis literature and its comparison with that of other OR/MS fields", *Journal of the Operational Research Society*, 55(9), pp. 911-935.
- Gaynor, Andrea Seaton Kelton, Molly Mercer, and Teri Lombardi Yohn., (2016), "Understanding the Relation between Financial Reporting Quality and Audit Quality", *Journal of Practice & Theory*, 35(4), pp. 1-22.
- Ge W and McVay, S., (2005). The Disclosure of Material Weakness in Internal Control After The Sarbanes-Oxley Act. *Accounting Horizons*, 19(3), pp. 137-158.
- Gelinas, J.U., et al., (2014)., *Accounting Information Systems'* South Western. Cengage Learning
- Gerbing, D. W. and Anderson, J. C., (1988). "An Updated Paradigm for Scale Development Incorporating Unidimensionality and Its Assessment", *Journal of Marketing Research*, 25, pp. 186-192.
- Ghasemi, V. Shafeiepour, M. Aslani and E. Barvayeh., (2011). "The Impact of Information Technology (IT) on Modern Accounting", *Procedia - Social and Behavioral Sciences*, 28, pp. 112-116.
- Goitom G., (2003), *Accounting Policies, Professionalism, Competence and Quality of Accounting Information in Public Enterprises in Ethiopia*, Unpublished dissertation, Makerere University Business School.

- Grande, E. U., Estébanez, R. P., & Colomina, C. M., (2011), "The impact of accounting information systems (AIS) on performance measures' Empirical evidence in Spanish SMEs", *The international Journal of Digital Accounting Research*, 11, pp. 25-43.
- Greenwood, D. (1991). An overview of neural networks. *Systems Research and Behavioral Science*, 36, pp. 1-33.
- G.L. Gray, (2002). "Discussion of investigating the impact of auditor-provided systems reliability assurance on potential service recipients", *J. Inf. Syst.*, 16, pp. 91–96.
- Greenberg, R., W., Li, and B., Wing., (2012), " The Effect of Trust in System Reliability on the Intention to Adopt Online Accounting Systems", *International Journal of Accounting and Information Management*, 20(4), pp. 363-376.
- Guerreiro, M.S. et al., (2008), "The preparedness of companies to adopt International Financial Reporting Standards. Portuguese evidence", *Accounting Forum*, 32, pp. 75-88.
- Hair Jr., J. F., Black, W., Babin, B., Anderson, R. E., and Tatham, R., (2006). *Multivariate data analysis*. 6th Edition, New Jersey, Prentice Hall.
- Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E. & Tatham, R. L. (2010). *Multivariate data analysis*, Prentice hall Upper Saddle River, NJ.
- Hair, F. H., Hult, G.T.M., Ringle, C.M., & Sarstedt, M., (2014) *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Thousand Oaks, Sage Publications.
- Hair, J.F.J., Hult, G.T.M., Ringle, C.M. and Sarstedt, M., (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd Edition., Sage, Thousand Oaks, CA.
- Haykin, S. & Network, N. (2004). A comprehensive foundation. *Neural Networks*, 2(41).
- Hall, J, A., (2011), *Accounting Information Systems.*, 7th Edition, South-Western Cengage Learning, USA.
- Havelka D, Sutton SG, Arnold V., (1998), A methodology for developing measurement criteria for assurance services' An application in information systems assurance", *Auditing* 17, pp. 73–92.
- Haverals, J., (2007), "IAS/IFRS in Belgium; Quantitative analysis of the impact on the tax burden of companies". *Journal of International Accounting, Auditing and Taxation*, 16, pp. 69-89.
- Hayale, H. and Abu Khadra, A., (2006), "Evaluation of the Effectiveness of Control Systems in Computerised Accounting Information Systems. An Empirical Research Applied on Jordanian Banking Sector", *Journal of Accounting Business Management*, 13(3), pp. 39-68.
- Heng Xu, Cheng Zhang, Pan Shi, and Peijian Song., (2009), "Exploring the role of overt vs. covert personalization strategy in privacy calculus," *Academy of Management Proceedings* (August Meeting Abstract Supplement), pp. 1–6.
- Henri, J. F., Boiral, O., & Roy, M. J., (2014), "The tracking of environmental costs" Motivations and impacts", *European Accounting Review*, 23(4), pp. 647-669.
- Henry Laurie., (1997). "A Study of the Nature and Security of Accounting Information Systems. The Case of Hampton Roads", Virginia", *the Mid- Atlantic Journal of Business.*, 33, (63) pp. 171-189.

- Hermanson, D.R., Hill, M.C. and Ivancevich, D.M., (2000), "Information technology related activities of internal auditors", *Journal of Information Systems, Supplement*, 14(1), pp. 39-53.
- Hirst, D., Hopkins, P. & Wahlen, J., (2004). "Fair Values, Income Measurement, and Bank Analysts' Risk and Valuation Judgments", *The Accounting Review*, 79(2), pp. 453-472.
- Holmes-Smith, P., Coote, L., and Cunningham, E., (2006), "Structural equation modelling. From the fundamentals to advanced topics", Melbourne, School Research, Evaluation and Measurement Services.
- Hood, K. L. and J. Yang., (1998), "Impact of Banking Information Systems Security on Banking in China. The Case of Large State-Owned Banks in Shenzhen Economic Special Zone - An Introduction", *Journal of Global Information Management*, 6(3), pp. 5 - 15.
- Hooper, D., Coughlan, J., and Mullen, M., (2008)," Structural Equation Modelling. Guidelines for Determining Model Fit", *Electronic Journal of Business Research Methods*, 6, pp. 53-60.
- Hu, L.T. and Bentler, P.M., (1999), "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis. Conventional Criteria Versus New Alternatives," *Structural Equation Modelling*, 6(1), pp. 1-55.
- Hui Feng., (2002). "Real-Time or Current Vintage. Does the Type of Data Matter for Forecasting and Model Selection?."
- Hung, M., Subramanyam, K.R., (2007). "Financial statement effects of adopting international accounting standards. The case of Germany", *Review of Accounting Studies* 12, pp. 623-657.
- Hunton, J. E. (2002), Blending Information and Communication Technology with Accounting Research., *Accounting Horizons*, 16(1).pp. 55-67.
- Hoitash, R. Hoitash and J. C. Bedard., "Corporate governance and internal control over financial reporting; a comparison of regulatory regime", *Account. Rev.*, 84(3), pp. 839-867.
- Hussey., J. and Hussey, R. (1997), "*Business Research: A practical guide for undergraduate and postgraduate students*", Macmillan Press Ltd.
- IASB., (1989), Framework for the Preparation and Presentation of Financial Statements. London
- IASB., (2008), Exposure Draft on an improved Conceptual Framework for Financial Reporting: The Objective of Financial Reporting and Qualitative Characteristics of Decision-useful Financial Reporting Information, London.
- IASB., (2008). Impairment of assets, Amended by Annual Improvements to IFRSs 2007 (disclosure of estimates used to determine a recoverable amount.
- IASB 39., (2008), Financial Instruments. Recognition and Measurement – Treating loan prepayment penalties as closely related embedded derivatives/ Amendment to IAS 39 for reclassifications of financial assets.
- Iatridis, G., (2010), "International financial reporting standards and the quality of financial statement information", *International Review of Financial Analysis*, 19, pp. 193–204.
- Iceman & Hillson., (2012), Distribution of Audited Detected Errors by Internal Control", *Journal of Accounting, Auditing & Finance*, 5(4), pp. 527-543.
- IIRC and AICPA., (2013). 'Materiality. Background Paper for', <http://www.theiirc.org/wp-content/uploads/2013/03>.

- Insurance Regulatory Law., (1999). "Law No. 33 for the Year 1999", Jordanian Official Gazette No. 4389, pp. 4271, Amman, Jordan.
- International Accounting Standards Board (IASB) (2006), 'Preliminary Views on an Improved Conceptual Framework for Financial Reporting', Discussion Paper, IASB, London.
- Irny, S. I. & Rose, A. A., (2005)., "Designing a Strategic Information Systems Planning Methodology for Malaysian Institutes of Higher Learning ", *Issues in Information System*, 6(1), pp. 325-331.
- ITGI., (2004), Managing enterprise information integrity: security, control and audit issues. USA. IT Governance Institute.
- Iu, J. & Clowes, C., (2004), Evaluating a measure of content quality for accounting narratives (with an empirical application to narratives from Australia, Hong Kong, and the United States). Working paper series.
- Jo, H., and Kim, Y., (2007),"Disclosure frequency and earnings management", *Journal of Financial Economics*, 84, pp. 561-590.
- Jonas, G. & Blanchet, J., (2000), "Assessing Quality of Financial Reporting", *Accounting Horizons*, 14(3), pp. 353-363.
- Jöreskog, K. G. and Sörbom, D., (1982), "Recent development in structural equation modelling" *Journal of Marketing Research*, 19(4), pp. 404-416.
- K. Campbell et al., (2003), "The Economic Cost of Publicly Announced Information Security Breaches. Empirical Evidence from the Stock Market," *J. Computer Security*, 11(3), pp. 431–448.
- Kaplan, S. E., & Nieschwietz, R. J., (2003), "A Web assurance services model of trust for B2C e-commerce", *International Journal of Accounting Information Systems*, 4, pp. 95–114
- Khazanchi, D. and S.G. Sutton., (2001). "Assurance services for business-to-business electronic commerce. a framework and implications," *Journal of the Association for Information Systems*, 1, pp. 1-53.
- Khther, R. and Othman, M., (2013), "Cobit Framework as a Guideline of Effective it Governance in Higher Education", *International Journal of Information Technology Convergence and Services*, 3(1), pp. 21-29.
- Kieso, D., Weygandt, J., and Warfield, T., (2015). *Intermediate Accounting*, 2nd Edition United States of America, John Wiley & Sons.
- Kim, H. W., Xu, Y., & Koh, J., (2004), "A comparison of online trust building factors between potential customers and repeat customers", *Journal of the Association for Information Systems*, 5(10), pp. 392–420.
- Kim, H., Hoskisson, R. E., & Wan, W. P., (2004)," Power dependence, diversification strategy, and performance in keiretsu member firms", *Strategic Management Journal*, 25(7).
- Kim, J., Simunic, D., Stein, M. & Yi, C.H., (2007), Voluntary Audits and the Cost of Debt Capital for Privately Held Firms, Korean Evidence, Working paper series.
- Kim, J-B., B. Y. Song, and L. Zhang., (2011). "Internal control weakness and bank loan contracting. Evidence from SOX Section 404 disclosures", *The Accounting Review* 86 (4). pp. 1157-1188.

- Kinney, W. R., (2000), "Research Opportunities in Internal Control, Quality and Quality Assurance", *A Journal of Practice and Theory*, 19(4), pp. 83-90.
- Kinyua, J.K., Gakure, K., Gekara, R., & Orwa, M., (2015), "Effect of internal control environment on the financial performance of companies quoted in the Nairobi Securities Exchange", *International Journal of Innovative Finance and Economics Research*, 3(4), pp. 29-48.
- Klamm, B.K., and Watson, M.W., (2009). "SOX 404 Reported Internal Control Weaknesses: A Test of COSO Framework Components and Information Technology," *Journal of Information Systems*, 23(2), pp. 1-23.
- Kline, R., (2005). *Principles and practices of structural equation modeling*, 2nd Edition, New York. Guilford Pres
- Knechel, W. P., Wallage, A., Eilifsen, and B., Praag., (2006). "The Demand Attributes of Assurance Services Providers and the Role of Independent Accountants", *International Journal of Auditing*, 10, pp. 143-162.
- Kneller, R., and Stevens, P.A., (2002), 'Absorptive Capacity and Frontier Technology: Evidence from OECD Manufacturing Industries', NIESR, Discussion Paper No. 202.
- Konrath, L. F., (2002). *Auditing - A Risk Analysis Approach*. 5th Edition, Thomson Learning. Canada.
- Kothari C.R., (2010), *Research Methodology: Methods and Technique*, New Delhi. New Age International Publishers.
- Kovar, S.E. and Mauldin E.G., (2003), Antecedents of Demand for Assurance Services: A Model for Analysis with Applications in B2B E-Commerce, Working paper, The University of Missouri – Columbia.
- Krishnan, R., Peters, J., Padman, R., & Kaplan, D., (2005). On data reliability assessment in AIS. *Information Systems Research*, 16(3), pp.307-326. doi.10.1287/isre.1050.0063.
- Lam, C. T. and Kolic, M., (2008). 'Effects of Semantic Incompatibility on Rating Response', *Applied Psychological Measurement*, *Sage Publications*, 32(3), pp. 248–260.
- Lambert, R., Leuz, C. and Verrecchia, R. E. (2007), "Accounting information, disclosure, and the cost of capital", *Journal of Accounting Research*, 45(2), pp. 385-420.
- Law of Organizing the Practice of the Public Accounting Profession., (2003). "Law No. 73 for the Year 2003", Jordanian Official Gazette No. 4606, pp. 3292, Amman, Jordan.
- Lee, M., (2009), "Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit", *Electronic Commerce Research and Applications*, (8), pp. 130 – 141.
- Leedy, P. D., & Ormrod, J. E., (2005), *Practical Research. Planning and Design*, 8th Edition ed.), Upper Saddle River, NJ, Prentice Hall.
- Lehmann, D.R. and Hulbert, J., (1972). "Are three-point scales always good enough?", *Journal of Marketing Research*, 9(4), pp. 444-446.
- Levy Y. and Ellis T.J., (2006), "Towards a framework of literature review process in support of information systems research", Proceedings of the 2006 Informing Science and IT Education Joint Conference, Salford, UK – June 2528,171181.

- Lincoln, Y.S. & Guba, E.G., (2005), "Paradigms and Perspectives in Contention", In N. Denzin and Y. Lincoln (eds.), *Handbook of Qualitative Research* 2nd Edition, Thousand Oaks, CA. Sage.
- Loch, K. D., Carr, H. H., & Warkentin, M. E., (1992), "Threats to Information Systems: Today's Reality, Yesterday's Understanding", *MIS Quarterly*, 16(2), pp. 173–186.
- Lyu, M. R., (1996), *Handbook of Software Reliability Engineering*. NY. McGraw–Hill/IEEE Computer Society Press.
- MacCallum, R. C., Browne, M. W., and Sugawara, H. M., (1996), "Power analysis and determination of sample size for covariance structure modelling", *Psychological Methods* 1. pp. 130–149.
- MacKinnon DP, Taborga MP, Morgan-Lopez AA., (2002), "Mediation designs for tobacco prevention research", *Drug & Alcohol Dependence*. 68, pp. S69–S83.
- Maines, L., and Wahlen, J., (2006), "The nature of accounting information reliability; Inferences from archival and experimental research", *Accounting Horizons*, 20(4), pp. 399-425.
- Malhotra and Malhotra, (2013). A. Malhotra, C.K. Malhotra, "Exploring switching behavior of US mobile service customers", *Journal of Services Marketing*, 27(1), pp. 13-24.
- Mangan, J., Lalwani, C. and Gardner, B., (2004), "Combining quantitative and qualitative methodologies in logistics research", *International Journal of Physical Distribution and Logistics Management*, 34(7), pp. 565-578.
- Mansour, E., Mohammad, A., Missi, F. and Hamdan A., (2009), Examining the Existence of (SYSTRUST) Model and its Impact on Jordanian Commercial Banks Performance; European and Mediterranean Conference on Information Systems (EMCIS2009). July 13-14. Crowne Plaza Hotel. Izmir.
- Marshal B, Romney PJS., (2015). *Accounting Information Systems*. Thirteen Edition. Pearson Education Limited, pp. 214-234
- Matthew Hall., (2010), "Accounting information and managerial work", *Accounting, Organizations and Society* 35(3) pp. 301-315.
- Mbobu E. and N. Ekpo., (2016). "Operationalizing the qualitative characteristics of financial reporting"; *International Journal of Finance and Accounting*, 4, pp. 184-192.
- McDaniel, L., Martin, R., & Maines, L., (2002), "Evaluating financial reporting quality. The effects of financial expertise vs. financial literacy", *The Accounting Review*, 77, pp. 139-167.
- McDonald, R. P. and Ho, M. H. R., (2002). "Principles and practice in reporting structural equation analyses", *Psychological Methods*, 7(1), pp. 64-82.
- McMurray, A., Pearson, Paul Spoonley David George, Scott, D. and Pace, R.W., (2004). *Research, A common sense approach*, Cengage Learning Australia.
- McPhie, D., (2000)., AICPA/CICA SYSTRUST[TM] *Principles and Criteria*. *Journal of Information Systems*. American institute of Certified Public Accountants, Canadian Institute of Chartered Accountants.
- Meharia, P., (2012). "Assurance on the reliability of mobile payment system and its effects on its' use. an empirical examination", *Accounting and Management Information Systems*, 11(1), pp. 97-111.

Meiryani., (2014), “ Influence of Top Management Support on The Quality of Accounting Information System and its impact on the Quality of Accounting Information”, *Research Journal of Finance and Accounting*. 5(11), pp. 124-132

Mohamed Z. Elbashir, Philip A. Collier, Steve G. Sutton., (2011). “The Australian National University The University of Melbourne University of Central Florida”, *The Accounting Review*. 86(1), pp. 155-184.

Moser, C & Kalton G, (1989). *Survey Methods in Social Investigation*. Hampshire, UK: Gower Publishing

Mudrajad Kuncoro., (2009), *Research Methods for Business and Economics*, 3rd Edition, publisher.

Müller, M. A., E.J. Riedl, and T. Sellhorn., (2015), “Recognition versus disclosure of fair values”, *The Accounting Review* 90(6). pp. 2411-2447.

Murtagh, F. & Heck, A. (2012). *Multivariate data analysis*, Springer Science & Business Media

National Institute of Standards and Technology, (2003). Computer Security Division, Information Technology Laboratory, Standards for Security Categorization of Federal Information and Information Systems, Initial Publication Draft, Version 1.0, May.

Nelson, R. R., Todd, P. A., and Wixom, B. H., (2005), “Antecedents of information and system quality. An empirical examination within the context of data warehousing”, *Journal of Management Information Systems*, 21(4), pp. 199–209.

Neuman, W. L., (2011), “Social Research Methods. Qualitative and Quantitative Approaches”. *International Journal of Business and Management* 9(11), pp. 2014 233

Nichols, D. & Wahlen, J., (2004), “How Do Earnings Numbers Relate to Stock Returns? A view of Classic Accounting Research with Updated Evidence”, *Accounting Horizons*, 18(4), pp. 263-286.

Nicolaou, A. I., (2000), “A contingency model of perceived effectiveness in accounting information systems. Organisational coordination and control effects”, *International Journal of Accounting Information Systems*, 1(2), pp. 91-105.

Nunnally, J. C., and Bernstein, I. H. (1994) *Psychometric theory*, 3rd Edition, New York, NY. McGraw-Hill, Inc.

Nunnally, J., (1967) *Psychometric Methods*, New York. McGraw-Hill Book Co.

Nur, I and Bambang S., (2011), *Business Research Methodology For Accounting and Management*, 1st Edition, BPFE, Yogyakarta.

Ogneva, M., (2010), “Accrual quality, realised returns, and expected returns.; The importance of controlling for cash flow shocks”, *The Accounting Review*, 87(4), pp. 1415- 1444.

Onaolapo, A. A., and Odetayo, T. A., (2012), “Effect of Accounting Information System on Organizational Effectiveness’ A Case Study of Selected Construction Companies in Ibadan, Nigeria”, *American Journal of Business and Management*, 1(4), pp. 183-189.

Papazoglou, A. Tsalgaidou., (2000), “Editorial. Business to business electronic commerce issues and solutions”, *Decis. Support Syst*, pp. 301-304.

- Pascan I.D. & Turcas M., (2012), "Measuring the impact of first - time adoption of International Financial Reporting Standards on the performance of Romanian listed entities", *Procedia Economics and Finance* 3, pp. 211-216.
- Pathak, J. and Lind, M.R., (2002), "Integrated information systems, SAS 94 & auditors", *Journal of Corporate accounting & Finance*, 19(1), pp. 57-67.
- Pérez, R., Urquía, E., & Muñoz, C., (2011), "The impact of Accounting Information Systems (AIS) on performance measures: Empirical evidence in Spanish SMEs", *International Journal of Accounting and Information Management*, 18(1), pp. 39-57.
- Peter Teru, S. and Tin Hla., D. (2015), Evaluation of the usefulness of efficiency of the accounting information system", *Business Management and Economics*, 5(19), pp. 76-89.
- Peter, J.P., (1979) 'Reliability. A review of psychometric basics and recent marketing practices', *Journal of Marketing Research*, 16, pp. 6-17.
- Petreski, M., (2006)., "The Impact of International Accounting Standards on Firms" 4th Annual Midyear Financial Accounting and Reporting Section, 27-28 January, Atlanta, Georgia.
- Pierce, G., (2002). "Multiple Regression and Mediation Analyses Using SPSS".
- Poshakwale, S. and Courtis, J., (2005)., "Disclosure level and cost of equity capital. Evidence from the banking industry", *Managerial and Decision Economics*, 26(7), pp. 431-444.
- Preacher, K. J., and Hayes, A. F., (2004), SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior Research Methods, Instruments, and Computers*, 36, pp. 717-731.
- Pugliese, A. and Halse, R., (2000), "SysTrust and WebTrust., Technology assurance opportunities" *CPA Journal*, 70(11), pp. 28-34.
- Qurashi A. and Siegel J., (1997), "The Accountant and Computer Security", *National public Accountant Journal*, 42(3).
- Rajgopal, S. And Venkatachalam, M., (2011), "Financial reporting quality and idiosyncratic return volatility", *Journal of Accounting and Economics*, 51, pp. 1-20.
- Ramamurthy, K.R., Sen, A. and Sinha, A.P., (2008), "An empirical investigation of the key determinants of data warehouse adoption", *Decision Support Systems*, 44(4), pp. 817- 841.
- Raupeliene, A., Stabingis, L., (2003), "Development of A model for Evaluating Effectiveness of Accounting Information Systems" Conference, EFITA, pp. 339-345.
- Rea, L. M., and Parker, R. A., (2006), *Designing and Conducting Survey Research*, San Francisco, Jossy-Bass
- Ribeiro, J. and Gomes, R., (2009), "IT Governance Using COBIT Implemented in a High Public Educational Institution - A Case Study", *Computing and Computational Intelligence* pp. 41-52.
- Ricchiute, D, N., (2006), *Auditing*. 8th Edition, Thomson Learning. Singapore
- Richard, P. J., Devinney, T. M., Yip, G. S., and Johnson, G., (2009), Measuring organizational performance; Towards methodological best practice", *Journal of Management*, 35(3), pp. 718-804.

- Robert K, Vanstraelen, A. and Zerni, M., (2015), “Does the Identity of Engagement Partners Matter? An Analysis of Audit Partner Reporting Decisions”, *Contemp Account Res*, 32, pp. 1443–1478.
- Rom, A. and Rohde, C., (2007), “Management accounting and integrated information systems, A literature review”, *International Journal of Accounting Information Systems*, 8, pp. 40-68
- Romney MB, Steinbart PJ., (2017), *'Accounting information systems'*, Pearson Prentice Hall.
- Rubino, Michele & Vitolla, Filippo., (2014), Internal control over financial reporting. Opportunities using the COBIT framework, *Managerial Auditing Journal*. 29, pp. 736-771.
- Ryan, S. D. and B. Bordoloi., (1997), “Evaluating Security Threats in Mainframe and Client / Server Environments”, *Information and Management*, 32(3), pp. 137 - 142.
- Shanker. S, (2013). “How is Information Technology Used in Accounting?”, *Chron Small Business Demand Media*.
- Sandeep Vij, Harpreet Singh Bedi, (2016) "Are subjective business performance measures justified?" ,*International Journal of Productivity and Performance Management*, Vol. 65 Issue: 5, pp.603-621,
- Saira, K., Zariyawati, M. A., & Annuar, M. N., (2010), “Information system and firms’ performance, The case of Malaysian small medium enterprises”, *International Business Research*, 3(4), pp. 28-35.
- Sajady, H., M. Dastgir and H.H. Nejad., (2008) “Evaluation of the effectiveness of accounting information system”, *Int. J. Inform. Sci. Technol.*, 6, pp. 49-59.
- Salehi, M., Rostami, V and Mogadama A., (2010), “Usefulness of accounting information system in emerging economy. Empirical evidence of Iran”, *International Journal of Economics and Finance*, 2(2), pp. 186–195.
- Samukri., (2015). Influence Effectiveness of Internal Control System and Implementation of Financial Accounting Information System on the Quality of Accounting Information”, *Research Journal of Finance and Accounting*, ISSN. 2222-1697, 6.
- Santos, J. B. & Brito, L. A. L., (2012), “Toward a subjective measurement model for firm performance”, *Brazilian Administration Review (BAR)*, 9(6), pp. 95–117.
- Saunders, M., Lewis, P. & Thornhill, A., (2009), *Research methods for business students*. 5th Edition, Harlow. Financial Times Prentice Hall.
- Saunders, M., Lewis, P. & Thornhill, A., (2015), *Research methods for business students*, 7th Edition, New York. Pearson.
- Sawyer, L., (2003), “Sawyer’s Internal Auditing”, The Practice of Modern Internal Auditing. Altamonte Springs, FL, *The Institute of Internal Auditors*.
- Schipper, K., (2003), “Commentary. Principles-Based Accounting Standards”, *Accounting Horizons*, 17(1), pp. 61-72.
- Schleicher, T, Tahoun, A & Walker, M., (2010)., “IFRS adoption in Europe and investment cash flow sensitivity. Outsider versus insider economics”, *The International Journal of Accounting*, 45(2), pp. 143–68

- Scott, J. E. & Walczalk S. (2009). Cognitive engagement with a multimedia ERP training tool: Assessing computer self-efficacy and technology acceptance. *Information & Management*, 46, pp. 221-232.
- Securities Law, (1997), "Law No. 23 for the Year 1997", Jordanian Official Gazette No. 4204, pp. 2185, Amman, Jordan
- Securities Law, (2002). "Law No. 76 for the Year 2002", Jordanian Official Gazette No. 4579, pp. 6218, Amman, Jordan.
- Sekaran Jr., J. F., Black, W. C., Babin, B. J., and Anderson, R. E., (2010), *Multivariate data analysis, A global perspective*, 7th Edition Pearson Education International.
- Sekaran, U. and R. Bougie., (2013), *Research methods for business: A skill-building approach*. Chichester, John Wiley and Sons.
- Sekaran, Uma, (2009). *Research Methods for Business - Research Methods for Business*, 4th Edition, Salemba Four.
- Shmueli, G. & Koppius, O. R. (2011). Predictive analytics in information systems research. *Mis Quarterly*, pp. 553-572.
- Siegel, S., (1956), *Nonparametric statistics*. New York. McGraw-Hill Book Company, Inc.
- Simms, L. J. & Watson, D., (2007), The construct validation approach to personality scale construction. In R.W.Robins, C. R. Fraley, & R. F. Krueger (Eds.), *Research Methods on Personality Psychology*, New York, The Guildford Press.
- Siponen M. T., and Oinas-Kukkonen, H., (2007), "A Review of Information Security Issues and Respective Research Contributions," ACM SIGMIS Database, (38.1), pp. 60-80.
- Sobel ME., (1982), "Asymptotic confidence intervals for indirect effects in structural equation models ", *Sociological methodology* 13, pp. 290–312.
- Solove, D., (2006), 'A taxonomy of privacy', *University of Pennsylvania Law Review* 154(3), pp. 477–560.
- Straub, D. W., Gefen, D., and Boudreau, M-C., (2005), *Quantitative research, Research in information systems: A handbook for research supervisors and their students*, Amsterdam. Elsevier.
- Streiner DL, Norman GR., (2008), *Health measurement scales: A practical guide to their development and use*, 4th Edition, Oxford. Oxford University Press, Chapter 8.
- Sugiyono, (2011), *Methods of Research Administration*, 19th Edition, Publisher Alfabeta, Bandung.
- Sutton, S.G., (2006), "Enterprise systems and the re-shaping of accounting systems. A call of research", *International Journal of Accounting Information Systems*, 7, pp. 1-6.
- Szylar, C., (2013), *Risk management under UCITS III/ IV. New Challenges For The Fund Industry*, John Wiley & Sons.
- Tabachnick, B. G., and Fidell, L. S., (2007), *Using Multivariate Statistics*, 5th Edition, Boston. Allyn and Bacon.

- Taghian, M., D'Souza, C., and Polonsky, M. J., (2015) "A stakeholder approach to corporate social responsibility, reputation and business performance", *Social Responsibility Journal*, 11(2), pp. 340-363.
- Taiwo, J.N., and Agwu, M.E., Edwin., (2016), "Effect of ICT on Accounting Information System and Organizational Performance", *European Journal of Business and Social Sciences*. 5, pp. 01-15.
- Tan, Y-H., and W. Thoen., (2012), "Toward a generic model of trust for electronic commerce", *International Journal of Electronic Commerce* 5(2), pp. 61-74.
- Tan, Y W., (2002), 'Formal aspects of a generic model of trust for electronic commerce' *Decis., Support Syst.*, pp. 233–246
- Tasios, S. and Bekiaris, M., (2012)., "Auditor's Perceptions of Financial Reporting Quality: The Case of Greece", *International Journal of Accounting and Financial Reporting*, 2 (1), pp. 57-74.
- Topash, N.K., (2014), "Evaluation of Efficiency of Accounting Information Systems: A Study on Mobile Telecommunication Companies in Bangladesh", *Global Disclosure of Economics and Business*, 3(1), pp. 40-55.
- Tu, J. V. (1996). Advantages and disadvantages of using artificial neural networks versus logistic regression for predicting medical outcomes. *Journal of clinical epidemiology*, 49, pp. 1225-1231.
- Van Beest, F. V., Braam, G. and Boelens, S., (2009), "Quality of Financial Reporting. Measuring Qualitative Characteristics", Working Paper, Radboud University, Nijmegen, Netherlands, pp. 1-108.
- Van der Meulen, S., Gaeremynck, A., & Willekens, M., (2007), "Attribute differences between US GAAP and IFRS earnings: An exploratory study", *The International Journal of Accounting*, 42(2), pp. 123-142.
- Visser, C.B. & Erasmus, P.W., (2008), *The Management of Public Finance: A practical guide*. Cape Town, Oxford University Press.
- W. Ballada and S. Ballada., (2011). "Basic Accounting", *Dom Ricchiute Publishing*, 20, pp. 88-90.
- Wagner, S.M., Rau, C. and Lindemann, E. (2010), "Multiple informant methodology. A critical review and recommendations", *Sociological Methods and Research*, 38(4), pp. 582-618.
- Wall, T. D., Michie, J., Patterson, M., Wood, S. J., Sheeran, M., Clegg, C. H., & West, M., (2004), "On the validity of subjective measures of company performance", *Personnel Psychology*, 57(1), pp. 95-118.
- Walsham, G., (2006). "Doing Interpretive Research", *European Journal of Information Systems* 15(3), pp. 320-330.
- Warren, M.J., (2002), "Security Practice. Survey evidence from three countries", *logistics Information Management*, 15, pp. 347-351.
- Weaver, K. and Olson, J.K., (2006), "Understanding paradigms used for nursing research", *Journal of Advanced Nursing*, 53(4), pp. 459-469.
- Weijters, Bert., Devarajan R., Falk, T and Niels Schillewaert (2007). "Determinants and Outcomes of Customers' Use of Self-Service Technology in a Retail Setting," *Journal of Service Research*, 10 (1), pp. 3–21.

- Westerheijden, DF., (2005), "Walking towards a moving target. Quality assurance in European higher education", *Aukštojo mokslo kokybė, Quality of higher education*, (2), pp. 52-69.
- Westland, J. C. (2000, "Modeling the Incidence of Postrelease Errors in Software Information" *Systems Research*, September, pp. 320-324.
- Wheaton, B., Muthen, B., Alwin, D., F., and Summers, G., (1977), "Assessing Reliability and Stability in Panel Models," *Sociological Methodology*, 8(1), pp. 84-136.
- White, G.W. and Pearson, S.J., (2001), "Controlling corporate e-mail, PC use and computer security", *Information Management and Computer Security*, 9(2/3), pp. 88-93.
- Whitman, M. E., (2004), "In defense of the realm: Understanding threats to information security". *Informational Journal of Information Management*, 24, pp. 3-4.
- Willekens, M., (2008), "Effects of external auditing in privately held companies", Empirical evidence from Belgium, Working paper series.
- Woodroof, J - Searcy, DeWayne., (2001), "Continuous audit. Model development and implementation within a debt covenant compliance domain", *International Journal of Accounting Information Systems* 2(3), pp. 169-191.
- Wright, Arnold and Wright, S., (2012), "The Relationship Between Strength Assessments of Internal Control and Error Occurrence, Impact and Cause", *Accounting and Business Research* 27(1).
- Wright, S. and A. Wright., (2002), "Information system assurance for enterprise resource planning systems: Implementation and unique risk considerations", *Journal of Information Systems*, 16, pp. 99-113.
- Witten, I. H., Frank, E., Hall, M. A. & Pal, C. J. (2016). *Data Mining: Practical machine learning tools and techniques*, Morgan Kaufmann.
- Zhang., X (2007), "Economic consequences of the Sarbanes-Oxley Act of 2002" *Account. Econ.*, 44 (1), pp. 74-115.
- Yurisandi, T., & Puspitasari, E., (2015), "Financial Reporting Quality- Before and After IFRS adoption using nice Qualitative Characteristics Measurement", Second Global Conference on Business and Social Science, GCBSS-2015, pp. 17-18.
- Zhou, T., (2011), "Examining mobile banking user adoption from the perspectives of trust and flow experience", *Information Technology and Management*, 13(1), pp. 27-37.
- Zhang., X (2007), "Economic consequences of the Sarbanes-Oxley Act of 2002" *Account. Econ.*, 44 (1), pp. 74-115.
- Zikmund, W. G., (2003), *Exploring marketing research*. Cincinnati, Ohio. Thomson/ South-Western.
- Zikmund, W.G., Babin, B.G., Carr, J.C. and Griffin M., (2013), *Business Research Methods*, 9th edition, Mason, Ohio. South-Western Cengage Learning.

Appendix A

Variables Operationalization's

(1) The Quality of Financial Reporting

1. Relevance		
Items	Items Description	Sources
R1	The annual reports discloses forward-looking information help forming expectations and predictions concerning the future of the company	Cole et al., (2007); FASB, (2013); Sajady et al., (2008) Beest , et al., (2009), Mamic Sacar & Oluic (2013); Samukri, (2015).
R2	The annual reports discloses information in terms of business opportunities and risks complement the financial information	
R3	The company uses fair value instead of historical cost.	
R4	Information helps you confirm profitability levels of the business	
R5	Financial reports are presented annually as required by regulatory bodies of accounting	
R6	No undue delays in the presentation of financial reports.	
R7	The annual report provides feedback information on how various market events and significant transactions affected the company	
2. Faithful representation		
F1	The annual report explains the assumptions and estimates made clearly; valid arguments provided to support the decision for certain assumptions and estimates in the annual report	Beuselinck and Manigart, (2007) ; FASB, 2013;; Beest , et al., (2009); Mamic Sacar & Oluic (2013)
F2	The annual report explains the choice of accounting principles clearly	
F3	The annual report highlights the positive and negative events in a balanced way when discussing the annual results	
F4	The annual report includes an unqualified auditor's report	
F5	The annual report extensively discloses information on corporate governance issues	
3. Understand ability		
U1	The annual report presented in a well-organised manner	Jonas & Blanchet, (2000); Maines and wahlen, (2004); Beest, et al., (2009), Samukri, (2015).
U2	The notes to the balance sheet and the income statement are s sufficiently clear	
U3	Sources and level of expenditure can easily be understood	
U4	Business assets are easy to know in terms of value and nature	
U5	the presence of graphs and tables clarifies the presented information	
U6	The use of language and technical jargon is easy to follow in the annual report	
U7	The annual report included a comprehensive glossary	
4. Comparability		
C1	The notes to changes in accounting policies explain the implications of the change	Willekens,(2008); Sajady et al., (2008) ; Beest , et al., (2009); FASB, (2013); Mamic Sacar & Oluic (2013); Samukri, (2015).
C2	The notes to revisions in accounting estimates and judgments explain the implications of the revision	
C3	The company's previous accounting period's figures are adjusted for the effect of the implementation of a change in accounting policy or revisions in accounting estimates	
C4	The results of current accounting period are compared with results in previous accounting periods	
C5	Information in the annual report is comparable to information provided by other organizations	
C6	The annual report presents financial index numbers and ratios.	

(2) The Business Performance

1. Non-financial performance

Items	Items Description	Sources
Nf1	Environmental performance	Tuanmat and Smith (2011), Antonio Pérez-Méndez, Santos. & Brito, (2012), Ángel Machado-Cabezas, (2015). Sandeep and Bedi, (2016)
Nf2	Success rate in launching new products, services or programs	
Nf3	Shareholders satisfaction	
Nf4	Employees satisfaction	
Nf5	Customer satisfaction	
Nf6	Level of innovation	
Nf7	Social performance	
Nf8	Business growth	
Nf9	Reputation in its sector	
Financial Performance		
F1	Economic value added (EVA)	Dozier and Chang, 2006; Benner and Veloso, (2008); Ittner and Larcker, (1997); Crabtree and DeBusk (2008) ;; Ejoh and Ejom (2014), Sandeep and Bedi, (2016)
F2	Return on equity (ROE)	
F3	Return on assets (ROA)	
F4	Return on investment (ROI)	
F5	Level of profitability (Gross Net margin)	
F6	Productivity of employees	
F7	Earnings per share growth	
F8	Earnings per share (EPS)	
F9	Net profit margin	

(3) SysTrust Principles

1. Availability		
A1	The system availability requirements of authorised users, and system availability objectives, policies, and standards, are identified and documented.	AICPA, (2013) Al Hanini,(2015); Greenberg, et al., 2012, Satio, T (2012)Bedard, et al., (2005); Najafi, A (2014)
A2	The entity's system availability are periodically reviewed and approved by an authorised people.	
A3	A formal process exists to identify and review contractual, legal, and other service-level agreements and applicable laws and regulations that could impact system availability objectives, policies, and standards.	
A4	There are procedures to ensure that personnel responsible for the design, development, implementation, and operation of system availability features are qualified to fulfill their responsibilities.	
A5	Management has assigned responsibilities for the maintenance and enforcement of the entity's availability policies to the CIO.	
A6	The entity's user training program includes modules dealing with the identification and reporting of system availability issues, security breaches, and other incidents.	
A7	Employees are trained to make substitute copies of the programs.	
A8	Employees are trained on special procedures concerning reducing the time of system's stop as possible.	
A9	There is formal communication of system availability objectives, policies, and standards to authorised users through means such as memos, meetings, and manuals.	
A10	The firm makes preventive maintenance to the computerised information system periodically and regularly.	
A11	The firm adopts policies and procedures for fast dealing with computerised accounting information system's mistakes to achieve a continuous availability to the system.	
A12	Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies	
A13	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, monitored, and maintained to meet availability commitments and requirements	

2. Security		
S1	The firm's security policies have approved and documented the security requirements of authorised users.	AICPA, (2013) Warren, M.J (2002); Zoeilf ,In`am Mohsin (2009); Abu-Musa, (2005); McKnight, D, et al., (2002), Wu, K, (2011); Satio, T (2012) .. Baldvinsdottir, et al.(2012), Steinbar, (2005); Maines, and Wahlen, (2006
S2	The entity's system security is periodically reviewed and compared with the defined system security policies	
S3	The firm has classified the data on the basis on its criticality and sensitivity and kept in the main devices.	
S4	The firm uses appropriate procedures to separate duties, tools and functions of the system's administration from net administration	
S5	A security awareness program has been implemented to communicate the entity's IT security policies to employees	
S6	Personnel receive training and development in system security concepts and issues.	
S7	Major computers are kept in closed place and the authorised people are allowed to access in to it.	
S8	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorised individuals by card key systems and monitored by video surveillance.	
S9	Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations.	
S10	Documented procedures exist for the identification and escalation of potential physical security breaches.	
S11	Firewall events are logged and reviewed daily by the security ad- Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers.	
S12	the firm uses physical selector as fingerprints or eyes' to access into data Firewalls are used and configured to prevent unauthorised access	
S13	The entity uses industry standard encryption technology, VPN software, or other secure communication systems (consistent with its periodic IT risk assessment) for the transmission of private or confidential information over public networks, including user IDs and passwords.	
S14	The firm takes suitable steps to protect the main devices by keeping them away from danger and in fire resistant places	
S15	Personal computers are programmed to be locked electronically after finishing work with a limited period.	
S16	The firm takes special control procedures prevent transferring the computers outside	
S17	Updating continuously the antivirus software used in the computerised systems.	
S18	Logical access security measures have been implemented to protect against unauthorised	
3. Integrity Processing		
Ig1	The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group	AICPA/CICA (2006); Greenberg, et al., (2012); McKnight, D, et al., (2002); Mauldin, B (2005); Satio, T (2012); Bashar, (2015); Boritz, J (2005).; Maines, & Wahlen (2006); Baldvinsdottir, et al., (2011)
Ig2	Firm's' administration develops procedures to make sure f the completion and accuracy of documents that represent sources of data.	
Ig3	There are special tests to make sure of the integration of input data to check data validity before processing	
Ig4	Fields' frequency and their capacity are reviewed and high and low limits are examined to check the reliability and accuracy of the inputs	
Ig5	Data is inserted by authorised people	
Ig6	Make sure of the computer's response to every item of the input	
Ig7	Computerised accounting information systems includes a pointer appeared as a message whenever something wrong happened in input process.	
Ig8	Make periodically the settlements' procedures between sub accounts computerised information systems.	
Ig9	Files of data are named with appropriate names.	

Ig10	All the system's outputs are revised in terms of logic and formation accuracy	
Ig11	The compatibility between inputs and outputs are reviewed daily	
Ig12	Computer's reports are distributed into the appropriate users	
Ig13	The sensitive outputs are protected from unauthorised access	
Ig14	Any mistake in the outputs is corrected when it is discovered.	
Ig15	There are control procedures for protecting information when they are transferred via nets as coding and checking of the transmission.	
Ig16	System output is complete, accurate, distributed, and retained in accordance with processing integrity commitments and requirements.	
Ig17	Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements	
4. Confidentiality		
C1	The entity's system confidentiality and related requirements are established and periodically reviewed and approved by a designated individual or group.	AICPA/CICA (2006); Greenberg, et al., (2012); McKnight, D, et al., (2002); Mauldin, B (2005); Satio, T (2012); Bashar, (2015); Boritz, J (2005).; Maines, & Wahlen (2006); Baldvinsdottir, et al., (2011).
C2	The system confidentiality and requirements are communicated to authorised users.	
C3	The entity publishes its confidentiality and related security policies on its corporate intranet.	
C4	The security administration team has custody of and is responsible for the day-to-day maintenance of the entity's confidentiality and related security policies and recommends changes to the CIO and the IT steering committee	
C5	The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorised users.	
C6	Error messages are revealed to authorize personnel.	
C7	Confidentiality processes exist to restrict the capability to input information to only authorised individuals.	
C8	Management has developed a reporting strategy that includes the sensitivity and confidentiality of data and appropriateness of user access to output data	
C9	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has been granted access.	
C10	.logical access controls are in place that limit access to confidential information based on job function and need.	
C11	Requests for access privileges to confidential data require the approval of the data owner. Business partners are subject to nondisclosure agreements or other contractual confidentiality provisions.	
C12	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorised parties in accordance with confidentiality commitments and requirements.	
5. Privacy		
P1	The entity defines documents, communicates, and assigns accountability for its privacy policies and procedures.	AICPA/CICA (2006) Greenberg, et al., (2012); Bashar, (2015); Boritz, J (2005).
P2	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed	
P3	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.	
P4	The entity collects personal information only for the purposes identified in the notice	
P5	The entity limits the use of personal information to the purposes	

	identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purpose	
P6	The entity provides individuals with access to their personal information for review and update.	
P7	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual	
P8	The entity protects personal information against unauthorised access (both physical and logical).	
P9	The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.	
P10	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes	

Appendix B

The Questionnaire

Dear Manager,

The main theme of this study is to explore the overall reliability of accounting information system using SysTrust's framework implementation and its influence on the business performance via a mediating role of financial reporting among shareholding companies in Jordan. The research aspires to obtain an overview of internal control system in Jordan, and believed it will be a valuable contribution to the available literature. Hereby, I am kindly asking for your assistance in completing this research by answering the attached questionnaire objectively, since your contribution is vital for this research accomplishment. Kindly note that the questionnaire will not take more than 15 minutes to complete, and all received information will be confidential and used solely for the research objectives.

It is not compulsory to participate in this study and you may choose to withdraw at any time even if prior consent has been given. Also you do not have to give reasons for withdrawal and there are no consequences attached to your decision if you withdraw.

Please, If you have any concerns or complaints regarding the ethical elements of this project, you can talk with me directly or at my telephone 0795595958. I highly appreciate your precious cooperation in advance.

Respectfully yours,

Ahamed Hani Al-Dmour

❖ **GENERAL INFORMATION**

1. What type of business are you currently in?

- Financial service (e.g. banks, real estate, insurance) Industrial
 Other service (non-financial service

2. How many employees are currently working at the organization?

- Less than 100 employees 100-199 employees 200-299 employees
 300-399 employees 400 and more

3. How long has your organization been in business (experience)?

- Less than 5 year's
 5 – 9 years
 10- 15 years
 More than 15 years

4. Your accounting system is.

- Manual, no computers are used.
 A combination of manual and computer processed.
 Completely computerised.

Part Two.

Please indicate to which extent the following requirements for the reliability of accounting information system have been achieved / implemented at your company.

Level practice

Not totally achieved/ practiced						Totally achieved/ practiced
1	2	3	4	5	6	7

Code	Availability. The system is available for operation and use as committed or agreed	Level of achievement					
A1	The system availability requirements of authorised users, and system availability objectives, policies, and standards, are identified and documented clearly.						
A2	The entity's system availability are periodically reviewed and approved by an authorised people.						
A3	A formal process exists to identify and review contractual, legal, and other service-level agreements and applicable laws and regulations that could impact system availability objectives, policies, and standards.						
A4	There are procedures to ensure that personnel responsible for the design, development, implementation, and operation of system availability features are qualified to fulfil their responsibilities.						
A5	Management has assigned responsibilities for the maintenance and enforcement of the entity's availability policies to the CIO.						
A6	The entity's user training program includes modules dealing with the identification and reporting of system availability issues, security breaches, and other incidents.						
A7	Employees are trained to make substitute copies of the programs.						
A8	Employees are trained on special procedures concerning reducing the time of system's stop as possible.						
A9	There is formal communication of system availability objectives, policies, and standards to authorised users through means such as memos, meetings, and manuals.						
A10	The firm makes preventive maintenance to the computerised information system periodically and regularly.						

A11	The firm adopts policies and procedures for fast dealing with computerised accounting information system's mistakes to achieve a continuous availability to the system.							
A12	Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies							
A13	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, monitored, and maintained to meet availability commitments and requirements							
	Security. The system is protected against unauthorised access (both physical and logical)							
S1	The firm's security policies has approved and documented the security requirements of authorised users.							
S2	The firm's system security is periodically reviewed and compared with the defined system security policies							
S3	The firm's has classified the data on the basis on its criticality and sensitivity and kept in the main devices.							
S4	The firm uses appropriate procedures to separate duties, tools and functions of the system's administration from net administration							
S5	A security awareness program has been implemented to communicate the entity's IT security policies to employees							
S6	Personnel receive training and development in system security concepts and issues.							
S7	Major computers are kept in closed place and the authorised people are allowed to access in to it.							
S8	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorised individuals by card key systems and monitored by video surveillance.							
S9	Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations.							

S10	Documented procedures exist for the identification and escalation of potential physical security breaches.							
S11	Firewall events are logged and reviewed daily by the security ad- Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers.							
S12	the firm uses physical selector as fingerprints or eyes' to access into data Firewalls are used and configured to prevent unauthorised access							
S13	The firm uses industry standard encryption technology, VPN software, or other secure communication systems (consistent with its periodic IT risk assessment) for the transmission of private or confidential information over public networks, including user IDs and passwords.							
S14	The firm takes suitable steps to protect the main devices by keeping them away from danger and in fire resistant places							
S15	Personal computers are programmed to be locked electronically after finishing work with a limited period of time.							
S16	The firm takes special control procedures prevent transferring the computers outside							
S17	Updating continuously the antivirus software used in the computerised systems.							
S18	Logical access security measures have been implemented to protect against unauthorised							
	Integrity Processing							
Ig1	The firm's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group							
Ig2	The firm's' administration develops procedures to make sure f the completion and accuracy of documents that represent sources of data.							
Ig3	There are special tests to make sure of the integration of input data to check data validity before processing							
Ig4	Fields' frequency and their capacity are reviewed and high and low limits are examined to check the reliability and accuracy of the inputs							
Ig5	Data is inserted by authorised people							

Ig6	Make sure of the computer's response to every item of the input							
Ig7	Computerised accounting information systems includes a pointer appeared as a message whenever something wrong happened in input process.							
Ig8	Make periodically the settlements' procedures between sub accounts computerised information systems.							
Ig9	Files of data are named with appropriate names.							
Ig10	All the system's outputs are revised in terms of logic and formation accuracy							
Ig11	The compatibility between inputs and outputs are reviewed daily							
Ig12	Computer's reports are distributed into the appropriate users							
Ig13	The sensitive outputs are protected from unauthorised access							
Ig14	Any mistake in the outputs is corrected when it is discovered.							
Ig15	There are control procedures for protecting information when they are transferred via nets as coding and checking of the transmission.							
Ig16	System output is complete, accurate, distributed, and retained in accordance with processing integrity commitments and requirements.							
Ig17	Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements							
	Confidentiality							
C1	The firm's system confidentiality and related requirements are established and periodically reviewed and approved by a designated individual or group.							
C2	The system confidentiality and requirements are communicated to authorised users.							
C3	The firm publishes its confidentiality and related security policies on its corporate intranet.							
C4	The security administration team has custody of and is responsible for the day-to-day maintenance of the entity's confidentiality and related security policies and recommends changes to the CIO and the IT steering committee							
C5	The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorised users.							

C6	Error messages are revealed to authorize personnel.							
C7	Confidentiality processes exist to restrict the capability to input information to only authorised individuals.							
C8	Management has developed a reporting strategy that includes the sensitivity and confidentiality of data and appropriateness of user access to output data							
C9	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has been granted access.							
C10	Logical access controls are in place that limit access to confidential information based on job function							
C11	Requests for access privileges to confidential data require the approval of the data owner. Business partners are subject to nondisclosure agreements or other contractual confidentiality provisions.							
C12	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorised parties in accordance with confidentiality commitments and requirements.							
	Privacy							
P1	The firm defines documents, communicates, and assigns accountability for its privacy policies and procedures.							
P2	The firm provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed							
P3	The firm describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.							
P4	The firm collects personal information only for the purposes identified in the notice							
P5	The firm limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains							

	personal information for only as long as necessary to fulfill the purpose							
P6	The firm provides individuals with access to their personal information for review and update.							
P7	The firm discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual							
P8	The firm protects personal information against unauthorised access (both physical and logical).							
P9	The firm maintains accurate, complete, and relevant personal information for the purposes identified in the notice.							
P10	The firm monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes							

Part Three. Quality Financial Reporting

How far do you agree with the following statements concerning the qualitative characteristics of the quality of financial reporting at your company?

Level of Agreement

completely disagree	substantially disagree	disagree somewhat	indifference	agree somewhat	substantially agree	completely agree
1	2	3	4	5	6	7

1.	Relevance						
R1	The annual reports discloses forward-looking information help forming expectations and predictions concerning the future of the company						
R2	The annual reports discloses information in terms of business opportunities and risks complement the financial information						
R3	The company uses fair value instead of historical cost.						
R4	Information helps you confirm profitability levels of the business						
R5	Financial reports are presented annually as required by regulatory bodies of accounting						
R6	No undue delays in the presentation of financial reports.						
R7	The annual report provides feedback information on how various market events and significant transactions affected the company						

2.	Faithful representation							
F1	The annual report explains the assumptions and estimates made clearly; valid arguments provided to support the decision for certain assumptions and estimates in the annual report							
F2	The annual report explains the choice of accounting principles clearly							
F3	The annual report highlights the positive and negative events in a balanced way when discussing the annual results							
F4	The annual report includes an unqualified auditor's report							
F5	The annual report extensively discloses information on corporate governance issues							
3.	Understand ability							
U1	The annual report presented in a well-organised manner							
U2	The notes to the balance sheet and the income statement are sufficiently clear							
U3	Sources and level of expenditure can easily be understood							
U4	Business assets are easy to know in terms of value and nature							
U5	the presence of graphs and tables clarifies the presented information							
U6	The use of language and technical jargon is easy to follow in the annual report							
U7	The annual report included a comprehensive glossary							
4.	Comparability							
C1	The notes to changes in accounting policies explain the implications of the change							
C2	The notes to revisions in accounting estimates and judgments explain the implications of the revision							
C3	The company's previous accounting period's figures are adjusted for the effect of the implementation of a change in accounting policy or revisions in accounting estimates							
C4	The results of current accounting period are compared with results in previous accounting periods							

C5	Information in the annual report is comparable to information provided by other organizations							
C6	The annual report presents financial index numbers and ratios.							
5.	Timeliness							
T1	Natural logarithm of amount of days it took for the auditor signed the auditors' report after book-year end.							

Part Four. Business Performance

Now, we would like to ask for your perception of the performance of the organizational unit. In your opinion, how would you compare your organization's performance over the 12 months to that of other organizations doing the same kind of work for each of the following dimensions? (*Check only one for each dimension*).

Level of comparison

Much Worse blow	Worse	Slightly Worse	indifferences	Slightly Better	Better	Much Better/above
1	2	3	4	5	6	7

	Business Performance	1	2	3	4	5	6	7
	1. Non –financial performance							
Nf1	Environmental performance							
Nf2	Success rate in launching new products, services or programs							
Nf3	Shareholders satisfaction							
Nf4	Employees satisfaction							
Nf5	Customer satisfaction							
Nf6	Level of innovation/ investment							
Nf7	Social performance							
Nf8	Business growth							
Nf9	Reputation in its sector							
	2. Financial Performance							
F1	Economic value added (EVA)							
F2	Return on equity (ROE)							
F3	Return on assets (ROA)							
F4	Return on investment (ROI)							
F5	Level of profitability (Gross Net margin)							
F6	Productivity of employees							
F7	Earnings per share growth							
F8	Earnings per share (EPS)							
F9	Net profit margin							
F10	working capital ratio							

The Questionnaire Translation

بسم الله الرحمن الرحيم

السيد المدير العام المحترم.

تحية طيبة وبعد ،،،

يسرني اعلامكم بانني طالب دكتوراة في جامعة (BRUNEL) في المملكة المتحدة في تخصص نظم المعلومات المحاسبية و أن موضوع اطروحتي يتناول (دراسة موثوقية نظام المعلومات المحاسبية واثره على جودة التقارير المالية واداء الشركات الاردنية) ويؤمل أن يشكل هذا البحث مساهمة قيمة في الادبيات المتوافرة حول نظم المعلومات المحاسبية.

ونظراً لأن مساهمتكم امر حيوي في نجاح هذا البحث ، ارجو التكرم بالايعاز لادارة قسم المحاسبية في تعبئة الاستبيان المرفق الذي لن يستغرق اكثر من 15 دقيقة، كما انني اؤكد لكم أن جميع المعلومات الواردة فيه ستعامل بسرية ، وتستخدم للغايات البحثية حصراً.

كما انني اؤكد لكم بانك لست مضطرا للمشاركة في هذه الدراسة ، وقد تختار الانسحاب في اي وقت دون بيان أسباب الانسحاب وليس هناك عواقب تعلق على قرارك إذا انسحبت. وإذا كان لديك أي مخاوف أو شكاوى بخصوص العناصر الأخلاقية لهذا المشروع ، يرجى التحدث معي مباشرة.

أشكر لكم تعاونكم المثمر ، وجهدكم الطيب اللذين هما موضع التقدير والاعتزاز

مع و ارد الود والاحترام ،،،

احمد هاني الضمور

وفي حال اردتم المزيد من الاستفسار يرجى التواصل على:

(الايمل : eepgaaag@brunel.ac.uk رقم الهاتف 0795595958)

في حال اردتم الاطلاع على نتائج البحث الرجاء وضع اشارة (√) في المربع:

أر في الاطلاع على نتائج البحث.

❖ معلومات عامة

1. ما هو مجال / طبيعة العمل الذي تقوم به المؤسسة حالياً؟
 - خدمات مالية
 - الصناعة
 - خدمات أخرى غير مالية (حدد...)
2. كم عدد العاملين حالياً في المؤسسة؟
 - أقل من 100
 - 100-199
 - 200-299
 - 300-399
 - 400 وأكثر
3. كم مضى على وجود المؤسسة في مجال العمل (عدد سنوات الخبرة)؟
 - أقل من 5 سنوات
 - 5-9 سنوات
 - 10-15 سنة
 - أكثر من 15 سنة
4. هل نظام المحاسبة لديكم:
 - يدوي، لا توجد حواسيب
 - مزيج بين العمل يدوياً واستخدام مستخدمة الحواسيب
 - محوسب بشكل كامل

الجزء الثاني

يرجى ذكر إلى أي مدى تم تحقيق/ تنفيذ/ تطبيق المتطلبات التالية لموثوقية النظام المحاسبي في مؤسستكم
مستوى التطبيق

لم يتم تحقيقه/ تنفيذه بشكل كامل	1	2	3	4	5	6	تم تحقيقه/ تنفيذه بشكل كامل
							7

الرمز	التوافر (الجاهزية) : النظام متوفر للعمل والاستخدام على النحو الملتمزم به والمتفق عليه	مستوى الإنجاز
A1	متطلبات جاهزية النظام المحاسبي للمستخدمين المخول لهم، وأهداف وسياسات ومعايير جاهزية النظام محددة وموثقة	
A2	نقوم بشكل دوري مراجعة جاهزية النظام في المنشأة وإقراره من جانب أشخاص مفوضين لهذه الغاية.	
A3	يوجد لدينا إجراءات رسمية مطبقة لتحديد ومراجعة الاتفاقيات التعاقدية والقانونية وغيرها من الاتفاقيات والقوانين واللوائح المعمول بها على مستوى الخدمة، والتي يمكن أن تؤثر على الأهداف والسياسات والمعايير المتعلقة بجاهزية النظام.	
A4	يوجد لدينا إجراءات مطبقة لضمان أن يكون الموظفين المسؤولين عن تصميم وتطوير وتنفيذ وتشغيل المزايا المرتبطة بجاهزية النظام مؤهلين للوفاء بمسؤولياتهم	
A5	تقوم الإدارة بتفويض المسؤوليات للمدير التنفيذي للحفاظ على سياسات جاهزية النظام وتطبيقها.	

							يتضمن برنامج تدريب المستخدمين في المنشأة وحدات تدريبية تتعلق بآليات تحديد وإعداد التقارير المرتبطة بمسائل توافر النظام والاختراقات الأمنية وغير ذلك من الحوادث.	A6
							يتم تدريب الموظفين على إعداد نسخ بديلة للبرامج الحاسوبية	A7
							يتم تدريب الموظفين على إجراء خاص يتعلق بتقليل مدة تعطل البرنامج بقدر الإمكان.	A8
							هناك تواصل رسمي مع المستخدمين المخولين بشأن أهداف وسياسات ومعايير توافر النظام عبر المذكرات الداخلية والاجتماعات والكتيبات.	A9
							تقوم المؤسسة بالصيانة الوقائية لنظام المعلومات المحوسب على أساس دوري ومنتظم	A10
							تتبنى المؤسسة سياسات وإجراءات وانظمة للتعامل السريع مع الأخطاء والمخاطر المحتملة المرتبطة بنظام المعلومات المحاسبية المحوسب لتحقيق الجاهزية المستمرة للنظام.	A11
							هناك إجراءات مطبقة للنسخ الاحتياطي والتخزين خارج الموقع والاستعادة والتعافي من الكوارث بما يتفق مع السياسات المعمول بها في المؤسسة لتوافر النظام وغير ذلك من السياسات الأمنية ذات الصلة.	A12
							تم تصميم وتنفيذ وتشغيل ومراقبة ادوات الحماية البيئية والبرمجيات وعمليات النسخ الاحتياطي للبيانات والبنية التحتية اللازمة لاسردها بطريقة تضمن تلبية التزامات ومتطلبات جاهزية النظام	A13
الأمن: النظام محمي ضد الوصول (المادي والمنطقي على حد سواء) غير المصرح به.								
							تقر وتوثق السياسات الأمنية للمؤسسة المتطلبات الأمنية للمستخدمين المخولين.	S1
							تتم مراجعة أمن النظام للمؤسسة بشكل دوري ومقارنته بالسياسات الأمنية المعمول بها.	S2
							تقوم المؤسسة بتصنيف البيانات على أساس أهميتها وحساسيتها وحفظها في الأجهزة الرئيسية	S3
							تستخدم المؤسسة الإجراءات المناسبة لفصل المهام والأدوات والوظائف بين إدارة النظام وإدارة الشبكة.	S4
							تقوم المؤسسة بنفيذ برنامج للتوعية الأمنية لإيصال سياساتها الأمنية لـ في مجال تكنولوجيا المعلومات للموظفين	S5
							يتلقى العاملين التدريب ويخضعون للتطوير في مجال مفاهيم ومسائل أمن الحواسي الشخصية	S6
							يتم الاحتفاظ بأجهزة الحاسوب الرئيسية في مكان مغلق ويسمح للمخولين فقط بالوصول إليها.	S7
							الوصول المادي إلى الغرف الحاسوبية التي تحوي موارد تكنولوجيا المعلومات للمؤسسة والخوادم الحاسوبية، والأجهزة ذات الصلة مثل جدران الحماية والموجهات مقتصر فقط على الأشخاص المخولين من خلال أنظمة تعمل بالبطاقة وتخضع للمراقبة بكاميرات الفيديو	S8
							طلبات الحصول على امتيازات الوصول المادي للمرافق الحاسوبية في المؤسسة تستدعي موافقة مدير العمليات الحاسوبية.	S9
							هناك إجراءات موثقة لتحديد وتدرج الخروقات الأمنية المادية المحتملة.	S10
							يتم تسجيل الأحداث المتعلقة بجدران الحماية ومراجعتها يوميا من جانب الجهة المسؤولة عن أمن النظام، وتعطيل خدمات	S11

						الشبكة غير الضرورية (مثل telnet, ftp, http) على خوادم المؤسسة.	
						تستخدم المؤسسة محدد مادي كبصمة الأصبع أو العين للوصول إلى البيانات. ويتم استخدام جدران الحماية وتكوينها لمنع الوصول غير المصرح به.	S12
						تستخدم المؤسسة تكنولوجيا التشفير أو برمجيات الشبكة الخاصة الافتراضية أو غير ذلك من أنظمة الاتصالات الآمنة الأخرى وفقاً للمعايير الصناعية (وبما يتفق مع تقييمها الدوري لمخاطر تكنولوجيا المعلومات) لنقل معلومات خاصة أو سرية عبر الشبكات العامة، بما في ذلك معرفات وكلمات المرور للمستخدمين.	S13
						تتخذ المؤسسة خطوات مناسبة لحماية الأجهزة الرئيسية من خلال حفظها بعيداً عن الخطر وفي أماكن مقاومة للحريق.	S14
						تستخدم المؤسسة محدد مادي كبصمة الأصبع أو العين للوصول إلى البيانات ويتم استخدام جدران الحماية وتكوينها لمنع الوصول غير المصرح به	S15
						تتخذ المؤسسة إجراءات رقابية خاصة لمنع نقل أجهزة الحاسوب إلى الخارج.	S16
						هناك تحديث مستمر لبرامج الحماية من الفيروسات المستخدمة في النظم المحوسبة.	S17
						تم تنفيذ تدابير أمنية للوصول المنطقي بهدف منع أي وصول غير مصرح به.	S18
سلامة العمليات							
						سياسات سلامة العمليات والسياسات الأمنية ذات الصلة مطبقة في المؤسسة وتتم مراجعتها بشكل دوري والموافقة عليها من جانب المخولين سواء أكانوا أفراداً أو مجموعة.	Ig1
						تطور إدارة المؤسسة إجراءات للتأكد من اكتمال ودقة الوثائق التي تمثل مصادر البيانات.	Ig2
						يتم استخدام اختبارات خاصة للتأكد من سلامة البيانات المدخلة للتأكد من صحة البيانات قبل معالجتها	Ig3
						تتم مراجعة تردد المجالات وقدرتها، وفحص الحدود العالية والمنخفضة للتحقق من موثوقية ودقة المدخلات.	Ig4
						يتم إدخال البيانات من جانب أشخاص مخولين للقيام بذلك.	Ig5
						يتم التأكد من استجابة جهاز الحاسوب لكل بند من بنود المدخلات.	Ig6
						تتضمن نظم المعلومات الحاسوبية المحوسبة مؤشر يظهر كرسالة كلما حدث خطأ ما في عملية الإدخال.	Ig7
						إجراءات التسوية بين الحسابات الفرعية محوسبة بشكل دوري.	Ig8
						تتم تسمية ملفات البيانات بأسماء مناسبة.	Ig9
						تتم مراجعة كافة مخرجات النظام من حيث المنطقية ودقة التشكيل.	Ig10
						يتم مراجعة التطابق بين المخرجات والمخرجات على أساس يومي.	Ig11
						يتم توزيع التقارير الحاسوبية على المستخدمين المناسبين	Ig12
						يتم قياس وتسجيل مدخلات النظام بشكل تام ودقيق وبالوقت المناسب وفقاً لمتطلبات والتزامات سلامة العمليات.	Ig13
						المخرجات الحساسة محمية من الوصول غير المصرح به.	Ig14
						تتم معالجة أي خطأ في المخرجات عند اكتشافه.	Ig15
						مخرجات النظام كاملة ودقيقة ويتم توزيعها والاحتفاظ بها وفقاً لمتطلبات والتزامات سلامة العمليات.	Ig16

							هناك إجراءات رقابية لحماية المعلومات عند نقلها عبر الشبكات مثل الترميز وفحص عملية الإرسال.	Ig17
							السرية	
							السرية والمتطلبات ذات الصلة بنظام المؤسسة مطبقة وتتم مراجعتها بشكل دوري والموافقة عليها من جانب المخولين سواء أكانوا أفراداً أو مجموعة.	C1
							يتم إيصال المسائل المتعلقة بالسرية والمتطلبات ذات الصلة بالنظام للمستخدمين المخولين.	C2
							تقوم المؤسسة بنشر السياسات المتعلقة بالسرية وغير ذلك من السياسات الأمنية ذات الصلة على موقعها الإلكتروني الداخلي.	C3
							يتحمل فريق الإدارة الأمنية مسؤولية المحافظة اليومية على سياسات السرية للمؤسسة وما يرتبط بها من السياسات الأمنية ذات العلاقة، كما يوصي بالتغييرات المقترحة للمدير التنفيذي واللجنة التوجيهية لتكنولوجيا المعلومات	C4
							يتم تبليغ الأفراد المخولين بالإجراءات المتبعة في إعلام المؤسسة بشأن خروقات السرية وأمن النظام وألية تقديم الشكاوى.	C5
							يتم كشف الرسائل المتعلقة بالأخطاء للأفراد المخولين	C6
							هناك عمليات مطبقة للسرية لتقييد القدرة على إدخال المعلومات بالأفراد المخولين فقط.	C7
							وضعت الإدارة استراتيجيات للتقارير تشمل حساسية وسرية البيانات ومدى ملاءمة وصول المستخدم إلى مخرجات البيانات.	C8
							الموظفين مطالبين بالتوقيع على اتفاق السرية كجزء روتيني من توظيفهم. ويحظر هذا الاتفاق الكشف عن أي معلومات أو بيانات أخرى يتم منح الموظف حق الوصول إليها.	C9
							ضوابط الوصول المنطقية مطبقة بحيث يقتصر الوصول إلى المعلومات السرية بناء على المهام الوظيفية ومدى الحاجة لها.	C10
							تستدعي طلبات منح امتيازات الوصول إلى البيانات السرية موافقة صاحب البيانات. ويخضع شركاء الأعمال لاتفاقيات عدم الإفشاء أو غيرها من أحكام السرية التعاقدية.	C11
							الوصول من خارج حدود النظام إلى المعلومات السرية والكشف عنها يقتصر على الجهات المخولة وفقاً للالتزامات والمتطلبات المتعلقة بالسرية.	C12
							الخصوصية:	
							تحدد وتوثق وتبلغ المؤسسة سياساتها وإجراءاتها المتعلقة بالخصوصية وتعين الجهات المسؤولة عنها	P1
							توفر المؤسسة إشعارات حول سياساتها وإجراءاتها المتعلقة بالخصوصية وتحدد الأغراض التي يتم من أجلها جمع المعلومات الشخصية واستخدامها والاحتفاظ بها والكشف عنها.	P2
							تصف المؤسسة الخيارات المتاحة للفرد وتحصل على موافقة صريحة أو ضمنية بشأن جمع المعلومات الشخصية واستخدامها والكشف عنها.	P3
							تجمع المؤسسة البيانات الشخصية للأغراض المحددة في الإشعار فقط.	P4
							يقتصر استخدام المؤسسة للمعلومات الشخصية على الأغراض المحددة في الإشعار والتي لأجلها منح الفرد موافقته الصريحة أو الضمنية. وتحفظ المؤسسة بالمعلومات الشخصية فقط طالما كان ذلك ضرورياً لتحقيق الهدف المعلن.	P5

									P6	تتيح المؤسسة للأفراد فرصة الوصول إلى بياناتهم الشخصية لمراجعتها وتحديثها.
									P7	تفصح المنشأة عن المعلومات الشخصية لأطراف ثالثة فقط للأغراض المحددة في الإشعار وبموافقة ضمنية أو صريحة من الفرد.
									P8	تحمي المؤسسة المعلومات الشخصية من الوصول (المادي والمنطقي على حد سواء) غير المصرح به.
									P9	تحتفظ المؤسسة بمعلومات شخصية دقيقة وكاملة وذات صلة بالأغراض المحددة في الإشعار.
									P10	تراقب المؤسسة مدى الامتثال لسياسات وإجراءات الخصوصية، ولديها إجراءات لمعالجة الشكاوى والمنازعات المتعلقة بالخصوصية.

الجزء الثاني: جودة التقارير المالية

إلى أي مدى تتفق مع العبارات التالية بشأن خصائص جودة التقارير المالية في مؤسستك؟

لا أتفق بشدة	لا أتفق إلى درجة كبيرة	لا أتفق إلى حد ما	متحايد	أوافق إلى حد ما	أوافق إلى درجة كبيرة	أوافق بشدة
1	2	3	4	5	6	7

العلاقة						
						R1
						R2
						R3
						R4
						R5
						R6
						R7
التمثيل الصادق						
						F1
						F2
						F3
						F4

							بدون تحفظ.	
							يكشف التقرير السنوي معلومات على نطاق واسع حول مسائل الحوكمة في المؤسسة.	F5
							قابلية الفهم	
							التقرير السنوي مقدم بطريقة على درجة عالية من التنظيم	U1
							الملاحظات على الحساب الختامي وبيان الدخل واضحة بما فيه الكفاية.	U2
							يمكن فهم مصادر ومستوى الإنفاق بسهولة.	U3
							يمكن معرفة الأصول التجارية بسهولة من حيث قيمتها وطبيعتها	U4
							يوضح وجود الرسوم البيانية والجداول المعلومات المقدمة	U5
							اللغة والمصطلحات التقنية المستخدمة شاملة في التقرير السنوي يسهل فهمها	U6
							قابلية المقارنة	
							تشرح الملاحظات على التغييرات في السياسات المحاسبية الآثار المترتبة على التغيير	C1
							تشرح الملاحظات على مراجعات التقديرات والأحكام المحاسبية الآثار المترتبة على المراجعة	C2
							يتم تعديل أرقام الفترة المحاسبية السابقة للشركة للتأثير على تنفيذ تغيير في السياسة المحاسبية أو مراجعات التقديرات المحاسبية	C3
							تتم مقارنة نتائج الفترة المحاسبية الحالية مع نتائج الفترات المحاسبية السابقة	C4
							المعلومات الواردة في التقرير السنوي قابلة للمقارنة مع المعلومات التي تقدمها المنظمات الأخرى	C5
							يعرض التقرير السنوي الأرقام والنسب القياسية المالية.	C6
							التوقيت	
							تعرض البيانات المالية الختامية في الوقت المحدد بعد الاغلاق الختامي للقيود (اي اللوغار يتم الطبيعي لعدد الأيام التي يستغرقها المدقق لتوقيع تقرير مدقق الحسابات بعد الاغلاق الختامي للقيود يعد مقبولاً).	T1

الجزء الثالث: أداء الأعمال

والآن، نود أن نسأل عن تصورك الخاص لأداء الوحدة التنظيمية. برأيك، كيف يمكن مقارنة أداء مؤسستك المالي وغير المالي على مدى 12 شهرا بالمنظمات الأخرى التي تؤدي نفس النوع من العمل لكل من الأبعاد التالية؟ (اختر واحدة فقط لكل بعد من الأبعاد):

مستوى المقارنة

أسوأ بكثير / وأقل من ذلك	أسوأ	أسوأ بشكل طفيف	لا يوجد اختلاف	أفضل بشكل طفيف	أفضل	أفضل بكثير / وأعلى من ذلك
1	2	3	4	5	6	7

أداء الأعمال							
1. الأداء غير المالي							
							Nf1
							الاداء البيئي
							Nf2
							نسبة النجاح في إطلاق منتجات أو خدمات أو برامج جديدة
							Nf3
							رضى المساهمين
							Nf4
							رضى الموظفين
							Nf5
							رضى العملاء
							Nf6
							مستوى الابداع/ الاستثمار في الابداع والابتكار
							Nf7
							الاداء الاجتماعي
							Nf8
							مستوى النمو في اعمال المؤسسة (ازدهار الاعمال)
							Nf9
							مستوى السمعة / الشهرة في القطاع
2. الأداء المالي							
							F1
							القيمة الاقتصادية المضافة
							F2
							العائد على حقوق المساهمين
							F3
							العائد على الأصول
							F4
							العائد على الاستثمار
							F5
							مستوى الربحية (هامش الربح الصاف)
							F6
							انتاجية الموظفين (معدل ايراد العامل الواحد)
							F7
							نمو الارباح
							F8
							ربحية السهم الواحد
							F9
							صاف الربح
							F10
							نسبة رأس المال العامل

Appendix C



College of Engineering, Design and Physical Sciences Research Ethics Committee
Brunel University London
Kingston Lane
Uxbridge UB8 3PH
United Kingdom www.brunel.ac.uk

30 January 2017

LETTER OF CONDITIONAL APPROVAL

Applicant. Mr Ahamed Al-Dmour

Project Title. Assessing the Reliability of Internal Control System in Accounting Information Process and its influences on Financial Quality Reporting and the Business Performance. An integrated model

Reference. 4762-LR-Jan/2017- 5488-3

Dear Mr Ahamed Al-Dmour

The Research Ethics Committee has considered the above application recently submitted by you.

The Chair, acting under delegated authority has agreed that there is no objection on ethical grounds to the proposed study. Approval is given on the understanding that the conditions of approval set out below are followed.

- The agreed protocol must be followed. Any changes to the protocol will require prior approval from the Committee by way of an application for an amendment.
- All data should be kept in a secure networked location on Brunel's server preferably the computing storage space provided to you by the University.

Please note that.

- Research Participant Information Sheets and (where relevant) flyers, posters, and consent forms should include a clear statement that research ethics approval has been obtained from the relevant Research Ethics Committee.
- The Research Participant Information Sheets should include a clear statement that queries should be directed, in the first instance, to the Supervisor (where relevant), or the researcher. Complaints, on the other hand, should be directed, in the first instance, to the Chair of the relevant Research Ethics Committee.
- Approval to proceed with the study is granted subject to receipt by the Committee of satisfactory responses to any conditions that may appear above, in addition to any subsequent changes to the protocol.
- The Research Ethics Committee reserves the right to sample and review documentation, including raw data, relevant to the study.
- **[delete for staff applications]** You may not undertake any research activity if you are not a registered student of Brunel University or if you cease to become registered, including abeyance or temporary withdrawal. As a deregistered student you would not be insured to undertake research activity. Research activity includes the recruitment of participants, undertaking consent procedures and collection of data. Breach of this requirement constitutes research misconduct and is a disciplinary offence.

A handwritten signature in black ink, appearing to read 'Hua Zhao'.

Professor Hua Zhao

Chair

College of Engineering, Design and Physical Sciences Research Ethics Committee Brunel University London



Date : 22/1/2017 التاريخ :

Ref.No: 13/2/145 الرقم :

To Whom It May Concern

Ref: Support Letter.

This is to confirm that **Amman Chamber of Industry** highly appreciates your support to the Ph.D. Student; **Ahamed Hani Al-Dmour** in his research project entitled "Assessing the Reliability of Internal Control System in Accounting Information Process and its influences on Financial Quality Reporting and the Business Performance: An integrated model" . Please facilitate his mission and provide him with the information that he needs to accomplish his project as he confirms that any obtained information will be confidential and will not be used beyond the project research objectives.



Dr. Nael Al Husami
CEO

Amman Chamber of Industry