

**A FRAMEWORK FOR INCLUDING SUSTAINABILITY IN
INFORMATION SYSTEM AUDIT**

ALIFAH AIDA LOPE ABDUL RAHMAN

**A thesis submitted in partial fulfilment of the requirements of the University of East
London for the degree of Doctor of Philosophy**

August 2016

ACKNOWLEDGEMENTS

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

It is usual to thank the people who have supported and encouraged you in the whole process of producing a research report of this kind. I therefore owe an enormous debt of gratitude to supervisors, family and friends for the constant motivation and inspiration to get started and to complete this thesis.

From an academic point of view, I wish to thank Dr. Ameer Al-Nemrat my Director of Studies for his unrelenting support, encouragement, constant monitoring and constructive comments on the preparation of this thesis. Also, I wish to thank Dr. Shareeful Islam for his support, advice, and always takes time to evaluate the different pieces of work, provide analytical insight and, give constructive criticism promptly. The contribution from both supervisors will be a long-term asset in enriching my critical thinking process.

Also, I wish to extend my sincere gratitude and appreciation to my beloved husband, Nizam for his encouragement throughout the whole venture and had taking great sacrifices physically and mentally to see the completion of my PhD. I would also like to thank my mother, Bonda Zaleha who had prayed fervently to see the successful completion of my PhD. I would like to dedicate my dissertation to them. My PhD friends and colleague at Research Centre who had been with me throughout these years.

Also a million thank are due to the IS auditors from the National Audit Department and State Audit Institution, who in spite of their busy work schedules was kind enough to participate in the progress of this research.

Copyright

I maintain that the work in this thesis was conducted in conformance with the guidelines of the University of East London and is novel except those specified by detailed reference. The thesis has not been made available to any other educational organisation.

Signed.....

Date.....

ABSTRACT

The information systems (IS) audit in public sector organisations is generally conducted to provide assurance about the effectiveness of IS controls, processes, resources, operations, and value for money in the IS investment. Public sector organisations are being confronted with various new demands from businesses, the public and other stakeholders because of the high level of IS investment, which takes long to complete and involves uncertainty of performance. This research argues that the current IS audit practice does not take a broad enough view in assessing the overall system. Hence, it is particularly challenging for an IS auditor not only to identify how well the IS supports the overall business objectives, but also to justify the continuity of IS operation and to produce an effective IS audit report. There have been several cases in which IS were unsuccessful and did not perform as the users expected. Due to the current IS audit practice, IS auditors are unable to recognise any inherent limitations that may exist in the design, development and implementation of application systems that will impact on the organisation's objectives and operational activities. Sustainability is a relevant and practical way to deal with limitations found in IS audit practice. Sustainability is future oriented and concerned with holistic and integrated systems consisting of humans, nature, social and technology infrastructure.

This research is conducted with the goal of incorporating sustainability within the IS audit framework as a strategy to minimise IS control risk, to reduce inherent risks faced by the IS auditors and to produce effective IS audit reports. This research found that the proposed framework known as the Sustainability Driven Information System Audit (SISA) is an appropriate alternative that can overcome these shortcomings, and effectively address risks associated with IS controls. SISA is also considered to reduce uncertainties in decision making by reviewing results, processes and input. It facilitates coordination and communication to produce an audit report that provides effective value to the key stakeholders and the public. This research also studies the appropriate method for IS auditors to make audit judgements, particularly in measuring IS controls. The applicability of the SISA framework to a real case study has been found to be very promising. The result showed that a systematic and numerical approach is suitable for prioritising audit criteria and in order to emphasise the key areas of concern for the audit purpose. The results indicate that the sustainability approach is a practical and reasonable method that can be employed at any public sector organisation. This research contributes theoretically, methodologically and practically to the IS audit body of knowledge.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	i
ABSTRACT	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	vii
LIST OF FIGURES	ix
LIST OF PUBLICATIONS BY THE AUTHOR	x
ABBREVIATIONS	xi
CHAPTER 1	1
1. Introduction	1
1.1 Background and motivation.....	2
1.2 The Problem Statement	3
1.3 Research aim and objectives	5
1.4 Research questions	5
1.5 Research contributions	6
1.6 The approach	7
1.7 Empirical evaluation.....	9
1.8 Thesis structure	9
CHAPTER 2	12
Literature review.....	12
2.1 Basic concepts.....	12
2.2 The regulatory requirements of the IS audit	16
2.3 Challenges to IS audit.....	18
2.4 Sustainability.....	19
2.4.1 Economic dimension.....	23
2.4.2 Environmental dimension	23
2.4.3 Social dimension	24
2.4.4 Technological dimension	24
2.5 Sustainability measurement	24
2.6 The need for sustainability assessment in IS audit	26
2.6.1 The need to increase accountability and transparency.....	26
2.6.2 The need to provide sustainability reporting in public sector organisation.....	27
2.6.3 The need to highlight risk in relation to sustainability dimensions.....	27

2.7 The Demspster Shafer Theory (D-S theory) of Evidence	28
2.7.1 Dempster’s Rule of Evidence Combination.....	30
2.8 Risk assessment	31
2.9 Overview on the INTOSAI Development Initiative (IDI).....	32
2.10 Population frame	33
2.11 Summary	34
CHAPTER 3.....	35
Research Methodology	35
3.1 Research paradigm	35
3.2 Research methods.....	37
3.2.1 Qualitative and quantitative research methods	37
3.2.2 Case study	38
3.2.3 Analysing data.....	40
3.3 Research design	40
3.4 Summary	44
CHAPTER 4.....	45
The Sustainability driven IS audit framework (SISA).....	45
4.1 SISA framework requirements	45
4.2 The SISA Framework	46
4.2.1 Conceptual view of SISA.....	46
4.2.2 Audit process in SISA.....	50
4.3 Generate IS audit report	64
4.4 Execute and reporting follow-up	66
4.5 Summary	66
CHAPTER 5.....	67
Evaluation	67
5.2 Empirical investigation and data collection	67
5.2.2 Study constructs.....	68
5.2.3 Validity of study results.....	69
5.3 Preliminary Survey	70
5.3.1 Data collection	70
5.3.2 Survey context	71
5.3.3 Survey results.....	72
5.3.4 Interview results	75
5.3.5 Survey conclusions.....	77
5.4 Empirical investigation.....	79

5.4.1 Case study 1 Investigation SISA in the NAD	79
5.4.2 Case study 2: Viability of cloud migration by using SISA	89
5.4.3 Case Study 3 Investigation SISA in the SAI	98
5.5 Summary	104
CHAPTER 6.....	105
Discussion.....	105
6.1 RQ1 How is the sustainability dimension incorporated into the IS audit process?.....	105
6.1.1 Phase 1 Audit plan	105
6.1.2 Phase 2 Audit execution	113
6.1.3 Phase 3 Audit report	117
6.2 RQ2 Could SISA be implemented in different types of organisations?	119
6.2.1 Defining the context	119
6.2.2 Defining the criteria, sub-criteria and indicators using SISA for the case studies	120
6.3 RQ3 To which extent does the SISA framework affect the IS audit process?.....	121
6.3.1 Issues related to SISA process.....	122
6.3.2 Analysis on output	122
6.4 RQ4 What are the challenges faced by the IS auditor when adopting a sustainability driven IS audit framework?.....	123
6.5 Summary	123
CHAPTER 7.....	124
Conclusions and recommendations.....	124
7.1 The fulfilment of the research objectives.....	124
7.2 Contribution to the body of knowledge	126
7.2.1 Theoretical contributions.....	126
7.2.2 Contribution to the real audit practice	126
7.3 Limitations and difficulties of the study.....	127
7.4 Further research.....	128
7.5 Summary	128
APPENDIX A	130
APPENDIX A1	134
APPENDIX B	135
APPENDIX C	138
REFERENCES.....	141

LIST OF TABLES

Table 4.1 Sustainability indicator	55
Table 4.2 Probability scale.....	60
Table 4.3 Risk impact scales	60
Table 4.4 Level of risk exposure.....	61
Table 5.1 Region and type of IS auditor	73
Table 5.2 Number and categories of respondents	76
Table 5.3 Issues in IS audit	78
Table 5.4 Summary of problems in IS audit and potential sustainability controls	78
Table 5.5 Evaluation of economic criteria	82
Table 5.6 Evaluation of environmental criteria	82
Table 5.7 Evaluation of social criteria	82
Table 5.8 Evaluation of technological criteria	83
Table 5.9 Summary of m-values	85
Table 5.10 Risk factors and m-values.....	85
Table 5.11 Risk exposure	86
Table 5.12 Risks and general controls	91
Table 5.13 Evaluation of economic criteria.....	94
Table 5.14 Evaluation of environmental criteria.....	94
Table 5.15 Evaluation of social criteria	95
Table 5.16 Evaluation of technological criteria	95
Table 5.17 Summary of m-values	96
Table 5.18 Risk factors and m-values	96
Table 5.19 Risk exposure	97
Table 5.20 Evaluation of economic criteria.....	101
Table 5.21 Evaluation of social criteria	101

Table 5.22 Evaluation of technological criteria	102
Table 5.23 Summary of m-values	102
Table 5.24 Risk factors and m-values	103
Table 5.25 Risk exposure	103
Table 6.1 Feedback on economic sustainability assessment.....	106
Table 6.2 Feedback on environmental sustainability assessment	108
Table 6.3 Feedback on social sustainability assessment.....	109
Table 6.4 Feedback on technological sustainability assessment.....	112
Table 6.5 IS control evaluation	114
Table 6.6 Estimate risk probability and impact	116

LIST OF FIGURES

Fig 1.1 Overview of the thesis structure	9
Fig 2.1 Sustainability dimensions	22
Fig 3.1 Summary of research design	39
Fig 4.1 Conceptual view	45
Fig 4.2 SISA process	48
Fig 4.3 Sustainability dimensions and sub-criteria.....	51
Fig 4.4 Risk assessment approach	54
Fig 5.1 Empirical study methods and context.....	65
Fig 5.2 Experience in IS audit	70
Fig 5.3 IS audit in the NAD and SAI	74
Fig 5.4 Factors impacting the performanc of the IS audit in the public sector	75

LIST OF PUBLICATIONS BY THE AUTHOR

Date of conference	Title
10-12 July 2014	A.B.L.A Rahman, A.Al-Nemrat, and D. Preston, 'Sustainability in information systems auditing', European Scientific Journal, Special Edition, vol. 3, pp.458-472, 2014
13-15 May 2015	A.B.L.A. Rahman Aida, S. Islam, and A.Al-Nemrat, 'Measuring sustainability for an effective information systems audit from public organisation perspective', 2015 IEEE 9 th International Conference on Research Challenges in Information Science, pp.42-51, Athens, DOI: 10.1109/rcis.2015.7128862
1-3 Oct 2015	A.B.L.A Rahman and S. Islam, 'Sustainability forecast for cloud migration', 2015 IEEE 9 th International Symposium on the Maintenance and Evolution of Service-Oriented and Cloud-Based Environments (MESOCA), pp. 31-35, Bremen, DOI. 10.1109/MESOCA.2015.7328123
26-28 June 2015	K.S.A. Azmi and A.B.L.A Rahman, ' E-Procurement: A Tool to Mitigate Public Procurement Fraud in Malaysia?', European Conference in e-Government, pp. 361-368, 2015

ABBREVIATIONS

ABBREVIATION	Description
IS	Information systems
CATTs	Computer Assisted Audit Tools and Techniques
COBIT	Control Objectives for Information and Related Technologies
COSO	The Committee of Sponsoring Organizations of the Treadway Commission (COSO)
INTOSAI	The International Organisation of Supreme Audit Institutions
ASOSAI	Asian Organization of Supreme Audit Institutions
ISACA	Information Systems Audit and Control Association
ISSAI	International Standards of Supreme Audit Institutions
MoH	Ministry of Health
NAD	National Audit Department
SAI	State Audit Institution
SISA	Sustainability driven IS audit

CHAPTER 1

1. Introduction

This study focuses on changes in the IT audit function following the introduction of sustainability into the information system discipline. Sustainability refers to progress that meets the needs of the present without compromising the ability of future generations to meet their own needs (Brundtland, 1987). Sustainability has been broadly implemented in many organisations to control economic, environmental and social aspect in their operations. The integration of sustainability into business function implies new ways of improving performance, leading to a new strategy of decision making and creating new control objectives for IS implementation (Kimaro and Nhampossa, 2007);(Silvius and Nedeski, 2011). Sustainability is considered to be the most important and significant aspect of IS evaluation, interacting with economic, environmental and social elements (Kimaro and Nhampossa, 2007). Sustainability is also perceived as a strategy for continuous improvement and so the three aspects (economic, environmental and social) have been adopted in IS development and implementation for managing IS projects, business functions and information (Jaca *et al.*, 2012). A wide review of studies has indicated that sustainability should be incorporated into IS evaluation and ICT projects in order to enhance operational activity and flexibility and to support system utilisation (Ali and Bailur, 2007); (Nurdin *et al.*, 2012).

Information systems audits play a significant role in IS development and implementation in assuring an effective IS control system, maintaining data integrity, achieving organisational goals effectively and consuming resources efficiently (Weber, 2002). An IS audit is a part of the overall audit process that facilitates the risk assessment process, control and IT governance. This study focuses on the IS audit process related to sustainability dimensions (economic, environmental and social) and the role of sustainability in contributing to the effectiveness of the IS audit process by evaluating IS control and risk assessment.

Most sustainability literature addresses sustainability as an opportunity to improve the performance of IS, which includes assessing risk and its impact on IS (Kimaro, 2006, 2007; Silvius, 2009; Jaca *et al.*, 2012). Concerns about sustainability outline that the current method of planning, organising, and evaluating IS performance needs to be improved. This claim was

supported by several issues raised in the Auditor General's Report, which clearly identified weaknesses found in IS controls that require effective risk assessment. For example, issues such as mismanagement of IS assets, absence of control tasks, lack of clearly defined organisational structure or limited segregation of duties, management and data reliability gaps and errors in data migration were all identified in the Auditor General's Report (Malaysia) from 2012-2014, the Australian National Audit Office (2012-2013) and the United Kingdom National Audit Office (2012-2013). The above findings provide an indication that IS projects and IS development are not being properly monitored and measured; most of these are recurring issues.

Given the above discussion, it is perceived that sustainability provides the opportunity for IS auditors from public sector organisations to conduct a comprehensive audit work pertaining to economic, environmental, social and technology as a strategy to reduce the potential of IS failures, cost overrun, interruption in the service delivery processes and project delays.

1.1 Background and motivation

Information technology has been recognised as a strategic enabler in improving public sector delivery systems. Due to the high level of IS investment and uncertainty of performance, public sector organisations are continually confronted with innovative technology and new requests from stakeholders, clients and the public. Clients, stakeholders and the public expect that IS will deliver value, for example, cost optimisation, effective services and reliable output. However, there are various systems being audited which are underutilised in terms of functionality; users do not make use of all the functionalities due to lack of knowledge about applying the features and delays in IS project implementation. Although management has often established control mechanisms to ensure information systems are functioning as expected, there are also cases in which the IS are unsuccessful and do not deliver everything that is expected of them. These findings are symptomatic of inefficiencies in controls of the systems; most IS problems within the public sector are related to economic, technical, managerial, planning, resourcing and environmental factors (Gauld, 2007).

This research is motivated by evidence that not all IS failures are connected to technology, but instead they tend to depend on expectation, IS process and pressure from public/client; some IS failures also have to do with psychological, social, and organisational issues (Jan Devos, Hendrik van Landeghem and Deschoolmeester, 2008). The work further incorporates

the concept of sustainability, which comprises economic, environmental, social and technology-related factors, to audit IS aids in analysing the changing demands of users, stakeholders and the public (Asif *et al.*, 2013) and to improve project value in terms of quality, productivity, life cost reduction and business enhancement (Abidin and Pasquire, 2007). Sustainability is taken into account when performing an IS audit for three reasons: 1) sustainability refers to long-term improvement/innovation; 2) sustainability consists of human, environmental, social and economic factors; and 3) the availability of the sustainability indicator as a performance indicator.

This research applied sustainability to bridge the gaps existing in IS control evaluation, to facilitate the decision making process and to increase the probability of IS success. Assessment without sustainability showed errors or had problems such as cost and schedule overrun, high reliance on a third party for advice, and a poorly defined purchase/IS contract. In this regard, a sustainability driven IS audit in relation to a risk-based approach is a critical area of concern. Therefore, this research is motivated by the need for an effective IS audit practice with an emphasis on risk assessment in order to reduce IS error or failure in public sector organisations.

1.2 The Problem Statement

IS auditors are responsible for formulating an opinion about the effectiveness of IS controls, user utilisation of the IS, value for money, system development practices and IS implementation in order to achieve the organisation's objective (Majdalawieh and Zaghloul, 2009). The importance of having effective IS control has motivated IS auditors to review corporate governance processes, system development and internal controls (Nurmazilah Mahzan and Veerankutty, 2011). In the course of auditing work, IS auditors are confronted with various inherent challenges, such as the developed system failing to meet the actual user needs or risks in IS projects not being adequately managed, which contributes to IT failures. According to Hunton *et al.* (2004), the IS audit is a complex task that requires an appropriate level of technical knowledge and also needs the auditor to interpret the situation. For example, when the disaster recovery plan is out of date, what would be the most useful interpretation of an IS audit findings to highlight the impact to the organisation, user and stakeholder? With this in mind, sustainability could drive IS auditors to change their method of conducting an audit by assessing the IS control environment from a sustainability point of view and move towards risk assessment.

The study of the failure of IS projects highlights several issues such as project overrun, cost overrun, inability to fulfil the user's requirements, poor audit trail, failure to achieve the objective of the project and inadequate management and technical practices (McManus *et al.*, 2007);(Nayan, Zaman and Sembuk, 2010) and (Boldt *et al.*, 2012). Even though there is a large amount of unsuccessful information systems development dealt with in the literature, this issue is almost hidden and often underreported by public agencies due to public sensitivity (Goldfinch, 2000). Management control is a major control level within an organisation which often influences the effectiveness of internal control. COBIT is a comprehensive framework of IT governance that provides an extensive guide for IT managers, but many organisations find COBIT too complex and difficult to implement (Bartens *et al.*, 2015). From the sustainability perspective, Merhout and O'Toole (2015) claimed that COBIT 5 does not adequately address sustainability within its processes due to the current absence of environmental and social stakeholder drivers, needs and objectives. Sustainability limitations within COBIT 5 include IT policies for outsourcing, sustainability procedures for utilisation and disposal of IT assets, failure to support the control and implementation of a sustainable information system, lack of emphasis on the organisation's attitude towards sustainability and overlooked sustainability considerations with regard to information systems development.

In order to enhance corporate governance, the public sector organisations need to demonstrate their credibility and capability to provide transparent information to users, the public and stakeholders. Sustainability provides the opportunity for IS auditors to review current IS audit practice and make improvements. In reality, sustainability is future oriented and can contribute directly to tangible economic value by reducing costs, identifying threats and decreasing risks for IS (Fiksel, 2003); (Kimaro and Nhampossa, 2007).

With this in mind, the researcher applied sustainability to develop an IS audit framework which emphasises IS control evaluation and risk assessment. Principally, the problem lies with the fact that the current practise of control and risk assessment is vague, and the existing IS audit frameworks fail to discuss evidence reasoning and its related concepts as part of the IS audit process. Due to the lack of easily justified control and risk evaluation in terms of its cause-effect relationship in the IS audit work, the research problem can be summarised as follows:

There is a still lack of methods and techniques related to how to integrate sustainability within the IS audit on a practical basis. A framework is needed to describe a new IS audit technique, a systematic method for implementing an IS audit on the basis of sustainability.

1.3 Research aim and objectives

The aim of this research is to develop a comprehensive sustainability driven IS audit framework that can be used by IS auditors in public sector organisations for an effective IS assessment. Based on this objective, this research will address sustainability to be included in IS audit work to evaluate IS control. In relation to the above, the following research sub-objectives are identified:

- RO1: To investigate the feasibility of the sustainability dimensions to enhance IS audit work;
- RO2: To investigate the usability of the framework in different sized organisations;
- RO3: To produce an extended IS audit report that includes the level of IS sustainability;
- RO4: To validate SISA in a real IS audit within public sector organisations and to provide a novel contribution to the IS audit and sustainability perspective.

1.4 Research questions

The research questions were formulated based on the literature survey and the current need to improve IS audit practice. The first research question seeks to explain the meaning of sustainability in IS and how it affects the IS audit practice in the public sector organisation.

How can we measure and analyse sustainability of information systems from the perspective of an IS audit of a public sector organisation?

This study approaches IS audit practice not only as a technical activity, but also as a socio-knowledge constructed activity. Traditionally, an IS audit has been conducted to ensure the effectiveness of IS control and to reduce control risk. However, it is now becoming increasingly important to include sustainability as an integral part of the audit report (Lee, 2014; Wallage, 2000a). Public sector organisations are entrusted with providing assurance about the effectiveness of IS control within public sector organisations. Therefore, this research focuses on providing assertions regarding sustainability dimensions (economic, environmental, social and technological) within IS audit reports. Based on the varied information related to IS audit practice and IS failure, research has found that there is a need

to adopt a sustainability perspective within IS audit practice. The following are identified problems that require investigation in this research:

RQ1: How can sustainability dimensions be incorporated into an IS audit process in order to have an impact on IS audits?

RQ2: Could SISA be implemented in different types of organisations?

RQ3: To what extent does the SISA framework affect the IS audit process?

RQ4: What are the challenges faced by the IS auditor when adopting a sustainability driven IS audit framework?

A framework developed based on sustainability dimensions was used to address the research questions in this work. The framework facilitates the development of an understanding of the social meaning of IS audit in its institutional and social context. Semi-structured interviews were employed as the main research method because these allow for an in-depth, contextualised study, which has been deemed appropriate to address the research questions. A survey questionnaire and archive documents from the public domain, including the Auditor General Reports and the INTOSAI, ASOSAI documents, were also examined to provide additional evidence to address the research questions.

1.5 Research contributions

This research makes a number of novel contributions to improve IS audit practice within public sector organisations. The contributions of this research to the research questions are summarised below.

- i) To the best of the researcher's knowledge, the Sustainability Driven IS Audit Framework (SISA) is the first framework to integrate sustainability. The framework consists of a conceptual model, a technique by which to evaluate IS control, risk assessment and analysis to achieve sustainability of IS within public sector organisations. SISA develops a structure that identifies four sustainability dimensions – economic, environmental, social and technological, that take into account technical and non-technical components such as cost minimisation, resources efficiency, flexibility of IS, scalability and continuity of the IS service. SISA provides a generic framework and can be customised according to IS complexity and the size of the organisation.
- ii) A methodological process that employs a risk-based approach to determine the level of IS sustainability was developed. The proposed process is systematic and

structured with defined tasks for IS control evaluation and risk assessment. It begins with the establishment of IS audit criteria within sustainability dimensions and development of the sustainability indicator, assessing IS control that enables identification of the potential risks to IS. The process includes numerical analysis that enables the evaluation of IS control and enhances audit judgment. The methodology can be used not only for IS audit practice, but also for cloud migration decisions.

- iii) The SISA can also be used to provide new insights into an IS audit decision process, consistency of decisions, focus on significant IS risk areas and effective audit judgment. Adopting SISA will enable auditors to document their audit judgments and reasoning. Interpretation on the level of sustainability based on risk exposure provides decision support to an IS auditor in deriving an audit opinion and making appropriate recommendations for preventive and correction actions for IS improvements.
- iv) The validation results indicate that SISA is able to address control risk within the significant complexity of IS control systems. As such, this framework is conceivably transferable to other large organisations with complex IS control systems.

1.6 The approach

The sustainability-oriented approach is introduced as a new dimension in IS audit practice with an emphasis on a risk-based approach. To examine how it is possible to achieve integration of sustainability within the IS audit, it is useful to involve key users – the organisation, public users and auditors – and analyse their needs as well as how IS will be of value to them. Factors related to the perceptions of key users are constructed from the literature and systematic reviews. The perceptions of key users are gained in order to be aligned with the business objectives before they are used to formulate the IS audit criteria. Based on a better understanding of key users' perceptions, a set of criteria is proposed to assist in the process of evaluating IS controls. The IS audit criteria are segmented into four sustainability dimensions which involve considering and integrating the economic, environmental, social and technological aspects into the IS audit framework. Economic criteria concern the IS investment or value for money; environmental criteria concern green IS practice; social criteria concern public service delivery of the IS; and technological criteria concern the security, reliability of information and flexibility of the IS. This part is then

presented as an itemised list of IS audit criteria for use in assessing IS controls and also as a data gathering technique.

Lack of control in IS may result in unexpected errors, threats or risks; therefore, this research investigates the potential for risk exposure that may affect the sustainability of the IS. As risk is connected to uncertainty, this research used the Dempster-Shafer theory (D-S) to evaluate IS controls. So that the IS audit could operate towards a risk-based approach, the research began by examining the adequacy of IS controls to be aligned with an organisation's objectives. The IS controls are segmented into four sustainability dimensions – economic, environmental, social and technological – and relevant sustainability indicators are used for data gathering in each dimension. Different sustainability dimensions require a different set of sustainability indicators depending on the IS audit criteria. The sustainability indicator is either implemented in-house or adopted from the current practise or standards. The adequacy of controls is measured based on the degree of belief in the D-S theory. Based on the current practice, an auditor is required to provide reasonable assurance about the internal control evaluation depending on the following categories: effectiveness and efficiency of operations; reliability of reporting; compliance with applicable laws and regulations; and adherence with sustainability requirements. Most of the standards (ISACA, COBIT, COSO) focus on providing guidance for control evaluation, but there is no method or technique available to provide a numerical analysis as a basis for making judgments. Taking this into account, the D-S theory is applied and the result obtained is used to measure the probability risk within each sustainability dimension.

Sustainability is about integrating short-term and long-term aspects. For example, the recession may impact the stability of the economic aspect in the short-term, however, for the environmental, technological and social aspects, impacts may occur in the long-term. The concern about sustainability indicates that it may have a negative or positive impact on the future. In this case, the weight of impact on each sustainability dimension varies from one to another. In the context of a risk-based approach, a quantified potential for risk exposure may be obtained after measuring the probability of risk and the impact of the risk within the sustainability dimension. Risk exposure provides an overview of risk based decision making with regard to the level of sustainability of IS.

1.7 Empirical evaluation

Empirical evaluation is carried out through three case studies undertaken in public sector organisations. An interview was conducted to explore the feasibility of the Sustainability Driven IS Audit (SISA) framework. In the interview, both structured and open questions were used. Structured questions included the scale type to be used for assessing degree of belief in D-S theory. Open questions were used to extract respondents' opinions on the topic being discussed, finding out more information about elements not included in the framework and considering any disagreement raised with regard to the proposed framework. The clarity of the questions and their relevance to the IS audit were crucial factors in gathering valid and accurate information. Therefore, an introduction session was used to explain the objective of the questions, providing instruction on scale type and how to finalise the IS audit findings. The respondents were the same as those who completed the questionnaire from the survey groups, including IS audit managers, IS audit middle managers and auditors from the NAD and SAI. The respondents included people from the IS audit sections, both internal and external audit divisions. SISA was implemented for the yearly audit program 2014/2015. The findings are presented in Chapter 5. The researcher believes that the empirical study results will contribute to a sustainability driven IS audit in public sector organisations.

1.8 Thesis structure

The first chapter presents the main research question of this thesis, along with some discussion on the background and motivation for the research. It sets the context for the study, presents its focus and research objectives and discusses the potential significance of this research effort. The links between chapters are presented in Figure 1.

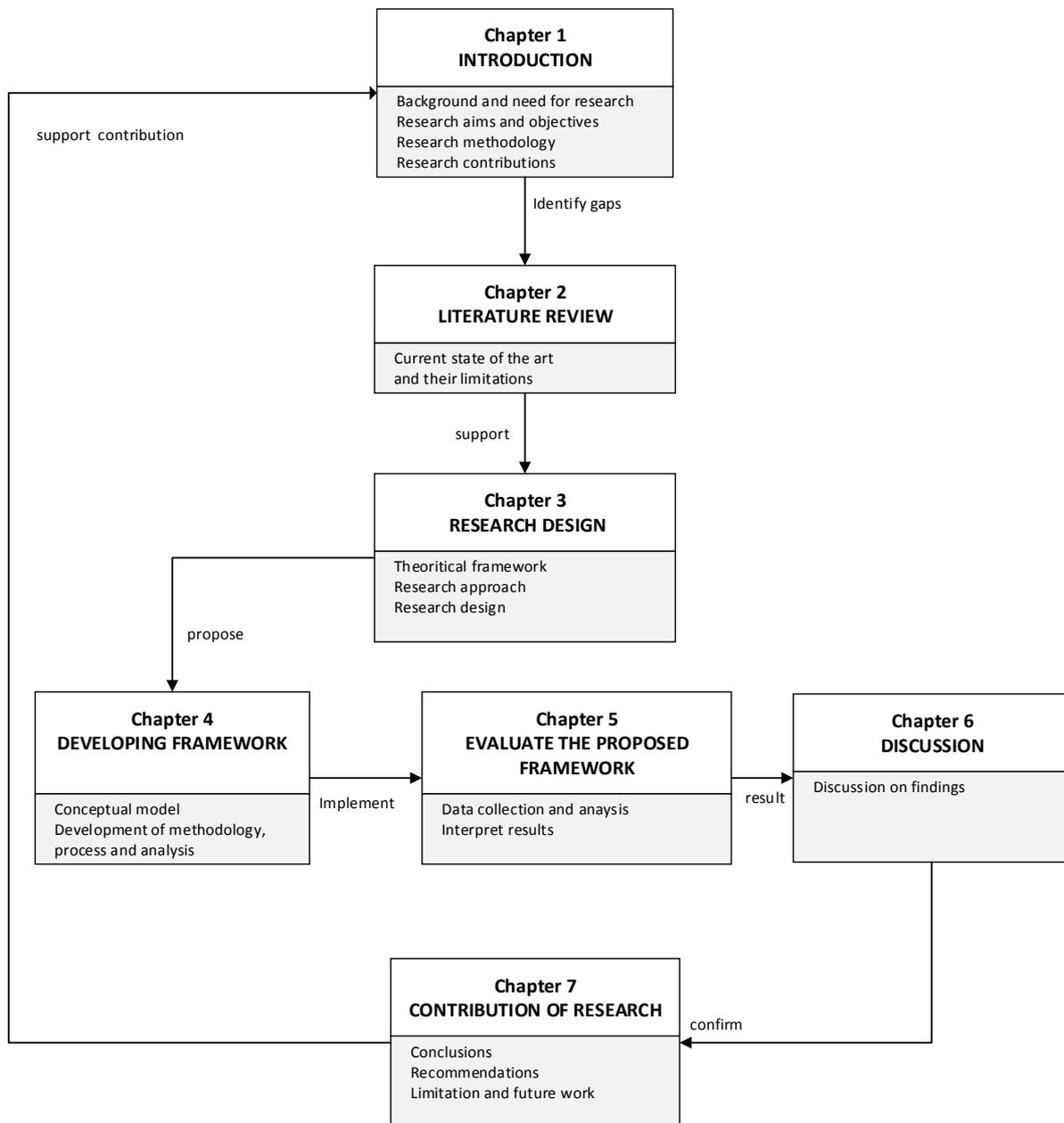


Fig 1.1 Overview of the thesis structure

Chapter 2 discusses the relevant literatures; this chapter provides a background and detailed discussion on the IS audit and sustainability. The discussion continues with a detailed explanation of the need for sustainability assessment in IS audit practice. This chapter also presents a discussion and identification of gaps in the literature, which is in general with regard to the lack of research in examining IS auditing from a sustainability perspective. Finally, the chapter summarises the existing state of affairs in relation to IS auditing and summarises the main contribution of the research.

Chapter 3 describes the research methodology, which includes a mixed method approach that formulates the research design of the thesis. This chapter justifies the philosophical assumption used in the thesis and the methods used for data collection and analysis.

Chapter 4 describes the development of the sustainable IS audit framework, which includes a conceptual model that this research is based on. The foundation of the proposed framework is based on sustainability dimensions and related IS audit processes. This provides guidelines on how to conduct an IS audit with an emphasis on sustainability requirements, the selection of sustainability indicators based on the sustainability criteria, assessment of controls and the associated risk and calculation of risk exposure as a basis to form a conclusion on the level of IS sustainability within public sector organisations.

Chapter 5 is the main contribution of this research, presenting the evaluation of the SISA framework. This chapter describes the process of the proposed framework and the analysis of the results. In particular, the activities included in the process are described and explained.

Chapter 6 presents a critical discussion of the SISA framework; it discusses the views that the IS auditors from public sector organisations expressed about SISA practice. An analysis of the key issues raised by the respondents is presented here and becomes the basis for identifying the feasibility of SISA to improve current IS audit practice.

Finally, Chapter 7 presents the conclusions of the empirical work of the study. Critical issues with regard to perceptions of sustainability driven IS audits in the public sector and the IS auditor context in which auditing is conducted are highlighted. This chapter concludes the thesis by considering the contributions and limitations of the study and by making suggestions for future research.

Appendix A comprises a questionnaire to identify current IS auditing practice.

Appendix A1 comprises interview questions to confirm findings from the survey.

Appendix B provides questions to evaluate the SISA framework.

Appendix C provides the audit program to perform SISA.

CHAPTER 2

Literature review

2 Introduction

The aim of this chapter is to conduct a review of the literature in relation to IS audit in the public sector. The chapter begins by presenting background information on IS audit, and then discusses IS problems in the public sector and the concepts of sustainability and risk which are relevant to this research. The chapter also includes several studies on the D-S theory of belief functions, which has been widely used for assessing audit risk.

2.1 Basic concepts

The main identified concepts of this study are audit context, sustainability and risk. These concepts are crucial to the domain of this study and will be considered in order to identify its objectives, characteristics and functions. A wide range of literature has defined 'audit' as a systematic process of obtaining and evaluating evidence relating to assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria and communicating the results to interested users. In general, audits are classified into three main categories: financial statement audits, compliance audits and performance audits. From the perspective of public organisation, compliance and performance audit are commonly practised, with financial audit embedded in compliance audit.

2.1.1 Financial audit

Financial audit is the assessment of financial statements for the purpose of certifying whether they are truly and fairly stated. According to the International Organisation of Supreme Audit Institutions (INTOSAI, 2009), the purpose of financial audit is to enhance the degree of confidence that users can have regarding the financial statements. Auditors are also required to ensure that relevant supporting documents and records are adequately maintained and that transactions have complied with legal or other regulatory requirements. This audit is typically concerned with financial performance rather than evaluating the performance of activities or programmes.

2.1.2 Compliance audit

The INTOSAI (2006) states that compliance audit is conducted based on significant relevant factors. They are:

- a) **Regularity** - the concept that activities, transactions and information pertaining to an audited entity are in accordance with authorising legislation, regulations issued under governing legislation and other relevant, laws, regulations and agreements, including budgetary laws and are properly sanctioned.
- b) **Propriety** – general principles of sound public sector financial management and conduct of public sector officials.

The implementation of compliance audit depends on the mandate of the audit institution; it may be an audit of regularity, propriety or both. Compliance audit works in a similar manner as internal audit, gathering sufficient evidence to conclude whether the information on a particular subject matter is compliant and also to provide assurance on the adequacy of the system of internal controls by testing its effectiveness and efficiency. Hamilton (1995) found that the fundamental objective of compliance audit is to ensure that appropriate controls are in place and functioning effectively, and these objectives are the same for the internal auditor. Reporting on compliance audit is based on a particular set of criteria, which are derived from the relevant frameworks, laws, regulations, parliamentary decisions, terms of contracts or agreements (INTOSAI, 2006). Nevertheless, there is a limitation to compliance audit, as it does not address efficiency, effectiveness or economy factors (Grönlund, Svärdesten and Öhman, 2011).

2.1.3 Performance audit

Performance audit is defined by INTOSAI (2013c) as an independent, objective and reliable examination of public sector undertakings, ensuring that activities, systems, operations and programmes are operating in accordance with the principles of economy, efficiency and effectiveness. Performance audit is widely used by public organisations to promote accountability and good governance of public administration and management of public funds. The principles of economy, efficiency and effectiveness can be defined as follows:

- a) **Economy** – minimising the cost of resources used for an activity while maintaining appropriate quantity and quality ensuring that resources are available when needed.
- b) **Efficiency** – getting the most from the available resources.

- c) Effectiveness – the extent to which objectives are achieved and the relationship between the intended impact and the actual impact of an activity.

Going by this definition, Daujotait and Macerinskien (2008) identified that performance audit works with concepts of performance management to plan, monitor and evaluate how public resources are used to achieve public policy objectives. Performance audit covers not only specific financial operations, but the full range of government activity, including both organisational and administrative systems, and may be conducted using both quantitative and qualitative assessment. Performance audit is perceived to be effective in improving management procedures in government agencies. It has been evidenced by Burrowes and Persson (2000) in their study that performance audit is essential for examining and promoting effectiveness and efficiency in central government by:

- a) Drawing the attention of central government and government agencies to efficiency problems; and
- b) Providing central government and its agencies with the information they need to take action to improve efficiency.

Under this consideration, the INTOSAI suggested the followings issues to be reported to parliament:

- a) The extent to which the objectives of specific government programmes have been achieved;
- b) The existence and capacity of the administrative machinery in place to inform the government as to whether the policies are meeting their objectives;
- c) The quality of the policy advice given to the government by officials.

As described above, the performance audit is flexible in determining the key area to be audited, developing the audit objective and defining the method, scope and criteria. The audit objectives are developed based on efficiency, effectiveness and economy, while activities or programmes are measured based on the predetermined audit criteria. From the performance audit perspective, a detailed and practical audit criteria can be established based on historical performance, benchmarking, expert opinions, engineered standards, discussion and agreement between interested parties or expectations from stakeholders and the public. A performance audit has a similar definition to a value for money audit. Different terms are used to identify concepts with the same meaning, or alternatively the same term may be used for different concepts. According to Jin'e and Dunjia (1997), a performance audit is an

activity that helps enterprises increase economic efficiency; it is part of the assurance services which include assessment, facilitation and remediation services. These are all value added activities that contribute to organisational success and strategic achievement.

2.1.4 IS Audit

The increased reliance on IS in public organisations to generate business activities has meant that audit practitioners have to evaluate how effective and efficient the IS are in supporting business activities in order to achieve the objective of the organisation. Currently, IS audits conducted in public sector organisations involve a combination of a compliance and performance audit approach. The compliance approach in IS auditing is essentially concerned with the evaluation to ensure that the information system is capable of safeguarding IS resources, preserving the system's confidentiality, integrity and availability, and confirming its compliance with applicable policies, procedures, standards, rules, laws and regulations (Nicho and Cusack, 2007; Nurmazilah Mahzan and Veerankutty, 2011; Sayana, 2002; Yang and Guan, 2004). The IS audit is also described as an independent and impartial assessment of the reliability, security, effectiveness and efficiency of automated information systems, the organisation of the automation department and the technical and organisational structure of the automated information processing (Yang and Guan, 2004). The performance audit approach is used when the IS auditors evaluate IS project management, which includes an assessment of effectiveness, efficiency and the economy of the IT investment and associated resources (Cerin and Vojković, 2013).

As IS have become more extensive and sophisticated, the Information Systems Audit and Control Association (ISACA, 2008) has specified the evaluation of IS cover areas that would have a significant impact on the electronic service delivery, including controls assessment, investment, systems reliability, software maturity, project management and information security management. This includes examinations of IS implementation, operations and controls of IS resources. Controls established within the IS environment which serve as the foundation of all controls are known as general controls. General controls comprise key areas to support business processes in IS, including physical and environmental, system administrative, network, business continuity, change management and third party service provider. The evaluation of application control is also conducted to ensure validity of input, accuracy in processing, completeness of output and data integrity. The audit assessment

should give assurance of the data integrity, suitable system controls and value for money by following compliance and performance audit practice (Majdalawieh and Zaghoul, 2009). The IS audit is also intended to ensure the information system is capable of safeguarding IS resources and to guarantee the system's confidentiality, integrity, availability and compliance with applicable policies, procedures, standards, rules, laws and regulations. In relation to IS audit project management, IS audit work also includes the assessment of effectiveness, efficiency and the economy of IT investment and associated resources. Compared with the traditional audit, the IS audit is able to extend the audit scope and enhance audit efficiency.

A number of previous studies have also emphasised the role of the IS audit in ensuring the success of IS implementation, for example, the e-government, in enhancing accountability. An audit is seen to provide assurance of achieving the efficacy and competence of operations, dependability and compliance with laws and regulations in public organisations. An audit is also capable of aiding public organisations to rectify IS weaknesses and strengthen the controls on information systems (Aman, Al-Shbail and Mohammed, 2013).

2.2 The regulatory requirements of the IS audit

The increased reliance on information systems (IS) has led to the need for assurance that IS accomplishes its business objectives. In recent years there have been considerable discussions on the information system (IS) audit process and governance. In general, the IS audit has been discussed in relation to two primary reasons: 1) high investment to improve business operations; and 2) the introduction of new rules and regulations related to the auditing of these operations (Stoel, Havelka and Merhout, 2012). The IS audit has been studied widely to examine the effectiveness of IT governance, controls, audit risks, security and also the role of IS auditors in an IT environment in order to explore opportunities for improvement and areas of weaknesses. In response, several regulatory requirements for auditing and governance have been set out in the United States, the United Kingdom and the European Union. The Public Accounting Oversight Board (PCAOB) Standing Advisory Group (SAG) emphasised the auditor's knowledge of information systems (IS), the importance of information technology (IT) and IT auditing of public companies. The United States' Sarbanes-Oxley ACT (Act) introduced rules, regulations and standards in relation to IS assurance on security and privacy. In addition to these regulatory compliance requirements, the IS audit comprises standards, frameworks and best practices such as the IT Governance produced by the ISACA (2005), COBIT (Control Objectives of Information and Related Technology), ISO 27000

(ISO 27001: 2005, ISO 27002: 2005), ITIL (IT Infrastructure Library) and, for public organisations, ISSAI – International Standards of Supreme Audit Institutions.

2.2.1 Principle and governance of IS audit in public sector organisation

The audit conducted in public sector organisations is governed by laws or constitutions and these are also required to comply with standards and regulations. Most public audit organisations are members of the International Organization of Supreme Audit Institutions (INTOSAI). The INTOSAI is a worldwide affiliation of public audit organisations and its members include the Office of Chief Financial Controller/Comptroller and The Auditor General Offices. INTOSAI holds conferences, establishes working committees, produces guidelines and publishes journals for public sector audits. The framework of professional standards is known as the International Standards of Supreme Audit Institutions (ISSAI), which functions as a benchmark for auditing public organisations. The 300 (2013) and INTOSAI (2013b) categorised the IS audit as needing to be conducted within the performance audit approach. In this regard, the ISSAI outlined several performance aspects of auditing in an IT environment, including the IT investment process, IS project management, system methodology, value for money, IS controls and system functions. ISSAI suggested that a performance audit in an IT environment should:

- a) Assess whether the IT systems enhance the economy, efficiency and effectiveness of the program's objective and its management;
- b) Ensure the output meets the required quality, service and cost;
- c) Identify any deficiencies in information systems and IS controls;
- d) Compare the IT system development and maintenance practices of the auditee to leading practices and standards; and
- e) Compare the IT strategic planning, risk management and project management practices of the auditee to leading practices and standards including corporate governance practices.

Reports from the National Audit Department of Malaysia and Australian National Audit Office demonstrated that IS audit findings are generated by the assessment of IS controls. Issues highlighted by these reports focused on IS governance, accounting and oversight of controls; for example, the Auditor General's Report (Malaysia) for 2006-2011 identified issues on non-compliance with IT policies, procedures and regulations such as absence of

controls tasks, lack of clearly defined organisational structure and limited segregation of duties. The Auditor General's Report from the Australian National Audit Office (2012-2013) also highlighted issues on IT controls, management arrangement and data reliability, while the National Audit Office of the United Kingdom emphasised performance criteria for assessing IS projects and desired results to achieve value for money.

2.3 Challenges to IS audit

In the process of undertaking audit work, auditors are confronted with various inherent challenges such as controls gaps arising from design, development and implementation of the IS projects. Despite the constant need to evaluate the effectiveness of controls, there are still cases of the information systems adopted for delivering services to public users not meeting expectations. This is generally due to inadequacies in management and technical practices, project overrun, cost overrun, inability to fulfil users' requirements and failure to achieve the objective of the project (McManus and Wood-Harper, 2007; Nayan, Zaman and Sembuk, 2010).

Goldfinch (2000) summarised that failures of IS development in the public sector derive from three aspects: project, system and user. Project failure refers to the inability of the project to meet contract agreements; system failure is when the system fails to perform as expected; and user failure is when users resist using the system. Whitney and Daniels (2013) defined four categories of IS failures: correspondence, process, interaction and expectation from stakeholders. Correspondence failures refer to when the system design objectives of specification are not fulfilled. Process failure is due to budget or time overrun. Interaction failure refers to user dissatisfaction with the IS and expectation failure is when the system does not meet stakeholder's expectations. Nawi, Rahman and Ibrahim (2011) highlighted that major failure factors in the government's IT project include technology, project management, organisational, complexity or size of the IT project and process of the IT. However, IS failures are often underreported by public agencies due to public sensitivity (Goldfinch, 2000).

One of the challenges that complicates the IS audit is the changing nature of technology. The rapid development in new technologies and technological innovations require a huge investment in IT infrastructure and continuous financial support. Public sectors are bound by rules and regulations for budgeting and allocating financial resources, which creates a challenge for the public sector to support all the requirements of the IS. This financial

constraint raises the issue of return and benefit of IS investment and the need to ensure sustainability and continuity. Sustainability is an important factor that improves the credibility of IS in the public sector and reduces the risk (Abu-Shanab and Bataineh, 2014). Security and privacy of information is another technical challenge in IS auditing when users are concerned about their information and transaction privacy. Therefore, effective security risk management is necessary to adequately assess and mitigate IS security risks.

The human factor is also considered as a key factor in the implementation of IS in the public sector and this is mainly presented by the public, shareholders and the organisation itself. The public sector adopted IS to deliver an effective service to the public and shareholders, as well as to improve the relationship between governments and their citizens. In this context, the value of the information system can be evaluated from the perspective of the public, shareholders and organisation. Value is not only considered from a financial point of view, but also from the human perspective, for example, what is important to them and what motivates them to use the system (Kujala and Väänänen-Vainio-Mattila, 2009). Due to growing concern about the perceptions of human factors in relation to the benefits, cost and risks of IT, there is an increasing need to re-think approaches to the evaluation of information systems in order to demonstrate the benefits and transparency of IT investment.

The quality of IS is also an important factor as poor design and implementation of the IS creates a bad reputation for the public sector in its delivery of an effective service to citizens. Failures in IS include project abandonment during the implementation stage (total failure), or the achievement of only some of the initial objectives (partial failure). It is important to note that even when IS has been implemented successfully, the system can fail the test of time (sustainability failure) and space (replication failure). In this respect, the IS audit needs to examine all project management organisations (Project Management Institute, International Project Management Association, Association of Project Management) in order to develop and update standards in order to secure project success in time, scope, quality and cost (Anthopoulos *et al.*, 2015).

2.4 Sustainability

Sustainability is defined as fulfilling the needs of the present without compromising the ability of future generations to meet their own needs (United Nations General Assembly Report of the World Commission on Environment and Development, 1987). This broad

definition emphasises environmental needs as a basic element of sustainability and it has been expanded into social and economy aspects by many studies. Many researchers have their own interpretation of sustainability within a wide range of disciplines. From the corporate sustainability view, Schneider (2014) concluded that business is either sustainability-oriented or market-oriented. Sustainability-oriented focuses on economic, environmental and social dimensions and the ultimate goal is geared to achieving the sustainable development of a business. In the case of market-oriented, environmental and social aspects were considered to gain an advantage in financial performance. Adoption of the concept of sustainability and implementation of sustainable activities are becoming a prerequisite for the success of businesses. Asif *et al.* (2013) claimed that the integration of sustainability into the business process is essential for the decision making process and in order to fulfil the changing demand of key users. In addition to improving business performance, sustainability has become a way to increase shareholder value (Horová, 2012) and also part of the strategic planning process for competitive advantage (Smith, 2012). Based on the concept of the three basic pillars of sustainability (economic, environmental, social), sustainability can be seen as the way a firm creates value for its shareholders by maximising the positive and minimising the negative effects of environmental, social or economic issues (Accenture, Chartered Institute of Management Accountants, 2011; Horová, 2012). Horová (2012) suggested that maximising the value of shareholders requires:

- i) Integrating sustainability into the business process management (sustainability must become an integral part of strategic management and business planning);
- ii) Integrating sustainability into the measurement and performance management (quantify the effects of sustainable activities in the financial performance and its impact on the growth of shareholder value);
- iii) Identifying appropriate business performance metrics (identification of social, environmental and economic indicators that influence the success of an organisation).

It is also found that sustainability is related to continuous improvement as many organisations aim to improve quality and their ability to adapt to change. Extending the view of organisational improvement, a number of change factors are considered that are related to sustainability, such as management commitment, key performance indicators, training and communication (Jaca *et al.*, 2012).

From the information systems perspective, Nurdin, Stockdale and Scheepers (2012) viewed sustainability as a technology capable of being maintained over a long period of time. Ali and Bailur (2007) emphasised that sustainability involves operational simplicity, flexibility, maintainability, robustness, availability and capability of technical and managerial personnel. Similarly, Nurdin, Stockdale and Scheepers (2012) claimed that sustainability is about making information systems work over time. In conjunction with technology advancement, Kimaro and Nhampossa (2007) noted that sustainability of IT is actually dependent upon technology as the main role of IT is to support system utilisation.

In view of the fact that sustainability is becoming a tool to improve performance, several studies in the domain of information systems have addressed the issues and challenges of sustainability with regard to several aspects, such as IS management (Harmon, Daim and Raffo, 2010; Korte, Lee and Fung, 2012), a strategy to incorporate environmental and social dimensions to enhance IT services, and the role of IT to promote sustainability within service oriented information technology (Harmon and Demirkan, 2011). From the previous literatures, it is commonly observed that sustainability has been discussed with regard to IS projects (Silvius, Brink and Smit, 2009), IS utilisation (Kimaro and Nhampossa, 2007), the development of an IT strategic plan (Harmon *et al.*, 2010), and IS management (Korte, Lee and Fung, 2012). Considering that sustainability preserves social benefits, a number of literatures have investigated the potential of the values based approach to support sustainability within the business process. In their study, Abidin and Pasquire (2007) mentioned that sustainability is capable of improving project value in terms of quality, productivity, profitability, life cost reduction and business enhancement. Going by this definition, they proposed a structural model for integrating sustainability issues into value management to assist sustainability implementation in three (3) phases: input, process and outcome. Gasparatos (2010) then explored the implications of incorporating value systems in a sustainability assessment tool in which values emphasise evaluating IS infrastructures and IS applications within IS audit practice in order to justify the benefits and impact of the IS adopted in the organisation. Bilgea *et al.* (2014) developed a model based approach for assessing value creation in order to enhance sustainability in manufacturing. Another aspect of sustainability is based on the hybrid systems perspective or systems of systems. Hessami, Hsu and Jahankhani (2009) introduced the Weighted Factor Analysis methodology (WeFA) to examine context, components, topology and the scope of sustainability from micro to macro systems.

The establishment of strategy to ensure that business continuity, resiliency and disaster recovery is able to endure is another definition of sustainability. According to Fiksel (2003), sustainability is not an end state to be reached; rather it is a characteristic of a dynamic, evolving system. For IS purposes, sustainability is considered as the capability of the system to provide effective service and valuable and consistent information to users (Kimaro and Nhampossa, 2007). Note that an IS cannot be sustainable in an absolute sense; to be effective, the IS must be evaluated from economic, environmental, social and technology points of view and it must also consider risks in the achievement of IS objectives. Therefore, sustainability in an IS audit is based on the practical challenges of IS in the auditing process to understand how IS interacts with business processes and delivers an effective service to users, the public and stakeholders. We define sustainability in an IS audit as:

The ability of IS to implement an effective collaborative socio-technical environment that contributes to business continuity, energy saving, cost effectiveness, flexibility, resiliency and agility of the system.

Sustainability is considered in four dimensions: economic, environmental, social and technological. These four dimensions need to be analysed to address the challenges of an IS audit, such as the growth of technologies, hidden cost, security and green IT requirements. Each sustainability dimension has specific objectives and sub-dimensions. Details of sustainability dimensions and sub-dimensions are shown in Figure 2.1.

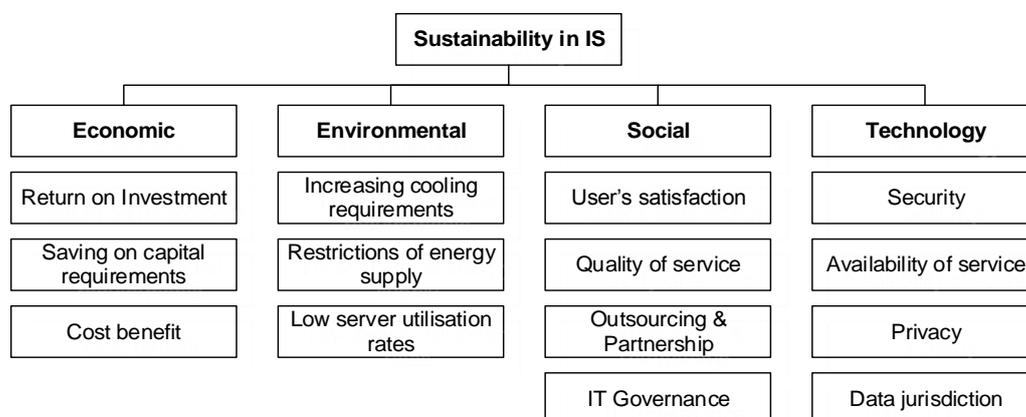


Fig 2.1 Sustainability dimensions

2.4.1 Economic dimension

The economic dimension aims to provide a measurement for cost estimation in IS implementation. The economic dimension is associated with the cost benefit feature, which includes budgeting, variance, hidden cost and continuous monitoring of the specified cost and investment. The stability of the economic factor is influenced by the external environment; for example, changes in government policy, a government transformation plan or emergence of new technology. In this view, the economic situation is exposed to a number of threats or risks such as cost overrun, schedule overrun, budget decline or the additional cost of adopting a new technology. Here, several risk factors for economic dimensions are determined including inadequate budget estimation, changes in legal policy and lack of continuous monitoring.

2.4.2 Environmental dimension

The environmental dimension focuses on providing eco-friendly IS settings as part of the social responsibility of green IS. To determine green settings, the selected configuration must support the requirements of multiple applications and minimise energy consumption. It is difficult to identify the optimal configuration that can meet a required response time from several applications and different hardware consumes variable power, so it is also hard to determine the level of energy consumption and energy savings. The availability of resources such as cost, IS infrastructure, governance and skills are the key components to achieve the objectives of green IS. While energy saving in automated computing is seen as an advantage for many organisations, there are risks associated with green IS implementation. The sustainability risk requires sufficient knowledge and skills to identify what type of configurations can meet a required response time and not affect the quality of services. Cost optimisation is also a risk since it is a challenge to define the operating cost by taking into account that different hardware use different energy levels. The structure and functionality of green IS can be a challenge to organisations, especially with regard to the way to define an optimal response time and promote energy savings without adversely impacting quality of service.

2.4.3 Social dimension

The social dimension aims to deliver quality services to clients, users and the public, which includes information quality, quality of service and availability of services. It is perceived that IS will be continuously performed, has scalable storage, is available for delivering services, applies elasticity to prevent denial of service attack and compliance with rules and regulations. Of these features, the IS is actually highly dependent on third party services, so it is essential to consider risk associated with service providers in relation to service level, transfer of knowledge, business continuity, incident management and licensing.

2.4.4 Technological dimension

The technological dimension aims to ensure that IS services and data are secured, protected and maintainable. Among the main advantages of IS is the sharing of resources and infrastructure with multiple clients, thereby promoting economies of scale. The distribution of cost and resources to several locations generates potential sustainability risks related to system performance, security and privacy in IS. These include falsification of messages, hardware interception, information leaks, traffic redirection and mis-delivery (Brender and Markov, 2013). Resilience is also considered within the technology dimension and it aims to ensure that the information system is able to maintain its service in the face of internal change and external disturbance (Wang, Gao and Ip, 2010). Applying resilience to IS auditing facilitates examination of whether the IS has the ability to defend against risk before adverse consequences occur (Erol, Mansouri and Sauser, 2009). For IS audit purposes, the resilience of the system is measured by the time from the impact of the disruptive event to the full recovery.

2.5 Sustainability measurement

Sustainability is perceived as a technique or method to improve business performance and to gain trust from stakeholders. Therefore, many organisations have established their commitment to sustainability by developing a strategic plan, organisational policies, vision, mission, corporate programmes and reports. Apart from the business's guidelines, standards and regulations to be complied with, many organisations have developed their own mechanism as sustainability performance indicators or sustainability metrics for assessing their sustainability performance. However, it has been discovered that measuring sustainability is complicated as it involves commitment and needs to highlight issues arising from internal and external environments. In this view, numerous factors have been considered

in measuring sustainability by using several criteria such as business competency, customer satisfaction, risks, economic value, environmental value and resources availability. Searcy (2009) proposed a conceptual model to guide the early stages in the development of a sustainability performance measurement system. He found that from the corporate perspective it is essential to diagnose the current situation and organisational goal, and identify the expected outcome in order to formulate the sustainability performance measurement.

According to Singh *et al.* (2009), the assessment of sustainability aims to ensure appropriate decisions are taken to preserve nature-society systems either in the short- or long-term. Generally, measuring sustainability includes methods for developing indicators and these are varied according to business process and level of control. Several methods have been identified for developing indicators such as summation, regression, mathematical assumption, weighting, ranking and data normalisation (Hutchins, 2009). In general, sustainability measures are categorised into two types: set of indicators (e.g. GDP per capita income) and aggregate indices resulting from sustainability variables (economic, social and environmental). The use of indicators is commonly selected as a tool to assess sustainability as the features of indicators are easy to understand, quantify and analyse.

There are numerous methods for developing sustainability indicators and these vary according to the business process. Korte, Lee and Fung (2012), mentioned that sustainability measurement includes benchmarking, key performance indicators and work goals. Delai and Takahashi (2011) denoted that sustainability measurement implementation needs to consider four (4) situations: 1) the sustainability measurement criteria; 2) themes and sub themes to be applied; 3) selection of groups in the measurement process; and 4) sphere of the company impacts to be taken into account. Ness *et al.* (2007) suggested that the sustainability framework may be developed based on indicator/indices, product-related assessment and integrated assessment tools. Singh *et al.* (2009), on the other hand, summarised details of the development of sustainability indicators, establishment of framework, scaling, normalisation, weighting and aggregation methodology. The authors specified that the sustainability framework and the sustainable development indicator (SDI) may be developed either by the top-down or the bottom-up approach. The top-down approach is when experts and researchers establish the framework and the SDI. The bottom-up approach means that stakeholders participate in the design of the framework and the SDI. Becker *et al.* (2015) introduced the

Karlskrona Manifesto for sustainability design to express the commitment of the software engineering community in relation to sustainability by taking into consideration the associate factors such as risks, cultures and technical features.

2.6 The need for sustainability assessment in IS audit

The previous literatures suggested three reasons for the need for sustainability in the public sector. It is needed as a commitment to increase accountability and transparency (Coyne, 2006; Gao and Zhang, 2006), to provide sustainability reporting to report on corporate governance of public sector organisations (Barret, 2005), and to highlight risk in relation to economic, environmental and social factors (Anderson and Anderson, 2009; ISACA, 2011).

2.6.1 The need to increase accountability and transparency

As described earlier, IS auditing may be performed in connection with a financial statements audit, compliance or performance audit. From a sustainability perspective, auditing is defined as a ‘process that enables an organisation to assess its performance in relation to society’s requirements and expectations’ (Elkington, 1997; Gao and Zhang, 2006). One of the objectives of sustainability auditing is to enhance the accountability and transparency of public sector organisations by providing a wider and deeper range of issues related to an organisation’s activities, products and services. Coyne (2006) argued that sustainability auditing is relevant to ensure that an organisation gives due consideration to its social responsibilities as well as to improving its performance. Accountability and transparency occurs when businesses disclose positive and negative facts about the current situation (Gherardi, Guthrie and Farneti, 2014) and if they fail to provide a balanced report (positive and negative facts), they risk underestimating social costs. Sustainability auditing is also relevant when making investment decisions. This is driven by the demand for socially responsible investing from stakeholders and investors (Coyne, 2006). In terms of corporate governance, the Sarbanese-Oxley Act also mentioned the disclosure requirements that specifically address sustainability reporting in relation to environmental costs and liabilities, identity and document events, emerging trends in environmental regulation or enforcement that could have a material financial impact on the company’s operations and establishment of procedures to evaluate and quantify potential environmental liabilities. In this regard, sustainability can be seen as an attempt to provide a comprehensive approach to increase the transparency and accountability of IS implementation in public sector organisations.

2.6.2 The need to provide sustainability reporting in public sector organisation.

The need to provide sustainability reporting in public sector organisations has become clear with increased in IS investment. Keil and Robey (2001) claimed that IS auditors are more objective in monitoring IS projects, while Nicho and Cusack (2007) mentioned that an IS audit is capable of developing quality assurance, benchmarking, and improving corporate governance. More recently, the IS audit has been identified as a means for improving sustainability through its potential to transform information and business processes (Thöni, Madlberger and Schatten, 2013). In relation to this point, sustainability reporting is relevant to public sector organisations as it allows for monitoring and control of results in connection with stakeholder expectations and it is able to address issues affecting society and financial aspects (Gherardi, Guthrie and Farneti, 2014). According to Wallage (2000b), the process of sustainability reporting is governed by the principle of accountability and concerns a reflection of the aspirations and needs of all stakeholders including future generations and the environment. Gherardi, Guthrie and Farneti (2014) identified that the most relevant motivations for disclosing sustainability reporting are public relations and transparency, stakeholder engagement, activity planning and organisation positioning, compliance with regulations, defensive tool/reputation effect, achievable sustainable development as promoted by the European Union and deficits in traditional accounting. Thus, it can be concluded that sustainability reporting is a useful tool to improve the performance of the IS of a public sector organisation by emphasising economic, environmental, social and technological motivations for the benefit of the auditee and the interest of the public.

2.6.3 The need to highlight risk in relation to sustainability dimensions.

There have some impressive IS successes as well as failures. Risk management is a technique that can reduce the possibility of IS failure/error. It is important to note that sustainability risks are the cross cutting concern of all sustainability dimensions and they may have potential negative impacts that could outweigh the expected IS benefits (Islam, Mouratidis and Weippl, 2014). Sustainability risks have already been addressed in academic literatures. Anderson and Anderson (2009) claimed that sustainability risk management can be thought of in terms of the 'triple bottom line' (TBL) developed by John Elkington. The TBL can be articulated as follows:

$$F + E + SR = TBL$$

Where F= financial performance, E = environmental performance, SR = social responsibility, and TBL = F – risk costs of E – risks costs of SR. According to Elkington, it is important to consider all three areas in order to maximise the triple bottom line. The risk management aspect of the TBL can be identified because the costs of risk are subtracted from profit (financial performance). If the environmental and social costs are reduced and everything else holds constant, the TBL will increase. Weber, Scholz and Michalik (2010) incorporated sustainability criteria into credit risk management. They identified that sustainability criteria can be used to predict the financial performance of a debtor and to improve the predictive validity of the credit rating process. Thöni, Madlberger and Schatten (2013) proposed an architecture for corporate risk management systems that provides an integrated view of environmental and social risks.

In conclusion, sustainability risks do exist whether the organisation recognises them or not. These risks must be identified and analysed as part of IS audit work and the IS auditor is required to disclose the identified risks to the management. In terms of risk identification and its mitigation, it is essential for the management to synchronise the mitigation method, from planning to implementation activities. This includes the formation of committee to analyse sustainability risks, to formulate an appropriate method for risk mitigation and to develop appropriate controls.

2.7 The Dempster Shafer Theory (D-S theory) of Evidence

In the IS auditing context, the assessment of IS focuses on the effectiveness of controls. The collection of audit evidences involves several audit techniques such as interviews, document review, physical inspection and observation. According to the Committee of INTOSAI (2009), audit evidence needs to be sufficient, relevant and reliable to enable the auditor to formulate an opinion. To date, the measurement of evidence is based on auditors' professional judgement, which is influenced by the materiality of evidence, the inherent risk, internal control system, previous audit experience and economic decision making (Tysiac, 2014). To ensure the decision made by the auditors is objective and independent, the D-S theory is used as a strategy to evaluate evidence and to help auditors arrive at sound professional judgments and effective decision making.

The Dempster-Shafer theory of evidence was introduced by Shafer (Dempster, 1968; A.P. Dempster, 1967) to represent and reason uncertain and incomplete information. The D-S

theory uses the concept of ‘degree of belief’ for modelling reasoning under uncertainty and provides a combination rule for aggregation of evidence. The degree of belief can be described as the degree of expectation that an alternative yields with regard to an expected outcome on a particular criterion (Sonmez, 2007). The D-S theory has been widely used for business decisions, auditing, sustainability evaluation and risk assessment. For example, Beynon, Cosker and Marshall (2001) and Sun, Srivastava and Mock (2006) applied D-S theory for risk assessment; Awasthi and Chauhan (2011) used the theory for decision making; Srivastava (2005) applied D-S theory to develop formulae for assessing fraud risk in a financial statements audit. The D-S theory can be interpreted as a generalisation of probability theory where probabilities are assigned to sets as opposed to mutually exclusive singletons. In contrast to traditional probability theories that have evidence for one possible event, the evidence derived from the D-S theory is associated with multiple possible events. In this sense, evidence in the D-S theory is more meaningful and able to demonstrate precision with regard to varying levels of information.

Basically, the D-S theory uses the concept of ‘degree of belief’ for modelling reasoning under uncertainty and incomplete information. There are three basic functions that are important for the D-S theory: basic *probability assignment functions or m-values*, *belief functions* and *plausibility functions*. The description of these is as follows:

- i. *Basic probability assignment functions (m-values).*

The basic difference between m-values and probabilities is that probabilities are assigned to individual elements or states of a frame (Θ). The frame of discernment is a set and it is mutually exclusive. The sum of all probabilities is one. The m-values in the belief functions represent the uncertainties assigned to individual elements or states and to a set containing any two elements, three elements, and so on for the entire frame. Similar to probabilities, all these m-values add to one:

$$\sum_{A \in \Theta} m(A) = 1$$

where A represents a proper subset of the frame (Θ), and the m-value for the empty set is 0, i.e. $m(\emptyset) = 0$.

ii. *Belief functions*

Given a bpa, we can compute the total belief provided by the body of evidence. The belief in a subset of a frame (θ), say A, is equal to the sum of all m-values for the individual elements in the subset A:

$$Bel(A) = \sum_{B \in A} m(B)$$

$Bel(A)$ is the total belief committed to A, which is the bpa of A itself plus the bpa attached to all subsets of A.

iii. *Plausibility functions*

The plausibility (Pl) function provides complementary value of belief. The plausibility in a subset of a frame (θ), say A, represents the maximum uncertainty that could be assigned to A if all future evidence supported A. This is defined as:

$$Pl(A) = \sum_{A \cap B \neq \emptyset} m(B) = 1 - Bel(\sim A)$$

The ambiguity in A is measured as $Pl(A) - Bel(A)$

2.7.1 Dempster's Rule of Evidence Combination

Similar to Bayes' rule in probability theory, Dempster's rule is used in D-S theory to combine independent items of evidence. In order to derive the general form of Dempster's rule for a binary variable, Srivastava (2005) considered two items of evidence and generalised them for n-items of evidence. Let us consider two items of evidence, E_1 and E_2 pertaining to a frame (θ), and the corresponding belief masses as represented by m_1 and m_2 . The combined belief masses (m-values) for a subset A of the frame (θ) using Dempster's rule are given by Shafer (1976) as follows:

$$m(A) = (1/K) \sum \{ m_1(B_1) m_2(B_2) \mid B_1 \cap B_2 = A, A \in (\theta) \},$$

where K is the 'renormalisation' constant given by:

$$K = 1 - \sum \{ m_1 (B_1) m_2 (B_2) \mid B_1 \cap B_2 = \emptyset \},$$

K measures the conflict between the pieces of evidence. The larger the K, the more the sources are conflicting and the lower the sense of combination. If K=0, this shows complete compatibility and if $0 < K < 1$, it shows partial compatibility. If K=1, the orthogonal sum does not exist and the sources are completely contradictory.

The lower and upper bounds of an interval can be determined by using bpa, which includes belief and plausibility. The lower limit of belief is considered as the lower bounds and the plausibility as the upper bounds. This interval represents the range where the probability may lie and it can be determined by subtracting belief from plausibility. The narrow uncertainty band represents more precise probabilities. The plausibility function also represents material errors that exist in the evidence and can be applied to measure risk (Sun, Srivastava and Mock, 2006).

The belief and plausibility functions are given below:

$$\text{Bel} = \text{Bel} (A),$$

$$\text{Pl} (A) = 1 - \text{Bel} (\sim A) = 1 - (\sim A) = \sum_{i=1-n} (1 - m_1 (\sim A))/K$$

$$\text{Pl} (\sim A) = 1 - \text{Bel} (A) = 1 - m (A) = \sum_{i=1-n} (1 - m_1 (A))/K$$

2.8 Risk assessment

System success is related to many risks associated with IS development and not all settings require complete control. Therefore risk assessment is essential to identify risk factors and implement mitigation measures to bring risk to an acceptable level with an acceptable cost. The common assessment methods for risk assessment include internal control assessment, risk factor analysis, qualitative risk assessment and fuzzy combined assessment. To assess uncertainties, the Delphi method, expert focus groups or D-S theory can be used as a technique to determine probabilities (Huang *et al.*, 2004; Srivastava and Li, 2008). According to Mahmoudi *et al.* (2013), there is basic agreement on three core components of risk assessment:

- i) Identification of risks: establishing the cause-effect link;

- ii) Assessment of exposure and/or vulnerability: modelling diffusion, exposure and effects on risk targets;
- iii) Estimation of risk: determining the strength of a cause-effect link.

Different disciplines may have different concepts of risk and depend on perception and risk analysis. The key task of risk assessment is the identification of the risk types, intensities and the likelihood of the consequences related to risks (Kalloniatis, Mouratidis and Islam, 2013). Risk analysis aims to evaluate each identified risk and assign probability and impact to each. Risk rating depends on the probability of impact and the level of impact. The probability of the occurrence of the risk is categorised as follows:

- a) Very unlikely to occur – <10%
- b) Unlikely to occur – 10-25 %
- c) Possible – 50%
- d) Likely to occur – 50-75%
- e) Very likely to occur – > 75%

Impact refers to loss to the organisation due to the occurrence of risk. In general, impact of risk can be categorised as very unlikely, unlikely, average, likely and very likely. The probability of an event, for example, cost overruns, could be classified as ‘very likely’; whereas the occurrence of the budget declining may be classified as ‘likely’. In order to evaluate the severity of the consequences, the following information is required: understanding the business organisation, the internal control environment, the legal provisions, the history of events, and the people or systems that may be exposed and affected. The exposure of risk is calculated based on probability and impact of risk to the organisation. The level of exposure is scaled at low, low to medium, medium, medium to high or high. The risks can be ranked according to the level of exposure and should be given priority based on the high exposure of risks.

2.9 Overview on the INTOSAI Development Initiative (IDI)

According to INTOSAI (2013a), the IDI is a non-profit organisation that acts as the capacity building secretariat of the International Organisation of Supreme Audit Institutions (INTOSAI), which today comprises 189 supreme audit institutions (SAIs). The IDI is a non-profit organisation organised as a foundation according to Norwegian laws. The Office of the Auditor General of Norway has hosted the IDI since 2001 in accordance with the Norwegian

Parliament's approval and in line with the resolution of the 16th INTOSAI Congress in 1998. The organisation comprises the IDI board, the IDI secretariat and the IDI advisory committee. The IDI is responsible for enhancing the institutional capacity of SAIs in developing countries through needs-based, collaborative and sustainable development programmes in INTOSAI regions and groups of SAIs in order to meet the emerging and existing needs of their stakeholders. In order to enhance the capacity of SAI, a number of activities such as training, knowledge sharing and capacity building are organised as a mechanism to increase transparency, accountability, and also for the achievement of good governance in public sector organisations. INTOSAI recognises seven regional groups established for the purpose of promoting the professional and technical co-operation of the member institutions on a regional basis. The INTOSAI regions are:

- i) AFROSAI: the African Organisation of Supreme Audit Institutions
- ii) ARABOSAI: the Arab Organisation of Supreme Audit Institutions
- iii) ASOSAI: the Asian Organisation of Supreme Audit Institutions
- iv) CAROSAI: the Caribbean Organisation of Supreme Audit Institutions
- v) EUROSAI: the European Organisation of Supreme Audit Institutions
- vi) OLACEFs: the Latin American and Caribbean Organisation of Supreme Audit Institutions
- vii) PASAI: the Pacific Association of Supreme Audit Institutions

2.10 Population frame

This research will cover IS auditors from public sector organisations in the NAD and SAI. External auditors are required to report their audit findings to the Public Account Committee (PAC) in the parliament. This committee will evaluate the issues and findings via the Auditor General and can call upon the Controlling Officers in response to any mismanagement and misuse of public funds. The committee also ensures that the accountability and integrity concepts are achieved in government spending.

Internal audits by the Internal Audit Department are seconded by the NAD and their representatives in various ministries, departments and agencies. The posts are known as cadre posts and the internal auditors will comprise trained and experienced auditors from the NAD. The internal audit department plays an important role in enhancing accountability and is an integral element of the internal control structure within the agencies.

2.11 Summary

This chapter has provided a description of the IS audit in public sector organisations and reviewed the relevant literature pertaining to sustainability. Based on the literatures, problems in IS auditing and how to improve the IS audit process were discussed in depth. From the literature, it can be concluded that:

- i) IS auditing needs improvement due to the changing needs of clients and stakeholders involved in IS adoption. The perceptions of the organisation, public users and auditors are deemed important as they contribute to the success of IS as well as to minimising control risk in IS projects.
- ii) Sustainability should be incorporated into the IS audit practice in order to address issues related to IS auditing in public sector organisations. There is a need for a sustainability report to emphasise transparency and accountability in IS investment and risk assessment.

CHAPTER 3

Research Methodology

3 Introduction

This chapter describes the research design adopted to address the research questions outlined in chapter 1. This will be based on the discussion of research philosophy, research approach, and followed by a discussion of the methodologies used in the field study. The techniques used for the data collection and analysis are also presented in this chapter.

3.1 Research paradigm

A research paradigm is a whole system of thinking, it is a set of philosophical assumptions about the nature of the world (ontology) and how we can understand it (epistemology). In other words, a research paradigm guides the researcher's view of the subject of the study, how to investigate it and it aids design research process and its direction. Based on the philosophical assumptions, the research paradigm is categorised into positivist, interpretive and critical research (Myers, 1997). The most common research paradigms that have been discussed by many researchers are positivist and interpretive. A positivist approach is based purely on facts, it is independent and there is no provision for human interest within the study. According to (Klein and Myers, 1999), the positivism paradigm involves the development of a hypothesis using independent and dependent variables as well as the measurement of the identified variables using quantitative methods. An interpretive research is typically associated with a qualitative research and understanding a phenomenon by a social construction such as language, shared meanings, tools, documents, etc. (Walsham, 1995). Instead of predefining dependent or independent variables, the interpretive approaches provide a better understanding of the social context of the phenomenon and a greater scope to address issues of influence and impact (Orlikowski and Baroudi, 1988). Critical research concerns the study of historical practices to generate knowledge. The critical approach requires the use of a relevant theoretical framework to critically evaluate the social world (Debra Howcroft and Trauth, 2004).

The differences between interpretive and positivist approaches can be addressed by considering their epistemological and ontological stances. In relation to epistemology, Archer (1998 cited in (Walsham, 1995) defined positivism as the position that facts and values are distinct and that scientific knowledge consists only of facts. This reality can be discovered through experimental reasoning or scientific observation and tested in terms of its cause-effect relationship among identified variables (Creswell, 2003). For the interpretive approach, knowledge is constructed through human interactions and it is open to adopt facts and values. Its emphasis is to understand the social world through the examination of the interpretation of that world by its participants. With respect to ontology, a positivist orientation regards that reality exists, it is observable and is expressed as factual statements. On the other hand, interpretive orientation explores the world naturally and it is non-manipulative, unobtrusive, and non-controlling (Ruth J. Tubey, Jacob K. Rotich and Bengat, 2015).

Information systems research has been predominated by the positivist paradigm (Orlikowski and Baroudi, 1988). Due to the changing role of information systems and the advancements in information systems research, an interpretivist paradigm is adopted. The interpretive approach in information system research is very popular and accepted as a valid research strategy within the IS research community. It is claimed that interpretive research has the potential to aid researchers in gaining knowledge about information systems phenomena, the management of information systems and information systems development (Walsham, 1995). As mentioned above, the interpretivist approach makes contribution to a body of knowledge through a study of meanings collected from a real world situation. As the realities are constructed by the interpretation of meanings extracted from people, objects and events, the interpretivist researchers concentrate on qualitative rather than quantitative methods of analysis (Wallen & Fraenkel, 2001; (Assalahi, 2015).

Based on the discussion above, an interpretive research is the most appropriate approach to guide this research. The researcher selected this paradigm for the following reasons. First, this study is exploratory in nature. The aim of the study as explained in Chapter 1 is to develop a comprehensive sustainability driven IS audit framework that is to explore and to identify issues relating to the existing IS audit practice. This is well suited within the interpretivist paradigm as discussed by (Orlikowski and Baroudi, 1988). This research does not aim to prove a hypothesis, but explores and explains how certain factors are related and are interdependent on particular social settings and also to address the complexity of the situation (Oates, 2006).

Second, this research investigates the perceptions of IS auditors, users and public in which their responds provide an opportunity to focus on significant issues in IS and help to identify areas for improvement. The development of the framework requires detailed investigation and understanding of sustainability and IS audit. Sustainability has many interpretations according to the field it used and applied, so its concept may be interpreted in differently by many organisations, people and in different domains. IS audit involves principles, techniques and specific criteria to provide independent assurance on the IS in a public organisation. Although the positivist approach can measure the phenomenon under study, the role of the researcher is limited to data collection, generalise findings to a population, and having minimal interaction with respondents. Under the interpretive approach, it is possible to understand the context of the phenomena as the researcher is able to integrate a human interest into a study, interpret values, experiences, and cultural phenomena in order to understand phenomena and shared meanings with respondents. In other words, the interpretive approach allows the researcher to explore the current practise of IS auditing and its level of complexity through the survey of IS auditors that expressed and discussed their experience, knowledge and competency in conducting audit work.

3.2 Research methods

3.2.1 Qualitative and quantitative research methods

The nature of qualitative research focuses on the examination of people's words and actions Maykut and Morehouse (1994; (Ashley and Boyd, 2006) and is particularly useful for exploring concepts, developing a model and/or a framework, and investigating sensitive issues. Qualitative research comprise of five general designs; narrative, phenomenology, grounded theory, ethnography and case study (Creswell, 2003). Quantitative research is concerned with scientific hypotheses' generation and the researchers set themselves separate from the testing process. Quantitative research is a more logical approach since people's opinion is interpreted in a statistical and numerical manner. With this practise, quantitative researchers neglect social and cultural constructions and the correlation between these two variables (Ashley and Boyd, 2006). The integration between qualitative and quantitative approaches is known as mixed methods and findings and conclusions are drawn by using both approaches (Creswell, 2003; Ostlund *et al.*, 2011). It is claimed that a mixed method approach is able to produce a concrete outcome as it combines an 'analytic' approach to understand variables (quantitative) or a 'systemic' approach to understand the interaction of variables (qualitative). In addition to a mixed methods approach, (Malina, Nørreklit and

Selto, 2011) claimed that using multiple methods and sources of data collection aids in producing ample evidence to address the research questions.

A mixed method approach is considered for this research due to the following reasons; In line with an interpretive epistemology, this approach is more relevant as mixed method research allows the researcher to analyse both data sets and interpret them to better understand the research problem (Creswell, 2003). The combination of qualitative and quantitative analysis enabled researcher to explore critical aspects and to confirm findings from the quantitative analysis.

From the IS audit perspective, this research is aim to explore the 1) limitation of IS audit practice, 2) consistent view on IS audit improvement and 3) to produce effective IS audit judgment. This approach can guide the researcher in meeting the objective of the study by exploring the role of the main actors that have an influence on conducting a sustainability driven in IS audit, how these actors perceive sustainability and how they can perform it. The interpretation of their perception towards sustainability dimensions is conducted through direct participation of the researcher who is an integral part of the study. In addition, the mixed method study allows data to be gathered from multiple sources.

This research focused not only on the application of theory but also on testing a framework and answering whether the proposed framework can enhance IS audit work and produce effective IS audit judgment from a sustainability perspective.

3.2.2 Case study

A case study research is selected for this research. A case study is defined as a strategy to focus on understanding the dynamics present within single settings (Eisenhardt, 1989; Klein and Myers, 1999; Qu and Dumay, 2011) claimed that a case study research is a valid research approach in information systems research and applies a multiple perspective as way to increase the validity of research findings (Walsham, 1995). There are three major research methods which are related to case studies; survey, experiment or controlled experiment and action research. A case study is used for exploratory and descriptive purposes. (Klein and Myers, 1999) defined three types of case study depending on the research perspective; positivist, critical and interpretive. When conducting a case study, the following process are involved (Runeson and Host, 2008); case study design, data collection and analysing data.

- Data collection

There are different sources of information that can be gathered and used in a case study either with quantitative, qualitative and mixed methods techniques. A number of data collection methods can be applied to a case study research, including document analysis, surveys, questionnaires, Delphi process, observations, interviews, archive analysis and physical artefacts such as devices, outputs and tools. As it provides a large number of potential data collection options, a case study research is a flexible tool for managers who want to make sense of specific issues or problems in the workplace (Turner and Danks, 2014). In response to data collection, this research applied a triangulation method for combining the data collected from different IS auditors (internal and external) and different organisations (the NAD and SAI) as well as triangulation by method (observation, interviews, documents, etc). This triangulation provides ‘stronger substantiation of construct and hypotheses’ (Eisenhardt, 1989).

i) Interviews

The main data techniques used in this research were interviews, group discussion, and secondary data analysis and participant observation. In qualitative research, there are two types of interviews; structured and semi-structured interview. A structured interview is rigid as the interviewer reads from a script and findings are generally straightforward. Unstructured interviews tend to be very similar to informal conversation as the interviewers do not know in advance all the necessary questions. Generally, semi-structured interview is the most common of all qualitative research methods (Alvesson and Deetz, 2000; (Qu and Dumay, 2011). The semi-structured is seen to be flexible, accessible, intelligible and capable of disclosing important and hidden facts of human and organisational behaviour. Often, it is the most effective and convenient means of gathering information (Kvale and Brinkmann, 2009; (Qu and Dumay, 2011). In this research, triangulated semi-structured interviews were performed in combination with surveys. Two versions of interview protocols were developed, one in Malaysian Language and another in English. Interviews were conducted during the initial survey to investigate the existing IS audit practice and later were performed to evaluate the SISA framework. All interviews were transcribed into texts using Microsoft Word and supplementary notes were also taken during the fieldwork. Interview transcripts and written notes were analysed systematically through iterative and repeated reading for the researcher to gain understanding of each interviewee’s viewpoint.

ii) Participant observations

In this research, participant observations were conducted to investigate how a certain task is performed. Participant observations were recorded and analysed.

iii) Secondary data analysis

Document analysis was used in this research which include reports from the Auditor General, minutes of meetings, IS Audit Guidelines, standards and best practices.

3.2.3 Analysing data

It is essential to evaluate data to identify relationships between the program, group, person, or process that had been identified in the problem statement. These relationships should address the research questions. (Eisenhardt, 1989) suggested analysing data between cases followed by cross-checking data between cases. Once each individual case has been analysed, similar themes between cases can be identified. (Dooley, 2002; (Turner and Danks, 2014) claimed that that there are two types of analysis in a case study research: structural analysis and reflective analysis. Structural analysis focuses on identifying patterns, while reflective analysis utilises the researcher's personal judgment to infer conclusions. This research applied a reflective analysis, that makes use of all relevant evidence, explore in detail all interpretation, and address the most significant aspect of the IS audit and sustainability.

3.3 Research design

This research focuses on the descriptive theory and the development of related procedures to facilitate IS auditors to evaluate IS control in public sector organisation. When establishing research design, the following criteria were considered:

- Establish a sound basis of knowledge about sustainability dimensions (economic, environmental, social and, technological),
- Include guidance on how to apply the descriptive theories,
- Different public sector organisations were selected for testing the proposed framework,
- The researcher was directly involved in testing the viability and relevancy of the framework,
- Experienced IS auditors from both departments (internal and external audit) were asked to evaluate the practicality of the proposed framework.

This research seeks to investigate the role of sustainability, concept and dimension and how these can be embedded and applied to IS audit practice for contributing IS success in public sector organisations. The focus area of investigation in an IS audit is the evaluation of control and risk assessment. The investigation is conducted by exploring the current IS audit practice from IS audit practitioners, users and the related literature on IS audit. In developing the research objective, this research explored the current practices of IS implementation in public sector organisations, and the expectations of key users (organisation, user and auditor) in relation to IS investment and IS adoption to organisation. After developing a comprehensive understanding on practical situations and its limitations, this research aimed to generate future-oriented concepts that include reasoning with uncertainty for a meaningful IS audit decision. The research focuses on socio-technical relationships in order to achieve the research objective and the interpretive approach allows the researcher to explore the current practices of IS auditing and its level of complexity through the survey of auditors that expressed their experience, knowledge and competency in conducting audit work. The summary of the research design, method and underlying steps for empirical testing of the framework is shown in Figure 3.1

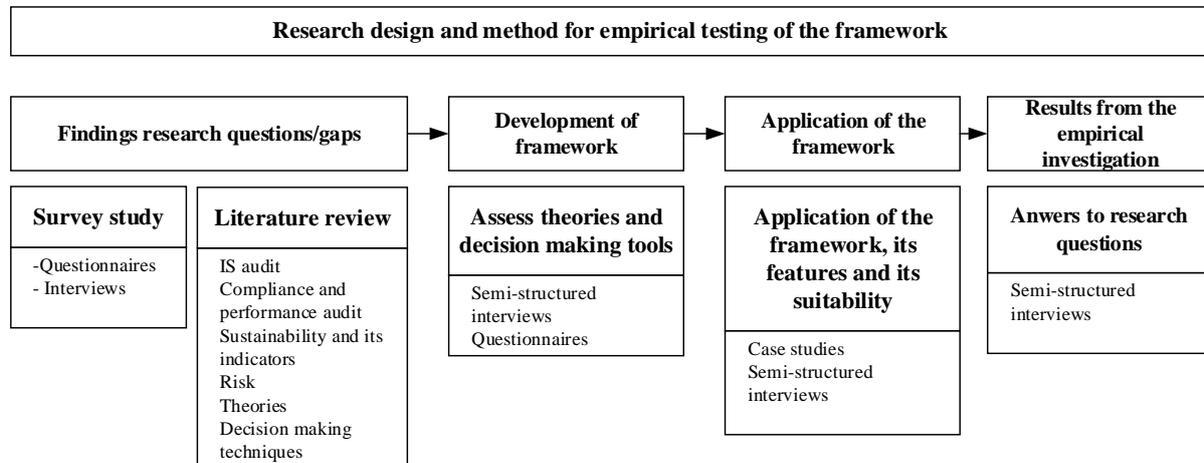


Fig 3.1 Summary of research design

The research was conducted into the following phases:

Phase 1 Initial survey – identifying current IS audit practice

The state of the art in sustainability and IS audit was constructed by reviewing the literature on sustainability and sustainability in information systems. The findings from the literature review was used to define issues of the existing IS audit practice. Empirical studies were conducted to investigate IS audit practice in public sector organisation and a mixed methods approach was followed to for triangulation purposes which gives a research data reliability and validity. The quantitative method involved the development of survey which was distributed to 80 IS respondents.

The qualitative method selected to triangulate the data was interviews. A set of semi-structured interviews was conducted with 25 IS auditors to confirm the findings from the survey and to explore the current state of IS audit, the expectations of the Auditor General, and the limitations of IS audit. This phase provided the foundation for developing the framework.

Phase 2 The development of the SISA framework

This phase consisted of defining IS audit criteria based on sustainability dimensions, applying Demspster-Shafer theory to evaluate IS controls and measuring risk probability value. Four sustainability dimensions are considered important in the developing of IS audit criteria. In SISA development, risk assessment is considered to evaluate risk factor taking into account the adequacy of existing controls and to decide whether or not the risk is acceptable. It is essential to measure the magnitude of impact of risk factor to sustainability dimensions. Therefore in this context, the following aspects are included;

- a) Sustainability dimensions and the adequacy of IS controls in relation to sustainability dimensions;
- b) The identification of value of risk factors;
- c) Identification of risk probability, impact and risk exposure values.

In order to provide precision judgment of the IS controls, the D-S theory is used to measure the adequacy of the IS controls provided by the public sector organisation. The D-S theory is selected as it is capable to collect multiple evidences including uncertain or incomplete information to support decision making. The D-S theory provides a mechanism to handle conflict in evidence in order to derive a common-sense expectation. By using the D-S theory to evaluate IS controls, it facilitates IS auditors to deal with risk and uncertainty and make

them confidence with their own judgment. In this research, the MS Excel Spreadsheet were used to program logic for D-S theory, to combine a large number of independent items of evidence and also to derive at a risk exposure value.

Phase 3 Evaluation case studies

This phase introduced the proposed framework to IS audit practitioners, explained how it will improve the IS audit process and used theory and decision making technique in concluding IS audit results. Three in-depth case studies were conducted to evaluate SISA in a real IS audit environment. The case studies began with an entrance meeting between the audit team and the auditee to set the IS audit objective, scope, methodology and related IS audit procedures. Audit evidence was acquired by using several audit techniques including walk through test, physical inspection, reconciliation, survey and interview with auditees. In addition, secondary information was gathered from relevant documents such as IS contract, Budget Book, minutes of meeting, and Policies and Procedures Handbook and kept in the audit working paper file.

Firstly, IS auditors were introduced to SISA and related procedures involved in each activity. This briefing was conducted in one day. It involved explanation on sustainability dimensions, establishing IS audit criteria using the sustainability dimensions and briefing on the D-S theory. IS auditors were also trained in selecting sustainability indicator and how to evaluate IS controls based on the degree of belief. During the audit execution, the researcher was around to observe and to explain further the SISA procedures with which IS auditors might face difficulties to proceed. The IS audit team performed two main activities during the IS audit execution; it produced a sustainability dimensions register (economic register, environmental register, social register and technological register) and it applied Excel as in Microsoft Office to update their degree of belief on IS control and for risk assessment. The sustainability register allowed the IS audit team to document the IS audit area that had been examined and the level of risk. The result obtained from Excel guide auditor was used to conclude on risk exposure and level of IS sustainability. During the IS control assessment, the IS audit team developed a survey and interviewed the personnel about the adequacy of the IS controls and obtained appropriate and sufficient evidence within this process. When performing the IS audit work, the IS audit team recorded audit findings and kept relevant documents in audit working paper files.

When SISA was completely performed by the IS audit team, they held an exit conference with the auditee to discuss the audit findings particularly on areas with significant risk exposure. This stage was also performed over an entire working day to allow a detailed discussion on findings. During this stage, the IS audit team highlighted issues or problems of IS within the economic, environmental, social and technological dimensions. The outcome of this stage was the brief report for auditees and top management.

Phase 4 Discussion on the usability of SISA

When the case studies were completed, an attempt was made to judge the practicality and usability of SISA to enhance the IS audit work. This research applied two methods of analysing the practicality and usability of SISA; first by comparing the findings of SISA with previous IS audit findings and second by organising a focus group interview to explore their feedback and reaction to SISA. Direct questions were asked about the usefulness of SISA to provide effective judgment on IS control evaluation and audit report. Interviews conducted were semi-structured and involved 15 IS auditors from the NAD and 5 from SAI. At this stage, IS auditors were encouraged to give suggestions or comments about procedures on IS control evaluation, risk analysis and finalising IS audit findings.

3.4 Summary

This chapter has outlined the approach adopted in this research. The interpretive research explores the research domain of study by applying explanatory case studies and a qualitative method analysis.

CHAPTER 4

The Sustainability driven IS audit framework (SISA)

4 Introduction

This chapter presents the proposed framework for the Sustainability driven Information Systems audit. To develop such a framework, it is necessary to understand the requirements which are necessary to support a comprehensive IS audit practice considering sustainable dimensions. Sustainability is the ability for a system to operate with expected functionalities and user's needs for business continuity. For a sustainable system, this research considers sustainability from four different dimensions, i.e., economic, environmental, social and technological, which were identified as IS audit criteria. These four dimensions need to be analysed to address the challenges of IS, such as the growth of technologies, hidden costs, security and green IT requirements. This framework adopts and includes various concepts and processes which are presented in this chapter.

4.1 SISA framework requirements

The requirements for the SISA were derived from and developed based on the literature review and the survey study. The motivation for these requirements is to add value to the current IS audit practice in fulfilling the changing demands from the public, the users and stakeholders specifically when it comes to factors related to the economy, environment, society and technology (Asif *et al.*, 2013). In order to implement the framework, the five following requirements are essential:

Requirement 1: The framework should consider the relevant and determining factors which can support a sustainable information system. The selected sustainability factors are economic, environmental, social and technological.

Requirement 2: A list of indicators is necessary to measure IS control and these indicators are also used as an additional control for IS.

Requirement 3: Risk assessment is performed to measure value of probability and risk impact. Risk assessment shall consider the potential risks that could have an impact on the IS project and the overall audit.

Requirement 4: The framework shall provide guidelines for a comprehensive audit towards achieving a sustainable information system. Therefore, it should include and implement the necessary concepts and processes to guide the auditor in a systematic way.

Requirement 5: The outputs produced by the process shall guide the auditor to make the audit decision based on the context.

4.2 The SISA Framework

Sustainability includes strategies, design, development, implementation and appropriate sustainability indicator to the achievement of objectives. The SISA framework was designed by integrating conceptual and practical determinants which include the principle or values, flow of actions, processes and strategies to achieve sustainability IS in public sector organisation. Therefore, the proposed framework consists of a language with a set of concepts and a process to support sustainable driven IS audit. The concepts are based on information system, sustainability, and audit concepts. The framework demonstrates an important set of characteristics to address the identified requirements. These are:

- i) The conceptual view unifies audit, sustainability and information system concepts and enables an auditor to evaluate the system based on audit criteria, sustainable indicators and risk exposure.
- ii) It supports providing early warnings of potential risks for the overall audit and information system and assess the risk so that appropriate control actions can be taken before the risk can be materialized.
- iii) It uses the same concepts throughout the process to overcome any misunderstandings due to different concepts while performing the audit activities.
- iv) The process introduces a structure approach to the analysis of the audit context considering sustainable dimensions and as such it produces a comprehensive audit report.

4.2.1 Conceptual view of SISA

The concept of IS audit emphasises the provision of assurance that a system or automated process will meet its objectives. In particular, the IS audit focuses on the management's

responsibility of controls over information assets and process by adhering to specific IS standards, policies and procedures. The risk assessment is performed by the public sector organization to identify the risks associated to information systems and resources, and for identifying key areas to be audited. In this research, IS audit introduces the concept of sustainability to develop a sustainability driven IS audit approach. To plan, begin, and implement sustainability driven in IS audit, it is necessary to combine the concepts from the existing IS audit practice such as actor, audit criteria, risk, report and proposed concepts by this work such as value creation, sustainability, and sustainable IS. This section provides explanations of the concept preference in sustainability and IS audit as well as the relationship between the concepts. An overview of the concepts is shown in Figure 4.1.

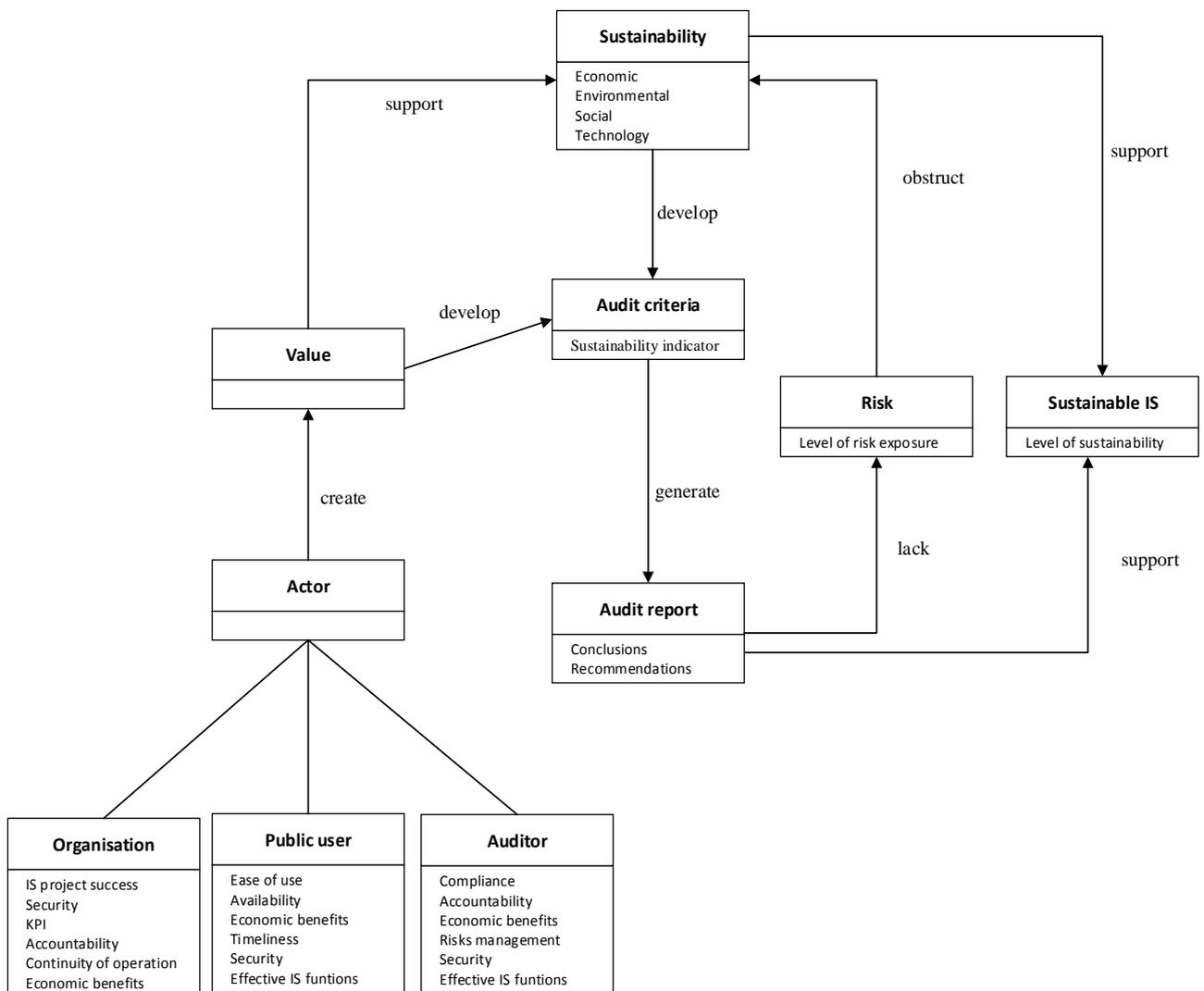


Fig 4.1 Conceptual view

Actor

An actor is as an entity that has strategic goals and intentions within a system or an organisational setting (Mouratidis, et al., 2012). An actor can be an organisation, system, or a human entity. In particular, we consider three different types of actors in our work; the Organisation, the User and the Auditor). The Organisation refers to the public organization in which the Information Systems are investigated by the public IS auditor, the user refers to the stakeholder who is also the community of the public organisation, and the auditor refers to the IS auditor of the public organisation. These three actors are the key users within our context.

Value creation

The value creation, as previously stated, is the expectation and benefits from the system. In particular, it is the actor's expectations from the overall system. The actor's expectation is the critical factor against which the success of a delivered IS will be judged. Even though the key users have different expectations, they have in common their needs which are basically associated with value for money of IS investment, continuity of service and security. These elements also contain a reference to sustainability dimensions for which the IS audit criteria is oriented to.

Sustainability

Three viewpoints of the sustainability concept were derived from the literature; these are: continuous improvement, ability to address efficiency and effectiveness of information systems and, resource savings. According to this view, sustainability dimensions focus on economic, environmental, social, and technological aspects of IS. The economic dimension refers to financial management or cost effectiveness of the IS. The environmental dimension refers to green IS practices which include energy saving, paperless practices, shared IT equipment and IS disposal policy. The social dimension is associated with organisation, public users and auditor's expectation of the IS such as security, accountability and key performance indicator of the IS. The technology-related dimension refers to the system security, flexibility and scalability of IS.

Audit criteria

Audit criteria are described as standards or controls against which an auditor assesses the actual condition of the information system implementation. In practice, IS audit criteria consist of laws, standards, best practices, expert opinions or requirements that need to be accomplished

by the organisation. Audit criteria include a sustainability indicator to measure progress toward building sustainability IS.

Audit report

The audit report is the independent contribution of an IS auditor with the aim to improve the current status of IS. The concept of extended view on the audit is applied in SISA where IS auditors are required to report on the level of sustainability of the IS. Additional views on IS audit findings in relation to economic, environmental, social, and technological factors means a change of focus of IS auditors verification of formal aspects of IS audit to the essential aspects of the sustainability dimensions. The relation between sustainability dimensions, risk assessment and risk impact assessment can determine the new shape of justification in audit findings and make a concrete audit report.

Risk

Risks are the potential negative consequences within the system for not achieving the sustainability of the system and not meeting the actors' expectations. Risk assessment is conducted during audit planning as a basis for the identification of negative consequences that may impair the effectiveness in relation to its design, development and implementation. Generally, such process should include how to identify the possible risks from the audit perspectives and to analyze the risks so that appropriate control actions could be identified and implemented.

Sustainable IS

Sustainable IS is determined according to the level of risk exposure and comprises of three categories; effective, reasonable and ineffective. The categories are defined as follows.

- *Effective* is defined when the value of risk exposure is at Very Low to Low level , that is between 0.0-0.4;

- *Reasonable* is defined when the value of risk exposure is at Medium level, that is between 0.41-0.6;
- *Ineffective* is defined when the value of risk exposure is at High to Extreme level, that is between 0.61-1.0.

4.2.2 Audit process in SISA

The audit process in SISA is inclusion of a risk-based approach and sustainability assessment. The SISA audit process comprises of three sequential phases, namely audit plan, audit execution (collect and analyse evidence), and conclusion & reporting. Each phase has its own steps. An IS auditor is an individual/organisation authorised to perform an independent examination on and verification of transactions, records, activities, programmes and projects. An Auditee represents an individual/organisation who/which is being audited. This may be Ministries, Departments and other public sector organisations. Details of SISA process are depicted in Figure 4.2.

Activity 1: Prepare IS audit plan in SISA

Sustainability benefits can be generated through an IS audit plan and are delivered through IS audit criteria. The IS audit plan serves as a tool for IS auditors to highlight area to be audited, the background of the entity, the complexity and the critical area of the information systems to be audited and appropriate selected audit techniques to be performed. In what follows, the steps taken to prepare an IS audit plan in SISA are illustrated in Figure 4.2.

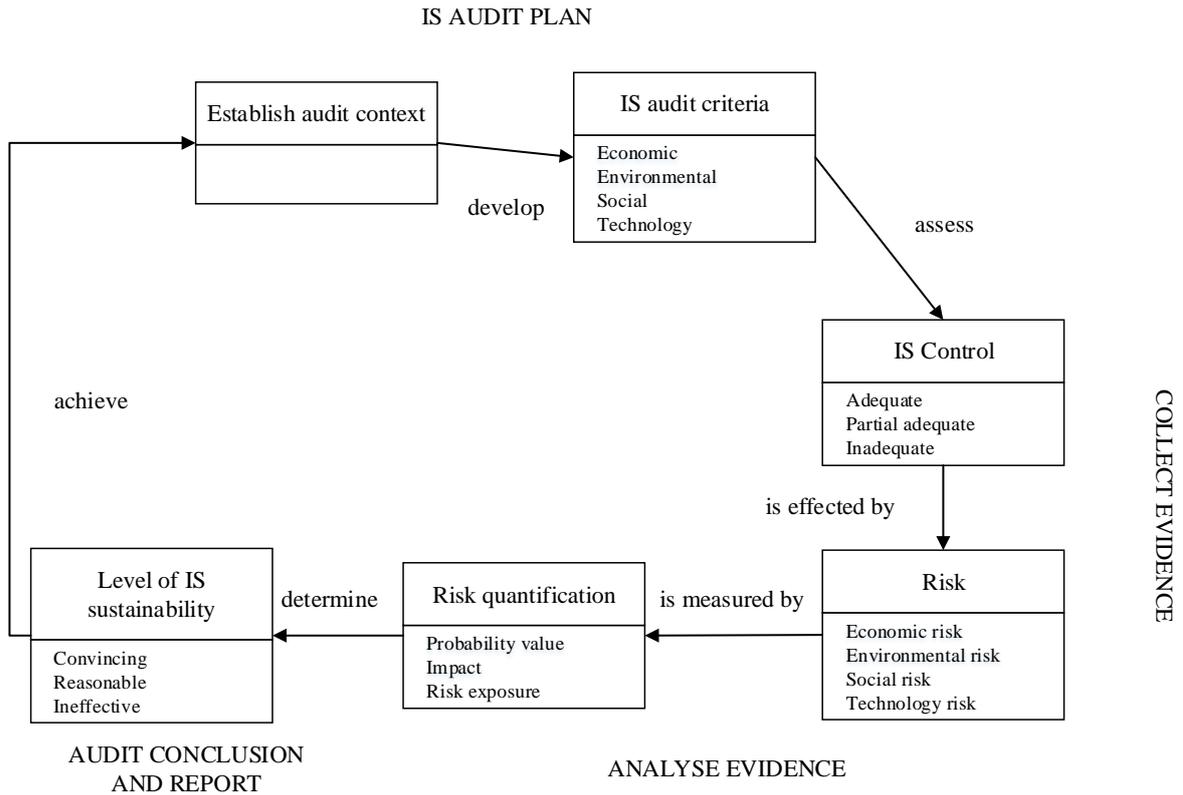


Fig 4.2 SISA process

Step 1.1 Establish IS audit context

In relation to a sustainability perspective, the IS audit objective aims to identify the level of sustainability of the IS adopted by an organisation. In addition to the current IS audit practices, sustainability enhances audit procedures to consider short term and long term factors that may influence the IS activities regarding their support to an organisation to achieve its business objectives. In establishing IS audit objective(s), actors’ requirements are taken into account as a base to assess the benefits of IS and IS effectiveness to deliver services to the public. In addition to audit objective(s), the audit scope is also defined as to assist IS auditors in identifying key systems to be audited, related programmes, modules or unit of IS to be reviewed. An audit methodology comprises of audit techniques to be performed for data gathering which include interviews, questionnaires, walk through tests, document reviews, physical inspections and observations. In this research, the audit is intended to verify that:

- i) The IS controls are operating in an effective and efficient manner under a state of sustainability dimensions;
- ii) The critical area of risks are identified as a result of IS controls evaluation;

- iii) To produce an IS audit report in relation to the level of sustainability of IS of public sector organisation.

The scope of IS audit within SISA may include the areas to be audited, a particular duration of a year, the key systems, programme, modules or unit within public sector organisation. In the course of preparing an IS audit plan, a set of procedures known as audit methodology are established to assess the systems, control, risk, and operational activities of the organisation. The audit methodology involves testing methods to examine accuracy, adequacy or efficiency of the IS control. Once the context is completely developed, the next step is to define the IS audit criteria.

Step 1.2 Establish IS audit criteria

Normally, IS audit criteria are standards or controls against which an auditor assesses the actual condition of the information system implementation. In SISA, audit criteria are developed based on sustainability dimensions which are economic, environmental, social, and technological. The evaluation of the effect of the above dimensions on IS audit must involve the sustainability indicator that demonstrate the contribution of the sustainability to minimize risk or errors in IS. For example, the effect of economic sustainability in IS involve the improvement of financial management or cost effectiveness for IS investment. In this view, an IS auditor is required to examine the validity of financial transactions, completeness of the transactions processed, and examine the IS cost allocation. After finalizing IS audit criteria in SISA, which are environmental, social and technological, the IS auditors proceed with risk assessment procedures. Details of sustainability dimension and sub-criteria are shown in Figure 4.3. Once the sustainability dimension and the sub-criteria are defined, it is essential for IS auditors to develop or select an appropriate sustainability indicator to be used in IS control evaluation.

Step 1.3 Construction of sustainability indicator

The sustainability indicator is constructed based on the preliminary requirements of sustainability, its criteria and sub-criteria. It is essential to verify if there is any indicator already available in the organisation to measure economic, environmental, social, and technological dimensions. If there is no indicator available, a list of performance indicators related to the sustainability dimensions is selected. The indicators selected are customised according to the context of the organisation so as to achieve the sustainability objectives.

Then, the attributes of the indicators, its formula and sources of data are finalised with the IS audit process. The summary of the indicators designed can be seen in Table 4.1.

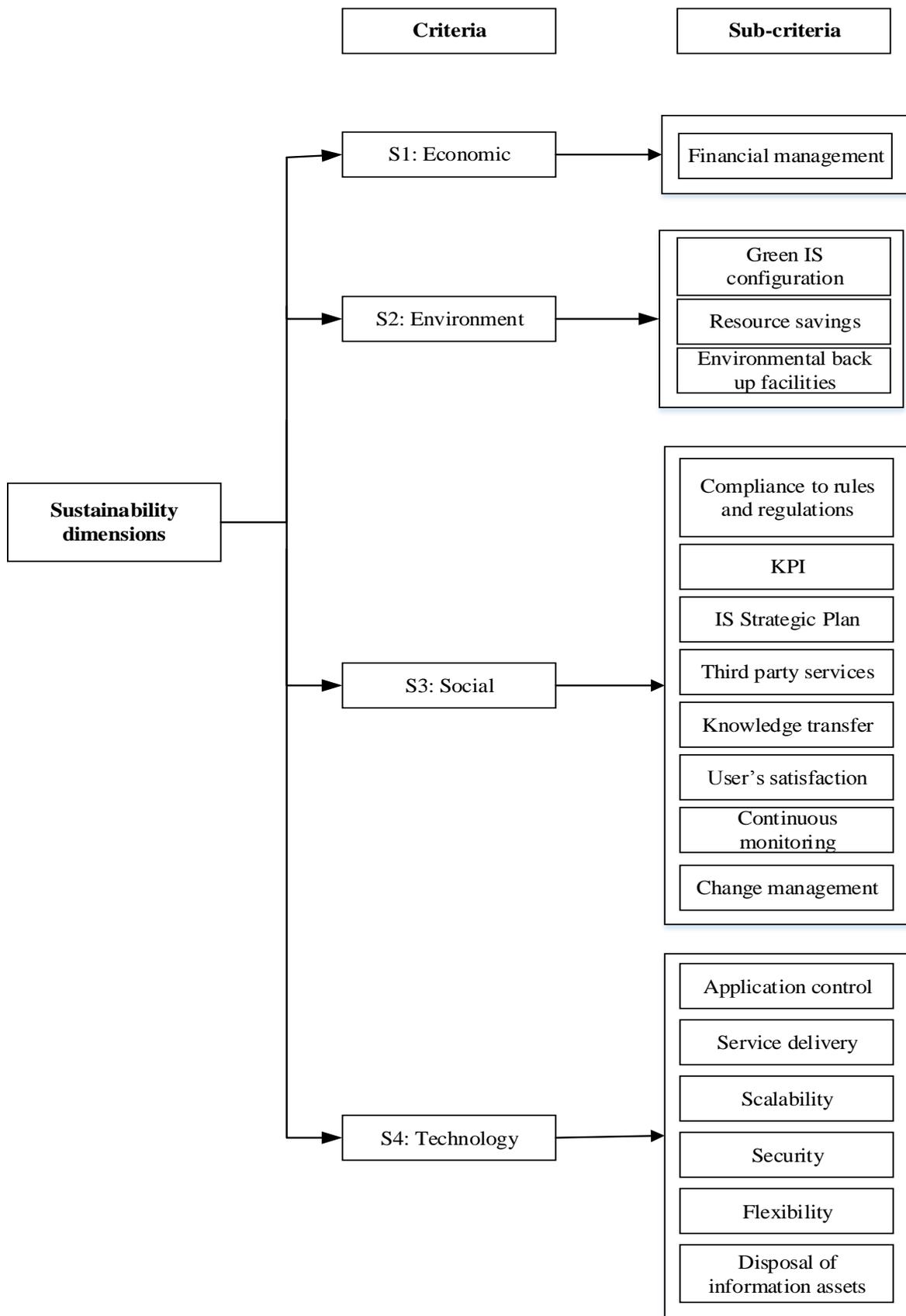


Fig 4.3 Sustainability dimensions and sub-criteria

CRITERIA	SUB-CRITERIA	INDICATOR
ECONOMIC	Cost effectiveness	<ul style="list-style-type: none"> • Satisfaction assessment on cost and benefit
ENVIRONMENT	Green IS configuration Paperless Energy savings	<ul style="list-style-type: none"> • Percentage savings for paperless environment • Percentage savings for recycling • No of IT equipment shared • Availability of green oriented disposal policy • Percentage energy savings • Percentage of reduction for generated waste.
SOCIAL	Compliance to rules and regulations Outsourcing Key Performance Indicator IS Strategic Plan Knowledge transfer User's satisfaction Continuous monitoring Procurement process	<ul style="list-style-type: none"> • Satisfaction assessment on compliance with rules and regulations (Percentage of objective attained) • Satisfaction assessment of control policies and procedures for application control (Percentage of objective attained) • Satisfaction assessment of policies and procedures for managing third party provider (Percentage of objective attained in Service Level Agreement) • Percentage of employees who know the system's function (responsiveness, user friendly) • Percentage of employees who can perform system maintenance procedures • Satisfaction assessment for KPI achievement
TECHNOLOGY	Application control Service delivery Flexibility Security Scalability IS disposal procedures	<ul style="list-style-type: none"> • No of system's incident reported • Average time for system's failures • Percentage of accurate and reliable information produced by the IS • Average time for output generated • Average time for application processing • No of interaction for continuity of operation (the availability of back-up plan, storage facilities) • Satisfaction assessment of system scalability • Average time for network connectivity • Percentage of accurate output generated according to sources • No of report produced from the audit trails. • Average time taken for the system to be activated after service down • Average time taken for the data to be restored after service down • Ability to add, modify and remove any software, hardware or data components from the IS infrastructure • Availability of destruction procedures

Table 4.1 Sustainability indicator

Activity 2 Risk assessment

The proposed risk assessment in SISA is based on the degree of belief relating to the uncertainty involved in the IS control evaluation. The process consists of three sequential systematic collections of activities and each one of these activities has specific inputs and results in specific outputs artefacts. The risk assessment begins with defining IS sustainability and identifying risks and IS controls. Figure 4.4 specifies the process of the risk assessment approach.

Step 2.1 Define IS sustainability

This step defines the sustainability driven IS audit to justify the level of IS sustainability in the public sector. In this view, it is essential to consider appropriate sustainability indicators to measure IS controls. Assessing IS includes evaluation on IS investment, security, third party services and the availability of IS services.

Step 2.2 Assess IS controls and estimate risks

This step assesses the possibility of IS control to mitigate risk from economic, environmental, social and technological dimensions. In this step, auditors gather evidence based on the assessment of four sustainability dimensions (economic, environment, social, and technological). These data are obtained via audit techniques such as inspection, review documents, records, transactions produced by the IS, surveys, re-performance, and interviews of the practitioners and experts within the organization. The method used to gather these data is influenced by the factors of the sub-criteria. In this step, the threats on IS controls are estimated based on collected evidence. The D-S theory is used to provide predictions of the adequacy of IS controls and to combine multiple pieces of evidence. The results of IS controls represent the risk factor of each sustainability dimension.

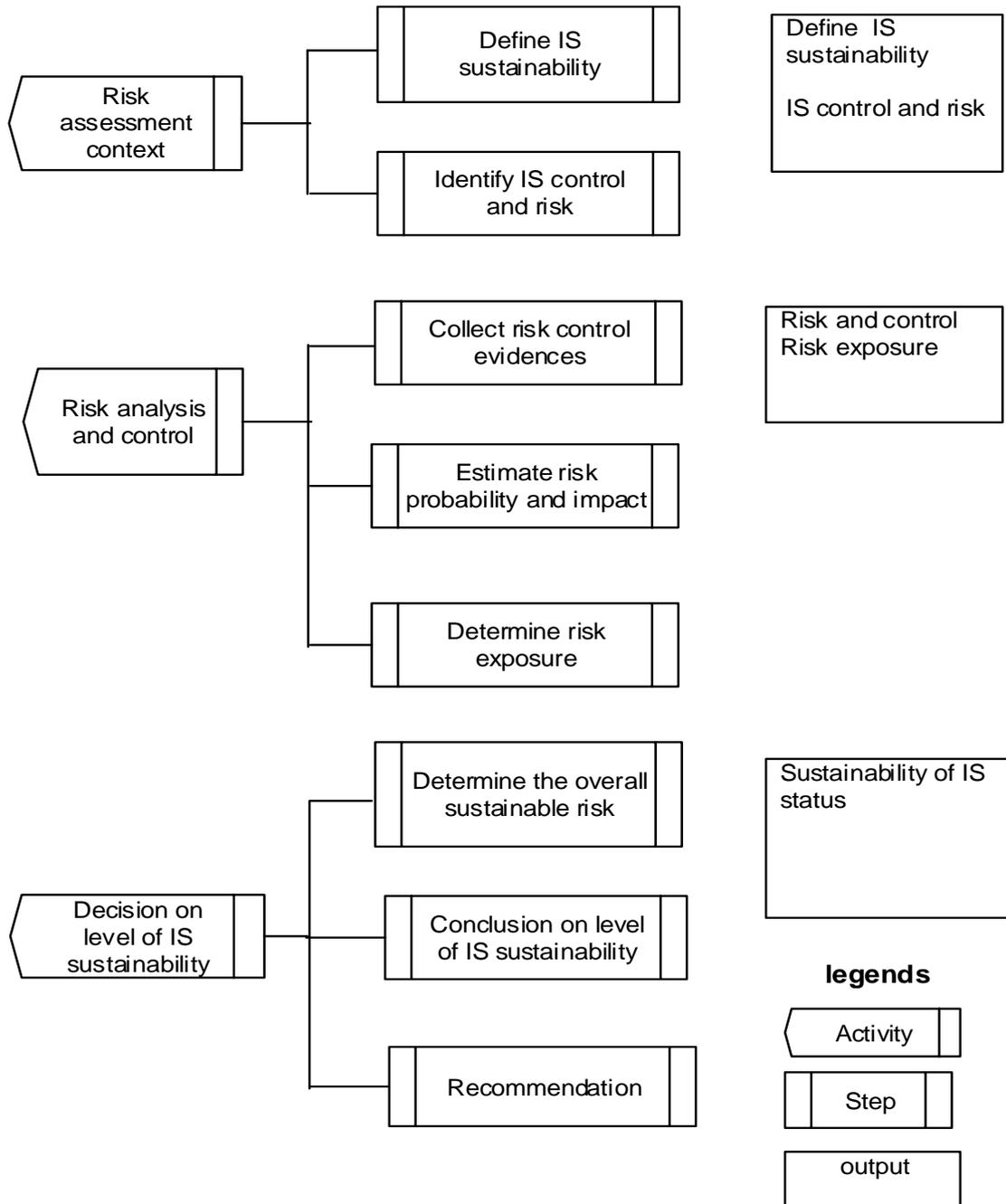


Fig 4.4 Risk assessment approach

Activity 3 Risks analysis and control

Once the risk factors for each sustainability dimension are identified, it is necessary to calculate the risk exposure in order to determine its severity. This research follows subjective judgement depending on individual perception as a semi-quantitative assessment for determining the risk exposure value.

Step 3.1 Collect risks control evidence

In this step, IS auditors gather evidence based on the assessment of four sustainability dimensions (economic, environment, social, and technological). These data are obtained via several audit techniques such as walk through test, document review, by using CAATTs, surveys, and interviews of the users and management within the organization. The method used to gather these data is influenced by the factors of the sub-criteria. For instance, an economic sub-criterion is financial management and the influencing factors for financial management are accurate accounting procedures, acceptable variance, account for contingency, and analysis of trend of payment, ensuring that cost of storage capacity is for at least 5 years, training and maintenance of cost. It is worth mentioning that the data used for sub criteria are collected from IS contractual agreement, electronic payment systems, electronic procurement systems and annual budget documents.

This research used the Dempster's rule as simplified by Shrivastava to combine multiple items of evidence for a risk factor. For example,

Control 1: $m_{C1}(a)$, $m_{C1}(\sim a)$, $m_{C1}(\{a, \sim a\})$

Control 2: $m_{C2}(a)$, $m_{C2}(\sim a)$, $m_{C2}(\{a, \sim a\})$

Control n : $m_{Cn}(a)$, $m_{Cn}(\sim a)$, $m_{Cn}(\{a, \sim a\})$

Then, combine and propagate the belief masses (m-values) from several controls to their related risk factor. This research used (Sun, Srivastava and J.Mock, 2006) to derive m-value for risk through 'AND' relational node. The value of K is written as follows:

$$\mathbf{K} = \sum_{i=1-n} (1 - m_{C1..n}(a)) + 1 - \sum_{i=1-n} (1 - m_{C1..n}(\sim a)) - \sum_{i=1-n} (m_{C1..n}(\{a, \sim a\})) \quad (1)$$

and the m-values are:

$$m_{C1}(a) = 1 - \sum_{i=1-n} ((1 - m_{C1}(a))/K) \quad (2)$$

$$m_{C1}(\sim a) = 1 - \sum_{i=1-n} ((1 - m_{C1}(\sim a))/K) \quad (3)$$

$$m_{C1}(\{a, \sim a\}) = \sum_{i=1-n} (m_{C1}(\{a, \sim a\})/K) \quad (4)$$

The belief and plausibility functions are given below:

$$\text{Bel} = \text{Bel}(a),$$

$$\text{Pl}(a) = 1 - \text{Bel}(\sim a) = 1 - (\sim a) = \sum_{i=1-n} ((1 - m_{C1}(\sim a))/K) \quad (5)$$

$$\text{Pl}(\sim a) = 1 - \text{Bel}(a) = 1 - m(a) = \sum_{i=1-n} ((1 - m_{C1}(a))/K) \quad (6)$$

Step 3.2 Estimate risk probability and impact

This step estimates the risks event probability based on the belief of existing controls for the risk mitigation. Evidence is gathered pertaining to particular assertions and is measured to determine the overall belief and plausibility whether the assertion is adequate, partially adequate or inadequate. The Dempster's rule as simplified by Shrivastava is used to combine multiple pieces of evidence for a risk factor. IS auditors are provided with an Audit Program to carry out assessment on IS control, see Appendix C for an example. In assessing the IS control, IS auditors are required to judge whether the existing IS control is adequate to mitigate risk. We divide the evidence into three different scales. These are given below:

- Adequate (0.51-1.0): Control exists that is able to mitigate a risk
- Partially adequate (0.21-0.5): Control exists that is either able or unable to mitigate a risk
- Inadequate (0.0-0.2): Control exists that is not able to mitigate a risk

The value of belief according to the evidence scales is as follows:

- Bel (M) = 1 implies that controls exist to mitigate risks based on the evidence,
- Bel (M) = 0 implies that there is no evidence that control exists to mitigate a risk.

There can be values between 1-0; depending on the degree of belief about the control that could mitigate the risks. If there are multiple controls for a specific risk then the m-value is assigned to each control and combined using equations (1), (2), (3), (4) and (5) to determine belief and plausibility functions. The plausibility function obtained from this step measures the maximum amount of probability that can be distributed in the element in Control (mC1...n). Using the D-S theory of belief functions, risk can be modelled by applying the notion of the plausibility (i.e. risk) of a negative outcome. The plausibility function also represents material errors that exist in the evidence and can be applied to measure a risk. Thus, the estimation of probability value of risk follows either equation (5) or (6). The probability value is estimated as follows and Table 4.2 shows the risk probability scales.

$$Prob (R_1) = Pl (R_1) = 1 - Bel (M) = 1 - (M) = \sum_{i=1-n} (1 - m_{R_1} (M)/K) \quad (7)$$

R_1 : represents the individual risk.

$Pl(R_1)$: represents plausibility function to mitigate a risk in (R_1)

Score	Likelihood	Likelihood of Occurrence
5	Expected	More than 90% chance of occurrence
4	High	65%-90 % chance of occurrence
3	Moderate	35%-65 % chance of occurrence
2	Low	10%-35% chance of occurrence
1	Not likely	Less than 10 % chance of occurrence

Table 4.2 Probability scale

This research follows five different scales to determine the impact of the risks. The scales are given below in Table 4.3

Score	Impact classification	Impact
5	Extreme	Such as significant overrun to the budget, requires additional personnel to perform business operations, severe disruption on operational activity that may lead to work/task cancellation, damage of reputation, unable to deliver key objectives of IS/cloud migration.
4	Major	Such as significant overrun to the budget, requires additional personnel to perform business operations, severe disruption on operational activity that may lead to work/task cancellation, damage of reputation, unable to deliver key objectives of IS/cloud migration.
3	Moderate	Such as short term loss due to excess consumption on energy, service disruption, unable to perform business continuity strategy for IS/cloud computing, additional resource required to execute IS/cloud's operations.
2	Minor	Such as delay in operational activities, minor impact on efficiency and environmental sustainability, and fewer IS incidents reported.
1	Incidental	Such as delay in operational activities, fewer service disruptions and IT governance compliance.

Table 4.3 Risk impact scales

Step 3.3 Determine Risk Exposure

The final step of this activity determines the risk exposure for each sustainability dimension. The risk exposure value is the multiplication of risk event probability and impact as shown in equation (8) and maps to the qualitative scales as shown in Table 4.4 to determine the level of IS sustainability.

$$RE(ri) = P \times I \quad (8)$$

ri: Individual risk of any category, i.e., economic, environmental, social and technology

i=1.....*n*

RE : Exposure of risk *ri*

P: Probability of risk *ri*

I: Impact of risk *ri*

Risk exposure level	Score	Risk exposure description
Extreme (Ineffective sustainability of IS)	0.81-1.0	Economic: Budget deficit, cloud migration is suspended. Environmental: Unable to comply with green IS strategy and cost optimisation. Social: Incapable to monitor service performance from the supplier and managing change. Technological: Incompetent to handle IS incidents, to accomplish IS control objectives or to provide security for IS or for cloud migration.
High (Ineffective sustainability of IS)	0.61-0.8	Economic: Budget deficit, cloud migration is reschedule at a later date. Environmental: Able to comply with green IS strategy but incur additional cost. Social: Incapable of monitoring service performance from the supplier and managing change. Technological: Business continuity, crisis management plan and IS strategic plan are not established.
Medium (Reasonable sustainability of IS)	0.41-0.6	Economic: Limited budget estimate, cloud migration is possible. Environmental: Only some equipment is green IS compliant due to limited budget. Social: Capable of defining service level and managing change. Technological: Business continuity, crisis management plan

		and IS strategic plan are established and but not tested.
Low (Effective sustainability of IS).	0.21-0.4	Economic: Reasonable budget estimate, adequate resource for cloud migration. Environmental: Equipment is green IS compliant. Social: Capable of defining service level and managing change. Technology: Business continuity plan, crisis management plan and disaster recovery plan are available and tested.
Very Low (Effective sustainability of IS)	0.0-0.2	Economic: Moderate budget estimate, adequate resource for cloud migration. Environmental: Equipment is green IS compliant. Social: Capable of defining service level, provides adequate IS controls, storage and managing change. Technology: Business continuity plan, crisis management plan and disaster recovery plan are available, tested and sufficient.

Table 4.4 Level of risk exposure

Activity 4 Derive audit conclusion

This final activity undertakes the decision on the level of sustainability of IS in a public sector organisation. In a context of decision making under risk, this research uses total risk exposure as a basis for reaching conclusions on the level of sustainability. This activity consists of three steps which are outlined below.

Step 4.1 Determine the overall sustainable risk

Once the risk exposure values are obtained from sustainable dimensions, each risk values from each dimensions are averaged and can be written by following equation 9.

$$Rsustainable (Economic) = \frac{Risk\ exposure\ (1) + Risk\ exposure\ (2) + Risk\ exposure\ (n)}{Number\ of\ Risk\ exposure\ (Economic)} \quad (9)$$

Similar equations are applied to environmental, social and technological dimensions. IS auditors derive conclusions based on the value of risk exposure which is used a basis to

conclude the level of IS sustainability. It may be concluded that the level of sustainability of IS according to risk exposure is as follows:

Step 4.2 Determine the level of sustainability

The level of sustainability is determined based on the overall identified sustainable risk. This research considers three different levels of sustainability. They are effective, reasonable and ineffective. Details of the judgment are described below:

Effective sustainability of IS

An effective sustainability of IS is when the level of risk exposure is between very Low to Low and the value of risk exposure is between 0.51-1.0. This judgement is concluded based on the following criteria:

- a) The number of sustainability dimensions that linked to a high risk exposure should be less than three.
- a) Risk exposure is insignificant and can be mitigated by the existing controls.
- b) The controls are adequate and have been designed in accordance with relevant legislations, regulations or best practises for the sustainability dimension which is deemed to be important.

For the purpose of cloud migration decision:

- a) Possible to migrate.
- b) There is adequate justification and documentation relevant to the cloud migration procedures and practised.
- c) The cloud migration is for noncomplex application systems or the migration size is small.

Reasonable sustainability of IS

A reasonable sustainability of IS is described when the risk exposure is at Medium level. This judgement is concluded when the following circumstances exist:

- a) The number of sustainability dimensions that linked to a high risk exposure should be less than two.
- b) There are evidence that threats or risk are manageable.

For the purpose of cloud migration decision:

- a) Possible to migrate
- b) There is adequate justification and documentation relevant to the cloud migration procedures and practised.
- c) The migration is intended for core systems of the organisation and the existing controls are effective and efficient to mitigate risks. Appropriate control measures are designed to minimise risk for each sustainability dimensions.

Ineffective sustainability of IS

Ineffective sustainability is when three or four of sustainability dimensions have high risk exposures. This judgement is issued when the following circumstances exist:

- a) The controls are not adequate to mitigate risks.
- b) The controls have not been designed in accordance with relevant legislations, regulations or best practises.

For the purpose of cloud migration decision: It is not possible to migrate.

Example of how IS audit findings can be concluded in the IS audit report

An example of how an IS auditor may articulate the audit findings for effective sustainability of IS is given below:

Audit conclusion

Based on the above findings, we conclude that a sustainable IS is derived and our IS audit objective has been met. However, there is an exceptions or weaknesses have been noted in environmental practices by the Department. The audit found that green IS policy has not been effectively practiced by the Department such as paperless practice and equipment sharing.

4.3 Generate IS audit report

The final activity consolidates the entire audit findings to come up with a conclusion. In SISA, IS auditors were required to report on the level of sustainability of the IS as well as the following elements:

- i) The SISA objective,
- ii) The IS audit scope and methodology, The IS audit criteria and sub-criteria,
- iii) Sources of evidence,
- iv) Audit findings and relevant evidence.

The audit report should highlight the three scales of sustainability level (effective, reasonable, and ineffective). If the level of sustainability is classified as ineffective, this indicates low sustainability of the IS implementation and auditors may need to justify the findings based on the high risk exposure of the sustainability dimension. For instance, 'Environmental' has ineffective level of sustainability, and sub-criteria for 'Environmental' are green IS, resource savings and power back-up supply. Among these three, if we suppose that the high risk is the power back-up supply then an IS auditor may conclude that the level of IS sustainability implemented by the public sector organization is ineffective according to the sustainability requirements. If the factor influenced is due to the 'Environmental' dimension and this results to ineffective sustainability then the organization may require executing a comprehensive revisit of the elements under the 'Environmental' factor of the IS. These findings can lead to a new data gathering and further analysis would be required to explain the weaknesses. An example on how to highlight sustainability in the audit report is shown below.

Audit findings

This study found that green IS policy has not been effectively practiced by the organization. Out of five units of the auditee organization, two units have planned to implement green IS for sharing IS equipment and exercise paperless environment. The directors of these two units agreed to execute the plan by next four months.

Corrective and/or preventive actions

Appropriate preventive actions should be taken by the organization to enhance the enforcement of Green IS policy and motivate employees work in a paperless environment for their administrative work.

Recommendations

Organization should make its employees aware of green IS, its concept and implications by providing them with training or brainstorming session. In addition, the implementation of green IS policy should be communicated effectively with users by actively involving them in each administrative, finance and operational component process.

It is important to note that the choice of SISA is directly determined by sustainability goals. Some organizations may be limited by financial resources, knowledge and have a less complex IS. Large business organization may involve integration of IS, complex and sophisticated IS where IS security is crucial. For an efficient implementation of SISA, auditors may consider changes to be made to sub-criteria as key users may have different perceptions regarding this issue depending on whether they are in small businesses or large business organizations.

4.4 Execute and reporting follow-up

The IS auditors will visit the auditee once again to examine whether the IS audit recommendations have been implemented. If the issue is significant and there is no actions have been taken, the IS auditor will need to advise to the Auditor General accordingly and will probably modify risk assessment for the next audit. Report on the follow-up consists of the following items;

- i) State matters done.
- ii) State matters outstanding.
- iii) State matters to be considered in future follow-ups.

The IS auditor may also need to inform the auditee of any outstanding matters that would be included in the Auditor General's report to Parliament. The information contained in this follow-up report should be considered in the planning phase of the next IS audit.

4.5 Summary

The chapter presents the main contribution of this thesis. The researcher propose to incorporate the sustainability dimensions into the existing IS audit practice for evaluating different aspects of IS within the public sector organizations. The proposed framework is based on the evidential reasoning approach using the D-S theory of belief and it unifies the necessary concepts relevant to audit and sustainability. It allows decision makers to justify the adequacy of controls provided by the public sector organisations to mitigate risks. The role of SISA is seen to reduce uncertainties in decision making by reviewing results, processes and input. It also facilitates coordination and communication to produce an effective audit report that provides effective value delivery to stakeholders and the public.

CHAPTER 5

Evaluation

5 Introduction

This chapter focuses on the evaluation of the proposed sustainability driven IS audit framework. The main purpose of the evaluation is to determine the applicability of the framework in a real information system audit context. This chapter also includes our initial research findings through a survey before developing the SISA framework. The main purpose of that initial survey is to understand the limitations of the existing audit practice. Therefore, the evaluation part of the research includes the results from the preliminary study relating to existing audit practice and empirical investigation through three case studies relating to the applicability of SISA framework.

5.2 Empirical investigation and data collection

The empirical investigation part presents the results from three case studies on the application of SISA framework in the public organisations. The main aim of this investigation is to evaluate the SISA framework and to determine how effectively SISA enables auditors in public sector to assess IS performance based on sustainability and potential risks. A survey and three case studies were conducted in order to formulate and test SISA framework at the perception level as well as at the action levels. The survey was distributed at initial stage of this research to better understand the current limitations of the existing IS audit practice. The survey also involved interviewing practitioners to obtain their views about IS audit. The three case studies were conducted to evaluate and confirm the practicality and the usefulness of the proposed framework. The results of the survey and case studies are related with each other and contribute to the research conclusions.

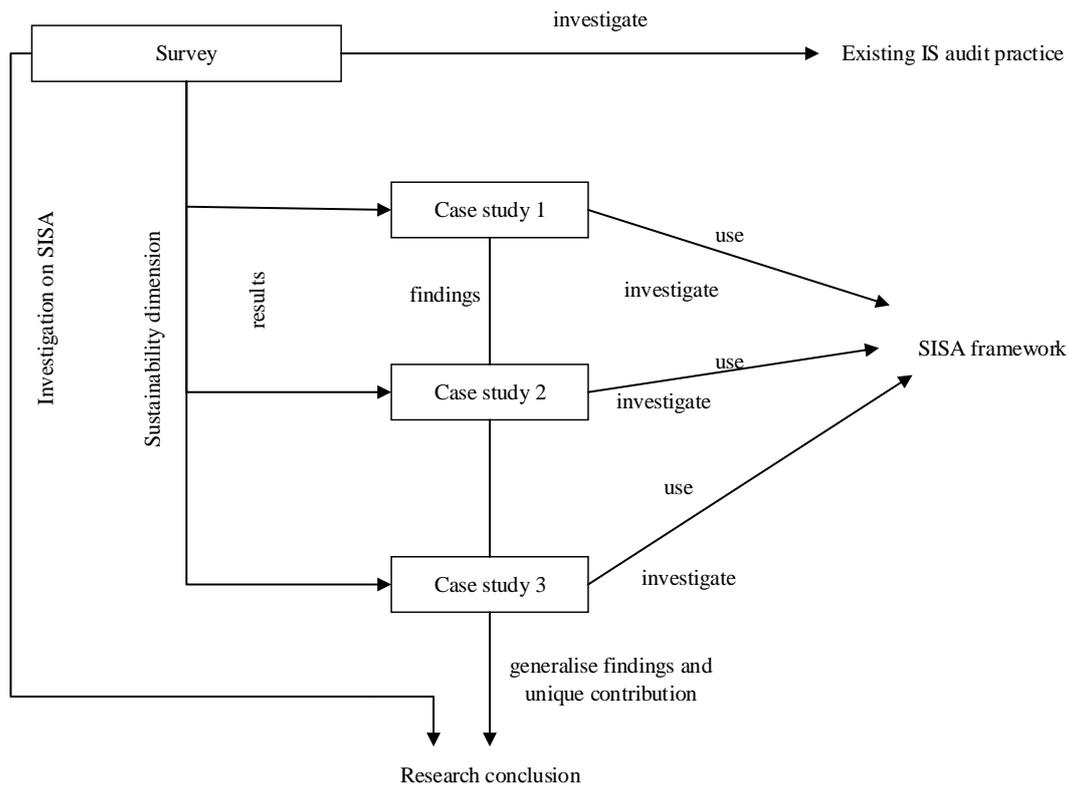


Fig 5.1 Empirical study methods and context

The first evaluation technique was a survey, and respondents were IS auditors in the NAD and the SAI, of the United Arab Emirates. The second evaluation technique was explanatory case studies conducted in both organisations.

5.2.2 Study constructs

Three main constructs were considered to evaluate the SISA framework. The constructs were investigated to arrive at definite conclusions about the SISA context.

- i) A sustainable dimension to an IS audit, which implies that an IS auditor assesses the actual condition of the IS performance from four dimensions; economic, environmental, social and technological dimensions.
- ii) A SISA method to support an IS audit, which evaluates the applicability of SISA to assist an IS auditor in examining the adequacy of IS control and with the decision making process.
- iii) A risk-based approach is effective for a sustainable IS audit, which facilitates an IS auditor to locate the most critical areas and their impact on the IS so that appropriate measures can be taken at an early stage. The risk-based approach is

established on three risk management steps i.e., determine risk probability value, define impact of risk and ascertain risk exposure.

5.2.3 Validity of study results

The internal and the external validity were considered for the conducted studies. Internal validity refers to the degree that gives investigators the confidence to conclude that the outcome of the study is indeed the result of the treatment. To ensure internal validity that the research's result can be interpreted accurately, three different case studies were conducted from different selected public sector organisations. Respondents from three different organisations interpreted the practicality and usefulness of SISA based on their experience, skills, beliefs and perceptions.

External validity refers to the degree to which the results of a research can be generalised and hold for other populations. To ensure external validity, this research applied triangulation procedures where multiple sources of data were involved, rather than a single data source. Therefore, in terms of gathering information about the IS audit practice, various data were collected from documents from the NAD and the SAI, and research publications about the IS audit practice. To ensure validity, this research corroborated the data through interviews, documents and observations to construct the SISA framework. This research also developed a chain of evidence where findings from the interviews were compared with findings from the existing reviewed documents or observations. This allows to confirm that the description of IS audit activities and the reality found tally. It also allows to generalise the findings.

In term of reliability, this research focuses on whether the SISA framework can be used to assess IS control in different IS areas. This was achieved by adopting SISA in assessing general controls, making decision for cloud migration and customised SISA according to the size of the organisation. Results from the use of the framework were recorded as concrete as possible, supported with the semi-structured interview to clarify any incomplete information given, and ensure congruence between the research issues to be investigated and study design in the research design phase. In addition, a systematic database was developed to organise notes during the interviews, the interview transcripts, and the analysis of evidence. Finally, a chain of evidence was also maintained to aid in drawing conclusions, in the citation and reporting.

By using SISA, this research builds on research that identifies economic, environmental, social, and technological aspects as orientation for sustainability effects and it enables IS auditors to define the level of IS sustainability. The results show that SISA guides an organisation to highlight areas of IS control that need improvement, as a tool for decision-making purposes and it introduces a risk-based assessment to measure sustainability.

5.3 Preliminary Survey

A preliminary survey was performed to examine the existing IS audit practice and its limitations in public sector organisations. This preliminary survey was divided into two phases: 1) electronic questionnaires and 2) interviews.

5.3.1 Data collection

Phase 1: Electronic questionnaires

Electronic questionnaires were used to investigate key areas in IS audit process, and factors impacting on the performance of the IS audit in public sector organisations. A total of 80 potential participants were contacted and questionnaires, together with a covering letter, were emailed to them (see Appendix A). This survey was conducted from 28th December to 28th February, 2013.

Phase 2: Interviews

Several interviews were conducted to confirm the findings from the survey and to investigate on how to improve IS audit practice in public sector organisations. Interview sessions were conducted from 1st to 21th October, 2013 at the NAD and phone/skype interviews were performed for the SAI on 7th-13th December, 2013. Twenty auditors were selected which came from the internal and external sectors of the NAD and five IS auditors (external) from the SAI. The same respondents from the survey with the following criteria were selected:

- i) Participating or having participated in an information system auditing between the years 2008-2014,
- ii) Having attended a course/seminar related to an IS audit.

Respondents were informed about the guide of the interview (see Appendix A1) and the Informed Consent Letter before participating in the session. The longest interview was approximately 40 minutes and the shortest interview took about 20 minutes. The average time

for the interview was about 21 minutes. During the interviewing process, respondents provided

different perspectives and opinions. Their ideas were extracted and analysed for research purposes. Their contributions were reasonably satisfying, however, due to time limitation, some answers were not specific and to some extent, quite general in nature.

5.3.2 Survey context

The sample of survey was determined based on two criteria:

- The public sector organisations are members of International Organization of Supreme Audit Institutions, (INTOSAI);
- The selected participants have at least three years practical experience in IS audit.

The NAD is a public sector organisation and a member of the International Organisation of Supreme Audit Institutions (INTOSAI) in the Asian Region known as ASOSAI, a worldwide affiliation of governmental entities. By the year 2014, the NAD had conducted 25 IS audits in several agencies with the examination of the effectiveness of the IT controls, system development practices and system performance. The NAD has 2,174 audit officers in total and 60 IT auditors who conduct IT audits in various Departments, Ministries and Agencies. The IS audit is performed according to the IS Audit Guidelines, Financial Management Practices and Performance Audit including data analysis, transactions verification, and IS controls evaluation.

The SAI is also a public sector organisation and a member of INTOSAI in the Arab Region known as ARABOSAI. The SAI has been established to ensure efficiency of financial and accounting systems implemented in public sector agencies. The SAI's products consist of regulatory audits, performance audits, as well as investigation and information systems audits. By the year 2014, the SAI had performed 18 IS audit throughout their region.

The survey consisted of two parts; the first part involved questions representing the current IS audit practices and factors impacting on the performance of IS audit and the second part involved acquiring the demographic data of respondents. IS auditors were allowed to express how much they agree or disagree with a current IS audit practice in their organisations by using a Likert-Scale measurement of 1-5, where a value of 5 represented the *most perform/most agree*, and a value of 1 represented the *not perform/not agree*. These measurement scopes were later used to determine and reach conclusions regarding the IS

audit practice in public sector organisations. Once the context was completely developed, the next step was to design the survey questions. For the first question, respondents were asked about key areas in IS audit. Details of the areas are depicted below:

- i) Develop IS audit criteria based on the IT controls objective(s): Establish criteria based on the IT Audit Manual, Best Practices, ISACA, INTOSAI and COBIT.
- ii) Develop knowledge on the entity's operations: Understanding the entity's operation includes understanding the nature of the business, business objective, the organisational structure and financial management.
- iii) Develop knowledge on the entities IS operations: Understanding the information system's operation in term of its application procedures, restoration procedures and system work flow.
- iv) Establish audit objective(s) to assess the effectiveness, efficiency and the economy of the IS investment/IS project(s).
- v) Establish audit plan including risk assessment.
- vi) Produce audit report based on the effectiveness of IS controls rather than having a value for money IS investment.

The next question was about the potential factors that may impact the performance of IS audit based on the follows areas:

- i) IS audit was not able to detect all IS weaknesses.
- ii) IS audit work was limited by control evaluation.
- iii) There was inadequate objective of performance audit in IS.
- iv) There was inadequate risk quantification.
- v) Sometimes errors remained undetected by the audits.

The second part involved the demographic data which comprised of types of auditor (internal or external), region (NAD or SAI), number of years servicing in an audit section and number of years servicing in an IS audit section.

5.3.3 Survey results

A complete set of questionnaires (see Appendix A) was emailed to the selected respondents. About 60 replies were received representing a 75% response rate, which were used for the data analysis. A quantitative analysis was performed using the SPSS software. In total, 50

respondents were from the NAD and 10 from the SAI. The demographic profile of the respondents is shown in Table 5.1.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SAI	10	16.7	16.7	16.7
	NAD	50	83.3	83.3	100.0
	Total	60	100.0	100.0	
Valid	External	28	46.7	46.7	46.7
	Internal	32	53.3	53.3	100.0
	Total	60	100.0	100.0	

Table 5.1 Region and type of IS auditor

In order to better understand the profile of the IS auditor surveyed, a specific question regarding their working experience as an IS auditors was asked. Figure 5.2 showed that 77.33% of the respondents had 5 to 10 years' IS audit experience, 16% of them had 5 to 10 years' working experience, and the remaining 6.67% respondents had less than 5 years' working experience.

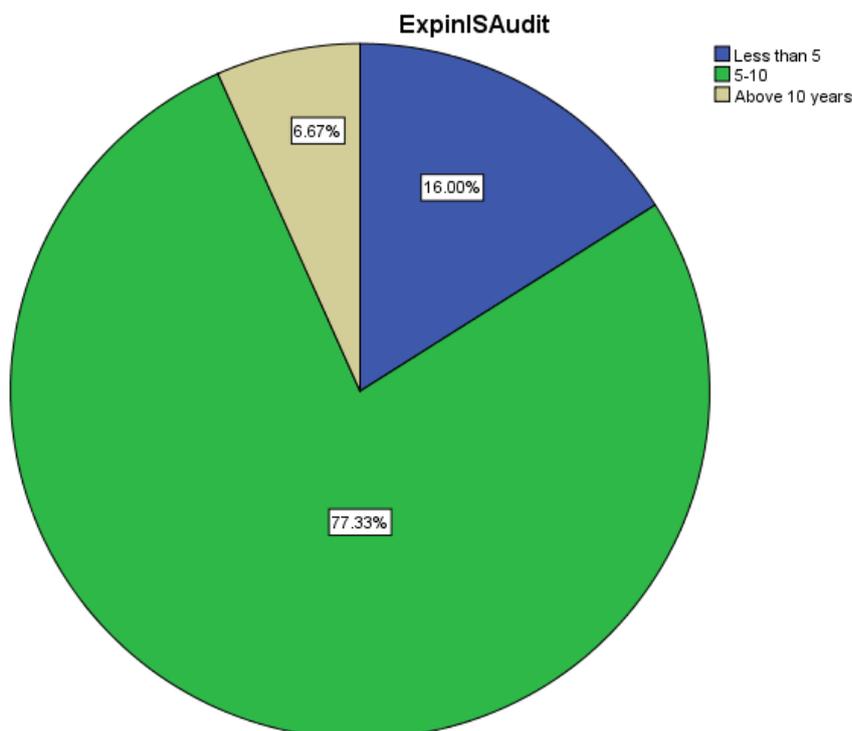


Fig 5.2 Experience in IS audit

Respondents were asked about the current IS audit practice in their organisation. Figure 5.3 shows that auditors in the public sector paid more attention to developing IS audit criteria based on IT controls objectives and gave less attention to a value for money audit and risk assessment. In the NAD, IS auditors focused more on the assessment of value for money compared to other IS audit objective. The NAD and SAI produced IS audit reports in compliance with the rules and regulations rather than opting for a value for money audit. The produced audit report was based on the completeness, validity and reliability of IS controls rather than value for money IS investment.

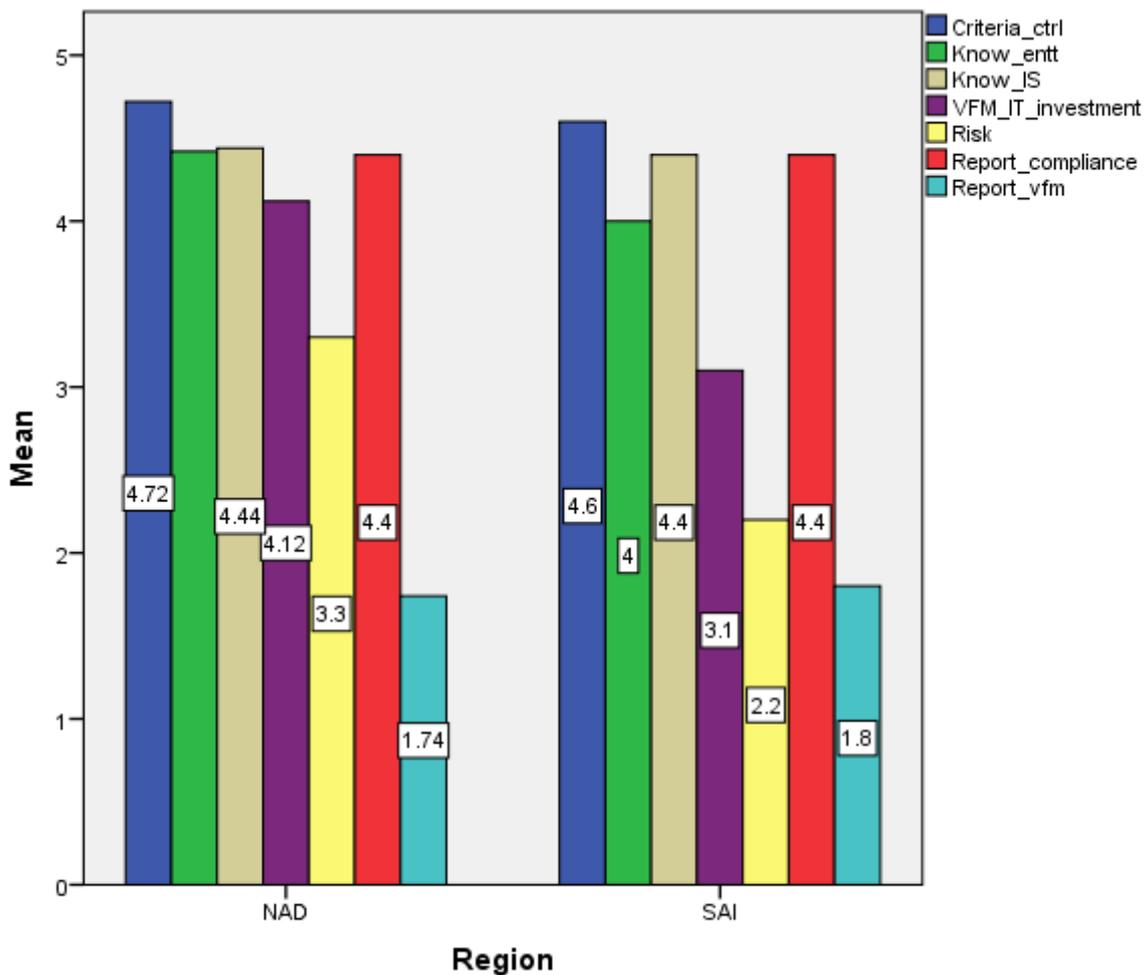


Fig 5.3 IS audit in the NAD and SAI

In order to identify problems that an IS auditor faces, specific questions were asked regarding the factors affecting the performance of IS audit. From the statistical data, IS auditors from both organisations pointed out that the current IS audit work was limited in its control evaluation and was not be able to detect all IS weaknesses. It can also be observed that there was inadequate objective to carry out performance audit in IS audit assessment and sometimes errors remain undetected by the audits. In addition, there was also inadequate risk quantification when performing an IS audit.

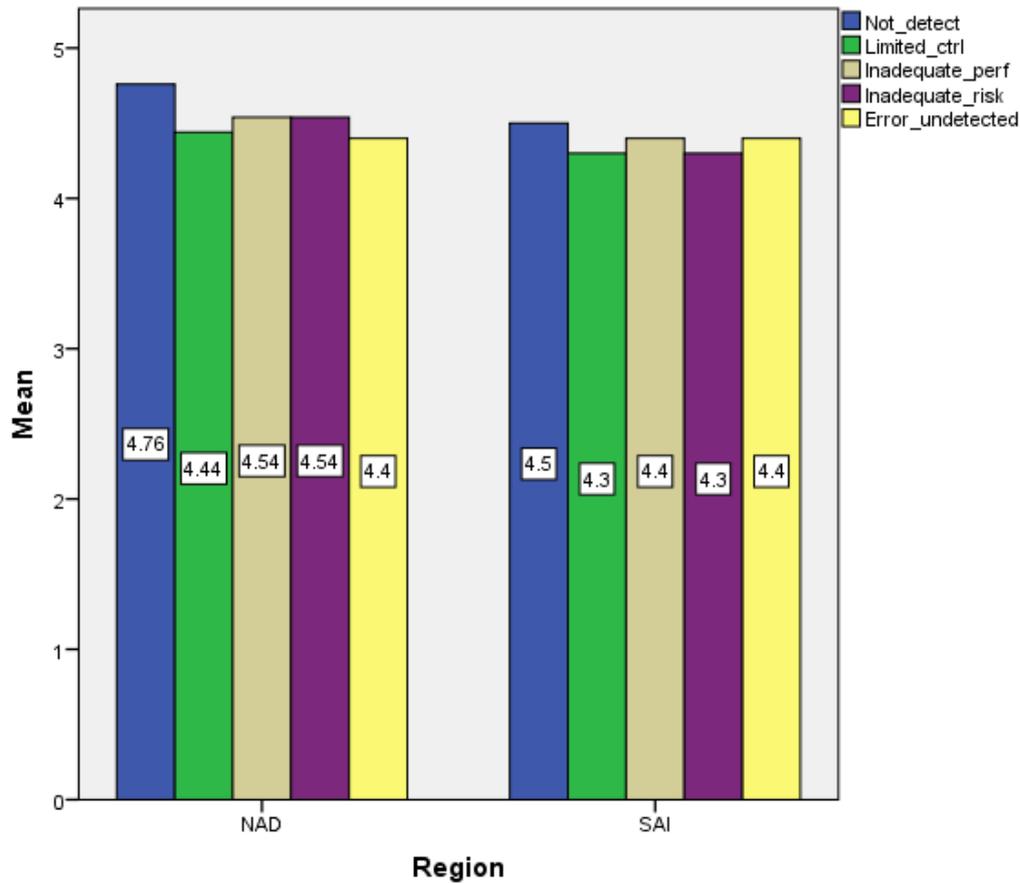


Fig 5.4 Factors impacting the performance of the IS audit in the public sector

5.3.4 Interview results

This section explores the perspective of IS auditors on critical factors in relation to IS audit issues. Issues and difficulties found in the IS audit were analysed and potential suggestions for improvement were given. Table 5.2 shows the number of interviews conducted for each organisation.

Category	NAD	SAI

Director of IS audit (external)	1	None
Director of IS audit (internal)	1	None
IS audit manager (external)	1	1
IS audit manager (internal)	1	None
Team leader (external)	3	1
Team leader (internal)	3	None
IS auditor (external)	5	3
IS auditor (internal)	5	None

Table 5.2 Numbers and categories of respondents

An interview protocol containing all of the questions is attached to Appendix A1. Interview questions covered four main areas. These were issues/problems found in the IS audit practice, the extent of risk assessment in IS audit, strategy to enhance IS audit work and suggestions to improve IS audit report. Key findings of each set of interviews are presented in Table 5.3.

Description	Respondent's view
Issues/problems in IS audit	<ul style="list-style-type: none"> • Lack of guidelines to assess IS flexibility and functionality. • Lack of guidelines for conducting risk assessment and its quantification. • Incompetent IS auditor in detecting IS error/failure. • IS adopted were not meeting expectations. • IS auditors faced inherent risk. • Lack of criteria to measure IS performance. • Auditor General found the audit findings insufficient. • Several areas have not been adequately addressed throughout the auditing processes due to limitation of audit scope and audit objectives. • Ineffective IS audit of outsourcing/third party services. • Inadequate service level indicator in relation to reliability, quality and time of service provided by a third party. • No specific method or technique that can assist auditors performing IS risk assessment in a systematic manner. • The public has a set of high expectations about the audit report and regarding controls effectiveness they were of the opinion that it may not be adequate for today's complex business environment.

	<ul style="list-style-type: none"> • Lack of monitoring on economic situation.
Impact of issues on IS audit performance	<ul style="list-style-type: none"> • Error in IS remains undetected. • IS failure continues. • Generic audit report produced which an emphasis on the effectiveness of IS controls. • Information system audit does not add value to the organisation. • Inadequate IS audit findings resulted in overlooking potential IS problems.
Strategy to enhance IS audit work.	<ul style="list-style-type: none"> • Include assessment on IS functionality and flexibility. • Consider assessment on technical values such as scalability of the systems. • Include examination on related costs for IT investment. • Produce a clear set of criteria to assess IS from a performance audit perspective. • Implement continuous monitoring.
Strategy to enhance audit report.	<ul style="list-style-type: none"> • IS audit report should provide more assurance on the ability of the auditee's information system to sustain, maintain and continue to offer a good service delivery to the public. • Highlight a high risk area in IS. • Include other aspects such as potential impacts relating to the benefits of IS to the user, the organisation and the public, views on intangible and tangible benefits of IS, user's satisfaction and management's perception, technological issues and potential impacts relating to IS application, economic matters and green IS.

Table 5.3 Issues in IS audit

5.3.5 Survey conclusions

Based on the responds from the participants, this research concludes that there are a number of limitations in the existing audit practice as shown in Table 5.3. The table also shows that there are commonalities between our survey findings with the existing literature. We have concluded that a sustainability driven approach is necessary to provide additional support for IS performance. Hence, this can also help to overcome the limitations of the existing IS audit practices and also to contribute to the minimization of IS risks or errors.

Problems	Examples of sustainability control systems	Literature
Lack of monitoring on economic matters	Measure cost effectiveness of each related cost to IS. Long range planning covering a five years period for cost allocation.	(Harmon, Daim and Raffo, 2010)
-Unable to detect IS error. -Lack of guidelines to assess IS flexibility and functionality. -Communication failure	Measure IS flexibility, scalability, availability, security.	(Hessami, Hsu and Jahankhani, 2009)
-Ineffective IS audit of outsourcing/third party services. -Inadequate service level indicator in relation to reliability, quality and time of service provided by a third party.	Measure number of disputes between user and provider. Measure number of service delays.	(Schmidt <i>et al.</i> , 2009)
Lack of guidelines for conducting risk assessment and its quantification.	Measure risk assessment for sustainability dimensions.	(Krysiak, 2009)
-Auditor General found the audit findings were insufficient. -Public has a set high expectations about an audit report and regarding controls effectiveness they believed that it may not be adequate for today's complex business environment. -Several areas have not been adequately addressed throughout the auditing processes due to limitation of the audit's scope and audit's objectives.	Reporting on IS performance based on economic, environmental, social and technology aspects.	(Gao and Zhang, 2006a)

Table 5.4 Summary of problems in IS and potential sustainability controls

The results from the survey show a significant number of controls from a sustainable perspective that could support the overall IS audit. There is a common aim for both sustainability and IS audit, i.e., improving the performance of IS in relation to economic, environmental, social and technological aspects and by considering the numerous expectations from the users, the public and stakeholders. Summary of problems in IS and potential sustainability controls are shown in Table 5.4.

5.4 Empirical investigation

This section reports on the experience of the IS auditors by conducting a case study on the application of SISA in Malaysia Ministry of Health and the State Audit Institution of the SAI (SAI). The purpose of this section is to evaluate the SISA framework and to examine the impact of the framework on actual audit practices. Three case studies were selected, conducted and monitored and data was collected over time. These case studies were chosen due to the following reasons:

- i) The IS audit has been performed in the NAD since 2006 and in the SAI since 2008; therefore, there is an adequate sample of well experienced respondents to give feedback on the SISA framework.
- ii) Both public organisations are members of INTOSAI and practise the same ISSAI standards for conducting an IS audit.
- iii) Adequate resources are available and sufficiently stable to enable any changes in the nature and extent of the audit work related to SISA implementation.

5.4.1 Case study 1 Investigation SISA in the NAD

i) Study context

The selected IS project for this study is the Hospital Information Systems (HIS) of the Malaysia Ministry of Health. The Ministry of Health (MoH) is a public organisation and it is located at the Head Quarters in Putrajaya. HIS is a comprehensive, integrated information system which was fully financed by the Government of Malaysia. The HIS was launched in 2006 and it stores health care information about patients' health profile, medical history, billings and other hospital-related procedures to support the continuity of both the care given to patients as well as for research purposes. The development of HIS is expected to overcome problems faced by the public hospitals in Malaysia, such as inefficient services and escalating negligence cases due to improper medical documentation. The case study concerns the implementation of HIS in relation to financial management, environmental, social benefits and technological aspects. The case study is appealing for a number of reasons:

- i) The MoH has been granted a huge allocation for IS investment, so it essential for auditors to examine whether the public funds are managed in accordance with laws, rules and regulations,
- ii) To contribute towards enhancing the standard of accountability in the public sector from a sustainability perspective,
- iii) To produce a reliable and objective audit report to the auditee.

Execution of the case study 1 was as follows:

Case 1 (External IS audit team)

- 2 Nov 2015- briefing on SISA at the NAD
- 3-4 Nov 2015- finalising on the sustainability indicator
- 5-6 Nov 2015- getting familiar with estimating degree of belief for IS control evaluation
- 9 Nov 2015- entrance conference and fieldwork at the MoH
- 28 Nov 2015- exit conference and a brief about the IS audit findings

ii) Study objective

The main objective was to analyse the SISA implementation in a public sector organisation. For evaluation purposes, four aspects were considered:

- i) To investigate the viability of the sustainability dimensions to enhance the IS audit practice;
- ii) To explore the impact of the SISA framework on the IS performance of public organisation;
- iii) To ascertain whether the SISA framework has causes any real change in the way IS auditor conduct IS audit work.

iii) Applying SISA in assessing general and application controls

The researcher enhanced the traditional IS audit process by measuring risk within a sustainability perspective in mind and drawing audit conclusions based on the level of sustainability. In particular, there are three different types of roles in IS audit work, namely auditee, user and IS auditor. Auditee refers to the public organisation, user is the stakeholder and the community of the public sector organisation and auditor is the IS auditor of the public sector organisation. The goal of this step was to obtain feedback on the SISA implementation so as to produce effective justification for risk assessment and IS audit findings.

- 1) Phase 1 Define IS audit plan

IS audit plan is an important document for IS auditors as it specifies the IS audit objective (s), the IS audit scope, the methodology, the IS audit criteria and the audit-related information as a guide to be followed by IS auditors when carrying out the audit works. The scope of IS audit

is general controls and application controls evaluation. The IS audit team was given 3 weeks to conduct the audit fieldwork including understanding business process and the key systems, program, module or unit within the organization. The IS audit team had a thorough discussion on developing sustainability criteria, sub-criteria and appropriate sustainability indicators for general and application controls. The proposed sub-criteria for sustainability were as follows:

- i) Budget (cost effective analysis)
- ii) Environmental (optimal configuration for green cloud, resources savings, power or air conditioning failure)
- iii) Social (transfer of knowledge, IS strategic plan, user's satisfaction)
- iv) Technological (continuity, flexibility, scalability).

The specified IS audit criteria were then used to evaluate the current implementation of IS, provide a basis for analyzing the evidence, developing audit findings, and reaching conclusions in order to identify whether the current process meets the sustainability requirements.

- 2) *Phase 2 Execute the IS audit*

The IS audit execution is about collecting and analyzing the evidence for reaching the audit conclusion. Therefore, the scope and objective from the previous activity is necessary to understand what types of evidence are required for the IS audit. This involves five steps as follows:

Step 2.1 Collect evidence

In this step, IS auditors gathered evidence based on the assessment of four sustainability dimensions (economic, environment, social, and technological). The data were obtained via the audit techniques such as inspection, review documents, records, and transactions produced by the IS, survey, re-performance, and interviews of the practitioners and experts within organization. The method used to gather the data is influenced by the factors of the sub-criteria. For instance, the economic sub-criterion is cost effectiveness and the influencing factors for cost effectiveness are operating cost, development cost, maintenance cost, integration cost, migration cost, and training cost. It is worth mentioning that the data used for the sub-criteria are collected from IS contractual agreement, electronic payment systems, electronic procurement systems and annual budget documents. Examples of evidence collection are as follows:

		Value	A	P	I
		BUDGET (Cost Benefit analysis)			
Attributes	Risk/Control	Description of controls/sustainability indicator			
	R1	Budget is prepared in accordance with rules and regulations			
	C1	*Accurate accounting procedures	0.9	0	0.1
	C2	*Determine acceptable variance	0.9	0.1	0
	C3	**Contingency (new tax, new fin. Policy)	0.9	0	0.1
	C4	** Analyse trend of payment throughout the year	0.9	0	0.1
	C5	** Cost of storage capacity for at least 5 years	0.8	0.1	0.1
	C6	**Maintenance cost, training for 5 years	0.8	0.1	0.1
	C7	*Accurate accounting procedures	0.8	0.1	0.1

Table 5.5 Evaluation of economic criteria

		Value	A	P	I
		ENVIRONMENTAL			
Attributes	Risk/Control	Description of controls/sustainability indicator			
	R2	Optimal configuration for green cloud			
	C8	*Hardware used	0.8	0	0.2
	C9	*Cooling requirements	0.8	0	0.2
	R3	Resource savings			
	C10	*Paperless	0.9	0	0.1
	C11	*Auto logged off (light, PC, photocopier)	0.7	0	0.3
	R4	Power or air conditioning failure			
	C12	*Back up (continuous) power supply	0.9	0	0.1

Table 5.6 Evaluation of environmental criteria

		Value	A	P	I
		SOCIAL			
Attributes	Risk/Control	Description of controls/sustainability indicator			
	R5	Availability of IS related policies and procedures			
	C13	*Personnel policies and procedures	1	0	0
	C14	*Security policies and procedures	1	0	0
	C15	* Acquisition/Outsourcing policies and procedures	1	0	0
	C16	* Change management policies and procedures	1	0	0
	C17	* Operational policies and procedures	1	0	0
	C18	*Physical and environmental control policies and procedures	1	0	0

	C19	*Logical access policies and procedures	1	0	0
	C20	* Business continuity policies and procedures	1	0	0
	R6	Key Performance Indicator of business and IS			
	C21	** Average time of IS delivery (continuity of service)	0.9	0	0.1
	C2	**Planned delivery date vs actual delivery date	0.8	0	0.2
	C23	** Mean time to repair (if failure occurs)	0.9	0	0.1
	R7	IS Strategic plan			
	C24	** Setting priorities	0.9	0	0.1
	C25	** Monitoring project plan and resources	0.9	0	0.1
	R8	Examine third party services			
	C26	** Number of service level targets set out in SLA being met	0.9	0	0.1
	C27	**Number of disputes between user and provider (Customers, requirements analyst, software engineers understand each other?)	0.6	0.1	0.3
	C28	**Number of service delays	0.8	0	0.2
	C29	** Availability of escrow agreement	0.5	0.3	0.2
	R9	Transfer of knowledge			
	C30	** Percentage of staff competency working with new systems.	0.9	0	0.1
	C31	* *Number of complaints from staff due to new systems	0.8	0	0.2
	R10	Assessing user's satisfaction			
	C32	**Review response time	1	0	0
	C33	**Review modules/deliverables	0.9	0.1	0
	C34	**Review user's involvement in acceptance testing	0.9	0.1	0
	R11	Continuous monitoring			
	C35	**Review feasibility study report for system development (costs, benefits, risks, justifications)	0.8	0	0.2
	C36	** Market study is conducted for hardware	0.8	0	0.2
	C37	** Post implementation review	0.9	0	0.1
	R12	Information security			
	C38	**Number of incidents related to information confidentiality	0.7	0.2	0.1
	C39	**Number of incidents related to information integrity	0.7	0.2	0.1
	C40	**Number of changes related to information confidentiality and integrity	0.7	0.2	0.1

Table 5.7 Evaluation of social criteria

		Value	A	P	I
		TECHNOLOGICAL			
Attributes		Description of controls/sustainability indicator			
	R13	Availability of application control			
		Input, process and output control			
	C41	*Volume of input within specified timeframe (efficiency)	1	0	0

	C42	*Sequence of input	1	0	0
	C43	* Data validation checks	0.9	0.1	0
	C44	* Access control	1	0	0
	C45	* Atomicity: Transaction is completed entirety or not processed at all. *Consistency: Transactions are consistent with one another. * Isolation: Each transaction is isolated from the other transactions.	1	0	0
	C46	*Produce output in a timely manner	1	0	0
	R14	Service deliver to users			
	C47	** Number of disruptions	0.9	0.1	0
	R15	Scalability			
	C48	** Ability of the IT system to be upgraded and maintain a specified level of performance as the workload of the system increases	0.8	0.2	0
	R16	Security			
	C49	**Audit trails	0.9	0.1	0
	C50	**Number of security incidents reported.	0.9	0.1	0
	C51	**Type of incident – information exposure	0.9	0.1	0
	C52	*Type of incident – information system theft (laptop, mobile device)	0.9	0.1	0
	C53	*Type of incident – information corruption (malware, virus)	0.9	0.1	0
	R17	Flexibility			
	C54	**Ability to share any type of information across any technological component	0.9	0.1	0
	C55	*Ability to add, modify, and remove any software, hardware, or data components from the IS infrastructure.	0.9	0	0.1
	R18	Disposal of information asset			
	C56	**Remove data, wipe data, refurbish for reuse or recycle old IS equipment - complies with applicable regulations	0.8	0.2	0

Table 5.8 Evaluation of technological criteria

Step 2.2 Analyse the evidence

This step presents an analysis of the collected evidence. The evaluation of IS controls is performed by identifying the adequacy of controls to mitigate risk. The audit criteria used for assessing IS controls consist of a combination of rules and regulations, best practices, standards in relation to IT and also appropriate sustainability indicators. The audit team applied degree of belief under the D-S theory based on the evidence obtained from the IS controls assessment.

Step 2.3 Estimate risk probability and impact

This step determines the risk probability and impact based on the identified risks and evidence of controls. Within this context, the degree of belief that control is able to mitigate a risk for C1 is 0.9 and for control which exists that is either able or unable to mitigate a risk the degree of belief is 0.1. The m-values for these controls are shown in Table 5.9. Note that, the result showed risk from the economic dimension and similar procedures were performed to assess the environmental, social and technological dimensions.

Sustainability dimension	Risk factor	Control ID	m-values		
			Adequate	Partial	Inadequate
		C1	0.9	0	0.1
	R1	C2	0.9	0.1	0
Economic		C3	0.9	0	0.1
		C4	0.9	0	0.1
		C5	0.8	0.1	0.1
		C6	0.8	0.1	0.1
		C7	0.8	0.1	0.1

Table 5.9 Summary of m-values

The m-values identified from controls were propagated to risk factor. For the economic dimension only one risk is applicable and the result obtained is shown in the table above. The above m-values denotes that evidence in economic evaluation provides 1 level of support, on a scale of 0-1, that is 0 is inadequate or partially adequate to mitigate a risk for economic. Meaning, controls provided within economic dimension are adequate to mitigate risk in economic (R1).

$$\text{Bel (A)} = 1, \text{Bel (P)} = 0.$$

$$\text{Pl (A)} = 1 - \text{Bel (P)} = 1 - 0 = 1$$

$$\text{Pl (P)} = 1 - \text{Bel (A)} = 1 - 1 = 0$$

From this analysis, it shows that the probability value for R1 is 0.

Sustainability dimension	Risk factor	m-values		
		Adequate	Partial	Inadequate
Economic	R1	1	0	0
	R2	0.04	1	0.04
Environmental	R3	0.03	1	0.03
	R4	0.1	1	0
	R5	1	0	0
Social	R6	0.997	0.0022	0
	R7	0.98	0.02	0
	R8	0.9936	0.0044	0.00189
	R9	0.9977	0.0022	0
	R10	0.002	0.99783	0
	R11	0.004	1	0.004
	R12	0.9497	0.0502	0
	R13	0	1	0
Technological	R14	0	1	0
	R15	0.012195	0.987805	0
	R16	0	1	0
	R17	0.0989	0.0109	0
	R18	0.8	0.2	0

Table 5.10 Risk factors and m-values

Step 2.4 Determine risk exposure

The final step of the activity determines the risk exposure for each sustainability dimension. The risk exposure value is the multiplication of risk event probability and impact as shown in equation 8. Finally, the risk exposure values are referred to the qualitative scales as shown in Table 4.4 to determine the acceptable level of risk. Then the results are interpreted in relation to the level of sustainability.

Sustainability dimension	m-values			Plausibility value	Impact	Risk exposure
	A	P	I			
Economic						
R1	1	0	0	0	0	0
Total						0
Environmental						
R2	0.04	1	0.04	0.96	0	0
R3	0.03	1	0.03	0.97	1	0.97
R4	0.1	1	0	0.9	0	0
Average						0.323
Social						
R5	1	0	0	0	1	0
R6	0.997	0.0022	0	0.003	1	0.003
R7	0.98	0.02	0	0.02	1	0.02
R8	0.9936	0.0044	0.00189	0.0064	1	0.0064
R9	0.9977	0.0022	0	0.0023	0	0
R10	0.002	0.9978	0	0.998	1	0.998
R11	0.004	1	0.004	0.996	0	0
R12	0.9497	0.0502	0	0.0503	1	0.0503
Average						0.359233
Technological						
R13	0	1	0	1	1	1
R14	0	1	0	1	1	1
R15	0.1219	0.9878	0	0.8781	1	0.8781
R16	0.002	0.9978	0	0.998	1	0.998
R17	0.8	0.2	0	0.2	1	0.2
R18	0.8	0.2	0	0.2	1	0.2
Average						0.712683

Table 5.11 Risk exposure

Step 2.5 Determine the overall sustainable risk and level of sustainability

Once the risk exposure values are obtained from the sustainable dimensions, the risk values are averaged and can be written by following equation 9. As depicted in Table 5.11, three sustainability dimensions have Low risk exposure (Economic, Environmental and Social) and Technological has High risk exposure. This information can be interpreted as an ‘Effective sustainability’ in relation to the level of sustainability. Effective sustainability indicates that there is awareness from the management that they need to apply proper sustainability objectives but there is lack of effective implementation. An effective phase requires further IS

audit assessment to identify problems in Technological dimensions which has High risk exposure particularly on flexibility of IS and IS assets disposal procedures (R17 and R18).

- 3) *Phase 3 Aggregate IS audit findings*

This activity includes steps to prepare an IS audit report that reflects the findings and conclusions of the audit.

Step 3.1 Generate audit report

In SISA, IS auditors are required to derive opinion on the level of sustainability of the IS in the final IS audit report. They are also need to include whether the IS sustainability requirements have been met. Based on the obtained result Table 5.11, it was observed that an average score of risk exposure showed that the level of sustainability is at 'Effective' phase which provides an indication of the sustainability level of IS. However, the technological dimension has a High risk exposure (0.71263) as compared to the economic, environmental, and social dimensions. These findings can lead to a new data gathering and further analysis to explain the weaknesses.

Step 3.2 Corrective and/or preventive actions

Appropriate preventive actions should be taken by the organization to enhance the enforcement the IS control regarding the technological dimension which include control in processing, output, access and incident management.

Step 3.3 Recommendations

An organization should improve access control and incident management so that unauthorized or inappropriate access is prevented or tracked. The organization should also monitor the data and software and make sure that they are disposed appropriately and legally. Equipment must be disposed of in line with the E-waste Electrical and Electronic Equipment in Malaysia, 2010 while data must be treated in line with the Data Protection Act 2010.

- *Agency response*

Agency response was received after four months the IS audit report were sent to them. Their response are shown below;

“The Malaysia Ministry of Health, on behalf of the Public Health Department, accepts the findings, and will take appropriate action following the recommendations made by the Auditor General”.

5.4.2 Case study 2: Viability of cloud migration by using SISA

In this case study, SISA is applied to measure the viability of cloud migration. This case study is different from case study 1 as it focused on a cloud migration context. This section presents an overview of the case study and its results.

i) Study context

Public hospitals in Malaysia are categorised into two types; regional/state and district hospitals. The MoH is a public organisation and its operations are located at the Head Quarters in Putrajaya. To date, there are 139 branches of MoH that provide public healthcare services nationwide. Currently, there are more than 70,000 personnel in the MoH. Email is the key medium of communication in the MoH besides teleconferencing and other social media. Hence, MoH has a huge amount of email transactions and an internet connection of 32Mbps in the Head Quarters. Every user is allocated 500Mb email storage and this allocation varies depending on the hierarchy, roles and responsibilities of the MoH staff. The high volume of emails requires regular maintenance on the storage, transmission, delivery and access to the emails.

The goal of the study is to Support MoH with cloud-migration decision. This means to:

- Identify risks and possible controls for making a viable sustainable decision;
- Examine the applicability of using the sustainability approach and assess the risk of the cloud migration decision.

Due to budget constraints and maintenance overhead, the MoH management’s decision was to migrate the whole e-mail service into cloud. The management required the migration to be performed by taking into account resource capabilities, e-mail archive, users’ expectations, organization and stakeholders, relevant controls and risks mitigation. In order to fulfill the study’s objective, a set of questionnaires were used to assess respondents’ perception on their

understanding of sustainability dimensions, cloud migration and the relative importance of the sustainability criteria and sub-criteria. About 20 questionnaires were distributed to the selected staff of MoH. The respondents were from the operational to the senior management level and had been in service for more than 5 years. Execution of the case study 2 was as follows:

Case 2 (Internal IS audit team)

- 11 Nov 2015 - briefing on SISA at the MoH
- 12-13 Nov 2015- finalising the sustainability indicator
- 16-17 Nov 2015- getting familiar with estimating degree of belief for IS control evaluation
- 18 Nov-2 Dec 2015- gathering information on cloud computing migration
- 3-4 Dec 2015- finalising findings on cloud migration
- 7-8 discussion of the audit findings and decision for cloud migration

ii) Study objective

The researcher implemented the proposed approach into a real migration use case at the Ministry of Health, Malaysia (MoH) for the purpose of evaluation. Results obtained from the study were used to aid in the forecasting of sustainability in cloud migration. The study objectives were:

- To evaluate the advantages and limitations of sustainability in aiding management for cloud migration.
- To improve understanding of the issues and factors of sustainability risks that influenced the cloud migration process.

iii) Migration use case

The MoH is a very large organization and employed more than 70,000 employees. In the MoH, email service is the main medium for communication among employees from all locations. The ministry follows paperless communication strategy. All emails are maintained on the mail server for legal/audit/documentary purposes and are archived for a period of 180 days. An allocation of 500MB email storage is provided to individual employee and the email storage varies according to the employees' roles and responsibilities. A total of five years IT infrastructure maintenance costs for managing the email service is £20,000- £40,000 and data will triple in size; the current size being 45 TB.

iv) Risk management process

The risk management team consists of researcher and IS audit team (internal audit and IT). The team held a kick –off workshop with the key MoH staffs to initialize the risk management

process. The first step of this activity was to define the migration profiles by analysing the migration scenario with the top MoH management. Cost reduction is one of the main goals that the management intends to achieve through cloud migration. However, it is also necessary to safeguard all e-mails through cloud.

The management of the MoH developed a migration strategy for the email services to be migrated into the cloud. The strategy began with the basic requirements prior to migration as stated below:

Migration type: Type II: Partially migrate due to not considering the whole MoH

Service model: SaaS

Deployment model: public

Security assessment: access controls, data governance, change management, business continuity, incident handling, third party management, compliance to rules and regulations, auditability of virtual records, data retention policies and physical security.

Migration size: the application and data requirements are identified. The application requirements include components, storage, integration point, business logic. Data requirements include files, registry information, and size of data, sources and storage. The category of data and its sensitivity are also taken into consideration. For risk management for cloud migration decision, six steps were involved:

Step 1 Identify Risks and General Controls

During this phase, a number of interviews with the IT staffs were conducted in order to identify the possible risks and to obtain evidence of existing controls from the MoH infrastructure. Ten respondents from IT section were selected for the interview. The respondents were from the operational to senior level of management and had a minimum of five (5) years' experience working with/in the MoH. The identified risks and general controls to mitigate the risks are shown in Table 5.12.

Risk	General controls	Internal control
R1: Inadequate budget estimation	C1: Budget review	Implement performance budget review for estimation and variance on a scheduled basis.
	C2: Type of migration	Type of migration is defined by the Steering Committee and the Technical Committee.
	C3: External factor	Consider external factors in the budget preparation such as natural disasters, hackers, socio-economic stability, government's rules and regulations, political condition.
	C4: Monitor budget	Monitor budget and update its position according to the completion of cloud migration status.
	C5: Future costs	Consider future costs due to the complication of the systems for example changes in cloud infrastructure, changes in SLA, additional training.
R2: New legal policy	C6: Short term budget plan	Implement a 5 years budget plan based on the current economic position, current resources and capital requirements.
	C7: Prepare operational detailed and variability plan.	Prepare operational expenditure, capital expenditure inclusive of fixed cost, variable cost, overhead, etc.
	C8: Update forecast.	Update forecast with the latest budget and actual on a periodical basis.
R3: Continuous monitoring	C9: Monitor SLA	Monitor initial deployment phase until the completion of applications and infrastructure.
	C10: Contractual payment	Payment to vendor is made based on the percentage of work completion and satisfying user's requirements.
R4: Optimal configuration for green cloud	C11: Hardware used	Analyse which hardware utilises less amount of energy.
	C12: Cooling requirements	Identify equipment to provide cooling facilities for cloud server, data centre and other IT facilities.
R5: Resource savings	C13: Paperless	Fully utilise automation facilities, less paper used.
	C14: Cost optimisation	Determine an appropriate cost for energy savings, optimal response time with satisfactory services.
R6: Highly dependent on third party services.	C15: Service level agreement	The organisation develops a service level agreement that defines a minimal level of service performance, the boundaries of the service scope, and service operation status.
	C16: Continuous	Establish a scheduled review of the response time,

	monitoring	scalability of storage, resolution time,etc.
R7: Change management	C17: Check compliance procedures	Check compliance procedures for managing change including approval for change, testing and implementation.
	C18: Identify capabilities	Identify capabilities to manage change including availability of resources, reason for change and competency of staff (knowledge transfer).
R8: IT Governance	C19: Continuous monitoring for compliance.	Check compliance procedures for IT Governance.
	C20: Establish appropriate policies and procedures.	Provide an IT policy for general and application controls.
R9: Information leakage	C21: Access control	Provide adequate access control to prevent unauthorised access.
	C22: Provide audit trail	Provide audit trail so as to make available documentary evidence of the activity, time, operation, procedure or event.
	C23: Provide encryption	Provide appropriate measures to protect data such as encryption.
R10: Business continuity	C24: Provide Business Continuity Plan (BCP)	Develop policy/framework for BCP to ensure continuity of services.
	C25: Evaluate the adequacy of the BCP	Evaluate the adequacy of back up facilities, disaster recovery plan and BCP to continue operation in the event of disruption.
R11: Storage failure	C26: Check scalability	Provide assessment of scalability.
	C27: Perform application response test.	Perform application response test to identify problems.
	C28: Provide data retention policy	Provide compliance assessment of the data retention policy for scalability purposes.
R12: Network threat	C29: Provide network security policy for network control.	Establish network security policy including wireless access, network scanning policy, remote access policy and internet connection policy.
	C30: Provide appropriate	Provide anti-virus, firewall and routers along with the

	control measures for network.	descriptions or lists of permitted and disallowed traffic.
--	-------------------------------	--

Table 5.12 Risks and general controls

Step 2 Collect risk control evidences

For collection risk control evidences, IS auditors and respondents were required to express their belief on the adequacy of controls provided by the organisation. From the assessment, Economic risk (R1) has five types of controls to mitigate risk related to budget estimation, monitoring and changes in policies. The Environmental has two types of controls, the Social has three types of controls and the Technological has four types of controls. Details of the collected risk control evidences are shown in Table 5.13 to 5.16.

		Value	A	P	I
Attributes		ECONOMIC			
	Risk/Control	Description of controls/sustainability indicator			
	R1	Budget estimation			
	C1	**Budget review	0.6	0.3	0.1
	C2	**Type of migration	0.5	0.5	0
	C3	**External factor	0.6	0.3	0.1
	C4	** Monitor budget	0.6	0.3	0.1
	C5	** Future costs	0.7	0.3	0.1
	R2	New legal policy			
	C6	** Short term budget plan	0.6	0.2	0.2
C7	** Prepare operational detailed and variability plan	0.6	0.2	0.2	
C8	**Update forecast	0.8	0.2	0	
R3	Continuous monitoring				
C9	**Monitor Service Level Agreement	0.8	0.1	0.1	
C10	**Monitor contractual payment	0.7	0.2	0.1	

Table 5.13 Evaluation of economic criteria

		Value	A	P	I
		ENVIRONMENTAL			
Attributes	Risk/Control	Description of controls/sustainability indicator			
	R4	Optimal configuration for green cloud			
	C11	*Hardware used	0.8	0.1	0.1
	C12	*Cooling requirements	0.8	0.1	0.1
	R5	Resource savings			
	C13	*Paperless	0.9	0.1	0
C14	*Auto logged off (light, pc, photocopier)	0.9	0.1	0	

Table 5.14 Evaluation of environmental criteria

		Value	A	P	I
		SOCIAL			
Attributes		Description of controls/sustainability indicator			
	R6	Dependent on third party services			
	C15	**Service level agreement	0.9	0.1	0
	C16	**Continuous review and monitor	0.8	0.2	0
	R7	Change management			
	C17	**Compliance procedures	0.9	0.1	0
	C18	**Identify capabilities	0.9	0.1	0
	R8	IT Governance			
	C19	**Continuous monitoring for compliance	0.9	0.1	0
	C20	**Appropriate policies and procedures	0.9	0.1	0

Table 5.15 Evaluation of social criteria

		Value	A	P	I
		TECHNOLOGICAL			
Attributes		Description of controls/sustainability indicator			
	R9	Information leakage			
	C21	**Access control	0.9	0.1	0
	C22	**Audit trail	0.7	0.2	0.1
	C23	** Encryption	0.9	0.1	0
	R10	Business continuity			
	C24	**Availability of the Business Continuity Plan	0.9	0.1	0
	C25	**Adequacy of the Business Continuity Plan	0.9	0.1	0
	R11	Storage failure			
	C26	** Scalability	0.7	0.2	0.1
	C27	**Application response test	0.8	0.1	0.1
	C28	**Data retention policy	0.9	0.1	0
	R12	Network			
C29	**Network security policy	0.9	0.1	0	
C30	**Network control measures	0.9	0.1	0	

Table 5.16 Evaluation of technological criteria

Step 3 Estimate risk probability and impact

This step determines the risk event probability and impact based on the identified risks and evidence of controls. The probability value is derived from the belief provided by the users based on the general controls provided by the organisation. From this analysis, it has been observed that mitigating controls for economic risks are provided by the organisation for cloud migration. Within this context, the degree of belief that control is able to mitigate a risk for C1 is 0.6, control exists that is either able or unable to mitigate a risk is 0.3 and control exists that is not able to mitigate a risk is 0.1. The m-values for these controls are shown in Table 5.17.

Sustainability dimension	Risk factor	Control ID	m-values		
			Adequate	Partial	Inadequate
		C1	0.6	0.3	0.1
		C2	0.5	0.5	0
	R1	C3	0.6	0.3	0.1
		C4	0.6	0.3	0.1
		C5	0.7	0.3	0.1
Economic	R2	C6	0.6	0.2	0.2
		C7	0.6	0.2	0.2
		C8	0.8	0.2	0
	R3	C9	0.8	0.1	0.1
		C10	0.7	0.2	0.1

Table 5.17 Summary of m-values

Similar procedures were adopted to assess R2 and R3. The m-values identified from controls are propagated to risk factor (R1, R2, and R3) and the result obtained is shown in Table 5.18. The above m-values imply that evidence in R1 provides 0.9259, on a scale 0-1, that control is adequate to mitigate risk, and 0.0740, that control is partially adequate to mitigate a risk. From this analysis, equation (7) is used to compute probability value. It shows that probability value for R1 is 0.0740 while for R2 it is 0.3333 and for R3 it is 0.0204.

Sustainability dimension	Risk factor	m-values		
		A	P	I
	R1	0.9259	0.0740	0.00
Economic	R2	0.6666	0.3333	0.00
	R3	0.9795	0.0204	0.00

Table 5.18 Risk factors and m-values

Step 4 Determine risk exposure

For decision making purposes, it is necessary to evaluate all risk factors and understand all the relevant issues. The summary of the complete assessment of overall m-values and risk exposure is depicted in Table 5.14

Sustainability dimension	m-values			Plausibility value	Impact	Risk exposure
	A	P	I			
Economic						
R1	0.9259	0.07404	0	0.0741	1	0.0741
R2	0.6666	0.25	0.0833	0.3334	2	0.6668
R3	0.9795	0.0204	0	0.0205	2	0.041
Average						0.2606
Environmental						
R4	0.7222	0.2222	0.05555	0.2778	1	0.2778
R5	0.8378	0.1351	0.027	0.1622	1	0.1622
Average						0.2200
Social						
R6	0.8974	0.0769	0.0256	0.1026	2	0.2052
R7	0.8591	0.1126	0.0281	0.1409	1	0.1409
R8	0.9523	0.0357	0.0119	0.0477	1	0.0477
Average						0.1313
Technological						
R9	0.9692	0.0307	0	0.0308	1	0.0308
R10	0.875	0.1111	0.1388	0.125	1	0.125
R11	0.918	0.0819	0	0.082	1	0.082
R12	0.922	0.0649	0.0129	0.078	1	0.078
Average						0.0790

Table 5.19 Risk exposure

Step 5 Determine the overall sustainable risk

In order to assess the feasibility of the cloud migration, it is necessary to identify risk for each sustainability dimensions. From Table 5.19, it showed that overall sustainability dimensions have very low risk exposure ((between 0.21-0.4).

Step 6 Decision for migration

It could be concluded that migrating to cloud is possible as overall controls are adequate to mitigate the economic risk, the environmental risk, the social risk and the technological risk.

v) Monitor the risk

As the decision for migration is taken, an initial monitoring activity should take into consideration the risk factors that do not have adequate evidence of control such as the economic and environmental dimensions. Furthermore, it is worth mentioning that once the migration has taken place, the MoH user new requirements need to be addressed. For example, if the management plans to expand the network capacity of cloud system, this decision may involve additional costs relating to integration, installation and maintenance. To show changes in the overall belief when estimation of cost changes, the above arithmetic measures are used to identify new degrees of belief, m-values as well as risk exposure within the economic dimension. If the changes vary in significant values and as such they may increase the probability for risk exposure, the organisation may reconsider to pay more attention to the budget estimation, which included hidden cost, monitoring and a contingency plan.

5.4.3 Case Study 3 Investigation SISA in the SAI

This case study is different from case study 1 and 2 as SISA is customised according to the size of organisation and the complexity of IS.

i) Study context

The State Audit Institution of the SAI was established in 1977 as an independent authority under the Federal Law of October, 1986. The SAI is accountable to audit government revenues, expenditures, management of the public funds and standards of governance across the SAI federal government. The SAI ensures that necessary precautions have been taken to safeguard the collection of revenues, expenses of public funds and maintenance of assets, and their disposals. In addition, the SAI also examined that activities and programs of the Federal organizations are achieved their objectives. The SAI has a total of 120 organizations to audit, twenty are Public corporations which are owned or partially owned by the Federal Government. The vision of SAI is to be recognised as the world's top audit institutions that promoting good governance in public sector. To date, the SAI has introducing a Guidelines in IS auditing, Best Practice for Compliance Audit and Quality Policy for IS auditors. Annual audit report on financial statements and operational activities of the public agencies is prepared and submitted to the Federal Council, to the Federal Supreme Council, the State President and the Council of Ministers.

The key objectives of the SAI are:

- i) To assess public finance management and operational activities,
- ii) To improve public service delivery and the management of public funds,
- iii) To identify fault and eliminate corruption,
- iv) To provide information to the public in relation to the management of public funds.

For SAI purposes, SISA is applied to review the IS control environment based on policies, standards and procedures. Under this context, SISA is used to identify of potential impairments of the ability to meet policies, standards and procedures, to monitor communication services, to identify threats/risks associated to IS performance and to examine on the usability of the IS in public sector organisation.

Execution of case study 3 was as follows:

Case 3 (External IS audit team)

- 30 June 2015 - briefing on SISA at the SAI
- 1-2 July 2015- finalising the sustainability indicator
- 6-7 July 2015 - getting familiar with estimating degree of belief for IS control evaluation
- 8-22 July 2015- fieldwork at the SAI
- 23-24 July 2015- concluding IS audit findings

ii) Study objective

The objective of this study is to examine to what extent the SISA framework can be applied in a medium size organisation and in a customised IS environment. We intend to analyse the most

important feature of the framework, elicit the needed requirements and use them to enhance the SISA framework.

1) Phase 1 Define IS audit plan

This phase begins with the selection of a public organization to be audited with the SISA framework. The case study was conducted in a medium-sized public organization. In order to protect the identity of the audited organization, all private information was set to be unidentified. The IS audit plan is similar to the previous activities by specifying the IS audit objective (s), IS audit scope, methodology, IS audit criteria and related audit information as a

guide to be followed by an auditor in performing the audit works. The first activity of the IS audit team is to identify the audit criteria in relation to the sustainability dimensions. In order to have a wide perspective on how the IS audit criteria interact with sustainability requirements, a series of discussions was performed to analyse the most appropriate criteria that can match the IS control objectives. In addition to the specified criteria for IS control evaluation, the organization decided to develop sub-criteria for sustainability.

These are:

- i) Social : Communication (responsiveness, complaints)
- ii) Technological: Usability (ease of use, user friendly)
: Performance (processing speed, security, information quality)

The second main activity is defining the audit scope of the SISA framework. The IS audit team decided that the scope of the audit was to review the organisation's general controls which include budget, physical controls, business continuity, change management, outsourcing, and security incident management. As a green IT was not widely implemented by public organizations in the ARABOSAI, the IS audit manager reserved the assessment for environmental sustainability for a future audit. Before beginning the audit, a pre audit meeting was held to discuss areas to be audited, sustainability dimensions and related indicators. IS auditors were also being introduced about D-S theory and the measurement of IS controls by using the evidence reasoning approach. Familiarity with the subject studied and methods used to carry out IS audit procedures were tested by the audit manager who discussed them in the course of meetings held with the audit team.

2) Phase 2 Execute the audit

The audit execution is about collecting and analyzing the evidence so as to reach to the IS audit conclusion. In this study, it involved five steps as narrated below:

Step 2.1 Collect evidence

In this step, the IS audit team gathered evidence based on the assessment of three sustainability dimensions (economic, social, and technological). The data was obtained via audit techniques such as inspection, review documents, records, and transactions produced by the IS, survey, re-performance, and interviews of the practitioners and experts within

organization. The method used to gather these data was influenced by the factors of sub-criteria. Summary of evidence collected are given in Table 5.20 – 5.22.

		Value	A	P	I
		BUDGET	ECONOMIC		
Attributes	Risk/Control	Description of controls/sustainability indicator			
	R1	Budget is prepared in accordance with rules and regulations.			
	C1	*Accurate accounting procedures	0.9	0	0.1
	C2	*Update budget and actual payment	0.9	0.1	0
	C3	*Authorised payment is made	0.9	0	0.1
	C4	*Determine acceptable variance	0.8	0.2	0
	C5	* Analyse trend of payment throughout the year	0.8	0.1	0.1
	C6	*Cost benefit analysis	0.8	0.1	0.1
	C7	*Timely budget report	0.8	0.2	0

Table 5.20 Evaluation of economic criteria

		Value	A	P	I
		SOCIAL			
Attributes	Risk/Control	Description of controls/sustainability indicator			
	R2	Availability of policies and procedures			
	C8	*Personnel policies and procedures	1	0	0
	C9	*Security policies and procedures	1	0	0
	C10	*Outsourcing policies and procedures	1	0	0
	C11	*Operational policies and procedures	1	0	0
	C12	*Physical assets policies and procedures	1	0	0
	C13	*Access control policies and procedures	1	0	0
	C14	*Business continuity control policies and procedures	1	0	0
	R3	Communication - Customer support			
	C15	**Responsiveness (24/7 effective)	0.9	0.1	0
	C16	**Complaints (effective resolution)	0.9	0.1	0
	R4	Availability of change management control			
	C17	*Examine change authorisation	0.9	0.1	0
	C18	* Examine version of change	0.9	0.1	0
	R5	Availability of outsourcing policy			
	C19	**Privacy (the safety of user data stored by the provider)	0.9	0.1	0
	C20	**The evidence that response time is according to SLA	0.9	0.1	0

Table 5.21 Evaluation of social criteria

		Value	A	P	I
		TECHNOLOGICAL			
Attributes	R6	Usability			
	C21	**Easy, simple and user friendly based on users' experience	0.8	0.1	0.1
	R7	Performance			
	C22	**Processing speed	0.9	0.1	0
	C23	*Security (transactions and communication are encrypted)	0.8	0.1	0.1
	C24	** Information quality	0.9	0.1	0
	R8	Disposal of information asset			
	C29	**Hardcopy destruction-cross-cut shred	0.9	0.1	0
	C30	**Soft copy destruction-erase with DoD 5220.22-M spec tool, deleted and empty recycle bin	0.9	0.1	0

Table 5.22 Evaluation of technological criteria

Step 2.2 Analyse evidence

This step presents an analysis of the collected evidence. The audit team measured the IS controls based on the evidence obtained from the IS controls assessment. Value of the adequacy of control is given based on the degree of belief according to the D-S theory

Step 2.3 Estimate risk probability and impact

This step determines the risk probability and impact based on the identified risks and evidence of controls. In this context, the degree of belief that control is able to mitigate a risk for C1 is 0.9 while the degree of belief that control exists that is either able or unable to mitigate a risk is 0.1. The m-values for these controls are shown in Table 5.23.

Sustainability dimension	Risk factor	Control ID	m-values		
			Adequate	Partial	Inadequate
		C1	0.9	0	0.1
	R1	C2	0.9	0.1	0
Economic		C3	0.9	0	0.1
		C4	0.9	0	0.1
		C5	0.8	0.1	0.1
		C6	0.8	0.1	0.1
		C7	0.8	0.1	0.1

Table 5.23 Summary of m-values

Similar procedures were followed to assess the environmental, social and technological dimensions. The m-values identified from controls were propagated to risk factor. The complete m-values are shown below.

Sustainability dimension	Risk factor	m-values		
		Adequate	Partial	Inadequate
Economic	R1	1	0	0
	R2	1	0	0
Social	R3	1	0	0
	R4	0.012195	0.987805	0
	R5	0.002736	0.997264	0
Technological	R6	0.1	0.45	0.45
	R7	0.666667	0.333333	0
	R8	0.012195	0.987805	0

Table 5.24 Risk factors and m-values

Step 2 4 Determine risk exposure

For decision making purposes, it is necessary to evaluate all risk factors and understand all the relevant issues. The summary of the complete assessment of overall m-values and risk exposure is depicted in Table 5.25.

Sustainability dimension	m-values			Plausibility value	Impact	Risk exposure
	A	P	I			
Economic						
R1	1	0	0	0	0	0
Average						0
Social						
R2	1	0	0	0	0	0
R3	1	0	0	0	0	0
R4	0.0122	0.9878	0	0.9878	1	0.9878
R5	0.0027	0.9973	0	0.9973	1	0.9973
Average						0.4963
Technological						

R6	0.5	0.45	0.05	0.5	1	0.5
R7	0.6667	0.3333	0	0.3333	1	0.3333
R8	0.1220	0.9878	0	0.9878	1	0.9878
Average						0.6070

Table 5.25 Risk exposure

Step 2.5 Determine the overall sustainable risk and level of sustainability

In particular, the number of sustainability dimensions that linked to a Low risk exposure is 2 (economic and social). Low risk exposure is interpreted as effective sustainability which indicate that risk exposure is significant and can be mitigated by the existing controls. However, technological dimension has a Medium level of risk exposure which indicate that there are evidence that technological risk are manageable.

3) Phase 3 Aggregate audit findings

The audit report that reflects the findings and conclusion is illustrated below.

Step 3.1 Generate audit report

Based on the obtained result in Table 5.25, it indicated that the overall sustainability dimensions have low risk exposure. These findings showed that continuous monitoring on IS controls is being conducted by the Department to ensure that economic, social, and technological issues are identified and resolved immediately as they arise.

Step 3.2 Recommendation

The Department should continue with its work to closely monitor the effectiveness of IS controls. All systems' aspects should be tested periodically to ensure business objectives are met and the reliability and the integrity of the information systems is sustained.

5.5 Summary

This chapter presents the evaluation of the SISA framework when applied in an IS audit practice in two public sector organisations with three different study contexts. SISA extends the traditional IS audit scope by adding the sustainability dimensions into the IS audit process. The results are further analysed and discussed in the chapter 6 to generalize our findings and assess the applicability of the SISA framework.

CHAPTER 6

Discussion

6 Introduction

This chapter discusses the results from the empirical investigation performed through three case studies context in Chapter 5. This chapter also demonstrates how the four research questions of this research were answered and justified. This chapter provides a summary response of the interviews and also discusses how the four research questions of this research have been addressed. Issues and difficulties faced in the IS audit are analysed and potential suggestion for improvement are given.

6.1 RQ1 How is the sustainability dimension incorporated into the IS audit process?

This question mainly considers the practicality of a sustainability driven approach for conducting IS control evaluation. The results and discussion of the questions showed that SISA was embedded in an IS audit process in the three audit phases; planning, executing and reporting. Feedback from IS auditors was classified into three related areas: relevancy, practicality and useful of SISA to be applied in IS audit process.

6.1.1 Phase 1 Audit plan

i) Economic dimension

The audit step of SISA in the audit planning phase was to include *economic* as an IS audit criterion with the selection of cost effectiveness analysis as a sustainability indicator. The cost effectiveness analysis was used to measure that the desired objective and anticipated benefits of IS investment were achieved. In reality, the cost effectiveness analysis was quite general to an IS auditor so it was possible to evaluate accounting procedures, variances, analyse trends of payment, cost of storage capacity, maintenance cost and training cost. The method of measuring these costs can be used to identify those public agencies which were limited by annual budget, and this information could be used as a monitoring tool as well as so as to minimise economic risk. Most of IS auditors indicated that cost effectiveness analysis allowed them to examine whether there was an optimum distribution of cost throughout the year. As such, if there are any changes or incremental changes in cost, it would be reflected in the account statement. In addition, IS auditors found that it was practical to measure the

maintenance cost of IS by applying indicators such as frequency of system offline, time between replacement/repair and the tested condition of the IS. The inclusion of cost-effectiveness analysis as a sustainability indicator for the *economic* dimension allowed IS auditors to concentrate on the efficiency of the cost management and the economic assessment giving quantitative information regarding which goals were reached and what actions to take to improve IS investment activities. Here, economic criteria were also used as a detective control for identifying IS control risk such as cost overrun, schedule overrun, changes in cost allocation as well as to be in line with financial rules and regulations. Example of feedbacks given by IS auditors in relation to economic criteria are shown in Table 6.1

Evidence	Source (Interviewees)	Interpretation
Case study 1		
“...such public spending is justified if we conduct cost effectiveness analysis; after all, it was mentioned in the government’s Guideline. The problem is that there is no enforcement to perform cost benefit analysis; in that case, we are just examining budget and other related IT costs.”	(01,03,05,)	Relevant
“I think that we need to conduct cost effectiveness analysis; we used to assess budget performance and I think that is sufficient.”	(07,09)	Relevant
“Cost benefit analysis was mentioned in the government’s Guideline, but there is no instruction or direction provided by the Guideline”.	(07)	Relevant
Case study 2		
“ ..assessment on cost effectiveness is especially for evaluating a huge amount of IS investment”.	(02,06)	Relevant
“We performed cost effectiveness only on ad-hoc basis”.	(04,08)	Relevant
“We didn’t normally perform cost effectiveness analysis, but we are planning to examine the benefits from using IS in our the next audit”	(02,06,)	Relevant
Case study 3		
“Defining sustainability indicator for sub criteria within economic dimension is uncomplicated as measuring economic performance in relation to IT investment is a typical practice carried out by an IS auditor.”	(13,15)	Relevant
“ ..cost effectiveness analysis can enhance the transparency and accountability of IS investment”.	(11, 12)	Relevant

Table 6.1 Feedback on economic sustainability assessment

- Justification on the inclusion of cost effectiveness as economic criteria in SISA.

IS auditors from case study 1 and 2 were of the opinion to conduct a cost effectiveness analysis due to several reasons. To start with, it is a requirement of the government to develop cost effectiveness analysis as stated in the Malaysian Guideline for ICT Procurement (2013), an economic analysis is important in event of impact assessment, and the cost effectiveness analysis assists and IS auditor to examine whether resources were under-utilised or whether they were mismanaged.

For public sector organization, revenue form the taxation is used to fund facilities, infrastructures, and IS projects and does not represent a net gain of expenditure. Therefore the IS auditors from case study 1 and 2 sometimes perceived that the evaluation of cost-effectiveness was irrelevant due to several factors; the public sector is not a profit oriented organisation, and a financial auditor might have performed the cost effective analysis.

While IS auditors from case study 3 were of the opinion to include cost effectiveness in the economic criteria. They perceived that cost effectiveness assessment can enhance transparency and accountability of IS investment in public sector organization.

ii) Environmental dimension

The environmental dimension is included in SISA as an effort to reduce environmental impact by applying green IS within public sector organisation. Green IS benefits the environment by improving energy efficiency, using less harmful materials and IS equipment, and encouraging reuse and recycling. Factors such as environmental rules and regulations, corporate images, and public perception increase motivation to the green IS implementation. Environmental dimension is relevant in SISA as the green IS will be continue to be an important issue for IS implementation. Example of feedbacks from the IS auditors are depicted in Table 6.2.

Evidence	Source (Interviewees)	Interpretation
Case study 1		
“We know that green IT is considered to be the subject of the IS audit, but policies and procedures on green IT are inadequate. We observe that certain functions in a public organisation do apply the green IT concept such as paperless practice and green IT disposal policy”.	(01,03,07)	Relevant
“It is common practice for an organisation to replace older IT equipment with a green friendly IT infrastructure, and we believe the overall energy	(05,07,09)	Relevant

consumption is reduced and efficient use of energy in operational activities is maximised”.		
“.. most of the green computing adoption in Malaysian public organisation focused only on data centres, and we are sure that the organisation adopted green IS infrastructure as stipulated in the EG meetings”.	(01,03)	
Case study 2		
“ The available IS Audit Guideline does not include environmental assessment, but we can always refer to the available Best Practice”.	(02,04)	Relevant
“Sometimes we assessed how organisation dispose their old IT assets, so far the disposal procedures are compliance to government rules and regulations, but we are unsure whether the procedures are adhered to environmental regulations”	(08,10)	Uncertain
Case study 3		
“We can only include environmental assessment for the next audit program if it is required by the organisation”.	(11)	Not relevant
“We don’t include the environmental dimension in our IS audit because it is not a compulsory at this moment”.	(13,14,15)	Not relevant

Table 6.2 Feedback on environmental sustainability assessment

- Justification on the inclusion of environmental criteria in SISA.

In relation to the environmental dimension, the NAD and the SAI have not seriously considered green IT assessment when conducting the IS audit. However, in Case study 1 and 2, observations were conducted informally on resource sharing such as printer sharing, photocopier sharing, paperless practice and green IT disposal for unused IT equipment (as mentioned by interviewees 01, 03, 07). Green IT has been widely discussed in the public domain. The interviewee (01, 03) claimed that Malaysian public sector organisation adopted green IS computing as stipulated in the Electronic Government’s meeting. However an appropriate policy and procedures with green IT controls do not yet exist for the IS auditors to used. Two interviewees highlighted their reasons why most public organisations lack in practicing green IT. According to (01, 03), the existing IS Audit Guideline does not include environmental assessment and also due to the existing IS audit objectives, which place less emphasis on green IS auditing (02, 04). While, IS auditors in Case study 3 completely removed green IS assessment from their audit work. The justified that green IS audit is not so crucial compared to IS control evaluation.

iii) Social dimension

Social sustainability concerns on the commitment form public sector organisation to provide effective service delivery to citizens. The social aspect of an IS audit covers a wide range of issues, but in this research, only the main components of the social dimension were included in SISA. Feedbacks from IS auditors are shown in Table 6.3.

Evidence	Source (Interviewees)	Interpretation
Case study 1		
“We don’t take seriously to evaluate IS Strategic Plan as we have a scheduled meeting on IT development within public sector chaired by the Malaysian Administrative Modernization and Management Unit (MAMPU)”.	(01)	Not relevant
“We, as external auditors, faced a huge challenge when evaluating IS performance in the public sector. There were a number of cases when the systems have been developed but have gone down as white elephants, using public money, giving back nothing. Now, the inclusion of IS Strategic Plan, and user’s satisfaction surveys, full assessment on the system design and development can be efficiently implemented”.	(01,09)	Relevant, useful
“The use of sustainability indicator in assessing technological dimension is very new for us, we found it a bit difficult to develop an appropriate indicator as it was none in the IS Audit Guideline. However, we agreed that these indicator are able to reflect the actual situation of the IS in the organisation”.	(05,07)	Relevant
Case study 2		
“We review minutes of meeting from the IT development committee meeting (MAMPU), not the IS strategic plan. With the inclusion of the IS Strategic Plan, we are able to determine the priority and budgeting cycle of the IS”.	(06,08)	Relevant
“Implementing SISA with an emphasis on the social aspect has enabled auditors to analyse IS and response to management needs through comprehensive reporting. With the use of the sustainability indicator, an auditor is able to ascertain a benchmark regarding the transfer of knowledge from the system developer to the public sector.”	(02,04,06)	Relevant, practical
Case study 3		
“Assessing social criteria in IS audit allows IS auditor to identify the current and potential IS problems in organisation”.	(10)	Relevant
“Time consuming for developing survey and approaching respondents to answer questions;	(11,12,14)	Relevant, useful

however, the results obtained have been very useful for an auditor”.		
--	--	--

Table 6.3 Feedback on social sustainability assessment

- Justification on the inclusion of social criteria in SISA.

Before implementing SISA, most of auditors in Case Study 1 and 2 paid less attention to the examination of the IS Strategic Plan. In their opinion, IS Strategic Plan was the only document which has little significance for IS control evaluation. As required by SISA, the IS Strategic Plan must be examined, therefore it was seriously analysed by IS auditors in terms of its actual implementation. As required by SISA, a number of documents were reviewed to explore matters related to in-house IS, IS project monitoring, and examining the control of all decisions contributing to the policy making, in terms of the effective and efficient use of IS resources. IS auditors in Case study 1 and 2 found that by examining the IS Strategic Plan, they were able to examine the mechanisms that help organisation to meet IS objectives, the IS priority and the budget allocation for the IS project (01, 05, 06, 08, 09). Apart from the IS strategic plan, the IS auditor also assessed third party services in relation to service delays, the number of service level targets set out in the SLA being met and the availability of escrow agreement.

As regards to social assessment, this research identified three factors that IS audit benefit most from social dimension in SISA:

- i) Interviewing user to gather information such as the effectiveness of transfer of knowledge, market study for hardware and user’s involvement in system development is useful and relevant;
- ii) Sustainability indicator drives IS auditor to really understand about the efficiency and the effectiveness of IS controls by interacting physically with the organisation’s business environment;
- iii) Assessing KPI for business and KPI for IS. SISA allows IS auditor to examine the track organisation’s performance and IS performance.

In social dimension assessment, the IS auditors were required to apply sustainability indicator to assess social criteria. The implementation of the sustainability indicators required IS auditors to spend more time to develop questionnaires, analyse, and reach a conclusion from their findings. In this case, IS auditor from Case study 3 claimed that development of sustainability indicator is time consuming and tedious. However, they agreed that the

assessment of social criteria is relevant as the current and potential IS problems in organisation can be identified and determined.

iv) Technological dimension

The technological dimension in SISA concerns on the continuity of IS to deliver service, assessing user’s satisfaction, maintenance, flexibility, and scalability. The technological assessment has the potential to highlight risk areas and emphasis on effectively and efficiency of IS to support business objective (s). Example of feedbacks given by IS auditors are shown in Table 6.4.

Evidence	Source (Interviewees)	Interpretation
Case study 1		
“In practice, we need to understand entity’s business operation and information systems background such as application process, administrative, controls and procedures. We most concern on how do the application systems work or does the auditee encounter any problem or error during implementation. After gathering some information on the system background, we get ourselves familiar with the system by studying their User Manual, Implementation Report and by performing a walk through test. As SISA has introduced a number of assessments in relation to the technological aspect, we have extended our work to examine flexibility, continuity of process, and scalability of the IS which are very relevant to IS auditing.”	(01,05,07)	Relevant, practical
“The IS audit is usually the process through which to evaluate the effectiveness of IS controls which focus on general and application controls. The SISA adoption covers a wider area such as scalability, flexibility and availability service to users.”	(05,09)	Relevant, useful, practical
“We found the application of sustainability indicator was practical, it is new for us but we have no problems to use it for the next audit program”.	(05,07)	Practical
Case study 2		
“We have to audit all types of controls, either within the systems or outside the systems, by having indicators based on which to assess technological dimension; it makes our audit work easier and, at the same time, it improves IS audit procedures particularly for assessing the technical aspect”.	(02,04,06)	Relevant, useful
“Including technological aspect and other sustainability dimensions in SISA, it has broaden the scope of internal control assessment and enabled internal auditors to do an in-depth analysis of IS	(02,08)	Relevant, useful

control issues in order to provide a concrete advice to the management”.		
“Assessing scalability allows IS auditor to examine the response time and network performance of the IS”.	(04,06)	Relevant, Useful
Case study 3		
“The IS audit is to evaluate the effectiveness of IS controls which we normally do. The SISA adoption covers a wider area such as scalability, flexibility and availability service to users We found it very positive and informative”.	(13,14,15)	Relevant
“It is new for us on assessing scalability and flexibility of the IS. This two sub-criteria can tell IS auditor how sustainable of the IS in public organisation”	(11,12)	Useful

Table 6.3 Feedback on technological sustainability assessment

- Justification on the inclusion of technological criteria in SISA.

There is an increasing appreciation by the IS auditors in Case study 1 and 2 about incorporating technological dimension in SISA. This is motivated by the impact on the IS failures to user, organisation and also to IS auditors. IS auditors were, at some degree aware on the important of assessing scalability, flexibility, disposal of information assets as well as security in the IS audit process (01,02,05,07,08). By evaluating scalability, IS auditor is able to identify the ability of the IS system to be performed in a certain workloads and identify problems if system overloaded with a huge amount of users (01, 03, 05). Risk associated to scalability such as network latency, and delay on the system can be easily addressed by the IS auditors (04, 06). In Case study 3, technological criteria in term of scalability and flexibility are new for the IS auditors, and found it very informative. They were optimist about IS audit findings for technological dimensions as it can reflect how sustainable of the IS in public sector organisation.

Summary of the audit planning phase in SISA

From the above discussion, it is evident that no significant problems were found in the audit planning stage. 90% of IS auditor found that SISA support for an effective IS audit by applying a wider approach to the control evaluation from different perspectives and various angles. IS auditors in both IS Audit departments (NAD & SAI) found it difficult to change the focus from their current practice to a sustainability driven approach. Auditors had to be advised to develop sustainability indicators according to specific sustainability dimensions.

The main reason why auditor perceived the development of sustainability sub-criteria and indicators as complicated was that IS auditors only focus on the Department IS Audit Guidelines. This in turn, caused them to fail to include sustainability requirements in the audit process. After several hours of discussion during the interviews, the interviewed IS auditors agreed that they could develop and adapt the new IS audit criteria, sub-criteria and indicators. They also agreed that this stage is the core of an IS audit process, and intensive and advanced training is essential for IS auditors to help them to distinguish the most appropriate sub-criteria and the indicator of sustainability. 85% of the interviewed IS auditors preferred to keep the SISA indicators for future audit work rather than developing their own from scratch until they feel confident to develop their own indicators. It was also found that the results of an IS audit can vary depending on the nature of business of the organisation, and this may require auditors to develop a new sustainability indicator. Such developing indicators tend to be restricted by the measurable area and keeping indicators up to date by constant reviewing is much more important than developing indicators.

6.1.2 Phase 2 Audit execution

i) IS control evaluation

In a real working environment, IS auditors must exercise professional judgment at all phases of the audit process and there is no arithmetical analysis involved. Most of interviewed IS auditors were familiar with terminology ‘reasonable assurance’ in financial auditing; this is when the auditors obtain sufficient appropriate audit evidence to reduce the audit risk. From an IS audit perspective, the effectiveness of IS control comes from subjective judgment in relation to whether there is “reasonable assurance” that the objectives of the control are met. Within this content, it is very important to mention here, that SISA enabled IS auditors to provide appropriate levels of judgment/“reasonable assurance” based on their experience, skills and perception. Using SISA, IS auditors could start their process of seeking “reasonable assurance” by assigning m-value to the selected IS control that represent one observation. These m-values were then aggregated to determine the probability value for each risk factor.

At the beginning of the implementation and due to lack of systematic checklists and guidance, most of IS auditors faced difficulties in giving their judgment about the adequacy of IS control to mitigate risk. However, they found it very straightforward, uncomplicated and that it made their judgment more reliable after they became familiar with SISA. 95% of interviewed IS auditors believe that SISA provides a relevant, practical and reliable approach for giving one’s

judgment. They suggested that a customised audit checklist should be made available to ensure that auditors implement SISA in the best way possible, to reduce the time spent in the field and as an added value to the auditor’s competency. Examples of the findings are shown in Table 6.5.

Evidence	Source (Interviewees)	Interpretation
Case study 1		
“Different control requires different audit procedures. First we reviewed documents such as policies and related regulations to obtain information about the control, then we conducted a walk through test to confirm the effectiveness of controls; then only we can determine the adequacy of controls”.	(01,09)	Practical
Case study 2		
“Documents might be misplaced or missing and may not be available for some reasons. In such case, we would reach the conclusion that this control is not adequate. In relation to such cases, SISA is helpful because it provides us with a selection of three categories, which I think is practical and convenient”.	(02,08,10)	Practical and helpful
Case study 3		
“Sometimes control systems are available, but it is only when we carry out additional tests on the figures such as reconciliation, completeness, then only we discovered errors in IS. For such scenarios SISA proved to be very effective and assisted us to justify about the adequacy of control.”	(11,13,14)	Relevant, Practical
“SISA facilitate us to make decision, when we discovered that we found less audit evidence to assure the adequacy of control, we assumed the control is less effective, so we judged it was ‘Partially adequate’”.	(12,15)	Practical

Table 6.5 IS control evaluation

- Justification on IS control evaluation

In both IS Audit departments (NAD & SAI), IS auditors gave positive and constructive feedback. They found that the introduction of numerical analysis in the IS audit work is very practical, easy to understand and it also justifies their findings. They also appreciated the need of collecting detailed data or evidence in order to work with such complex level of analysis. A clear definition of ‘Adequate’, ‘Partially adequate’ and ‘In-adequate’ were given

in the SISA framework. Therefore, there was no confusion to IS auditors about how to judge the adequacy of IS controls. In addition, the framework did provide sufficient guidance about how to assess whether the IS control is ‘Adequate’, ‘Partially adequate’ and ‘In-adequate’ to mitigate risks. During the SISA implementation, 5% of less experienced IS auditors were reluctant to provide value (degree of belief) for certain IS controls due to the following reasons:

- Insufficient guidance to establish the value,
- Uncertainty whether the evidence obtained was satisfactory and,
- Difficulties in providing justification for their judgments.

It is evident that SISA facilitates IS auditors to derive a final judgment on the IS controls evaluation. It was evident in Case study 2 and 3 where (02, 08, 10) claimed that the IS control categories is practical and convenient. While (12, 15) mentioned that SISA assists them to justify about the adequacy of IS controls.

ii) Estimate risk probability and impact

In SISA, risk probability and impact are determined in order to arrive at risk exposure. Based on the degree of belief, IS auditors were required to measure risk probability and impact. During the IS evaluation, IS auditors interviewed personnel who were involved in key process activities to achieve better results in providing judgment on audit evidence. IS auditors from both IS Audit departments found that by reaching an audit conclusion according to the level of risk exposure, IS auditors were capable to focus on the right dimension to prioritise risk impact. Evidence of the feedbacks of IS auditors are shown in Table 6.6.

Evidence	Source (Interviewees)	Interpretation
Case study 1		
“I think SISA is relevant and has the capability to assess control risk in key areas within an organisation; however there is a paradox related to the size of the organisation. Small public organisations such as Local Authority don’t really emphasise on environmental and social aspects as they’re not exposed to great risks”.	(01,03,05)	Relevant Useful
“The rationale of an IS audit is to ensure the effectiveness and the efficiency of IS controls. This risk assessment was	(05,07,09)	Relevant Useful

complicated but very useful in assisting an auditor to form an audit opinion.”		
Case study 2		
“It is bit complicated to measure probability of risk, since it has a long formula, but the result was very informative and useful”.	(02,06,)	Relevant Useful Informative
“Risk assessment has been continuing interest for auditors such as inherent risk and control risk. In particular, we need a quantitative model to distinguish both risks and their interdependencies. SISA guides the auditor to measure control risk from four key dimensions as well as risk indicators, which I found very useful”.	(08,10)	Relevant Useful
Case study 3		
“Sometimes, IS auditors are known as business advisers. In this view, measuring risk exposure to form an audit opinion is quite new but it aid IS auditor to highlight area that need proper attention from the management. Also I agreed outcome of SISA is capable to produce concrete IS audit report”.	(11,12,13,14)	Relevant Useful

Table 6.6: Estimate risk probability and impact

-Justification on estimate risk probability and impact

65 % of IS auditors in both IS Audit departments (NAD & SAI), thought that assessing risk exposure as a basis to form an audit opinion about the sustainability level of IS has accelerated the communications and decision making process between the auditors, users and the organisation. However, for this assessment, only an experienced auditor who possesses reasonable audit skills and knowledge can provide appropriate judgment as less experienced IS auditors were not confident to measure IS controls as mentioned above. 90% of IS auditors considered that the IS control evaluation method is reliable and can be used by both types of auditor (internal or external). They suggested focusing only to critical areas such as financial dimension rather than the environmental dimension so as to reduce the time needed for gathering evidence. For example (01,03,05) claimed that SISA approach is relevant and has the capability to assess control risk in key areas within an organisation; however there is a paradox related to the size of the organisation. Small public organisations such as Local Authority don't really emphasise on environmental and social aspects as they're not exposed to great risks.

55% IS auditors were of the opinion that SISA has introduced comprehensive methods in risk assessment, which is different from the current practise according to which IS auditors are required to provide just a “yes” or “no” answer. (11, 12, 13, 14) claimed that IS auditor needs to produce effective IS audit report as their role is not only auditor but also business adviser. In this view, they agreed to measure risk exposure as they are able to derive a practical and effective conclusion based on the risk exposure analysis. From the SISA evaluation, it was also found that IS auditor prefer to have a quantitative model to measure controls and risks. So that, they can see a problem more quickly (08, 10).

At the execution phase, IS auditors from both IS Audit departments prepared notes to be included in the working paper files for SISA. This discussion notes bring together findings and evidence for a specific segment of the audit. The discussion notes were used to ensure that the IS auditors correctly understood the process or activities and to assist them in the discussion of major issues that have emerged during the course of an audit. Before arriving at a conclusion on the audit findings, it is common practice that they have to confirm the finding facts with the auditee. By doing so, the auditee becomes aware of the weaknesses in their system or activities that would be reported in the audit report.

Difficulties were faced at the initial step, when IS auditors have to execute the IS control evaluation for the first time. IS auditors in both IS Audit departments found it difficult to measure probability of risk by using the formula given. However, after several practical sessions, they got familiar with the concept and the calculation. 92% experienced IS auditors believe that knowledge on how to measure risk exposure is very important as a basis to form level of IS sustainability. Finally, they were asked about how they felt about using SISA for IS control evaluation and risk assessment, 90% stated that it was relevant and result was useful. 93% of IS auditors agreed that SISA provides a systematic way to analyse risk for decision making.

6.1.3 Phase 3 Audit report

A formal meeting known as exit conference is usually held at the conclusion of the audit. The audit team and the officers in charge attend the meeting to discuss about the audit findings, and when appropriate they may include recommendations. This was also followed in the SISA implementation. The interviewed IS auditors who were represented by their team leader held an exit conference to present their findings and feedback on using SISA. It was agreed that

presenting findings related to the level of IS sustainability was an entirely new process for an auditee. It was clear that the auditee was quite unfamiliar with the terminology and the approach. However, after a detailed explanation about the purposes of the sustainability perspective by IS auditors, this new terminology became clear to them and they agreed to proceed with the discussion. It also worth mentioning that during the meeting, auditors presented their findings on economic, environmental, social and, technological issues. The draft report covered the following points:

- The level of sustainability for IS,
- Prediction on IS weaknesses/failures within sustainability dimensions,
- The assessment and sources of IS control risk, how knowledge of this risk can help users/organization understand the audit findings,
- A way to bridge the gaps in environmental and social efforts.

Furthermore, during the exit conference, how to reach common understanding particularly on financial management and third party service performance was discussed. In addition, 77% of the IS auditors also raised other matters, which might not be significant enough to be included in the audit report, to be addressed for improvement, such as environmental sustainability. However, at this stage, only the draft findings were presented.

Usually, many organizations tend to take a defensive and arguing position when it comes to responding to the audit finding. However, SISA provided additional evidence on IS control evaluation that clearly gave the facts and reasons for what was argued. The interviewed IS auditors were also asked about their feelings on using the SISA for reporting findings from a sustainability perspective. They agreed that the results obtained added value to the current audit report. In addition, they willingly added that SISA has extended the role of IS auditors to detect and report weaknesses found in public agencies information systems. They believed that development of risk exposure allowed them to determine more clearly the weaknesses in the sustainability dimensions that they had to assess. They also agreed that the fact that the uncertainty of estimation is supported by a suitable measurement precision helps in providing an effective audit opinion on IS.

To sum up, by adopting SISA, IS control evaluation can be assessed effectively by using appropriate sustainability indicator. As the integration of SISA in the IS audit process started

with the sustainability dimensions as audit criteria, 85% of IS auditors found that sustainability criteria were less complicated to develop, but the procedures followed to judge the adequacy of IS control were not an easy task to accomplish. They suggested the following in order to improve SISA:

- i) Provide definition if no control available,
- ii) Design checklist which explains how to execute SISA, including IS control evaluation and risk assessment and,
- iii) Develop tools for calculating aggregate evidence.

On the other hand, they pointed out that they found the sustainability indicator to be very useful in measuring IS from both non-technical and technical aspects. Auditors also stated that assessment on risk exposure provides significant information for IS auditors to give their opinion to the auditee about the level of IS sustainability. Finally, all of the IS auditors agreed that the procedure was relevant and useful in enhancing the IS audit process. In fact, the Director of IS Audit from both IS Audit Departments claimed that the risk assessment procedures were acceptable and justified because they provide information to detect weaknesses in the IS that they would have otherwise neglected.

6.2 RQ2 Could SISA be implemented in different types of organisations?

This research investigates the practicality of SISA to be implemented within different types of organisations. In other words, this means different situations in terms of firm size, complexity of IS control systems, and strength of controls. Therefore, the first case study used in this research, represented an actual large-size organisation, with IS control systems of high complexity, and a reasonably strong IS control structure. The second case study represented a medium-size organisation, a fairly strong IS control structure and have a different IS audit scope. The third case study represented a medium-size organisation with less complex and well-controlled computer systems.

6.2.1 Defining the context

Firstly, the context, scope, and audit objectives of the SISA were defined. Meetings and discussions are the main techniques used by the organisations under study to define the context. Preparation for conducting SISA began with a meeting to review the guidance materials provided to the audit staff, to have a discussion about the new methodology and review several Departments to be selected for implementing SISA. It is important that the

SISA framework is addressed carefully and understood to prevent any unnecessary use of resources.

The selected cases to be investigated were chosen for the following reasons;

- The first selected case has sufficient size and complexity to demonstrate that the change in current audit practice would be reflected in the working papers and audit report;
- The second selected case study has additional IS project such as cloud migration plan;
- The third selected case study has medium size and complexity, as field work for data collection was limited.
- The availability of IS audit team (internal and external) and related resources for the empirical investigation.

6.2.2 Defining the criteria, sub-criteria and indicators using SISA for the case studies

The first case study focused on explaining the complete process of SISA including assessment on general controls and application controls. IS auditors were involved in case study 1 and they gave very positive and constructive feedback about SISA. SISA was used in the second case study as a basis for decision making process. It is important to mention that SISA sustainability criteria remained the same but the sub-criteria were tailored by IS auditors according to the needs of cloud migration process of the organisation under study. There is no specific guidance to select sub-criteria for cloud migration, it was performed by a discussion between the IS auditor and the management. Finally, in case study 3, SISA was implemented in a medium size organisation which has less complex information systems. The IS auditors in this organisation (case study 3) excluded the environmental dimension and focused only on economic, social and technological dimensions. Sub-criteria and indicator were also developed and customised according to the size and objective of this organisation.

No problems were found when implementing SISA in a different organisation and with a different audit scope. SISA was found usable, i.e., practical and operational, in all three different types of IS audit scopes. As SISA was new to IS auditors, they had to be reminded on the development of sub-criteria of sustainability dimensions and its indicators. The IS audit report process was deemed to be effective and informative by most of IS auditors. The result from risk exposure was very useful to provide relevant information to IS auditors to highlight significant issues of an auditee's information system. What is more, the results from

the studied context concluded that the SISA approach was applicable and flexible to support the auditee with their cloud migration decision.

The three case studies were performed in a real IS audit practice, and all of the procedures in the SISA were followed by the three case studies for making decisions and producing an IS audit report. Because of SISA, feedbacks from respective agencies were received, for case study 2, cloud migration decisions were made. This showed that the SISA has a good degree of usability and can be customised depending on the size of organisation and level of IS complexity.

6.3 RQ3 To which extent does the SISA framework affect the IS audit process?

The SISA framework offers the opportunity for experimentation with IS auditors, and provides new insights into an IS audit process, consistency of decision and effective audit report. During the experimentation, feedback from IS auditors was collected to examine three key factors, i.e., whether:

- They have reasonable knowledge about SISA,
- SISA procedure can be easily followed, and
- They are able to provide effective audit opinion based on economic, environmental, social, and technological dimensions.

Feedback from the practitioners supported this research finding relating to integrating sustainability dimensions to IS audit practice. It demonstrated the appropriateness of the degree of belief technique for the specific risk assessment as a basis to highlight weaknesses in information systems. The most important quality factor for the new framework to be adopted by users is understandability which is also an attribute for usability (Bae, Chae and Chang, 2013) and acceptability. Testing the understandability of the framework is considered crucial in order to ensure its relevancy to the IS audit work. The understandable framework can support maintenance activities to analyse, modify and extend a system for correction, adaptation, and perfection (Bae, Chae and Chang, 2013). To ensure understandability within SISA, it is important that SISA is consistent in each audit activity. This means that the audit team has the same level of understanding when using SISA in establishing audit criteria, performing judgment on IS control, and measuring risk exposure. To ensure this, the following three points were discussed.

6.3.1 Issues related to SISA process

87% of IS auditors gave positive and constructive feedback about the SISA process. They found that the incorporation of sustainability into IS audit criteria is very practical, relevant and flexible to integrate into the existing audit activities. The evaluation of economic and part of social and technology aspect are similar to the current IS audit process. While assessing environmental compliance is new to most auditors, they found it useful and auditable. The proposed techniques to perform audit work for measuring the adequacy of control and computes the probability value of risk, most of auditors faced difficulties in performing these two important tasks. Measuring audit judgment was a challenging task for them in practice even though in theory, they were aware of professional judgment, inherent risk and control risk.

However, confusion was expressed by some auditors about how to judge the adequacy of controls in a numerical form. They asked for clear definitions about what constitutes a 'Partially adequate' and 'Inadequate'. They also found that 'Partially adequate' and 'Inadequate' are no different in terms of control implementation. 93% of the auditors need more guidance on how to aggregate risk to derive the value of risk probability. However, when the problem of aggregating risk was solved and the process completed, they faced no challenge in identifying the impact of risk and the overall sustainability risk. When finalising the outcome of the SISA, all of auditors agreed with the sustainability scale provided and the process of how to formulate their opinion on the level of IS sustainability were fully understood.

6.3.2 Analysis on output

Output from SISA is the most significant for IS audit work as it reflects an independent opinion of an auditor to the public, the user and the organisation. Output from SISA was very much appreciated specifically on risk exposure analysis in order to decide the level of IS sustainability. Auditors agreed to report on risk analysis rather than a compliance-based analysis and SISA seems to meet the requirements. The use of professional judgment and support from analysis proved to be very useful and innovative for the current practice. As the sustainability issue becomes more important nowadays, the management agreed that results obtained with the use of SISA were better than those obtained by taking the common compliance approach. Auditor (05 and 09) said that there were errors or issues that they overlooked when conducting IS audit, but with SISA they were able to address those issues when we performed a survey on user's satisfaction for system implementation. In addition to

highlighting controls assessment and value for money, an auditor may include findings in the audit report in relation to social concerns, economic benefits, technical aspects and environmental concerns as an adding value for the IS auditing practices.

6.4 RQ4 What are the challenges faced by the IS auditor when adopting a sustainability driven IS audit framework?

A sustainability driven IS audit framework emphasises a risk based approach as a basis to form an opinion about the level of sustainability of IS in public sector organisations. The level of sustainability guides IS auditor to highlight weaknesses in IS from an economic, environmental, social, and technological perspective. However, there are also challenges associated with SISA. Some of the observed challenges are given below:

- The interaction of SISA with the auditee, and the extent of IS audit testing.
- To identify the sustainability indicator and to justify the selection.
- To reduce the bias when making IS control evaluation based on theory of belief.

6.5 Summary

The results of the evaluation showed that SISA provides a comprehensive approach of IS audit. SISA is designed based on the basic definition of the audit and measures IS performance from the view of key users. The above discussion shows that the underlying activities within the SISA process were easy to follow, implying that it has a good degree of practicality and usability. Issues relating to the lack of proper checklist and lack of clarity of some definitions were noted during the course of IS audit work. However, despite these issues, the IS audit team from all three case studies agreed that SISA was practical and aided the IS audit team to produce concrete IS audit findings based on the level of IS sustainability. This indicates that SISA is able to enhance IS audit work regardless of the fact that some documents need further improvements.

CHAPTER 7

Conclusions and recommendations

7 Introduction

The purpose of this research is to develop a comprehensive sustainability driven IS audit framework that can be used by IS auditors in public sector organisations to highlight significant IS risk area and to produce effective IS audit judgment. In order for the framework to be successfully implemented, it is necessary for the research to reach an understanding about the IS audit practice, the sustainability dimensions, and evidential reasoning theory.

7.1 The fulfilment of the research objectives

The SISA has been designed, developed and validated against three case studies in order to meet the aims of the research which was *to develop a comprehensive sustainability driven IS audit framework that can be used by IS auditors in public sector organisation for an effective IS assessment*. Four objectives were set and pursued to successfully achieve the research aim. These are stated below.

Objective 1: To investigate the feasibility of the sustainability dimensions to enhance IS audit work.

During the process of achieving this objective, sustainability dimensions were researched and determined. This formed the basis of the search to improve the existing IS audit practice. Objective 1 has been met in Chapter 2 and Chapter 5. Chapter 2 discussed the background of the IS audit and sustainability dimensions were introduced to be incorporated into the IS audit work for evaluating different aspects of IS within public organisations. In Chapter 5 it was shown that the applicability of sustainability driven IS audit process to a real case study has been very promising. The results indicate that the sustainability approach is a practical and reasonable method that can be employed at a public sector organisation. However, the proposed IS audit process needs refinement based on the feedback obtained from the case studies. In this case, the researcher is planning to redefine the activities such as providing a

comprehensive Guideline which will include an audit program, a template for finalising IS audit judgment and an automated tool for documenting the degree of belief (result from the D-S theory).

Objective 2: To investigate the usability of the framework from different size of organisation.

Objective 2 has been fulfilled in Chapter 5 and Chapter 6 in which the research found that SISA is effectively integrated in organisations of different sizes and with different IS objectives. This research compares the applicability of four sustainability dimensions within IS audit process. The outline sustainability dimensions and their indicators were considered based on their general applicability to IS audit process. Upon applying SISA, this research found that the IS audit processes are understood in many ways, and are applied according to the size and the need of the organisation. Thus it seems that the SISA can be used for assessing IS controls of high complexity, for cloud migration decision and can be customised according to the size organisation with-less complex and well-controlled computer systems. IS auditors can easily learn and use the SISA; the only prerequisite is the basic knowledge of IS audit, risk management and the selection of sustainability indicator. The IS auditors who integrated SISA into the IS audit process were satisfied with the outcome as SISA accelerates the decision making process and highlights IS risk area.

Objective 3: To produce an extended IS audit report with the inclusion of a level of IS sustainability.

Objective 3 has been accomplished in Chapter 5 and Chapter 6. An assessment of the interview data indicated that sustainability is capable to address consequences that may impair the effectiveness of IS control and the success of cloud migration such as IS investment, cost estimation, service level management and security. These consequences or threats were further analysed and narrowed down for identifying the level of IS sustainability. Positive feedback was received from IS auditors, specifically on risk exposure analysis as a basis to form an IS audit opinion about the level of IS sustainability.

Objective 4: To validate SISA in a real IS audit within public sector organisations and to provide a novel contribution to the IS audit from a sustainability perspective.

Objective 4 is fulfilled in Chapter 5 and Chapter 6. Once the SISA had been developed, it is important to validate it the aid of an appropriate case study. Three case studies in a real

auditing conditions were selected to evaluate the applicability of SISA to enhance IS audit work. The case studies allowed the assessment of SISA in great detail, and the IS audit procedures were assessed using two key factors; understandability and acceptability. The validation results support the view that that SISA can be applied in IS audit practice in order to help public sector organisation to better measure their IS performance. The SISA also provides IS auditors with a solid justification about the level of IS sustainability, to enhance the scope of IS audit work, improve IS auditor's competency and, as a result, add real value to the public sector organisation through IS audit.

7.2 Contribution to the body of knowledge

This research has contributed theoretically and practically to the existing body of knowledge, particularly in relation to IS audit practice.

7.2.1 Theoretical contributions

The theoretical contributions are reflected in the findings, the methodologies adopted which underpinned the interrelationships of the IS audit, the sustainability approach as well as the concept of risk and uncertainty.

- i) This research is the first study to contribute to the literature by covering sustainability dimensions, sustainability indicator to judge how the Information Systems of a public sector organisation are performing.
- ii) This research is the first to conduct a comprehensive assessment of the IS audit practice in Malaysia.
- iii) This research provides a framework on how IS audit practice can be improved through an application of risk exposure analysis to decide on the level of IS sustainability.
- iv) This research is the first study to introduce the D-S theory of belief functions into the SISA framework for representing uncertainties in the IS audit.

7.2.2 Contribution to the real audit practice

To start with, there is the development, refinement and testing of a SISA framework to conduct IS audit with a focus on the level of IS sustainability. The results of this research should be of interest to both academics and IS audit practitioners. The SISA framework is designed to be used in decision making process, aid IS auditors in formulating an audit

opinion and giving appropriate recommendation for preventive and correction actions for IS improvements.

7.3 Limitations and difficulties of the study

During the research process of the SISA framework, some limitations and difficulties were identified.

- i) A specialised team is required to perform the tasks within the activities.
In general, IS auditors found the methodology clear, transparent and reliable to produce an audit opinion on the level of IS sustainability, even though the process is slightly complicated. They mentioned that a few hours are needed to develop and complete the analysis. A group discussion is needed for the IS audit team to agree upon the final decision of the risk impact analysis. In addition, a big sample of IS needs detailed analysis in order to decide on specific risk categories that may have significant impact on the IS.
- i) Several sustainability indicators have been proposed in the literature; however, there is no guidance currently available as to which of the possible sustainability indicators provide information on economic, environmental, social and technological value to be applied in the IS audit practice.
- ii) The D-S theory is found appropriate and relevant for establishing degree of belief about the IS audit evidence for economic, environmental, social and technological dimensions. Some IS auditors were not familiar with this technique, so it is possible that this problem might occur in the future. This would suggest that IS auditors should be made fully aware of the D-S theory before beginning to use the SISA framework.
- iii) There was some difficulty experienced by the IS auditors when trying to be consistent with all judgments. Yet, when given a clear definition of the degree of belief (i.e. 'Adequate', 'Inadequate' and 'Partial adequate') the IS auditors were able to achieve consistency in their judgments.
- iv) Time constraints meant only a limited number of organisations could be investigated in this research.
- v) The case studies were only conducted in the NAD and SAI. Hence, different factors and variables in other countries may affect the results of the case studies.

7.4 Further research

This research provides a framework for conducting IS audit, which can be adopted by public sector organisations in various countries. The proposed framework presented practical and usable tools, techniques and methods to carry out IS audit work and to produce an effective IS audit report. The work carried out in this research has identified a number of areas that can be the subject for further research:

- i) The analysis conducted for this research reveals that public sector organisations are continually renewing the administrative aspects of IS investment. In this case, there is room for more research to implement SISA and update its findings.
- ii) As seen in the evaluation of the results, the SISA framework was designed with the possibility to be extended so as to adapt to dynamic environment. Such extension can be considered in future work by incorporating more variables to adapt to different scenarios of IS.
- iii) It is suggested that the SISA framework should be automated and able to be implemented in a real-time environment that allows analysis on an ongoing basis.
- iv) In relation to time efficiency to complete the audit task, SISA is constrained by the complexity of the IS, the size of auditee and the number of IS control evaluations. Since this audit work required only small samples, for example, IS control in each dimension is limited by numbers (in this case only 2-4 items were included for each control task), the audit work was completed within the time limit. Future audit work should more rigorously examine these consequences by creating a thorough IS controls list and by creating a sub-team to test the sustainability dimensions separately.
- v) In future, processing systems will be becoming more complex due to the expansion of businesses and networks. As times and technologies change, the coverage of the SISA framework may be customised to suit the Big Data environment, particularly in analysing other forms of data, examining correlations, and establishing predictions for IS sustainability.

7.5 Summary

This research has addressed issues in IS audit practice, and has achieved its key objectives in establishing a novel approach to improve the existing IS audit work. The SISA framework is based on the relevance of sustainability-oriented and risk-oriented analysis to form IS audit opinion in relation to IS performance. The SISA is presented in a practical format familiar to

IS auditors, and has been validated by practical testing in different organisations. The researcher believes that the SISA framework has a promising future in enhancing the current IS audit practice either in a public or private organisation.

APPENDIX A

THE IMPLEMENTATION OF THE INFORMATION SYSTEMS AUDITING IN PUBLIC SECTOR ORGANISATION

Dear Respondent,

In partial fulfilment of the requirements for obtaining my PHD Degree in IS auditing from the School of Architecture, Computing and Engineering, University of East London, I am conducting a survey on risk assessment and auditor's opinion in information systems auditing. The objective of this survey is to investigate the current practices of risk evaluation from the auditor point of view. The investigation will also cover the perception of decision makers and auditor's professional judgment about risk assessment and the importance and impact of risk factors to information systems performance.

Your input is crucial for my research project and it will be highly regarded. The information given by you will be treated confidentially. The information is going to be used for educational purposes only and only the researcher and his supervisory team will have access to it. This project has been approved by the UEL School Research Ethics Committee, Ethics Code: 30114

I would like to thank you in advance for your time and your answer. I will be very grateful for your quick response. Should you have any questions about completing the questionnaire, please do not hesitate to contact me at the contact details shown below.

Alifah Aida Lope Abdul Rahman

PhD Candidate

School of Architecture, Computing and Engineering,

University of East London

E-mail: alifahaida@yahoo.com

Best regards,

Alifah Aida

Consent form

Thank you for taking time to participate in this research. If you agree to participate in this study, you will be asked to complete a brief questionnaire and also interview questions afterwards.

The researcher would like to emphasise that your participation will be completely anonymous. The session should take approximately 10 minutes. Your participation in this study is voluntary and you may withdraw from the study at anytime without penalty.

By signing below or email the response to the researcher, you acknowledged that you have read and understand the above statement and have given your consent to participate in this study.

Signature

Please read carefully and tick one number only for each row of descriptive statement. Number '1' indicates that the stage does not performed and '5' indicates that the stage is most performed.

1. IS audit key areas

	Not perform	Slightly perform	Neither perform nor not perform	Perform	Most perform
Elements	1	2	3	4	5
Develop criteria based on the IT controls objective					
Develop knowledge on the entity's operations					
Develop knowledge on the information system's operations					
Establish audit objective to assess the effectiveness, the efficiency and the economy of the information system (VFM)					
Establish IS audit plan which include risk assessment					
Audit report produced based on compliance to rules and regulations and VFM					

2. In you experience, are any of these factor impacting on the performance of your IS audit practice?

	Not agree	Slightly agree	Neither agree nor disagree	Agree	Strongly agree
Statement	1	2	3	4	5
IS audit process was not able to detect all IS weaknesses.					
IS audit work was limited by control evaluation.					
Inadequate objective to conduct performance audit in IS audit work.					
Inadequate risk quantification.					
Sometimes errors remain undetected by the audits.					

3. Demographic data

a) Section: Internal

External

b) Region: NADM

SAI

c) Years of service in IS audit section:

Less than 5 years

Between 5 to 10 years

Above 10 years

APPENDIX A1

INTERVIEW QUESTIONS

1. Based on your experience in IS audit, how do you describe the current IS audit practice?
2. What are the limitations or problems that you identify when performing IS audit?
3. Can you name the limitations or issues found?
4. Do you think the existing IS audit criteria effective?
5. How do you find risk assessment in the current IS audit?
6. Was the risk assessment in IS audit effective?
7. How do you find the impact of the issues found in relation to IS audit performance?
8. What is your opinion to enhance the IS audit work?
9. Do you think that the existing IS audit report effective?
10. Do you think the present format of an IS audit report is adequate to meet user's requirement?

APPENDIX B
Interview questions for SISA

RQ1: How do sustainability dimensions be incorporated into an IS audit process that has an impact on IS audit?

Audit plan

Economic dimension

- 1) How do you find incorporating economic dimension as an IS audit criteria in IS audit?
- 2) Are procedures for reviewing economic are easy to follow?
- 3) Are this audit criteria relevant and measurable?

Environmental dimension

- 4) How do you find incorporating environmental dimension as an IS audit criteria in IS audit?
- 5) Are procedures for reviewing economic are easy to follow?
- 6) Are this audit criteria relevant and measurable?

Social dimension

- 7) How do you find incorporating social dimension as an IS audit criteria in IS audit?
- 8) Are procedures for reviewing economic are easy to follow?
- 9) Are this audit criteria relevant and measurable?

Technological dimension

- 10) How do you find incorporating technological dimension as an IS audit criteria in IS audit?
- 11) Are procedures for reviewing economic are easy to follow?
- 12) Are this audit criteria relevant and measurable?

Audit execution

- 1) What is your opinion on the use of degree of belief to form your opinion on IS control evaluation?

Relevant	<input type="text"/>	Less relevant	<input type="text"/>	Irrelevant	<input type="text"/>
Practical	<input type="text"/>	Less practical	<input type="text"/>	Impractical	<input type="text"/>
Useful	<input type="text"/>	Less useful	<input type="text"/>	Useless	<input type="text"/>

- 2) Are procedures for IS control evaluation effective?
 Yes No
- 3) Are procedures for IS control evaluation relevant and reliable?
 Yes No
- 4) Is the IS risk assessment process effective?
 Yes No
- 5) How do you find the process of aggregating evidence to determine risk factor?
- | | | | | | |
|-----------|--------------------------|----------------|--------------------------|-------------|--------------------------|
| Relevant | <input type="checkbox"/> | Less relevant | <input type="checkbox"/> | Irrelevant | <input type="checkbox"/> |
| Practical | <input type="checkbox"/> | Less practical | <input type="checkbox"/> | Impractical | <input type="checkbox"/> |
| Useful | <input type="checkbox"/> | Less useful | <input type="checkbox"/> | Useless | <input type="checkbox"/> |
- 6) To what extent your past experience is used for measuring risks in IS?
- 7) How do you find measuring risk exposure to determine level of IS sustainability?

Audit report

- 1) How do you consider risk when making audit conclusion?
- 2) How do you find level of sustainability to be included in the IS audit report?
- 3) How do you find sustainability as a basis to form decision on the IS performance?
- 4) Do you think the SISA format of an IS audit report is adequate to meet user's requirement?
- 5) Do you think that is would be beneficial to your organisation to adopt SISA for presenting IS audit report?

RQ2: Could SISA be implemented in different types of organisations?

- 1) Are procedures in place for SISA to deal with changes in scope?
- 2) Do you think that is would be beneficial to your organisation to adopt SISA for presenting IS audit report?

RQ3: To which extent does the SISA framework affect the IS audit process?

- 1) Are there any issues which you think should be addressed associated with SISA?
- 2) What is your opinion on the use of SISA in terms of practicality, usability, understandability and relevancy in IS audit practice?
- 3) Are procedures for establishing audit criteria, sub-criteria, identify, and apply sustainability are understandable and easy to follow?

RQ4: What are the challenges faced by the IS auditor when adopting a sustainability driven IS audit framework?

- 1) Based on your experience in conducting SISA, what are the challenges that you encounter to adopt SISA in IS audit process?
- 2) How do you describe the outcome of SISA?

**APPENDIX C
AUDIT PROGRAM**

ACTIVITY CODE:

IS AUDIT: ECONOMIC

DATE:

WORKING PAPER REFERENCE:

PURPOSE AND SCOPE:

To evaluate the adequacy of information system general controls.

To report on the understanding of the information system general controls and assessment of control risk in relation to economic, environmental, social and technological.

Value/IS audit areas	Adequate (0.51-1.0)	Partially adequate (0.21-0.5)	Inadequate (0.0-0.2)	Potential risk (if <0.5)	Confidence level (1-3)
Financial management (Budget review)					
a. Budget performance is reviewed on a scheduler basis.					
b. Any variance is notified in a timely manner.					
c. Accurate accounting procedures					
d. Any contingency is accounted for					
e. Storage capacity for at least 5 years					
f. Training and maintenance cost for at least 5 years					
g. Payment is made accordingly.					
h. Overall costs are considered for systems implementation such as license, maintenance, services, re-design, deployment and testing, integration and human resources implications.					

Value/IS audit areas	Adequate (0.51-1.0)	Partially adequate (0.21-0.5)	Inadequate (0.0-0.2)	Potential risk (if <0.5)	Confidence level (0-3)
Environmental criteria					
a) Optimal configuration for green IS implementation					
b) Provide environmental control such as temperature control, heating, ventilation, air conditioning, and power management system for server, data centre and other IT facilities.					
c) Resource savings: Fully utilised on automation facilities, less paper used.					
d) Provide energy savings techniques such as sleep scheduling and virtualisation of computing resources in cloud computing centres.					
Social criteria					
a) The organisation develops a service level agreement that define minimal level of service performance, boundaries of a service scope and agreed and service operation status.					
b) Provide audit log, access controls, risk assessment, operation management documentation.					
c) Checks compliance procedures for managing change include approval for change, testing and implementation.					
d) Compliance to the accepted IT rule, requirements, policies, procedures.					

Technology criteria					
a) Provide adequate access control to prevent unauthorised access.					
b) Provide audit log, access controls to register operation, procedures or event.					
c) Establish business continuity plan and cloud disaster recovery plan.					
d) Provide compliance assessment on data retention policy for scalability purposes.					
e) Provide appropriate control for network protection.					

Note*:

Auditor is required to mark their confidence level about the adequacy of the systems general controls. Confidence level represent 1 for less, 2 is moderate and 3 is strong

REFERENCES

- A.P.Dempster (1967) 'Upper and lower probabilities induced by a multivalued mappings', *The annals of mathematical statistics*, pp. 325-328.
- Abidin, N. Z. and Pasquire, C. L. (2007) 'Revolutionize value management: A mode towards sustainability', *International Journal of Project Management*, 25, pp. 275-282.
- Abu-Shanab, E. A. and Bataineh, L. Q. (2014) 'Challenges Facing E-government Projects: How to Avoid Failure?', *International Journal of Emerging Science*, 4(4), pp. 202-217.
- Ali, M. and Bailur, S. (2007) 'The challenge of “sustainability” in ICT4D –is bricolage the answer?'. *Proceedings of the 9th International Conference on Social Implications of Computers in Developing Countries*. Sao Paulo, Brazil. pp. 1-19.
- Aman, A., Al-Shbail, T. A. and Mohammed, Z. (2013) 'Enhancing public organizations accountability through E-Government systems', *International Journal of Conceptions on Management and Social Sciences*, 1(1), pp. 15-21.
- Anderson, D. R. and Anderson, K. E. (2009) 'Sustainability risk management', *Risk Management and Insurance Review*, 12(1), pp. 25-38.
- Anthopoulos, L., Reddick, C. G., Giannakidou, I. and Mavridis, N. (2015) 'Why e-government projects fail? An analysis of the Healthcare.gov website', *Government Information Quarterly*, pp. 1-13.
- Ashley, P. and Boyd, W. E. (2006) 'Quantitative and Qualitative Approaches to Research in Environmental Management', *Australasian Journal of Environmental Management*, 13(2), pp. 70-78.
- Asif, M., Searcy, C., Zutshi, A. and Fisscher, O. A. M. (2013) 'An integrated management systems approach to corporate social responsibility', *Journal of Cleaner Production*, 56, pp. 7-17.
- Assalahi, H. (2015) 'The Philosophical Foundations of Educational Research: A Beginner's Guide', *American Journal of Educational Research*, 3(3), pp. 312-317.
- Awasthi, A. and Chauhan, S. S. (2011) 'Using AHP and Dempster–Shafer theory for evaluating sustainable transport solutions', *Environmental Modelling & Software*, 26(6), pp. 787-796.
- Bae, J. H., Chae, H. S. and Chang, C. K. (2013) 'A metric towards evaluating understandability of state machines: An empirical study', *Information and Software Technology*, 55, pp. 2172-2190.
- Barret, P. (Year) 'Sustainability reporting-the role of auditors', *Commonwealth Auditors-General Conference*. Wellington, New Zealand.
- Bartens, Y., De Haes, S., Lamoen, Y., Schulte, F. and Voss, S. (Year) 'On the Way to a Minimum Baseline in IT Governance: Using Expert Views for Selective Implementation of COBIT 5', *System Sciences (HICSS), 2015 48th Hawaii International Conference on*. pp. 4554-4563.

- Becker, C., Chitchyan, R., Duboc, L., Easterbrook, S., Penzenstadler, B., Seyff, N. and Venters, C. (2015) 'Sustainability Design and Software: The Karlskrona Manifesto'. *37th International Conference on Software Engineering*. Florence, Italy.
- Beynon, M., Cosker, D. and Marshall, D. (2001) 'An expert system for multi-criteria decision making using Dempster Shafer theory', *Expert Systems with Applications*, 20(4), pp. 357-367.
- Bilgea, P., Badurdeen, F., Seliger, G. and Jawahir, I. S. (2014) 'Model-based approach for assessing value creation to enhance sustainability in manufacturing'. *Variety Management in Manufacturing. Proceedings of the 47th CIRP Conference on Manufacturing Systems*.
- Blumberg, B., Cooper, D. R. and Schindler, P. S. (2011) *Business Research Methods*. 3rd. European ed. edn. London, McGraw Hill.
- Boldt, I., Lapao, L., Rodrigues, P. P., Freitas, A. and Cruz-Correia, R. (Year) 'Poor quality of Hospital Information Systems Audit Trails', *Information Systems and Technologies (CISTI), 2012 7th Iberian Conference on*. Madrid, Spain. IEEE, pp. 1-6.
- Brender, N. and Markov, I. (2013) 'Risk perception and risk management in cloud computing: Results from a case study of Swiss companies', *International Journal of Information Management*, 33(5), pp. 726-733.
- Burrowes, A. and Persson, M. (2000) 'The Swedish management audit: a precedent for performance and value for money audits', *Managerial Auditing Journal*, 15(3), pp. 85-97.
- Cerin, B. and Vojković, G. (Year) 'Regulating IT projects and information systems audit in public and state administration of the Republic of Croatia', *Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention on*. Opatija. pp. 1220-1225.
- Committee, I. P. S. *Financial Audit Guideline-Audit Evidence*. International Organization of Supreme Audit Institutions, I. Austria: INTOSAI-General Secretariat. (ISSAI 1500).
- Coyne, K. L. (2006) 'Sustainability auditing', *Environmental Quality Management*.
- Creswell, J. W. (2003) 'Research Design, Qualitative, Quantitative, Mixed Methods Approaches; Second Edition.' p. 26.
- Daujotait, D. and Macerinskien, I. (Year) 'Development of performance audit in public sector', *5th International Scientific Conference Business and Management*. Lithuania. pp. 177-185.
- Debra Howcroft and Trauth, E. M. (2004) 'The Choice of Critical Information Systems Research'. *Information Systems Research: Relevant Theory and Informed Practice*. Boston, MA: Springer US, pp 195-211.
- Delai, I. and Takahashi, S. (2011) 'Sustainability measurement system: a reference model proposal', *Social responsibility journal*, 7(3), pp. 438-471.
- Dempster, A. P. (1968) 'A generalization of Bayesian inference', *Journal of the Royal Statistical Society*, 30, pp. 205-247.

- Eisenhardt, K. M. (1989) 'Building Theories from Case Study Research.', *The Academy of Management Review*, 14(4), pp. 532-550.
- Gao, S. S. and Zhang, J. J. (2006a) 'Stakeholder engagement, social auditing and corporate sustainability', *Business Process Management Journal*, 12(6).
- Gao, S. S. and Zhang, J. J. (2006b) 'Stakeholder engagement, social auditing and corporate sustainability', *Business Process Management Journal*, 12(6), pp. 722-740.
- Gasparatos, A. (2010) 'Embedded values stems in sustainability assessment tools and their implications', *Journal of Environmental Management*, 91, pp. 1613-1622.
- Gauld, R. (2007) 'Public sector information system project failures: Lessons from a New Zealand hospital organization', *Government Information Quarterly*, 24, pp. 102-114.
- Gherardi, L., Guthrie, J. and Farneti, F. (2014) 'Stand-alone sustainability reporting and the use of GRI in Italian Vodafone: A longitudinal analysis', *Social and Behavioral Sciences*, 164, pp. 11-25.
- Goldfinch, S. (2000) 'Pessimism, Computer Failure, and Information Systems Development in the Public Sector', *Perspectives on Performance and Accountability in Public Administration*, pp. 917-929.
- Grönlund, A., Svärdesten, F. and Öhman, P. (2011) 'Value for money and the rule of law: the (new) performance audit in Sweden', *International Journal of Public Sector Management*, 24(2), pp. 107-121.
- Hamilton, R. A. (1995) Compliance Auditing. *The Internal Auditor*, 52, (6) 422-16.
- Harmon, R. R., Daim, T. and Raffo, D. (Year) 'Roadmapping the Future of Sustainable IT', *PICMET 2010 Technology management for global economic growth*. IEEE, pp. 1-10.
- Harmon, R. R. and Demirkan, H. (2011) 'The Next Wave of Sustainable IT', *IEEE*, pp. 1-25.
- Hessami, A. G., Hsu, F. and Jahankhani, H. (2009) 'A systems framework for sustainability', *Springer-Verlag Berlin Heidelberg*, pp. 76-94.
- Horová, M. (Year) 'Performance audit considering the sustainability: Approach of the czech enterprises.', *European Conference on Management, Leadership & Governance*. pp. 231-251.
- Huang, S.-M., Chang, I.-C., Li, S.-H. and Ming-Tong Lin (2004) 'Assessing risk in ERP projects: identify and prioritize the factors', *Industrial Management & Data Systems*, 104(8), pp. 681-688.
- INTOSAI (2006) 'ISSAI 4100: Compliance Audit Guidelines'. [in Austria: INTOSAI General Secretariat. 1-52. (Accessed:INTOSAI.
- INTOSAI (2009) *Financial Audit Guideline-Audit Evidence*. International Organization of Supreme Audit Institutions, I. Austria: INTOSAI-Professional Standards Committee. (ISSAI 1500).
- INTOSAI (2013a) 'Fundamental Principles of Performance Auditing'. [in *ISSAI 300*. Austria: INTOSAI. 1-20. (Accessed:INTOSAI.
- INTOSAI (2013b) 'ISSAI 300 : Fundamental Principles of Performance Auditing'. [in *ISSAI 300*. Austria: INTOSAI. 1-20. (Accessed:INTOSAI.
- ISACA (2008) 'IT-governance-frameworks', pp. 2-12.

- ISACA (2011) *Sustainability*. USA: Information Systems Audit and Control Association. 1-14 pp. Available.
- Islam, S., Mouratidis, H. and Weippl, E. R. (2014) 'An empirical study on the implementation and evaluation of a goal-driven software development risk management model.', *Journal of Information and Software Technology*, 56(2), pp. 177-133.
- Jaca, C., Viles, E., Mateo, R. and Santos, J. (2012) 'Components of sustainable improvement systems: theory and practice', *The TQM Journal*, 24(2), pp. 142-154.
- Jan Devos, Hendrik Van Landeghem and Deschoolmeester, D. (2008) 'Outsourced information systems failures in SMEs: a multiple case study', *The Electronic Journal Information Systems Evaluation*, 11(2), pp. 73-82.
- Jin'e, Y. and Dunjia, L. (1997) 'Performance audit in the service of internal audit', *Managerial Auditing Journal*, 12(4/5), pp. 192-195.
- Kalloniatis, C., Mouratidis, H. and Islam, S. (2013) 'Evaluating Cloud Deployment Scenarios Based on Security and Privacy Requirements', *Springer-Verlag*, 18(4), pp. 299-319.
- Keil, M. and Robey, D. (2001) 'Blowing the whistle on troubled software projects', *Communicating of the ACM*, 44(4), pp. 87-93.
- Kimaro, H. C. and Nhampossa, J. L. (2007) 'The challenges of sustainability of health information systems in developing countries: comparative case studies of Mozambique and Tanzania', *Journal of Health Informatics in Developing Countries*, 1(1), pp. 1-10.
- Klein, H. K. and Myers, M. D. (1999) 'A Set of Principle for Conducting And Evaluating Interpretive Field Studies in Information Systems', *MIS Quarterly*, 3(1), pp. 67-94.
- Korte, M., Lee, K. and Fung, C. C. (2012) 'Sustainability in Information Systems: Requirements and Emerging Technologies'. *International Conference on Innovation, Management and Technology Research*. Malacca, Malaysia. IEEE, pp. 481-485.
- Krysiak, F. C. (2009) 'Risk Management as a Tool for Sustainability', *Journal of Business Ethics*, 85, pp. 483-492.
- Kujala, S. and Väänänen-Vainio-Mattila (2009) 'Value of information systems and products: understanding the users' perspective and values', *Journal Of Information Technology Theory And Application*, 9(4), pp. 23-39.
- Lee, M. (2014) 'Shift to sustainability', *Internal Auditor*, pp. 74-75.
- Mahmoudi, H., Renn, O., Vanclay, F., Hoffmann, V. and Karami, E. (2013) 'A framework for combining social impact assessment and risk assessment', *Environmental Impact Assessment Review*, 43, pp. 1-8.
- Majdalawieh, M. and Zaghoul, I. (2009) 'Paradigm shift in information systems auditing', *Managerial Auditing Journal*, 24(4), pp. 352-367.

- Malina, M. A., Nørreklit, H. S. O. and Selto, F. H. (2011) 'Lessons learned: Advantages and disadvantages of mixed method research.', *Qualitative Research in Accounting and Management*, 8(1), pp. 59-71.
- McManus, J. and Wood-Harper, T. (2007) 'Understanding the sources of Information Systems Project Failure', *Management Services*, pp. 38-43.
- McManus, J., Wood-Harper, T., 732.256px, d. d.-a.-d.-c.-w. s. l., 796.44px, t., 16.6666px, f.-s., sans-serif, f.-f., . . . ">ood-Harper (2007) 'Understanding the source of information systems project failure', *Management services*, pp. 38-43.
- Merhout, J. W. and O'Toole, J. (Year) 'Sustainable IT Governance: Is COBIT 5 Adequate Model?', *Proceedings of the Tenth Midwest Association for Information Systems Conference*. Kansas, USA. pp. 1-6.
- Myers, M. D. (1997) 'Qualitative Research in Information Systems', *MISQ Discovery*, 21(2), pp. 241-242.
- Nawi, H. S. A., Rahman, A. A. and Ibrahim, O. (Year) 'Government's ICT Project Failure: A revisit', *2011 International Conference on Research and Innovation in Information Systems*. Kuala Lumpur. IEEE, pp. 1-6.
- Nayan, N. b. M., Zaman, H. B. and Sembuk, T. M. T. (2010) 'Defining Information System Failure in Malaysia:Result from Delphi Technique'. *IEEE*. pp. 1616-1621.
- Ness, B., Urbel-Piirsalu, E., Anderberg, S. and Olsson, L. (2007) 'Categorising tools for sustainability assessment', *Ecological Economics*, 60(3), pp. 498-508.
- Nicho, M. and Cusack, B. (Year) 'A Metrics Generation Model for Measuring the Control Objectives of Information Systems Audit', *40th Annual International Conference on System Sciences*. Hawaii. pp. 1530-1605.
- Nurdin, N., Stockdale, R. and Scheepers, H. (2012) 'Organizational Adaptation to Sustain Information Technology: The Case of E-Government in Developing Countries"', *Electronic Journal of e-Government*, 10(1), pp. 70-83.
- Nurmazilah Mahzan and Veerankutty, F. (2011) 'IT auditing activities of public sector auditors in Malaysia', *African Journal of Business Management*, 5(5), pp. 1551-1563.
- Oates, B. J. (2006) *Researching Information Systems and Computing*. London: SAGE Publications Ltd.
- Orlikowski, W. and Baroudi, J. J. (1988) 'Studying information technology in organizations:Research approaches and assumptions'. *Academy of Management Meeting*. CA, USA. Center for Digital Academy Research, STERN School of Business, pp. 1-39.
- Ostlund, U., Kidd, L., Wengstro`m, Y. and Rowa-Dewar., N. (2011) 'Combining qualitative and quantitative research within mixed method research designs: A methodological review', *International Journal of Nursing Studies*, 48, pp. 369–383.

- Qu, S. Q. and Dumay, J. (2011) 'The qualitative research interview', *Qualitative Research in Accounting & Management*, 8(3), pp. 238-264.
- Runeson, P. and Host, M. (2008) 'Guidelines for conducting and reporting case study research in software engineering.', *Empirical Software Engineering*, pp. 1-34.
- Ruth J. Tubey, Jacob K. Rotich and Bengat, J. K. (2015) 'Research Paradigms: Theory and Practice', *Research on Humanities and Social Sciences*, 5(5).
- Sayana, S. A. (2002) 'The IS Audit Process', *Information Systems Control Journal*, 1, pp. 1-4.
- Schmidt, N.-H., Kolbe, L. M., Erek, K. and Zarnekow, R. (2009) 'Sustainable Information Systems Management', *Business & Information Systems Engineering*, 5, pp. 400-402. doi: DOI 10.1007/s12599-009-0067-y.
- Searcy, C. (Year) 'Corporate Sustainability Performance Measurement: Lessons from System of Systems Engineering', *Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics*. USan Antonio, USA. pp. 1057-1060.
- Silvius, A. J. G., Brink, J. v. d. and Smit, J. (2009) 'Sustainability in Information and Communications Technology (ICT) Projects', *Communications of the IIMA*, 9(2), pp. 33-44.
- Singh, R. K., Murty, Gupta and Diskhit (2009) 'An overview of sustainability assessment methodologies', *Ecological Indicators*, 9, pp. 189-212.
- Smith, P. A. C. (2012) 'The importance of organizational learning for organizational sustainability', *The Learning Organization*, 19(1), pp. 4-10.
- Sonmez, M. (2007) 'Data transformation in the evidential reasoning-based decision making process', *International Transactions In Operational Research*, pp. 411-429.
- Srivastava, R. P. (2005) 'Alternative Form of Dempster's Rule for Binary Variables', *International Journal of Intelligent Systems*, 20(8), pp. 789-797.
- Srivastava, R. P. and Li, C. (2008) 'Risk and reliability formulas for systems security under Dempster-Shafer Theory of Belief Functions', *Journal of Emerging Technologies in Accounting*, 5, pp. 189-219.
- Stoel, D., Havelka, D. and Merhout, J. W. (2012) 'An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners', *International Journal of Accounting Information Systems*, 13, pp. 60-79.
- Sun, L., Srivastava, R. P. and J.Mock, T. (2006) 'An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions', *Journal of Management Information Systems*, 22(4), pp. 109-142.
- Thöni, A., Madlberger, L. and Schatten, A. (Year) 'Towards a data-integration approach for enterprise sustainability risk information systems', *7th International Conference on Research and Practical Issues of Enterprise Information Systems*. Prague. pp. 269-277.

- Turner, J. R. and Danks, S. (2014) 'Case Study Research: A valuable learning tool for performance improvement professionals', *International Society for Performance Improvement*, 53(4), pp. 24-31.
- Tysiac, K. (2014) 'Five elements of effective judgment process for auditors'. *Journal of Accountancy*.
- Vendrzyk, V. P. and Bagranoff, N. A. (2003) 'The evolving role of IS audit: A field study comparing the perceptions of IS and financial auditors', 20, pp. 41-163.
- Wallage, P. (2000a) 'Assurance on Sustainability Reporting: An Auditor's View', *A Journal of Practice & Theory*, 19, pp. 53-63.
- Wallage, P. (2000b) 'Assurance on sustainability reporting: An auditor's view', *A Journal of Practice & Theory*, 19, pp. 1-14.
- Walsham, G. (1995) 'Interpretive case studies in IS research: nature and method', *European Journal of Information Systems*, 4, pp. 74-81.
- Weber, O., Scholz, R. W. and Michalik, G. (2010) 'Incorporating sustainability criteria into credit risk management', *Business Strategy and the Environment*, 19, pp. 39-50.
- Whitney, K. M. and Daniels, C. B. (2013) 'The root cause of failure in complex IT projects: Complexity Itself', *Procedia Computer Science*, 20, pp. 325-330.
- Yang, D. C. and Guan, L. (2004) 'The evolution of IT auditing and internal control standards in financial statement audits: The case of the United States', *Managerial Auditing Journal*, 19, pp. 544-555.
- Yin, R. K. (2003) *Case study research-Design and methods*. SAGE.