# Assessing the Business Value of IT Control Configurations: A Design Science Study

Maher Al-Khazrajy
BE (University of Technology, Iraq), PgDipSci (University of Auckland, NZ)
MPhil (Auckland University of Technology, NZ)

A thesis submitted to Auckland University of Technology
in fulfillment of the requirements for the degree of
Doctor of Philosophy (PhD)

2016

School of Engineering, Computer and Mathematical Sciences

# Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

.....

Maher Al-Khazrajy

# Acknowledgements

This thesis was completed at the Faculty of Design and Creative Technologies of the AUT University in the New Zealand. Throughout the research duration the researcher received valuable support from many people who in one way or another, contributed immensely to the success of the research. It is with utmost pleasure and gratefulness the researcher would like to take this opportunity to thank all those people for their support, inspiration and motivation, which without, it would not have been possible to complete the research.

First and foremost the researcher wishes to thank the primary supervisor Dr. Brian Cusack for his constant mentoring and endless support, encouragement and advice throughout the time it takes to complete the thesis, which were vital for the completion of this thesis. The contribution of Dr. Cusack will be a very long-term asset in shaping the researcher and in assisting him to attain a higher academic level and professional work style. In addition, the research would like to thank Dr. Stephen Thorpe, the secondary supervisor, for his support and reviewing the research outcomes and providing a valuable feedback that helped immensely in improving the research deliverables.

Secondly, the researcher would like to thank the people who used, tested and evaluated the models designed in the research. Those people were the subject matter experts who spared their valuable time and participated in the evaluations, provided their feedback and shared their thoughts and experience enriched the research immensely. In this research the experts' evaluation is essential, therefore those experts' contribution was vital to the completion of the research. Thirdly, would like to thank family members who patiently helped and motivated the researcher throughout the research. Lastly, the researcher is grateful to friends, work colleagues and manager, whose support and encouragement were crucial for overcoming many hurdles.

The assistance of AUT administrators, in particular the Computing department administrators. AUT Postgraduate office is also acknowledged with gratitude. Various other people have helped the researcher in many ways to accomplish required tasks, including but not limited to staff at IT service and library, these are all acknowledged with appreciation.

# Publications

Cusack, B. & Al-Khazrajy, M. (2015). Forecasting Business Impact of Security Control Selections. *Digital Forensics Magazine*, 25, 8-12.

Cusack, B. & Al-Khazrajy, M. (2015). *Evaluating Policy Layer Security Controls for Value Realisation in Secure Systems.* Proceedings of the Australian Security Management Conference, 1-3 December, Perth, Western Australia.

# Abstract

The increasing complexity of IT systems and their interoperability has compounded the challenging task of assessing the IT risks and devising cost-effective mitigating measures. Risk factors such as business dynamics and changes arising from new technology and regulatory requirements, affect the risk profile, which requires reassessing the defined IT risks and the corresponding controls. Ensuring effectiveness and efficiency of the implemented controls is crucial to obtain an accurate sense of assurance that, in itself involves risk. Skilled professionals like IT risk managers, auditors, security managers, who assess risks and verify applied controls, conduct this challenging task. Currently IT Risk Assessors, auditors and practitioners use a set of criteria to estimate risk and then derive areas for control improvement. However, it is highly inefficient, subjective and little data is directly collected to support the decisions made. With improvements in technology a range of new organizational data can now potentially be used to support the selection of IT controls. Little empirical research has been conducted to date in this area.

A set of related problems is explored in this thesis and the research focuses on one particular researchable problem, stated as: **Selecting the best set of IT controls configurations in any situation for the highest business value outcomes.** Solving this problem aids, or contribute largely, in solving, the other identified problems. A research question has been derived from the research problem to guide the research processes: **What are the criteria for selecting the most effective and efficient controls configurations for the best business value outcomes?**

To answer the research question, methodologies were explored resulting in the selection of Design Science (DS) as the research methodology for this thesis. DS has been adopted in IT research, as DS has shown to be adequate to research complex and multi-domain problems, when sufficient knowledge is not always available. The key aspect of the DS methodology is to learn through doing. DS allows a researcher to iterate through the DS process' stages until new knowledge is obtained or existing knowledge is enhanced. A DS research roadmap and artefacts evaluation criteria have been adopted to ensure the research activities are executed objectively and the anticipated research deliverables are produced.

In this thesis a conceptualised solution of constructing a model-based interactive Decision Support System (DSS) to aid management, and practitioners, experienced and otherwise, determine the controls configurations that return the best business value, was developed. The first model called (C-Model) was based on analysing the distribution of cumulative impact probability of the defined IT risks and corresponding controls. An initial experts' evaluation of this model indicated that while the concept of a probability model was appreciated, however, there were a number of significant limitations. Identifying a number of serious limitations in the model resulted in the judging of the model as not fit for purpose, and the seeking of another alternative. Following the DS methodology process, other alternatives were theorised and explored. The second build of the model called (G-Model) resulted in game theory applications and a 3-player competitive game to solve the problem of selecting the best performing control configurations.

The Gambit software application was used to develop a 3-player game using COBIT 4.1, ITIL v3.0 and ISO 27001/2, security controls as the game players. Each player has two strategies: Implement and Not-Implement. A set of payoff values and guidance on how to calculate a payoff value was prepared along with a Risk Space Matrix definition. A risk register was employed as part of the DSS to capture and assess IT risks and also to apply the controls and processes resulting from the game theory based model. The DSS components were subjected to experts' evaluation, 7 experts in total participated in a two-stage evaluation. Oral and written feedback was obtained, analysed and reflected upon. The artefacts evaluation was benchmarked against an adopted evaluation criteria.

Reflecting, by the researcher, on the expert's feedback and artefacts evaluation, answers for the raised questions were formed, resulting in defining a selection criteria to aid practitioners in finding the best set of controls that return the best business value and mitigate the identified risks. That formed the research contribution to academia and business from the organisation's and practitioners' perspectives.

Lastly, in this thesis recommendations for further research are provided. To further investigate the G-Model and analyse the Nash Equilibrium value that results from solving a gaming file. The objective is to find the correlation with the corresponding payoff value to estimate the Capability Maturity Model Integration

(CMMI) level of the selected controls. Also, recommendations are made to develop sub-games so that controls can be defined at a granular level. Furthermore, in G-Model the most challenging part was calculating the payoff value. A recommendation is made about utilising the expanded ‘control capital’ concept to provide more information to calculate the payoff value.

This research investigates the application of the game theory based model in an interactive DSS that allows practitioners to examine the value of forming possible controls configurations. G-Model provides the means for practitioners to enter the payoff values, enabling them to assess the possible controls combinations, holistically and determine the best set of controls in almost real-time. The essence of an effective IT risk management, resource extensive process, is to be conducted timely, and be repeatable with ease. If gaming files are developed for the wider spectrum of IT General Controls (ITGC), and integrated in an interactive DSS software application. Practitioners would be able to assess IT risks as often as required and be able to select the set of controls that return the highest business value outcomes.

# Table of Contents

**Chapter Three - Literature Analysis: Problem Scope**



**Chapter Four - Methodology**

**Chapter Five - Results and First Evaluation**

**Chapter Six - Results and Second Evaluation**

**Chapter Seven - Research Contribution**



**Chapter Eight - Summary and Conclusion**

# List of Figures

# List of Tables

# List of Abbreviations

| | |
|---|---|
| AM | Access Management |
| AICPA | American Institute of Certified Public Accountant |
| BCP | Business Continuity Planning |
| BIA | Business Impact Analysis |
| BSC | Balanced Scorecard |
| CAB | Change Advisory Board |
| CAQDAS | Computer-assisted Qualitative Data Analysis Software |
| CIO | Chief Information Officer |
| CICA | Canadian Institute of Chartered Accountants |
| COBIT | Control OBjectives for Information and related Technology |
| CMMI | Capability Maturity Model Integration |
| COSO | Committee of Sponsoring Organisation |
| COSO-ERM | Committee of Sponsoring Organisation – Enterprise Risk Management |
| CSA | Control Self-Assessment |
| DRP | Disaster Recovery Planning |
| DS | Design Science |
| DSR | Design Science Roadmap |
| DSRM | Design Science Research Methodology |
| DSS | Decision Support Systems |
| EDP | Electronic Data Processing |
| ES | Expert Systems |
| ESS | Expert Support Systems |
| HIPAA | Health Insurance Portability and Accountability Act |
| IEC | International Electrotechnical Commission |
| IIA | Institute of Internal Auditors |
| IS | Information Systems |
| ISACA | Information Systems Audit and Control Association |
| ISEB | Information Systems Examining Board |
| ISMS | Information Security Management System |
| ISO | International Standards Organisation |

| | |
|---|---|
| IT | Information Technology |
| ITG | Information Technology Governance |
| ITGC | IT General Controls |
| ITGI | Information Technology Governance Institute |
| ITIL | Information Technology Infrastructure Library |
| KRI | Key Risk Indicator |
| MOF | Microsoft Operation Framework |
| NE | Nash Equilibrium |
| NIST | National Institute of Standards and Technology |
| NIH | National Institute of Health |
| OCTAVE | Operationally Critical Threat, Asset, and Vulnerability Evaluation |
| OGC | Office of Government Commerce |
| PCAOB | Public Company Accounting Oversight Board |
| PCI-DSS | Payment Card Industry Data Security Standard |
| PMI | Project Management Institute |
| Prince2 | PRojects IN Controlled Environments |
| RACI | Responsible, Accountable, Consulted and Informed |
| RISK IT | Risk IT, IT Risk Framework |
| RM | Risk Management |
| RMF | Risk Management Framework |
| RoI | Return on Investment |
| SAS | Statements on Auditing Standards |
| SDLC | System Development Life Cycle |
| SLA | Serviced Level Agreement |
| SNA | Social Network Analysis |
| SOX | Sarbanes-Oxley |
| TOGAF | The Open Group Architecture Framework |
| VAL IT | Value IT, IT Governance Framework |

# Chapter 1

# Introduction

## 1.0 INTRODUCTION

The aim of this research is to investigate how to select controls (mitigating measures) configurations that return the best business value outcomes. Controls are selected from recognised IT controls frameworks, best practices and standards. The controls configurations selection is initiated from identifying IT risks, with the objective of managing the defined IT risks by devising cost-effective mitigating measures.

There are a number of recognised control frameworks that are currently available for best business practice in IT Governance, IT Risk Management, IT Security Management and IT Assurance (Afzali, Azmayandeh, Nassiri, & Shabgahi, 2010; Monahan, 2008). A strategic question for any business is: What value do control frameworks give? The question concerns the costs associated with implementing and maintaining control frameworks compared with the benefits gained. Exploratory research shows that most business people view control frameworks as a cost and many see them as being an unnecessary hindrance in achieving business objectives (Information Technology Governance Institute (ITGI), 2008; Al-Khazrajy, 2012). Furthermore, only one third of the surveyed organisations have completely implemented control frameworks. Other researchers convey a similar view about ITIL and ISO 27001 management standards (Schlarman, 2007). Datardina (2005), indicates that each of those frameworks and best practices has some strengths and also weaknesses. To control an IT environment effectively there is therefore a need to integrate several of those frameworks, best practices and standards.

In this thesis the research question is: **"What are the criteria for selecting the most effective and efficient controls configurations for the best business value outcomes?"** Hence possibilities may be tested and strategies theorised. Each control framework contains many controls that may, or may not, benefit a particular

business situation. This research is aimed at testing different selections and combinations of controls to forecast probable impacts on business outcomes.

According to Leitch (2008) “Control objectives are the flip side of risks” (p. 76). By implementing cost-effective controls, risk is managed and desirable value is obtained (Al-Khazrajy, 2012). Furthermore, Leitch (2008) states that “Controls designed as an integrated system rather than by piecemeal can be more efficient and effective. This is particularly so, if special skill is applied and the focus is on value rather than just risk coverage” (p. 29). As IT systems underpin all business activities, IT risk exists wherever IT systems are planned, implemented, operated and managed (Murphy, 2002). Organisations must design, develop and maintain secure and reliable IT systems (Whitman & Mattord, 2004). To ensure IT systems are secure and reliable, IT risk has to be assessed and managed. However, a balance is to be struck between managing the perceived risks and developing the business opportunities for value creation. Managing IT risk within a business context requires considerable effort to accommodate many changing factors and skills in selecting the most relevant control sets (Murphy, 2002).

Chapter 1 introduces the research aspects in the following sections: section 1.1 explores the motivation while the challenges and the problem focus of the research are outlined in section 1.2. Section 1.3 identifies the research methodology; while section 1.4 introduces the research findings. In section 1.5 the theses organisation is laid out. The chapter is concluded in section 1.6. The following table shows the chapter structure along with sections heading and their corresponding page number. Similar table will be constructed for each chapter.

| **Structure of Chapter1** | |
|---|---|
| **Section** | **Page no.** |
| 1.1 Motivation | 2 |
| 1.2 Challenges and Problems | 4 |
| 1.3 Research Methodology | 5 |
| 1.4 Findings | 8 |
| 1.5 Research Organisation | 10 |
| 1.6 Conclusion | 13 |

## 1.1 MOTIVATION

Businesses today rely on IT systems and services to generate value. The cost to businesses in IT systems is managing the risk of both adverse and beneficial risk

(Whitman & Mattord, 2004; Hadden, DeZoort, & Hermanson, 2003). As a consequence the trustworthiness of business decisions comes under scrutiny and demands are made for evidence of predictable performance and assurance that valuable returns will come from investments. IT systems and services are complex and managers require models, frameworks, tools and formulae with which to calculate risk mitigation in relation to business returns. Auditing is one such strategy that provides assurance. Various internal and external audit reviews performed by staff and third parties on an organisation's structures and IT systems can generate an audit opinion (Henczel, 2001; Pathak, 2005). A level of assurance is not only required to meet business demands but also to comply with regulatory requirements (Abu-Musa, 2008; Merhout & Havelka, 2008). The outcomes of audit reviews consist of an objective assessment to the subject systems or processes, with mitigating measures in the form of controls and processes to rectify any anomalies (Pathak, 2005; Wright, Freedman, & Liu, 2008; Hall & Singleton, 2005; Champlain, 2003). Risk-based IT auditing is performed in a structured way to ensure devised controls are cost effective, auditable and high value assets are protected.

The rationale is to solve a management problem for which there is little literature published. The scope of the research in this thesis is to be limited to IT security controls that may be used as representative of the other sets of controls a business manager may have to choose from. The usefulness of IT security controls is that they apply across an organisation and are not typically domain specific; and hence the outcome of this research may be generalised and the methods used systematically for other control sets. Controls are developed and implemented to manage risk and the risks accepted contribute to value creation in businesses. Controls are represented in policies, procedures, practices and organisational structures. Controls are designed to provide reasonable assurance that the business objectives will be achieved and that undesired events will be prevented or detected and mitigated. Hence, controls are structured in frameworks or networks by a manager to balance the control of risk against the opportunity of realising value. A control in itself is a measurable object that has an effect. The issue arises in practice where there are many controls available, or in operation, and yet the net effect may

be questioned or challenged regarding best performance. Hence, obtaining the best controls configuration is constantly in a manager's mind.

## 1.2 CHALLENGES AND PROBLEMS

To manage IT risks, practitioners face a number of challenges to ensure the effectiveness of the IT risk management process. For example, risk is not simply a probability of loss, it is multilayered, and risk could affect various assets to a different degree. As the risk-driving factors change, it is imperative to re-assess risk parameters accordingly. This is a complex undertaking that requires robust modelling. On the other hand, IT auditors face a daunting task in reviewing systems, ensuring controls and processes effectiveness and efficiency and providing the business with an accurate sense for assurance. IT audit risk is defined as the likelihood that an IT auditor fails to uncover a material error. Such risk is required to be managed as well. Embedding IT risk management process and conducting IT audit reviews in an integrated IT assurance program, can overcome the noted challenges. However, the IT assurance program entails challenges in itself and requires ongoing reviewing to ensure its effectiveness and relevance. For example, in a 2016 global information security survey report (PWC, 2016) shows that 38% increase in detected IT security incidents in 2015 despite the existed controls and processes. The survey interviewed over 10,000 technology and business leaders across the globe and was conducted from May-June 2015. The report indicates that "prevention and detection methods have proved largely ineffective against increasingly adept assaults" (p. II). Furthermore, the report indicates that many organisations do not have the adequate capabilities to combat growing sophisticated attacks.

Establishing an IT assurance program through implementing recognised IT controls frameworks and best practices has a number of benefits. However, there are many frameworks and standards, and it is not viable to implement all controls and processes of those frameworks. Hence, it is necessary to integrate controls and processes in a setting that mitigates defined IT risk in the most cost effective way, and delivers a best business value. The management skill requires knowing those frameworks' architectures and their relationship with the corresponding business-IT processes and associated IT risks.

The existing issues and challenges of managing controls configurations to manage IT risk and to comply with IT auditing reviews, give rise to a number of researchable problems. A number of relevant problems are identified in Chapter 3 and evaluated. The identified problems were prioritized and selected, based on a feasibility analysis of research-ability, time and resources consumption; and potential value delivery. Consequently one problem was selected to be the research focus problem and is stated as:

**Selecting the best set of IT controls configurations in any situation for the highest business value outcomes.**

Resolving this problem contributes to solving the other identified researchable problems. Controls and processes will be selected based on their mitigating capability and value generating that facilitates establishing an effective IT assurance program and achieving business objectives.

## 1.3 RESEARCH METHODOLOGY

The research subject domain is a complex network of tensions that are dynamic and interrelate with human and technical constraints. It has many aspects and various levels, which require a pragmatic research approach to attempt to solve the defined problem. Thus the Design Science (DS) methodology was selected to be the research methodology for this thesis research. In DS, guidelines and roadmaps as well as artefacts evaluation criteria are adopted. According to Berndtsson, Hansson, Olsson and Luncell (2008, p. 10) to ensure the defined problem is researched in a systematic way. A methodology has to be defined and applied, to enable a researcher to obtain relevant data and to analyse it accordingly. IT research often, concerns complex systems, where technologies, people and organisations are interconnected and required to comply with various regulations (Berndtsson et al., 2008; Vaishnavi & Kuechler, 2008). IT research are based on multi-paradigms, and a pragmatic approach to produce a tentative solution. A researcher may not always have a full understanding of the whole system (Oates, 2006; Vaishnavi & Kuechler, 2008).

Lutui (2015) adopted DS in his doctorate research regarding digital forensics procedures for mobile devices. Lutui indicated that DS method used to identify a problem, design a solution and evaluate the produced artefacts.

Furthermore, DS method was utilised to develop decision support system for a nuclear reactor (Vaishnavi & Kuechler, 2008), which is detailed in Chapter 3, sub-section 3.5.3.

Vaishnavi and Kuechler (2008) suggest that design science research is applicable to IS because of the types of research questions that are naturally formed, and relevant to the interaction of many functions/processes with other non-IS related functions/processes. Oates (2006) also suggests that 'design and creation', or 'design science', as branded by Vaishnavi and Kuechler (2008); Hevner and Chatterjee (2010); Offermann, Levina, Schonherr and Bub (2009), can be used in IS research. Oates (2006) further describes the stages of 'design and creation' labeled as 'learning via making' in the following stages: Awareness of the problem, Suggestion, Development, Evaluation and Conclusion. These stages, are similar to the stages of 'Design Science' based research (Vaishnavi & Kuechler, 2008; Hevner & Chatterjee, 2010; Hevner, March, Park, & Ram, 2004; Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007; Offermann et al., 2009). All authors emphasise that those steps are not to be followed in a rigid fashion, but rather in a fluid and iterative cycle, aiming at enhancing the artefacts creation.

The DS researcher is a pragmatist (Vaishnavi & Kuechler, 2008). Simon (1996) has conceptualised DS paradigm and described it as a pragmatic research paradigm as it appeals for creating innovative artefacts to solve an identified problem. IS research projects, following 'learning via making' steps, backtracking and revisiting analyses and design are common and encouraged (Oates, 2006). Although, backtracking in DS has many challenges, which involves re-analysing that leads to re-scoping and re-designing of the research artefacts, however, it is an effective part of the DS method (Vaishnavi & Kuechler, 2008). Furthermore, according to Vaishnavi and Kuechler (2008, p. 19) DS is multi-paradigmatic, and "the philosophical perspective of the design science research changes as progress is iteratively made through the phases". In addition, according to Bunge (1984) who suggests that design science research is most effective when practitioners shift between pragmatic and realist perspectives, guided by a pragmatic assessment of the research progress.

Peffers et al. (2007) claimed that the use of the interpretive research paradigm has been accepted in IS research, however, "the resulting research

outcome is mostly exploratory and, it could be argued, not often applicable to the solution of the problem encountered" (p. 1). On the contrary, "design, is the act of creating an explicitly applicable solution to the problem" (p. 1), is accepted as a research paradigm in faculties such as engineering (Peffers et al., 2007). DS has been progressively, albeit slowly, accepted by IS researchers since 1990s, to improve effectiveness and utility of the produced IT artefacts (Alturki, Gable, & Bandara, 2011a). According to Hevner et al. (2004) a researcher adapting DS must further the existing knowledge that would help resolve the identified problem, and to develop and communicate findings to a target audience. However, adding new knowledge through developing validated artefacts is not an easy exercise to undertake and could require a number of iterations (Hevner et al., 2004). IT artefacts developed and implemented in an organisation context, require, often, behavioural-science research validation to explain the artefact's use, usefulness, and impact on practitioners and organisations (DeLone & McLean, 1992, 2003; Seddon, 1997). The experts' evaluation and insight are paramount to test the theoretical assertions in order to gain a wider view of the problem in any DS research.

Hevner et al. (2004) developed a set of guidelines (shown in Table 4.3). The principles outlined in the table emphasise what the authors have been arguing and theorising around DS aspects, in the design process, artefacts and the iterative nature of the processes. Based on (Hevner et al., 2004) guidelines, Hevner and Chatterjee (2010) defined three DS research processes (outlined in Figure 4.2). The three processes: 'Relevance', 'Design' and 'Rigor', where the research environment context is bridged with the DS activities through the first cycle. The design cycle is done iteratively between the core activities from identifying the problem to designing and evaluating proposed artefacts. Lastly, the third cycle connects the DS activities with the existing knowledge. Expertise related to the identified problem combined with the evaluated and finalised solution are utilised to add new knowledge or improve existing knowledge.

Peffers et al. (2007) developed the DS Research Methodology (DSRM) along with a framework (shown in Figure 4.3), to aid researchers in conducting of DS based IS research. However, some authors have indicated that the DS guidelines and the questions (depicted in Table 4.3 and Table 4.4 respectively), are all deemed

too abstract to follow (Peffers et al., 2007; Alturki et al., 2011a). Furthermore, the lack of specificity could cause conflicting issues (Alturki et al., 2011a; Alturki, Gable, & Bandara, 2013). To streamline tasks and activities at each stage, Alturki et al. (2011a) have developed a roadmap and further refined the roadmap as depicted in Figure 4.5, aligned with the three DS cycles.

The researcher believes that the best approach to achieve the research objectives is by adopting DS research methodology and following the DSR guidelines (Hevner et al., 2004) and DSR roadmap (Alturki, Gable, & Bandara, 2011b) to ensure deliverables are obtained according to the DS guidelines and roadmap activities.

Data will be collected from experts' oral and written feedback. Answers to a number of question sets formed around the usability of the developed artefacts and other aspects such as functionality, efficacy, performance, and fit for purpose. Furthermore, the researcher's critical reflection, notes and observations will be used for further analysis. The tests can be performed using the analysed qualitative data applying a quasi-judicial method, where a rational argument is used to interpret the data (Collis & Hussey, 2009).

## 1.4 FINDINGS

Two complete cycles of the DS framework were completed to build and then improve a Decision Support System (DSS) model component design artifact. The artefact provided solutions to the research problem and has also provided evidence on which to theorise other solutions and possible improvements. A design solution was conceptulised to develop an interactive DSS with the model in its core to help practitioners select the best controls combinations to mitigate defined IT risks. Such a DSS can enable practitioners to utilise their expertise in the subject domain, also to change, at ease, the risk parameters and corresponding controls' cost as circumstances change. In this way selected controls are kept current and the network of controls performing optimally for the mitigation of defined risks.

The DSS has four components: The Interface – Input /Output component; the Data; the Knowledge Base; and, the Model. The interface was partially developed to take only input for assessing IT risks. Further development of the interface can occur when the other three components reach a higher level of

resolution. The data was structured and loaded to represent a number of Access Management (AM) related risks and the security related risks. For the knowledge base, a number of controls and processes from recognised frameworks and best practices were selected (such as COBIT, ITIL and ISO 27001/2), utilising publicly available documents. The model was progressively developed through the DS cycles. This was the most challenging aspect of the research because there were many different solutions and possibilities but everything had to be brought within the scope of the timeframe and the technical complexity constraints. Two models have been developed, tested and evaluated. The first model is based on cumulative probabilities analysis; the second is a game theory based model; each is outlined in the relevant sections.

The first model called C-Model, was developed in Excel to simulate the cumulative impact distribution of the defined risks along with the associated controls configurations. A pilot test was conducted with the prototype that describes the distribution for the cumulative impact risks (R1, R2 and R3) and controls configurations (C0, C1, and C2) where C0 is a set of COBIT 4.1 controls; while C1 is a set of combined controls/processes from COBIT 4.1 and ITIL; and, lastly C2 comprises controls/processes from COBIT 4.1, ITIL and ISO 27001. Internal experts were approached to evaluate the model and to provide feedback. Oral feedback has been provided by three experts, which was reflected upon, and compared against the criteria that had been adopted to evaluate the artefact. A number of improvements were proposed to ready the C-Model for practitioners use and evaluation. However, the proposed C-Model, while it has some merits, it was deemed, by the researcher, inefficient in finding the best controls configuration. Subsequently, the C-Model component for the proposed DSS was judged incomplete, and hence not ready for external evaluation. Using the DS framework it was possible to build on this knowledge and to theorise different ways to solve the same problem. As a consequence a second DS iteration was undertaken and the development of the G-Model was completed. The concept of cumulative distributions was rejected in favour of game theoretic models.

Following the DS principles, the researcher explored other alternatives, and examined game theory applications. Game-Theory modeling could be utilised to build the DSS model for selecting the best controls. Utilising a software application

Gambit 14.1.0, a game theory based model called G-Model, was developed. G-Model is a three player game with selected controls from: COBIT 4.1, ITIL v3.0 and ISO 27001/2 2005. Each player had two strategies: Implement and Not-Implement. A set of payoff values for each player's strategy were developed and it was readied for external experts to evaluate. The G-Model was subjected to two types of evaluations; Artificial and Naturalistic. The 2-teir evaluations were noted by some authors (Venable, 2006; Ostrowski & Helfert, 2012) as Internal and External evaluation, with the aim of ensuring the quality of the produced artefact. Obtained experts' oral and written feedback, along with the updated game files, a risk register and play data were available and analysed by the researcher. A number of artefact evaluation criteria based on the system approach articulated by Prat, Comyn-Wattiau, and Akoka, (2014) and corresponding questions, were adopted by the researcher and used for the analysis. By reflecting on the artefacts evaluation outcomes, it was possible to answer the research sub-questions, evaluate the proposed hypotheses and lastly articulate the answer to the research main question. In that process, it has been argued that to integrate IT controls frameworks, best practices and standards, it is imperative to define an overarching framework. A number of criteria have been developed by the researcher as guidance to select such a framework. Similarly, criteria for selecting a supplementary framework have been devised. The two sets can be used when deciding what controls to select and which framework takes precedence when IT risk mitigation requires controls and processes from more than one framework.

In DS based research, it is imperative to communicate the findings to the target audience, which has two categories: academia and business. Research contribution is articulated based on the resulting outcomes to the target audience.

## 1.5 RESEARCH ORGANISATION

The thesis is structured in the following way: Chapter 2 establishes the literature foundation, where IT risk, terms and definitions will be reviewed and established. IT risk management process will be examined and discussed; also IT assurance is explored along with IT auditing process, aspects, objectives and challenges. This is followed by definition of relevant IT controls frameworks, best practices and standards. Implementing IT control-based structured environments faces some

challenges that will be discussed as well as the concept of control capital and the risk management cube model. A set of IT risk management and assurance issues are initially outlined.

In Chapter 3, seven reported problems, outlined from chapter 2 discussed issues and challenges, will be assessed to elect one of them to be the focus of the research. Then the proposed solution is theorised, and relevance of Decision Support Systems (DSS) and Game Theory applications are discussed. Furthermore, a review of work that utilises DSS and game theory to manage IT risk, also to aid practitioners and management in making reliable decisions in devising cost effective mitigating measures.

Chapter 4 outlines the research methodology that the researcher derives from reviewing other similar research studies. Then, the research focus problem is examined again to select a workable research question. In addition, research sub-questions and a set of hypotheses are to be devised to guide the researcher in finding answers to the research question. Furthermore, aspects from the selected research method, industry practices, data reporting and presentation methods, will be examined to identify the justification for the chosen methodology. That leads to justifying the grounds for selecting the research methods, which were derived and reasoned. Part of the research method is to define the data collection methods and to propose analysis, evaluation and reporting criteria.

Chapter 5 is where the evaluation of the first developed model, 'C-Model' is reported, and any issues and further improvements are proposed and justified. The developed artefacts are evaluated against the artefact evaluation criteria, and subsequently the outcomes of the model assessment are presented. Also, the research progress was benchmarked against the DS guidelines and adopted roadmap activities. In Chapter 6, the improved game theory based G-Model is detailed, and the proposed DSS components are outlined. Experts' evaluations are reported and the model evaluation stages, activities, and collected data are tabulated. In a similar fashion to Chapter 5, experts' feedback, oral and written, were collected, tabulated, analysed and discussed. Research progress is checked against the DS research roadmap.

Chapter 7 contains the assessment of outcomes resulting from experts' evaluation of the developed artefacts that were reported in Chapters 5 and 6. The

gathered data is analysed and reflected upon, then answers to the research sub-questions are substantiated. Furthermore, hypotheses are tested and evaluated by the obtained evidence to support or refute. The accumulated evidence then paves the way to answer the main research question. The research contribution to the target audience: to academic researchers, to business management and to practitioners are articulated.

In Chapter 8 the research is summarised and concluded with recommendations and suggestions for further research and related topics.

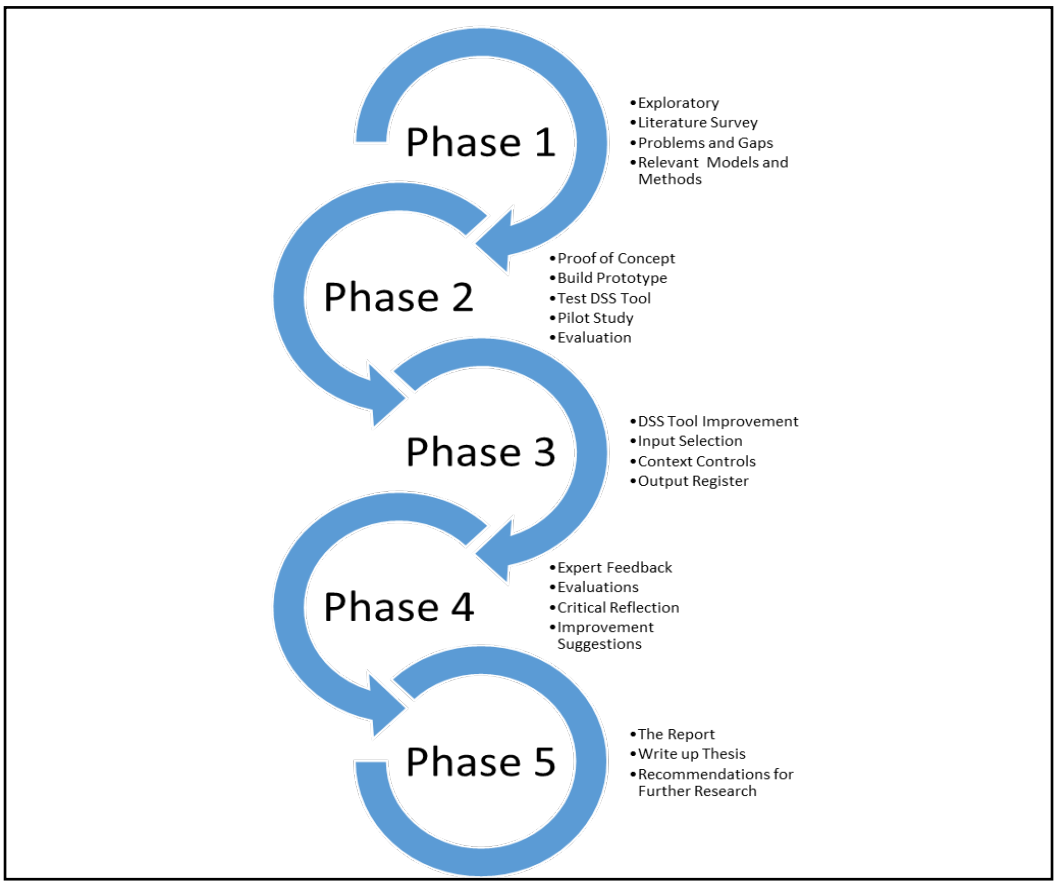


**Figure 1.1: Research 5-Phases**

In summary the research activities are executed in five phases as shown in Figure 1.1. Phase 1 activities are covered in Chapter 2, 3 and 4, while phase 2 activities are covered in Chapter 5, where the C-Model is developed and tested. Phase 3 activities are covered in Chapter 5 as well where the C-Model is evaluated and a number of improvements are suggested. As the C-Model is found inefficient and not fit for purpose at that stage. Following the first DS iteration of activity in phase 1 the reviewing of game theory application is conducted. Then phase 2 and 3 activities are repeated in Chapter 6, where the G-Model is developed, tested and a

number of experts evaluated the developed the DSS and the G-Model. Phase 4 activities are carried on partially in Chapter 6, and also in Chapter 7. Lastly, phase 5 activities are conducted and documented in Chapter 8.

## 1.6 CONCLUSION

The introduction chapter has outlined the research motivation, the focus problem for research and the selected research methodology that suits the research context, problem and questions. In addition, the findings are briefly stated. The thesis organisation was then outlined accompanied by a diagram depicting the research's 5 phases with the component activities to be carried out.

In chapter 2 a literature review analysis is undertaken to identify issues and problems in the chosen research area of IT risk management, IT audit, IT security management, IT controls and IT controls frameworks.

# Chapter 2

# Literature Review: Control Environments

## 2.0 INTRODUCTION

The increasing of business reliance on IT systems and the challenge of the increasing complexity of utilised technologies have made it paramount for organisations to ensure confidence in their IT systems (Whitman & Mattord, 2004; Hadden et al., 2003). The optimal solution is to have various internal and external auditing reviews performed by specialist staff and third parties on the organisation's structures and IT systems (Henczel, 2001; Pathak, 2005). The level of assurance is not only required to meet business demands but also to comply with regulatory requirements (Abu-Musa, 2008; Merhout & Havelka, 2008). Singleton (2007) claims that identity theft and data leaks incidents are on the rise, have pressured governments and industrial agencies to enact and regulate through acts and standards for organisations to comply.

IT assurance is obtained from conducting audit reviews (Wright et al., 2008; Senft & Gallegos, 2009). In addition, relevant policies, procedures and standards as well as governance structure and risk management methodologies must be included in the audit review scope to ensure their alignment with the respective business objectives (Wright et al., 2008; Hall &Singleton, 2005). Outcomes of the audit reviews consist of an objective assessment of the subject systems or processes, with mitigating measures to rectify any identified anomalies (Pathak, 2005; Wright et al., 2008; Hall & Singleton, 2005; Champlain, 2003). Risk based IT auditing is performed in a structured way to ensure devised controls are cost effective and high value assets are protected.

Every aspect of business has elements of uncertainty; hence risk is inherent in business. Risk is defined as "the effect of uncertainty on objectives" (Shortreed, 2008, p. 5). However, organisations must have the capability to seize opportunities when they arise, as Barnier and Fischer (2010) state that "To grow, an enterprise must take risks" (para. 9). In that view, risk represents value for business. Risk, however, needs to be analysed, identified, and managed to reduce the impact, which is the negative side of risk. According to Miccolis, Brehm, Dickson, Franklin,

Kirschner, Kollar, Mango, Morin, Nelson and Zubulake (2003) who stress: “Risk is an essential part of any business. Properly managed, it drives growth and opportunity” (p. 9) and that is the positive side of risk. The focus of the thesis research is on demonstrating business value outcomes through managing IT risk. To achieve this, a risk based IT assurance program implemented through integrated control frameworks, best practices and standards is advocated (Moeller, 2011; Mishra & Dhillon, 2008; Al-Khazrajy, 2012). The integration of control frameworks should generate the best IT controls configuration, which leads to establishing an effective and efficient risk based IT governance and obtain the best business value outcomes (Ramakrishnan, 2009; Schlarman, 2007).

In this chapter, a literature review is performed using online databases of journals and conferences papers in addition to industry publications as well as published books. The literature search was conducted following a thematic approach, where a set of key words (IT audit, IT assurance, IT control frameworks, IT controls, IT risk, risk management, business value, IT value, IT governance) was used to select the relevant papers. The search results were rated and filtered out based on recognised authors and reputed organisations in the field. This chapter is structured to catagorise the literature selected under the four related headings of Risk, Assurance, Control Frameworks and Control Configurations. A fifth section is included to discuss the related challenges and issues. Section 2.1 reviews models and systems used to evaluate risk in business context and the relationship between risk and value. Section 2.2 discusses the issue of the level of assurance an organization requires for confidence that the risk is adequately managed. The concept of a ‘control’ is defined and the logical practice of audit and IT audit are described. Section 2.3 reviews most used control frameworks, standards, and, best practice methodologies for IT audit, and IT risk management. In section 2.4 control configurations are reviewed and resultant effects in control capital are reported. Section 2.5 evaluates the literature reviewed in sections 2.1 to 2.4 to identify issues with potential for research. Section 2.6 is the final section, which concludes Chapter 2 and provides a link to Chapter 3 that completes the problem identification.

## 2.1 BUSINESS-IT RISK REVIEW

Monahan (2008) refers to the definition of an enterprise as "a unit of economic organisation or activity; especially a business organisation" (p. 1). In that view, Monahan indicates that organistaion as a term, doesn't reveal the size or nature of the business. Furthermore, Monahan (2008) defines Risk as "anything that produces a distribution of various outcomes of various probabilities" (p. 2), and emphasises to think of risk as a meaning of uncertainty. This view is shared by Shortreed (2008) who defines risk as "the effect of uncertainty on objectives" (p. 5). However, Smith and McKeen (2009) indicate that with the business-enabling role of IT systems, risk is not simply uncertainty or the possibility of a loss. The authors state that "Today, risk, is a multilayered concept which implies there is much more at stake" (p. 520). Risk has two aspects that can contribute either positively or negatively to an organisation: cost and benefit (Whitman & Mattord, 2004). Risks have to be analysed, identified, and managed to reduce its impact, which is the negative side of risk. On the opposite side, Miccolis et al. (2003) stress that "Risk is an essential part of any business. Properly managed, it drives growth and opportunity" (p. 9), which highlights the positive side of the risk. Organisations must have the capability to seize opportunities when they arise, as Barnier and Fischer (2010) state that "To grow, an enterprise must take risks" (para. 9). In that view, risk, if properly managed, represents a value to the business. Vose (2008) describes value as an opportunity when he states "a risk and opportunity can be considered the opposite sides of the same coin" (p. 3).

IT systems have become business enablers; Hadden et al. (2003) indicate that IT systems offer many advantages, for example operational efficiency, cost saving and reduction of human error. IT risk exists, as business risk does, within the asset and/or the processes that utilise and impact a number of assets. Hadden et al. (2003) stress that "heavy reliance on IT also increases organisational risk" (p. 28). To ensure effective and efficient IT risk management, the process objectives should be aligned with business objectives at all levels, as the business requires:

strategic, tactical and operational planning (Walser, Kuhn, & Riedl, 2009; Ames, 2007b).

This section explores business and IT risk definitions in sub-section 2.1.1, while sub-section 2.1.2 defines and elaborates on IT risk management process. In sub-section 2.1.3 a discussion of IT risk and business value is made, and sub-section 2.1.4 examines known risk measurements methodologies, and finally the section summary is outlined in sub-section 2.1.5.

### 2.1.1 IT Risk Definitions

IT systems have become business enablers. Like any business activity, IT systems are susceptible to risk, which is required to be assessed, evaluated (Whitman & Mattord, 2004). Once the risk is identified and evaluated it has to be treated through mitigating measures (Monahan, 2008). In many organisations, IT risk management has become the core function of the IT security management (Whitman & Mattord, 2004). While managing IT risk focuses on the technical aspects of IT systems from an IT security point of view. Marinos, Kirchner, and Junginger (2009) stress that risks of other types have to be identified and managed for example: project management, change management, Research and Development (R&D) and Quality Assurance (QA). Every aspect of business has an element of uncertainty; hence risk is inherent in business. Smith and McKeen (2009) indicate that “Today, risk, is a multilayered concept which implies there is much more at stake” (p. 520). Subsequently, Smith and McKeen add, organisations are referring to ‘Enterprise Risk Management (ERM)’ as a more comprehensive and integrated approach to manage risk holistically.

Risk Management Governance structure is required to be established as stated by Moeller (2011). Brand and Boonen (2005) in their definition of IT Governance (ITG) state that the structure is to be an integral part of ITG, which in turn is an integral part of the enterprise governance. Risk Management governance defines policies and procedures, and determines the organisation’s risk appetite and risk tolerance, and identifies roles and responsibilities. In addition, risk management governance determines the periodic reviews and reporting at a frequency that ensures effective and efficient Risk Management process (Walser et al., 2009). Risk Drivers and Controls, according to Monahan (2008), are “factors

that influence the outcome" (p. 5). Monahan differentiates between the two as follows: Risk Drivers are factors that increase uncertainty, while, Controls reduce the level of uncertainty to a manageable level.

Inherent Risk is the raw or untreated risk (Monahan, 2008). While Residual Risk is the remaining portion of the risk after applying the mitigating measures (Monahan, 2008). Residual risk could be caused by the deficiency of the control that has been devised in the treatment plan (Shortreed, 2008). In addition, factors like undetected risk and uncertainty in risk evaluation could contribute to the residual risk (ISACA, 2009a; Whitman & Mattord, 2004). Figure 2.1 depicts Residual Risk in relation to the overall risk of information assets.

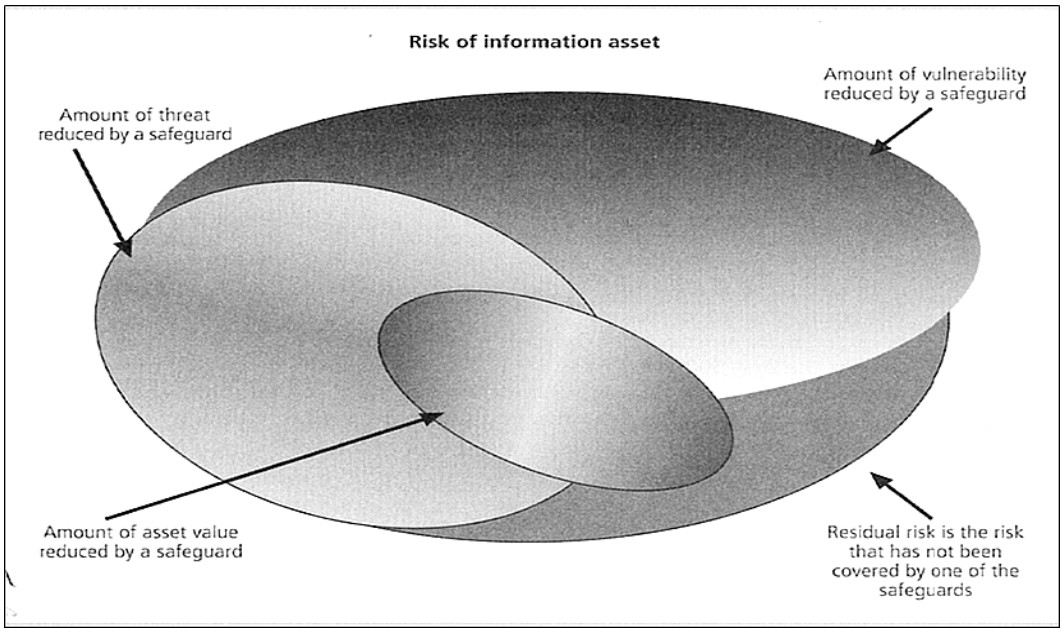


**Figure 2.1: Residual Risk (Whitman & Mattord, 2004, p. 341)**

According to Whitman and Mattord (2004) Risk Appetite is the quantity and the nature of risk that an organisation is willing to accept. Moeller (2008) indicates that Risk Appetite is the risk an organisation would accept in terms of the risk impact and likelihood, as Figure 2.2 illustrates. Risk appetite is defined by the senior management at the enterprise level that would consider two major factors: first, the enterprise's objective capacity to absorb loss in tangible (financial) or intangible (reputation) form. Second, the management culture towards risk taking: cautious or aggressive (ISACA, 2009a). Risk appetite is translated into standards and policies used to manage the risk level within the limits set by the risk appetite (Moeller, 2011).

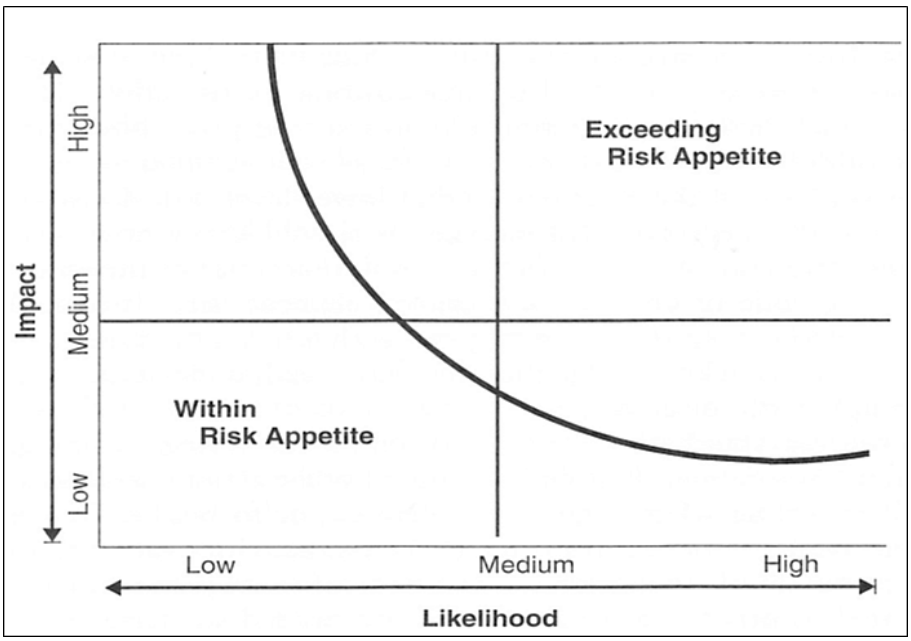


**Figure 2.2: Risk Appetite Map (Moeller, 2011, p. 61)**

Risk Tolerance, is the permissible deviation from the level of the risk appetite (Moeller, 2008, p. 254). Risk tolerance is defined by senior management and reflected in relevant policies at the enterprise level. At the operational level, however, exceptions can be tolerated as long as the overall risk has not exceeded the risk appetite (Moeller, 2011).

Setting Risk Appetite at the enterprise level helps organisations manage risk in a defined and methodical way. Moreover, defining Risk Tolerance adds an agility attribute to the organisation's capability and gives a needed and controlled flexibility should a business opportunity arise (ISACA, 2009b). Key Risk Indicators (KRIs) are metrics designed to indicate when a risk exceeds the defined risk appetite (ISACA, 2009b). Monahan (2008) defines KRIs as "metrics for risk drivers or early warning indicators" (p. 52). Monahan adds that KRIs are lead indicators of risk and vital to the success of Risk Management. The attributes of KRIs are designed specifically for each enterprise, considering their internal and external environments (ISACA, 2009b).

Risk Management process can be defined as "systematic application of management policies, procedures and practices to the tasks of communication, consultation, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk" (Shortreed, 2008, p. 5).

### 2.1.2 IT Risk Management

Marinos et al. (2009) stress that Risk Management is a recurrent process, which has been defined as noted in section 2.1.1. Furthermore, it was emphasised by Moeller (2011) that "Risk Management should be part of a decision-making process and be tailored in a systematic and structured manner" (p. 26). In addition, Marinos et al. (2009) indicate "IT Risk Management is a specialisation of Risk Management and focuses on the implementation of IT with respect to the overall organisational goals" (p. 369). The Risk Management task is depicted as a process in Figure 2.3. It commences with establishing the context, identifying, analysing and evaluating risk, and then devises a treatment plan. It is imperative to emphasise the inter-relation of 'Document and Consult' activity, in Figure 2.3, with the risk management process stages. Similarly, the 'Monitor and Review' activity inter-relates with all process stages in a similar fashion as the 'Document and Consult' stage. 'Monitor and Review', feeds back into the beginning of the process, which is the 'Establish the Context' activity. Conducting the 'Monitor and Review' part of the process in such a fashion is crucial for ensuring the risk management process is continuous, dynamic and responding to changing threats and vulnerabilities in a timely fashion (ISACA, 2007). Similarly, Moeller (2011) states that "Risk Management process should be dynamic, iterative and responsive to change with the capabilities of continual improvement and enhancement" (p. 26).

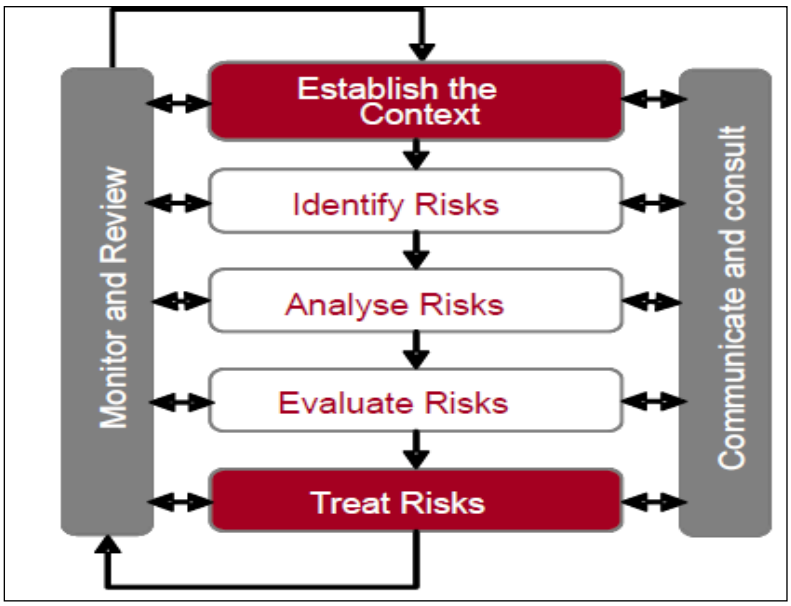


**Figure 2.3: Risk Management Processes (Shortreed, 2008, p. 5)**

An organisation must have the capability and ability to detect and respond in a timely fashion to a risk when it materialises. An effective risk management program, however, is complex and encompasses the entire organisation (ISACA, 2007; Whitman & Mattord, 2004; Monahan, 2008; Smith & McKeen, 2009).

### 2.1.3 IT Risk and Business Value

According to Curry, Flett, and Hollingsworth (2006), the role of IT systems has evolved from helping organisations improve operational efficiency and increase management effectiveness, to improve competitiveness through strategic information systems. Shin (2003) argues that high business value is gained from the interwoven relationship and strategic alignment between IT systems and the various business divisions' requirements, as shown in Figure 2.4. The solid line in the figure denotes the Business-IS strategic alignment in the key business processes. The alignment ensures effective operation and produced services are delivered to their customers. That requires high performing marketing and customer relationships, which all require adequate planning, along with support and supplier management. In line with that view, Chen, Huff, Barclay and Copeland (1997) stress the importanc of the Business-IS strategic alignment and its impact on business performance and IS effectiveness.

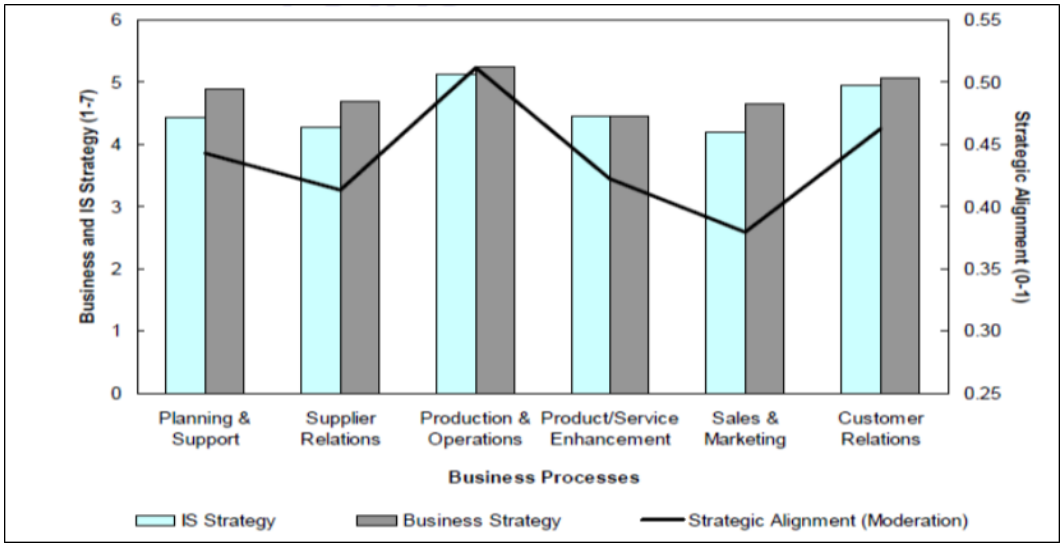


**Figure 2.4: Relating the Strategic Alignment to Business and IS Strategy (Shin, 2003, p. 13)**

Additionally, Murphy (2002) argues that IT value is gained from various business functions and divisions, as illustrated in Figure 2.5. The figure indicates the 'Ever changing Business context' and shows 'Risk' as one of the 'Pillars' a business is

based on, which ensures its existence. However, that doesn't mean risk is managed in isolation from the rest of the business divisions or Pillars. In fact, risk resides in each division and at all levels, and has to be managed holistically (Marinos et al., 2009; Smith & McKeen, 2009).

As IT systems underpin all divisions' activities, IT risk exists wherever IT systems are planned, implemented, operated and managed. Hadden et al. (2003) state that "While offering many advantages (operational efficiency, cost savings, and reduction of human errors, for example), heavy reliance on IT also increases organisational risk" (p. 28). Figure 2.5 by Murphy (2002) encapsulates risk in the dynamic of business action.

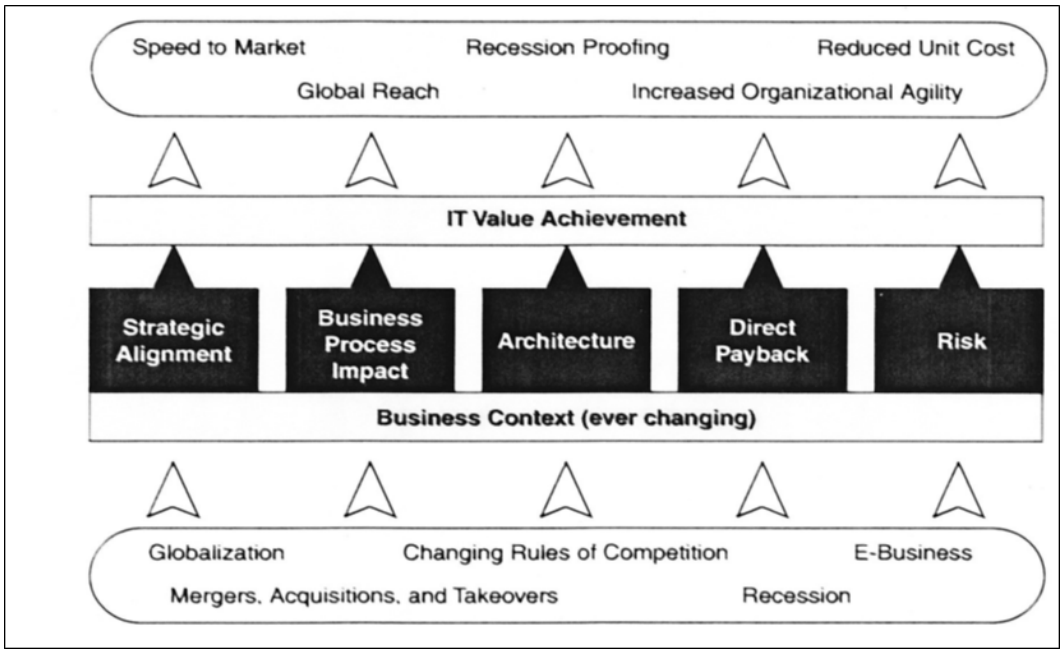


**Figure 2.5: The Five Pillars of Benefits Realisation (Murphy, 2002, p. 41)**

Whitman and Mattord (2004) indicate that because IT is now readily available to everyone, all organisations have access to all technologies should they opt to use them. However, implementing new technologies doesn't guarantee competitive advantage. A new and critical factor has emerged that is the concept of competitive disadvantage, when organisations fall behind the competition. Whitman & Mattord (2004) elaborate and state: "Effective IT-enabled organisations now quickly absorb emerging technologies, not to gain or maintain the traditional competitive advantage, but rather to avoid the possibility of losing market share" (p. 320). To shield their business, organisations must design, develop and maintain secure and reliable IT systems (Whitman & Mattord, 2004). This view is shared by Smith and

McKeen (2009). To ensure IT systems are secure and reliable, IT risk has to be assessed and managed. However, a balance needs to be struck between managing the perceived risks and opportunities. Moeller (2011) indicates that "Risk Management should create value and be an integral part of the organisational processes" (p. 26). Figure 2.6 shows the roles of IT as value enabler and value inhibitor.

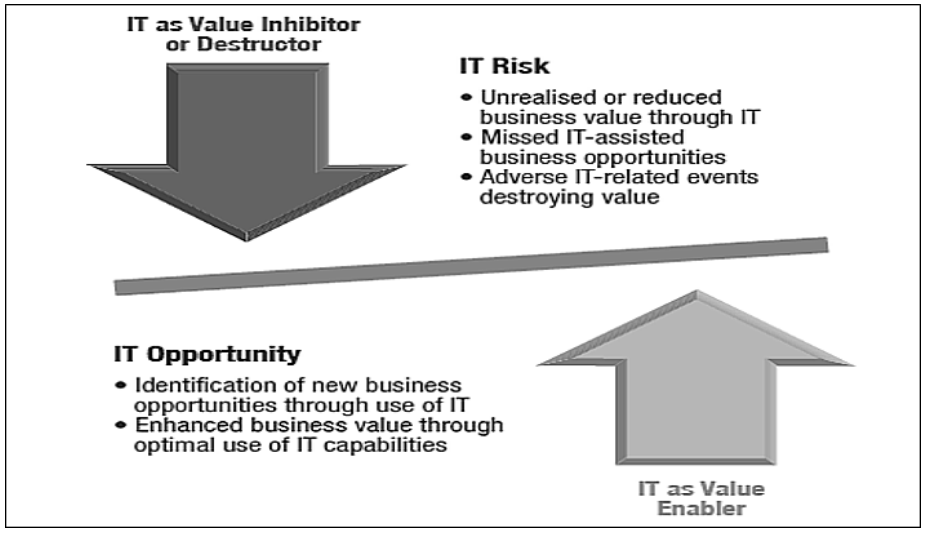


**Figure 2.6: Risk and Opportunity (ISACA, 2009d, p. 32)**

At the enterprise level, as shown in Figure 2.7, risk is categorised into the following: strategic risk, environmental risk, market risk, credit risk, operational risk and compliance risk. As IT has become a comprehensive business enabler, IT risk exists in all risk categories to various degrees, as depicted in Figure 2.7.

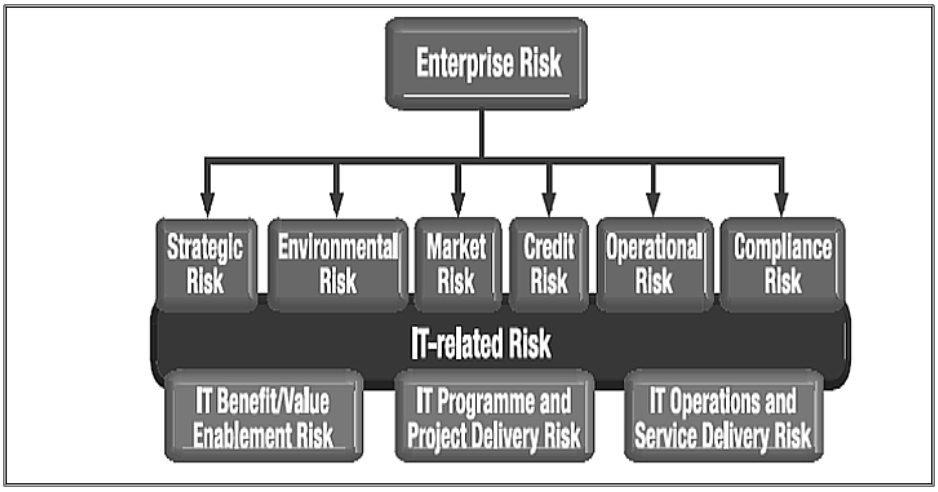


**Figure 2.7: IT Risk in the Risk Hierarchy (ISACA, 2009b, p. 11)**

The way IT systems enable businesses and influence the activities, leads to categorising IT risk in the following ways: IT benefit/value enablement risk, IT

program and project delivery risk and IT operation and service delivery risk (ISACA, 2009b). The operational risk seems to be the most challenging risk to address, as it frequently changes (Miccolis et al., 2003).

### 2.1.4 Measurement

Sademies and Savola (2005) claim that it is widely accepted principle that to be able to manage an activity it is imperative to measure it first. Similarly, Monahan (2008) states that "Measurement is absolutely fundamental to managing anything" (p. 59). The author further adds that measurement is the only way to ensure progress to date, if any, and it allows applying informed decisions. Measuring includes various aspects in business: strategic, operational and project objectives, IT performance, value, and risk. This section however, discusses measurement of IT risk and its implied Business-IT value.

#### 2.1.4.1 Measurement of IT Risk

In section 2.1.1 it has been discussed that the risk appetite and risk tolerance should be defined in order to manage risk methodically. The risk appetite could be measured qualitatively or quantitatively, as noted by Moeller (2008). Measuring risks is imperative for evaluating their impact on the business in order to cost effectively devise mitigating measures (ISACA, 2007). Risk management process is performed to identify, analyse, evaluate and treat risks, as noted in section 2.1.2. Part of the risk analysis stage is determining the risk likelihood and impact factors, for which data could be collated from respective stakeholders and relevant records from an incident management system (Whitman & Mattord, 2004). By combining the outcome of risk analysis with Business Impact Analysis (BIA), risks are further analysed and prioritised according to the asset business value (ISACA, 2007).

Risks are evaluated either qualitatively or quantitatively (Ames, 2007b; Moeller, 2011; Monahan, 2008). Moeller (2011) describes qualitative approaches as a quick best-guess, and quantitative as detailed and very mathematical ones. In that view, Leitch (2008) refers to the qualitative analysis as non-mathematical, while quantitative analysis is a mathematical method. A qualitative estimate is subjective and based on judgment, intuition and experience, where brain-storming sessions or surveys can be used. While, quantitative analysis provides numeral and possibly monetary value for risks and provides more accurate risk measurements

(Whitman & Mattord, 2004). However, for IT risk, an issue arises because it is difficult to quantify, and IT risk analysis is largely subjective (ISACA, 2007). Leitch (2008) indicates that financial risk including market and credit risk has long been mathematically driven and has utilised historical data about prices and loan defaults. Similarly, operational risk management in banks and insurance companies, have been managed on a mathematical basis. In contrast, IT security risk management, typically keeps away from mathematics. It utilises some approaches to derive financial calculations of the cost and value of risk and corresponding mitigating measures (Leitch, 2008).

Quantifying risks factors (impact and likelihood), in some forms, helps derive an expected value of the risk (Moeller, 2011). However, Moeller indicates that those risks are initially identified through brain-storming sessions, which suggests some level of subjectivity in determining the risk in the first place. Monahan (2008) stresses that "an analysis of risk likelihood and potential impacts can be developed through a series of qualitative and quantitative measures" (p. 259). While brain-storming could be used in the initial stage to identify risks and estimate their factors. However, brain-storming techniques draws some criticism for being too subjective and prone to be biased to the views of influential stakeholders (Moeller, 2011). Hence, some authors suggest using more robust methods to solicit stakeholders' responses in the initial stage of risk identification and its factors. For example, one well known method is the Delphi method, where risk is analysed and evaluated by collating information from stakeholders (Whitman & Mattord, 2004; Moeller, 2011).When risks and their factors are identified they could be represented in a risk impact matrix that is generated to work out the overall risk in forms of low, medium, and high, or their variations as noted in Figure 2.8. The outcomes of this risk analysis is compared to the risk criteria (risk appetite and risk tolerance) that should have been defined previously, to conclude whether the risk's magnitude is acceptable or requires further treatment, as noted in section 2.1.1. Monahan (2008) states that "numbers can be ambiguous, but numbers are less ambiguous than words" (p. 49).

| Likelihood of Risk Occurring | Consequences of Risk Occurring | | | | | |
|---|---|---|---|---|---|---|
| | | Insignificant | Minor | Moderate | Major | Severe |
| | Almost Certain | Medium | High | High | Excessive Very Critical | Excessive Very Critical |
| | Likely | Medium | Medium | High | High | Excessive Very Critical |
| | Possible | Low | Medium | Medium | High | Excessive Very Critical |
| | Unlikely | Low | Medium | Medium | Medium | High |
| | Rare | Low | Low | Medium | Medium | High |

**Figure 2.8: Risk Impact Matrix (Moeller, 2011, p. 278)**

Hence, when applying qualitative risk assessment methods, some ranking could be applied to the risk impact and likelihood, for example (1-9, 0-10) scale as noted by Whitman and Mattord (2004) and Moeller (2011). In addition, Monahan (2008) and Whitman and Mattord (2004) point out that it is feasible to quantify an IT asset's intrinsic and acquired values which would be used in the cost-benefit analysis that helps in decision-making to mitigate the identified risks. Figure 2.9 illustrates an example of risk-ranking along with the cost of impact and expected value of the risks.

| Identified Risk | Significance Probability | Likelihood Probability | Risk Score (P x L) | Rankings | Cost Impact | Expected Value of Cost | Risk Response Planning? |
|---|---|---|---|---|---|---|---|
| C | 0.79 | 0.66 | 0.52 | 1 | $ 120,600 | $ 62,881 | Yes |
| G | 0.62 | 0.72 | 0.45 | 2 | $ 785,000 | $350,424 | No |
| I | 0.90 | 0.45 | 0.41 | 3 | $ 15,000 | $ 6,075 | Yes |
| D | 0.77 | 0.45 | 0.35 | 4 | $ 27,250 | $ 9,442 | Yes |
| E | 0.35 | 0.88 | 0.31 | 5 | $ 52,350 | $ 16,124 | Yes |
| F | 0.54 | 0.49 | 0.26 | 6 | $ 1,200 | $ 318 | Yes |
| B | 0.88 | 0.24 | 0.21 | 7 | $ 12,650 | $ 2,672 | Yes |
| A | 0.55 | 0.30 | 0.17 | 8 | $ 98,660 | $ 16,279 | Yes |
| H | 0.66 | 0.20 | 0.13 | 9 | $1,200,980 | $158,529 | No |
| J | 0.12 | 0.88 | 0.11 | 10 | $ 88,600 | $ 9,356 | Yes |

**Figure 2.9: Risk-Ranking Response-Planning Example (Moeller, 2011, p. 44)**

With regards to the risk mitigating-controls there are different types of controls: Preventive, Detective, and Corrective. Each will be devised based on the risk assessment outcomes. Factors like asset type, its vitality to the business, feasibility and cost, would determine controls selection and implementation (Monahan, 2008; Leitch, 2008).

In section 2.1.3 and 2.1.4 it has been established that the necessity to manage IT risk holistically to ensure the resolution effectiveness and efficiency.

Risks could impact different business units and functions at various levels. In addition, risks could be interdependent of other risks (Moeller, 2011). That would surely increase the complexity of risk management process. According to Vose (2008), the biggest uncertainty in risk analysis is whether the analysis started off analysing the right things and in the right way. Whitman and Mattord (2004), define uncertainty in risk analysis as the lack of knowledge of the risk vulnerability and stress that "it is not possible to know everything about every vulnerability" (p. 310); as noted in the Risk analysis equation:

Risk = (Likelihood X Value of Asset) – (% of Risk mitigated by Control) + (Uncertainty of current knowledge of Vulnerability)

Whitman and Mattord (2004) further point out the uncertainty in estimating risk factors (impact and likelihood) that contribute to the overall risk uncertainty. In addition, other factors such as the residual risk that could contribute to risk uncertainty, as it has been discussed in section 2.1.1 and illustrated in Figure 2.1.When an organisation identifies many risks that are within the top right corner of Figure 2.8, where risks impact and likelihood are both high, the organisation might not have sufficient means to rectify all those risks (Moeller, 2011). Similarly, Proctor (2007), as cited in Smith and McKeen (2009) states that: "The shift to risk management requires an acceptance that you can't protect yourself from everything, so you need to measure risk and make good decisions about how far you go in protecting the organisation" (p. 519). Hence, it becomes necessary to prioritise those risks again, and a more precise measurement is needed (Moeller, 2011; Leitch, 2008; Vose, 2008). Given the level of uncertainty that is implied in the identified risks and their factors, re-prioritising such large list of risks becomes a daunting task for practitioners (Moeller, 2011).

"Monte Carlo simulation is a 'qualitative' risk analysis technique used for understanding and evaluating uncertain risks" (Moeller, 2011, p. 47). Other authors (Vose 2008; Leitch, 2008; Monahan, 2008) classify Monte Carlo simulation as a 'quantitative' analysis technique. Moeller bases his definition on the basis that initial values of risks factors, are estimated, or better guessed, by selected stakeholders who have sufficient expertise in the business unit/function/asset subject to the risk analysis. Setting or guessing the initial values remains subjective or qualitative. However, once these values are set, Monte Carlo simulation

performs quantitative analysis and produces a distribution of the expected values for the risks. Monte Carlo simulation helps managers apply probability rules to gain better understanding of a set of risks (Moeller, 2011; Monahan 2008; Leitch, 2008; Vose, 2008).

#### 2.1.4.2 Measurement of Business-IT Value of IT Risk

Monahan (2008) indicates that planning is required to ensure business strategic objectives are achieved. Monahan further adds, measurement is the best way to monitor how successful the execution plan is. With regards to Information Systems, Nicho (2006) stresses the necessity for IS to be measured from different dimensions and indicates that multidimensional aspects of IS (Time, cost, user satisfaction, and computer operations) were evident in early measurement studies of Powers and Dickson (1973, as cited in Nicho, 2006). While productivity was, then, the main key in measuring IS effectiveness, the concept of quality (timeliness, convenience, accuracy, reliability or availability, flexibility of adaptability, and relevance or selectivity) was proposed as well by Kriebel and Raviv (1980, as cited in Nicho, 2006). Furthermore, Brancheau and Wetherbe (1987, as cited in Nicho 2006) indicate that other aspects have been added to measuring IS effectiveness. For example, strategic planning, competitive advantage, IS's role and contribution and alignment with business.

With regards to business-IT value measurement methods Silvius (2008) researched this space and argues that "The relation between IT and value is a complex and disputed one" (p. 57). The former statement is aligned with Nicho's view, explored in the previous paragraph, on the complexity of value measurement. Similarly, McKay and Marshall (2004) state that "business benefits tend to be more intangible, less direct, and more interwoven and diffused across a range of organisational activities" (p. 3). Silvius (2008) explored various methods researched by a number of authors and categorised the methods in five main categories: Financial methods, Advanced financial methods, Multi-criteria methods, Ratio methods and Portfolio methods. Examining these methods' strengths and weaknesses identified that they influence the calculation and interpretation of results and the perspectives on risk. Frisk (2007, as cited in Silvius 2008) argues that Multi-criteria methods "aim to identify different relevant aspects of value and risk in order to enable a thorough discussion and an informed

discussion" (p. 57). However, the most important method of the multi-criteria category as pointed out by Silvius (2008) was called information economics. Although the method is suited for evaluating a single project or a portfolio of projects, yet, it examines the interwoven relationship between risk and value and their measurement method. In the information economics methods, projects are evaluated based on values and risks they entail and placed in the four quadrants of decision-making as illustrated in Figure 2.10. The figure demonstrates the investment-project evaluation based on the collective value and risk measures, and the associated decision with each quadrant.

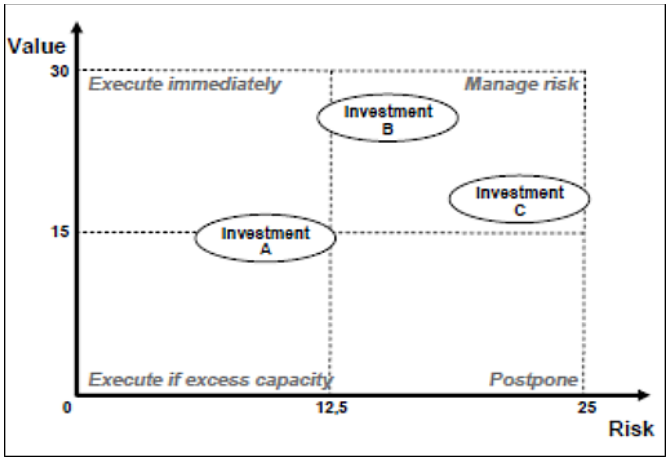


**Figure 2.10: A Typical Information Economics Presentation (Silvius, 2008, p. 61)**

Silvius (2008) concludes by stating that "value is a multidimensional concept that is difficult to express in a simple number" (p. 64). In addition, Silvius adds that value is circumstantial and argues that attention should be made to how IT assets impact business processes and how they enable the business in achieving its strategic objectives.

In section 2.1.3, it has been established that there is a business value in managing IT risk (Buckby, Best, & Stewart, 2009). This includes effective IT risk management as one of the outcomes of a robust ITG implementation. Heier, Borgman, and Maistry (2007) developed Table 2.1 that lists some examples of quantitative and qualitative business values that could be gained from IT Governance. Monahan (2008) indicates that managing IT risk leads to meeting business objectives, hence, these values are examples of the business values an organisation could gain from managing IT risk. In Table 2.1, it can be observed that an improved Capability Maturity Model (CMM) is one of the qualitative measures used.

**Table 2.1: Examples of Business Value Quantitative and Qualitative Measures (Heier et al., 2007, p. 241)**

| | |
|---|---|
| Portfolio Management Optimization | Qualitative outcomes:<br>▪ Improved alignment between business and IT strategies<br>▪ Improved executive communication and decision making (real-time)<br>Quantitative outcomes:<br>▪ Monetary savings through avoiding investments in non-viable IT projects<br>▪ Monetary savings through repurposed capital investments |
| Project Visibility and Control | Qualitative outcomes:<br>▪ Improved capability maturity level (CMM)<br>Quantitative outcomes:<br>▪ Percentage increase in healthy IT projects (i.e. fulfilling performance criteria, on budget, on time)<br>▪ Percentage increase in milestone delivery<br>▪ Percentage decrease in project management costs (percentage of total project costs) |
| IT Services Efficiency | Qualitative outcomes:<br>▪ Improved audit and regulatory compliance<br>Quantitative outcomes:<br>▪ Percentage decrease in operational IT spending (percentage of revenues), e.g. savings through increased IT productivity and lower IT staffing costs<br>▪ Percentage reduction in incident resolution times<br>▪ Time savings in deploying application changes (from change request to production) |

According to Self (2004) the Balanced Scorecard (BSC) is another measurement method that could be used utilising qualitative and quantitative means. In addition the author explores the defined set of metrics to develop BSCs in order to measure various facets of business performance and values. Monahan (2008) states that "the fact that measurement is important means we have to set metrics" (p. 48). Monahan further indicates that the benefit in setting metrics values is to measure progress to achieving strategic business objectives, the statement could be generalised to measure any objectives subject to measurement. Self (2004) states "selecting metrics is perhaps the most crucial part of the process. Once a metric is established, it has an organisational imprimatur" (p. 102). Self adds, defining the nature of measurement is important and points out that "the choice of metrics reflects the values of the organisation" (p. 102). In other words, the metrics should be designed and defined to measure what's relevant to the organisation, and this is one of the issues that has been highlighted by Neely and Bourne (2000) who investigated causes of failing measurement initiatives.

Neely and Bourne (2000) explored a number of case studies where BSC is designed to measure business-performance and value. The paper indicates that figures from Gartner showed that 40-60% of corporate businesses would have utilised BSC for performance and value measurement. However, it also indicates that almost 70% of the BSC implementation would fail for a number of reasons,

which the authors categorised mainly as Design and Implementation issues, and state: "There are two main reasons why measurement initiatives fail. The first is that measurement systems are often poorly designed. The second is that they are difficult to implement" (p. 3). The paper produced by Self (2004) outlines the same issues as Neely and Bourne (2000) findings. The first issue noted by Neely and Bourne (2000) is about what to measure, which is aligned with Self's (2004) findings. The second issue is the implementation process which is complicated and it is caused by political (organisational culture), infrastructure, and focus (Neely & Bourne, 2000). Self (2004) indicates that collecting data for metrics, designed to feed into a BSC system utilised to measure performance, consumed substantial amounts of time. The implementation process further required some expertise to collate data from various resources and to interpret the data adequately. Which is about having the right infrastructure of systems to extract relevant data with appropriate reporting schemes. Furthermore, Self (2004) emphasises that the organisation culture is imperative to the success of the data collection stage. As some staff might consider that as a management chance to apply strict measures, and turned to either avoid contributing to data collection or undermining the whole process. This view was noted by Neely and Bourne (2000) as the political underlying cause of implementation failure.

The National Institute of Standards and Technology [NIST] (2006) guideline for setting metrics for information security programs, points out the necessity of having a mature structured environment. The importance of that is in order to be able to collect sufficient and relevant data on timely fashion. Also being able to interpret the data and generate meaningful reporting so that actions are devised accordingly. While the guideline is about settings metrics for a security program, however, it measures various objectives depending on the maturity level the program is at. That seems to provide the answer to the issues that have been highlighted by Neely and Bourne (2000); and, Self (2004) on metrics design and implementation.

Figure 2.11 from NIST outlines the various maturity security program stages and the viability and difficulty in collecting data as well as the metrics types that could be applied. On the left hand, bottom up, the row headings are: Metrics types, Collection Automation, Collection Difficulty and Data Availability. While

the columns correspond to the maturity levels 1-5, which are: Policy Developed, Procedure Developed, Procedures and Controls Implemented, Procedures and Control Tested, and Procedure and Controls Integrated. As shown in Figure 2.11, for example, in Level1, where only policies are defined, metrics are merely about setting goals, while automation of data collection is not viable, and collected data is quite difficult. The higher the maturity level of the environment is, the more documentated, implemented and tested controls and procedures are. Subsequently, more data is available and it is collected automatically, with less difficulty. Ultimately, controls and procedures are integrated and data collection is fully automated, and there are more rigorous metrics designed for measurement.

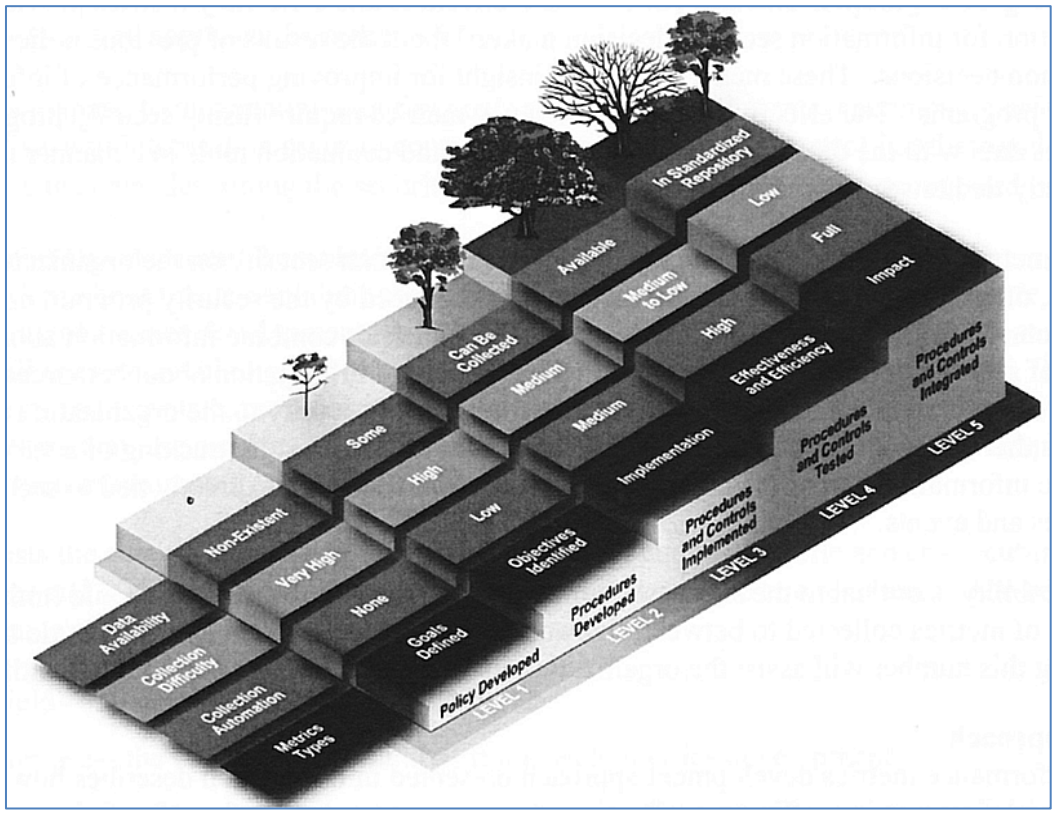


**Figure 2.11: Information Security Program Maturity and Types of Measurement (NIST, 2008, p. 12)**

Business contexts, both internal and external, are subject to change and accordingly the risk profile also changes. New assets could be introduced, and their business value and impact requires to be evaluated and included in the risk assessment. In addition, vulnerabilities and associated threats evolve and quite possibly new types are introduced for new and existing assets when the business process changes. For these reasons, it is crucial to monitor the risk profile and review the implemented controls that have been defined in the risk treatment plan to ensure the plan

effectiveness and efficiency and expected business value is gained (Ames, 2007a; Whitman & Mattord, 2004; Shortreed, 2008; Moeller, 2008; Moeller, 2011).

### 2.1.5 Section Summary

In section 2.1, the following key points have been accomplished:

- Key IT risk definitions were outlined;
- IT risk management process was defined and examined;
- The duality of IT risk and value was discussed in a business context; and
- IT risk assessment and evaluation alternatives are explored.

## 2.2 IT ASSURANCE REVIEW

In section 2.1 it has been established that organisations should develop adequate capabilities to be able to respond constructively to business dynamics. Senft and Gallegos (2009) indicated that "the unpredictability of customer needs and the shortness of products life cycle will cause a mix of production capabilities and underlying resources by the organisation to change constantly" (p. 7). Organisations continue to rely heavily on technology to perform daily transactions. However, technologies are associated with various types of risks that must be managed via various processes, mechanisms and mitigating measures (Hall & Singleton, 2005). Organisations are required to have a satisfactory level of assurance that their risks are managed adequately as and when required (Senft & Gallegos, 2009; Lovaas, Streff, Podhradsky, 2009, as cited in Lovaas & Streff, 2009). Senft and Gallegos (2009) stress that in the hope to avoid and prevent incidents such as the Enron and WorldCom collapses, "the role of information technology IT control and audit has become critical mechanism for ensuring the integrity of IS and the reporting of organisation finance" (p. 3). In addition, as IS are penetrating nearly all business functions and processes, "issues such as ITG, E-commerce, security and privacy and the control of public and enterprise information have driven the need for self-review and self-assurance" (p. 47). This view is shared by Merhout and Havelka (2008) and Mishra (2007).

This section is structured as follows: sub-section 2.2.1 assurance and auditing, sub-section 2.2.2 discusses IT controls, while sub-section 2.2.3 examines

role of IT auditor. Sub-section 2.2.4 details IT audit process stages and sub-section 2.1.5 discusses IT audit risk. Sub-section 2.2.6 summarises the section.

### 2.2.1 Audit and Assurance

According to Wright et al. (2008) “an audit consists of the evaluation of an organisation’s systems, process, and controls and is performed against a set of standards or documented process” (p. 5). The authors further add that audits are designed to provide an independent assessment through testing and evaluation of systems subject to review. Hall and Singleton (2005) referred to a definition of audit from the Accounting Review: “Auditing is a systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and establishing criteria and communicating the results to interested users” (p. 3). Wright et al. (2008) indicate that “Audit is about managing risk” (p. 27), and that the objective of audit is to act as a management means to measure and report risks, which should allow the management to make an informed decision.

It is imperative to indicate the necessity of audit independence (Senft & Gallegos, 2009). Senft and Gallegos further emphasise that audit report and opinion must be free of any bias or influence. A view shared by Merhout and Havelka (2008) who define audit as “an independent examination of an organisation’s management assertion that must follow a set of guidelines and standards promulgated by an external sanctioning body” (p. 264).

Hunton, Bryant, and Bagranoff (2004) describe attestation as one of the audit types, where auditor provides assurance on the subject that the client is responsible of. For example, a client is responsible of the effectiveness of the implemented internal controls. The auditor examines the subject systems, controls, processes and generates a report forming the auditor’s opinion in the audited subjects (Hunton et al., 2004; Hall & Singleton, 2005).

According to Hall and Singleton (2005) assurance encompasses, but is not limited to, attestation, as illustrated in Figure 2.12, which shows assurance, audit and attestation services, and how they interact. Furthermore, assurance is a professional services aim at providing business with quality information that helps decision-making to be more effective and trustworthy (Hall & Singleton, 2005).

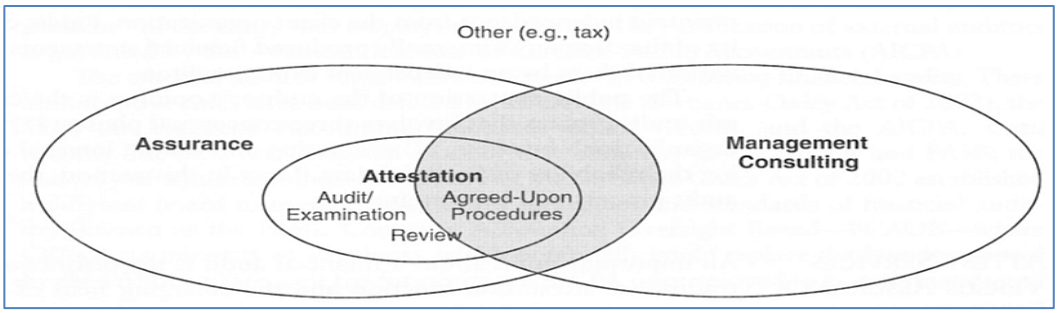


**Figure 2.12: Relationship between Assurance Service and Attest Service (Hall & Singleton, 2005, p. 6)**

Wright et al. (2008) and Hunton et al. (2004) list ISACA as the foremost professional society for IT audit, compliance and governance. While IIA (the Institute of Internal Auditors) is the professional association for internal auditors and risk advisers, that covers risks and audit fields from the financial to IT. Furthermore, the Federal Information System Controls Audit Manual (FISCAM) is the standard against which the FISMA (Federal Information Security Management Act) is measured (Wright et al., 2008). Another noted organisation in the audit field is the American Institute of Certified Public Accountants (AICPA) that confers the Certified Public Accountant (CPA) licence (Hunton et al., 2004). A CPA auditor performs IT audits as well as other aspects of accounting including tax, and consulting (Hunton et al., 2004). Moreover, the Auditing Standards Board (ASB) is the initiator of various Statements on Standards for Attestation Engagements (SSAE) (Moeller, 2008).

#### 2.2.1.1 Internal Audit- External Audit

According to Wright et al. (2008) the American Institute of Certified Public Accountants (AICPA) defines two classes of audit; internal and external. Internal audits involve assessing systems, process, internal controls, to provide the business with a reasonable level of assurance (Wright et al., 2008). While external audits are performed by an independent party, a third party vendor, with no rights or capability to change the system they are auditing. Senft and Gallegos (2009) define the internal audit function as control function within an organisation and state its primary objective is to assure to the management that implemented controls are adequate and applied effectively. Similarly, Hall and Singleton (2005) refer to internal audit definition from the Institute of Internal Audit (IIA) as “an independent appraisal function established within an organisation to examine and

evaluate its activities as a service to the organisation" (p. 3). If the internal audit group is adequately staffed, it could perform audit review of IT activities. In addition, with a continuously improving audit process, executive management would task the internal audit group with reviewing, testing responsibilities, which are often broader in scope than what an external auditor would be tasked with (Senft & Gallegos, 2009). Hall and Singleton (2005) state that "a truly independent internal audit staff adds value to the audit process" (p. 5). Internal audit plays an important role in assessing internal controls for the organisation as well as compliance and assurance activities (Merhout & Havelka, 2008).

Senft and Gallegos (2009) indicate that "external audit evaluates the reliability and the validity of system controls" (p. 67). In addition, the authors state that the prime objective of external audit is to minimise the amount of substantial auditing. The objectives of external audit, are mainly finance but would include other audits as deemed necessary to support the external audit objectives (Hall & Singleton, 2005). The authors, further add, that the external auditors are independent auditors, as they are not part of the organisation like internal auditors, who represent the interest of their organisation. However, internal auditors often cooperate with external auditors to enhance the audit efficiency and reduce the audit cost (Hall & Singleton, 2005).

Neither an internal or external auditor should be involved in the implementation or the design of a process or a mitigating measure (Wright et al., 2008). Wright et al. further argue that auditors could "assess the level to which a design or implementation meets its desired outcomes, but must not offer advice on how to design or implement a system" (p. 8). In addition, Wright et al. emphasise the necessity for auditors not to audit a system or process they designed or implemented, in order to ensure the audit independence.

#### 2.2.1.2 IT Audit

IT auditing, formally called electronic data processing (EDP), evolved as an extension of traditional auditing (Senft & Gallegos, 2009). At that time IT auditing was needed when auditors realised the need for specialists, as computers had impacted their ability to perform the attestation function (Senft & Gallegos, 2009; Pathak, 2005). The increasing impact of using computers in business, on professionals and in government, organisations recognised the need for IT control

and audit-ability (Hall & Singleton, 2005; Senft & Gallegos, 2009). IT auditing is an integral part of the audit function as it supports the quality of the information processed by information systems (Senft & Gallegos, 2009; Hall & Singleton, 2005). IT auditing as defined by (Senft & Gallegos, 2009): "is the evaluation of IT, practices, and operations to assure the integrity of an entity's information. Such evaluation can include assessment of the efficiency, effectiveness and economy of computer-based practices" (p. 54).

Similarly, Pathak (2005) defines IT auditing as "the process of collecting and evaluating evidence to determine if an information system safeguards assets, maintains data integrity, achieve organisational goals effectively, and consumes resources efficiently" (p. 5). Figure 2.13 illustrates how information systems - technology auditing has evolved with time. Currently virtulaisation, mobile and cloud computing have compounded the complexity level of information systems.

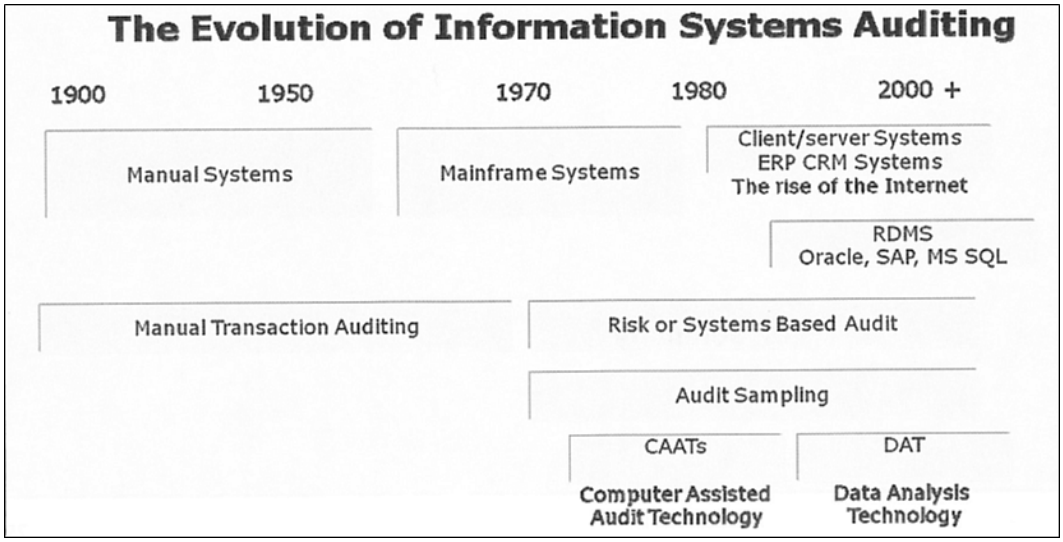


**Figure 2.13: The Evolution of IS Auditing (Wright et al., 2008, p. 26)**

Pathak (2005) adds another important element to IT auditing by stating that it is a study of inter-disciplinary methodologies mixes, from traditional auditing, computer science, behavioural science and information management. Henczel (2001) claims that the simplest definition for information audit developed by Guy St. Clair (1997) is as follows: "a process that examines how well the organisation's information needs and deliverables connect to the organistional mission, goals and objectives" (p. 12). Henczel (2001) further adds that regardless of what definition is favored, IT audit is a process that will evaluate the effectiveness of the current information environment. Skyme (1995), as cited in (Henczel, 2001) presents a

model for effective management for information resources, where information audit plays a key role in aiding the management of an organisation achieving its mission, goals and objectives as depicted in Figure 2.14. IT auditing complements the internal audit by providing reasonable assurance that assets are protected and information is timely and reliable. Also that any deviation from the organisation's defined policies and controls are detected and corrected in a timely fashion (Senft & Gallegos, 2009; Hall & Singleton, 2005).

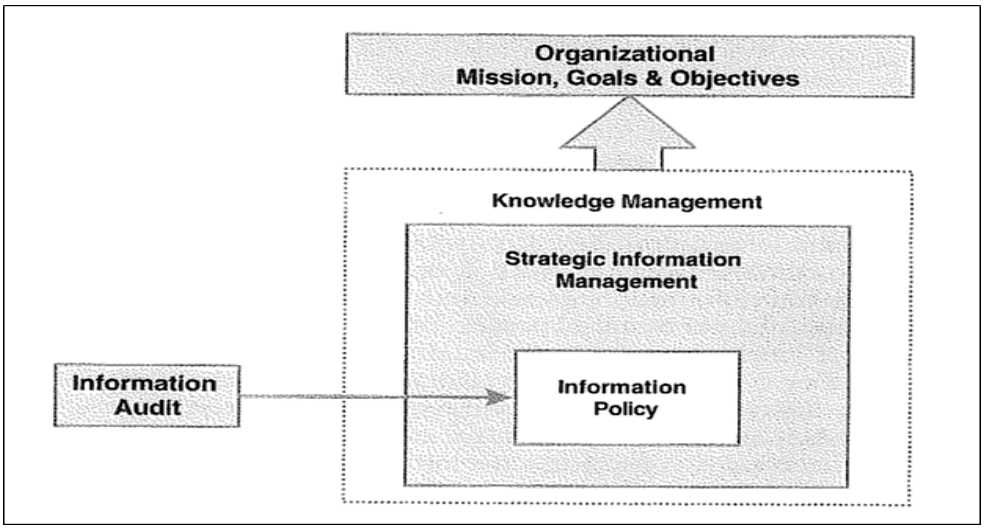


**Figure 2.14: From Information Audit to Knowledge Management (Skyrme, 1995, cited in Henczel, 2001, p. 12)**

It is imperative to mention that providing reasonable assurance should be a cost-effective process. The cost of achieving desired quality control should not exceed the gained benefits (Hall & Singleton, 2005). To be able to identify cost verses benefit, IT risk must be part of the equation. Hunton et al. (2004) state that "IT auditing is about controlling risks associated with information systems and technologies" (p. 13), a view shared by Hall and Singleton (2005) who indicate that IT audits are risk-based. According to Accounting_Web (2008), as cited in Lovaas and Streff (2009) an adequate risk assessment is the foundation of a high quality audit. While the IT risk assessment evaluates the use of technology to identify the risk and design compensating controls. IT audit evaluates the compliance and adequacy of those controls (Lovaas, Streff, & Podhradsky, 2009, as cited in Lovaas & Streff, 2009). Merhout and Havelka (2008) mention that an IT audit could be performed by external auditors, as part of the annual auditing of financial statements, to ensure the IT internal controls' effectiveness. The authors indicate

that internal auditors could perform the same audit for a similar purpose, but with the intent of satisfying management's responsibility surrounding governance.

Hunton et al. (2004) claim that in recent years, IT audit has shifted their approach from being control based into a risk based audit, and that the shift "represents a change in terms of the usefulness and influence of auditing" (p. 48). In that view, IT auditors evaluate an organisation's risks and accordingly select a set of controls that best mitigate the identified risk in a timely and cost-effective manner (Hunton et al., 2004; Hall & Singleton, 2005). Rissi and Sherman (2011) shed another light on effective auditing in modern, governance-based organisations and claim that auditing should be conducted with a business model in mind, otherwise it would be just punitive. Rissi and Sherman stress that "audit can and should be a function to validate controls of real life and important risk" (p. 153). The authors further indicate that an auditor could help educating organisation if they were engaged or are part of the strategy team. This view is aligned with what the Canadian Institute of Chartered Accountants (CICA, 1998) recommends, that internal audit senior management be a member of the IT and IT risk management steering committees, which emphasises the importance of the consulting role that an internal IT auditor should play. Wright et al. (2008) stress that "the goal of audit process is not to catch people out; it is to instill good governance principles and due diligence within information technology in an organisation" (p. 66).

### 2.2.2 Controls

According to Wright et al. (2008) controls are the mechanisms by which organisations reach their goals, however, controls are useless if they are not effective. As noted earlier, one of the audit objectives is to ensure controls effectiveness and efficiency. CICA (1998) refer to its Guidance on control:

> Control comprises those elements of an organisation (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organisation's objectives. Control is effective to the extent that it provides reasonable assurance that the organisation will achieve its objectives reliably (p. 11).

Hall and Singleton (2005) claim that "organisation management is required by law to establish and maintain an adequate system of internal control" (p. 14). Cash, Baily, and Whinson (1977) define internal controls as: "Internal controls are organizational arrangements and the actions instituted under such arrangements taken within an organisation to direct and regulate activities of that organisation." (p. 814). Cash et al. indicate that both management and auditors have recognised the potential benefits of effective internal control, a view shared by Pathak (2005). While it is the management's responsibility to implement required controls and ensure its performance, it is the auditor's responsibility to assure this (Wright et al. (2008). Committee of Sponsoring Organisations of the Treadway Commission (COSO) puts another but quite similar definition to internal controls:

> Internal control is broadly defined as a process, effected by an entity's Board of Directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operation, reliability of financial reporting, and compliance with laws and regulations. (Champlain, 2003, p. 213)

COSO's definition describes the control as a process that provides reasonable assurance, but not absolute, to optimise operation and comply with regulatory requirements.

#### 2.2.2.1 IT Controls

Brand and Boonen (2005) refer to the COIBT 4.1 control definition: "policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and dealt with" (p. 55). Similarly, Hall and Singleton (2005) indicate that internal control system comprises policies, practices and procedures employed. Wright et al. (2008) emphasise that policy is an important control, and without it, auditing is a shot in the dark and based on a personal opinion rather than the organisation's intent. The Canadian Institute of Chartered Accountants (CICA, 1998) state that controls should be designed to enable organisation's objectives, rather than being constraints, which could become business prohibitive. CICA (1998) further indicate that "while the technology is a key enabler, it is important to remember that control should be primarily business,

not technology, driven" (p. 22). COBIT also defines control objectives as "A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity" (Brand & Boonen, 2005, p. 55).

According to ISACA (2011) controls could be physical, technical or procedural. The technical controls could be categorised into three types:

- Internal accounting controls: for accounting operations
- Operational controls: for day-to-day operations
- Administrative controls: for operational efficiency and adherence to management policies

Pathak (2005) defines two main control categories: management controls and application controls. As for management controls the definition is similar to the administrative controls defined in (ISACA, 2011). As for the application controls they comprise the first two categories that the ISACA source has defined; the internal accounting and operational controls. CICA (1998) categorise enterprise technology controls in a model, as depicted in Figure 2.15, which seems more encompassing than what Pathak and ISACA have defined. The control classifications shown in Figure 2.15 demonstrates the importance of data related controls that interact with general computing controls, accounting and application controls. In turn those controls interact with each other along with the overarching corporate policy and administrative and management controls. Additionally, Hall and Singleton (2005) claim that IT internal controls are categorised in two broad categories: general controls and applications controls. Application controls focus is on a specific application, for example, payroll, customer service and the like systems. While, general controls cover a wider range of risks that could exist within IT environment (Hall & Singleton, 2005).


**Figure 2.15: Relationship of IT Controls (CICA, 1998, p. 28)**

#### 2.2.2.2 Test Controls and Substantive Testing

According to Hall and Singleton (2005) who state "test controls and substantive testing are auditing techniques used for reducing total audit risk" (p. 11). Champlain (2003) states that "often controls that were thought to be strong have been rendered inadequate by advances in technology" (p. 36). That requires control testing considering the changes in technology as well as regulatory requirements, which complicate the materiality measurement (Hall & Singleton, 2005). Hunton et al. (2004) indicate that audit scope determines the type and extent of controls testing to be performed. It is imperative to indicate that establishing materiality level is vital for controls testing and for risk assessment (Hunton et al., 2004). In IT auditing controls' materiality is determined for an information system or operation that process nonfinancial transactions by considering: the cost of the system, the criticality of the information processed and the potential of costs of errors, among other items (Hunton et al., 2004).

#### 2.2.2.3 Control Self-Assessment (CSA)

Control self-assessed is an important element in maintaining the effectiveness of internal controls, CSA defined as follows:

> Control Self-Assessment (CSA) is a leading edge process in which auditors facilitate group of staff members who have expertise in a specific process, with the objective of identifying opportunities for internal control enhancement pertaining to critical areas designated by management (Champlain, 2003, p. 211).

CSAs are importance to the continuous improvement of IT audit, however, Champlain (2003) indicates that "implementing CSA requires a major commitment from all parts of the organisation, including internal audit as well as all levels of management" (p. 213) .Furthermore, effective CSA, if designed adequately and executed diligently, would reduce immensely the cost of the assurance process, as it assists auditors in evaluating control effectiveness (Hunton et al., 2004).

### 2.2.3 Role of IT Auditor

Senft and Gallegos (2009) indicate that the IT auditor's role has evolved to provide assurance that implemented controls are adequate, however, the responsibility of

the implementation rests with the management. IT auditor's primary role, except when providing advisory services, is to "provide a statement of assurance as to whether adequate and reliable controls are in place and are operating in an efficient and effective manner" (p. 4). In general, auditors are allowed to provide other services as long as they do not compromise their independence (Vanstraelen & Willekens, 2008). An IT auditor could play a role of a counselor, a partner of senior management and as an investigator (Senft & Gallegos, 2009).

According to Wright et al. (2008) one of the greatest benefits of an audit is "an enchanted awareness of the issues facing the organisation" (p. 27). With regards to the organisation's policy, the auditor's role is to measure how well the organisation is aligned with its policies and report any deviations (Wright et al., 2008). Senft and Gallegos (2009) and Hall and Singleton (2005) stress that as new technologies introduce new risks that require new controls, the IT auditor have a visibility that enable them to holistically assess IT risks and their impacts on the business. Therefore, IT auditors could play a crucial advising role to the management for decision-making. In that view, the authors stress that IT auditors play a vital role in establishing an effective IT governance structure, controls and IS security, through various audit reviews (Senft & Gallegos, 2009; Hall & Singleton, 2005). Similarly, Hadden et al. (2003), Gramling and Hermanson (2006), D`Silva and Ridley (2007), as cited in Nuijten, Zwiers, and van der Pijl (2008), outline the contribution of internal auditors to ITG framework. Which comes in line with the view of (CICA, 1998) described in sub-section 2.2.1.2 to include the senior audit manager in the IT steering committee. Hunton et al. (2004) share the same view of the IT auditor's role in ensuring an effective ITG for an organisation. Accordingly, as the ITG importance and value increase, the IT auditor role's importance increases proportionally to manage IT risk and align IT objectives with the corresponding business objectives (Hunton et al., 2004).

As the internal control environment is too complex, and in order to perform good assessment, IT auditors are required to obtain sufficient knowledge of the internal controls to plan their audit (Hall & Singleton, 2005). Hunton et al. (2004) indicate that the role an IT auditor plays, is part of the financial audit, and the IT auditor may work hand-in-hand with the financial auditor through each engagement, utilising computer assisted audit tools (CAATs).

IT auditors face a number of challenges, as noted by Merhout and Havelka (2008) who also indicate that auditors should have a holistic view on how various processes and controls interact to assess them adequately. In addition, IT auditors should be capable of providing advice on competitive best practices and methodologies (Merhout & Havelka, 2008). Senft and Gallegos (2009) point out that IT auditors are faced with constant challenges to keep up with changes in business technical environment and regulatory requirements. Merhout and Havelka (2008) suggest that some audit practitioners' tasks have changed radically. Champlain (2003) argues that the 'old school' of auditing where auditors function as 'police' is an inappropriate approach, and suggest that the IT auditor's role is to be consulting, and counseling instead.

#### 2.2.3.1 IT Auditor's Skills

Wright et al. (2008) stress that an auditor must understand what is required to perform gap analysis in order to be able to identify any issues with control implementation. In addition, auditors are required to understand how to identify and quantify the effectiveness and cost of the various risk analysis techniques (Merhout, Flittner, & Havelka, 2008). Senft and Gallegos (2009) suggest that auditing of complex technologies comprises of various IT systems and communication protocols, for example different types of applications, networks and its infrastructures.

As security compliance has become a major factor in IT systems assurance, it is important for the IT auditor to understand security controls and measurement techniques to ensure the auditing of controls and processes is adequate (Wright et al., 2008). Senft and Gallegos (2009) stress that "Yes, IT controls are very important" (p. 16), and further add that IT control and security is everyone's business. The authors emphasise that for IT auditors the need to audit controls and security will be critical and will be a challenge as technologies evolve and advance.

Senft and Gallegos (2009) indicate that learning and adapting new ways of auditing is always a priority for IT auditors, internal or external. The authors further emphsise that "most auditors want tools or audit methodologies that will aid them in accomplishing their task faster and easier" (p. 56). Furthermore, as IT auditors evaluate complex systems they must have highly developed technical skills to understand the evolving methods of information processing (Senft & Gallegos,

2009). Merhout and Havelka (2008) point out that IT auditors should be trained and have the skills that allow them analyse and critique existing processes. So that, IT auditors could identify any redundant processes or gaps in controls, considering, the business strategic objectives.

Hunton et al. (2004) state that IT auditors are likely to hold a bachelor's degree and have a wide range of knowledge and expertise in various IT systems. In addition, Hunton et al. (2004); and, Merhout et al. (2008) emphasise the need for IT auditors to have a business education to evaluate business requirements in order to be able to perform quality auditing. IT auditors are required to obtain professional audit certifications from organisations like ISACA, and IIA (Hunton et al., 2004; Senft & Gallegos, 2009).

### 2.2.4 IT Audit Process

It has been indicated that the IT audit function objective is to assure the organisation assets are protected. Also that information must be timely and reliable and any deviations from the organisation's defined policies and controls are detected and corrected in a timely fashion. To ensure the effectiveness of the audit function and the continuous improvement, an audit process is required to be defined and adhere to. According to Hall and Singleton (2005) the high level of complexity into an IT audit postulates a logical framework to enable an IT auditor undertake a quality IT audits that identify all important processes and data. Senft and Gallegos (2009) point out that today's IT auditors face many concerns about the exposure of information systems to various risks and compliance requirements. In addition, the authors indicate that those concerns have driven objectives for the audit process. Hunton et al. (2004) state that "all IT audits go through a cyclical process that we call the 'IT audit life cycle'" (p. 208).

An efficient internal audit process provides assurance of the organisation's ITG structures as well as secure information systems (Mishra, 2007). The audit process depicted in Figure 2.16, by Henczel (2001). It comprises the following stages: Planning the audit, Data Collection, Data Analysis, and Data Evaluation followed by Communication Recommendations and Implementation Recommendations. The last element in the audit process is the Information Audit as a Continuum, which ensures that the IT audit is a process and not a one-off task

(Henczel, 2001). The last stage is crucial for ensuring the audit and risk management process is continuous and dynamic, and responds to changing threats and vulnerabilities in a timely fashion (ISACA, 2011). Hunton et al. (2004) describe IT audit process stages as follows: Planning, Risk Assessment, Prepare Audit Program, Gather Evidence, Form Conclusions, Deliver Audit Opinion and Follow up. While there may be different steps, but the objectives are similar to what is illustrated in Figure 2.16.

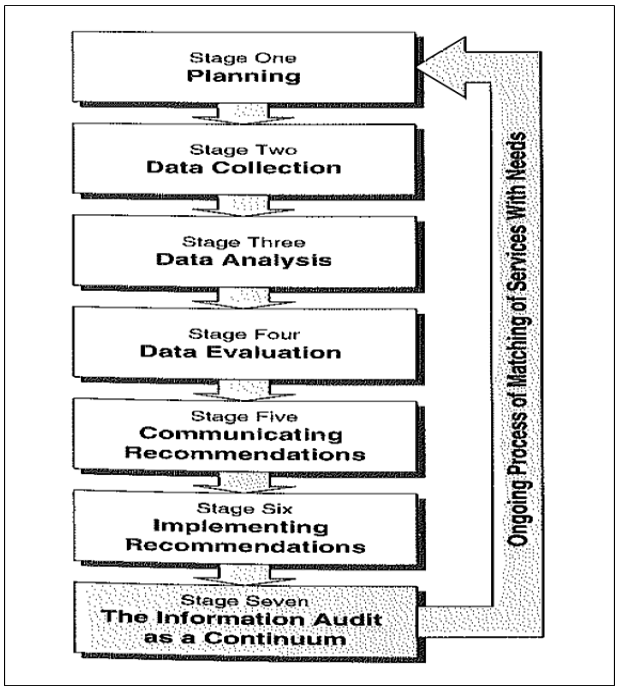


**Figure 2.16: The Seven-Stage Information Audit Model (Henczel, 2001, p. 17)**

#### 2.2.4.1 Planning

Wright et al. (2008) argue that planning is the most critical phase of any audits, as time and resources could be wasted for no gain. Senft and Gallegos (2009) stress that one of the most important tasks of an audit function is to establish an audit universe, which is an inventory of all the potential audit areas within an organisation. Building the audit universe is a collaborative effort by various stakeholders within the organisation and should be risk based (Senft & Gallegos, 2009).Performing risk assessment is the foundation of the audit function as it provides a framework for allocating audit resources to achieve maximum benefits. During the planning stage, the audit scope is defined, which is according to Wright et al. (2008) the most critical aspects of any audit. Furthermore, it is imperative to ensure the audit scope is defined before any engagement. Hunton et al. (2004) point

out that “risk assessment measurement is important because it allows IT auditors to narrow the audit scope and maximise efficiency and effectiveness” (p. 53). Senft and Gallegos (2009) highlight the fact IT auditors are faced with constant challenges to keep up with changes in business technical environment and regulatory requirements. Those changes necessitate updating the audit universe and re-assessing the risks.

#### 2.2.4.2 Data Collection

Senft and Gallegos (2009) point out that when an auditing review commences and a plan is devised and authorized; auditors start collecting data and evidence with various means depending on the environment, tasks and subject systems. Hunton et al. (2004) state that, “gathering evidential matter is the heart of the audit, as it provides the basis for the audit opinion that is eventually rendered”. Examples of data collection methods are; documents in hard copies or published on the organisation intranet, the risk register, charts, and interviews and surveys (Hunton et al., 2004; Hall & Singleton, 2005; Henczel, 2001). In addition, Hall and Singleton (2005) claim that gathering evidence could be done through testing internal controls to establish the controls are functioning as designed. Wright et al. (2008) point out the importance of defining in advance audit procedures, including testing techniques. The auditor must be prepared to alter the data gathering technique and adapt as circumstances change. It is imperative to collect a quantity of data that can be handled by the auditing capability (Henczel, 2001).

Kouns and Minoli (2007) argue that it is vital to get internal and external stakeholders’ inputs in building the organisation’s risk profile. According to Shortreed (2008) one important outcome of consulting the stakeholders is to record their perceptions of risk and value. Furthermore Doughty and O`Driscoll (2002) indicate that consulting stakeholders helps increase the participants understanding of their processes and the potential risk exposure.

#### 2.2.4.3 Data Analysis and Data Evaluation

Hunton et al. (2004) indicate that once audit evidence is gathered, in various forms as stated in section 2.2.4.2, it is the auditor’s job to analyse and evaluate the collected data. The outcomes of the Data Analysis stage are compared to the risk criteria (Ames, 2007b), and materiality level that have been set previously, to reach

an audit opinion (Hunton et al., 2004). Auditors would utilise their judgment to determine controls materiality, which is in the IT environment, a difficult decision to make because of the technology complexity and sophisticated internal control structure (Hall & Singleton, 2005). Data analysis and evaluation could be outsourced to a specialized party if required (Henczel, 2001). Pathak (2005) highlights that there is no single method of evaluating controls, and indicates that auditors should test controls for effectiveness and reliability. Furthermore, the author indicates the necessity for an auditor to check the control effectiveness in relation to the other implemented controls.

#### 2.2.4.4 Communicating Recommendations

ISACA (2007) state that when risk treatment plans are devised, it is vital to communicate the outcomes to all concerned parties. Hunton et al. (2004) indicate that the auditor's conclusions should not be a surprise to the management; substantial findings should be communicated to the management and rectifications are recommended. Should any of the findings remain unresolved, auditors may form an opinion including the contested findings (Hunton et al., 2004). In addition, Wright et al. (2008) highlight the good practice in reporting audit findings, where reports should be objectives, clear, concise, constructive and timely. A view shared by Henczel (2001) who also indicates that oral presentation could be utlised in communicating the audit findings.

#### 2.2.4.5 Implementing Recommendations

Write et al. (2008) state that management should review and approve the final audit report. An implementation plan should be devised with agreed upon and viable execution dates. It is vital to obtain the full sponsoring party support to ensure that agreed upon ratifications are implemented (Henczel, 2001). There are several different types of risk mitigating-controls, including: Preventive, Detective, and Corrective. Each will be devised based on the risk assessment outcomes. Factors like asset type, its vitality to the business, feasibility and cost would determine the type of controls to select and implement. When a risk control is devised a further analysis is instigated to assess the residual risk (ISACA, 2007). The aim, however, is not to bring the residual risk to zero level, as this could be too costly and/or business prohibitive (Whitman & Mattord, 2004).

#### 2.2.4.6 The Information Audit as a Continuum

Henczel (2001) argues that in order to ensure the information systems objectives are aligned with business objectives the information audit process should be performed regularly. As the business context, both internal and external, is subject to change, accordingly the risk profile also changes and some controls may become ineffective (Merhout & Havelka, 2008). New assets could be introduced, and their business value and impact need to be re-evaluated and included in the risk assessment (Whitman & Mattord, 2004). In addition, vulnerabilities and associated threats evolve and quite possibly new types are introduced by the new and existing assets when the business process changes (Merhout & Havelka, 2008). For these reasons, it is crucial to monitor the internal controls, through regular reviews, to ensure their effectiveness and efficiency (Merhout & Havelka, 2008).Hardy (2011) explores continuous auditing for reviewing financial applications and argues that the principles apply to IT auditing in general. The author states that "continuous auditing is performed by auditors for auditors and continuous monitoring maybe performed by anybody" (p. 8). The CSAs, discussed in sub-section 2.2.2.3 if well designed and implemented, could contribute immensely to the effectiveness and efficiency of the controls monitoring process (Champlian, 2003; Leitch, 2008). In addition, according to Hunton et al. (2004) this type of control environment, where management self-assess their internal controls, aids auditors and improves efficiency of the audit process. ISACA (2007) indicate that the Monitor and Review process ensures that management action plans remain relevant and updated timely. Shortreed, (2008) indicates that continuous improvement is an essential attribute of risk management processes and is a view that applies to the IT audit process. To achieve continuous improvement periodic and ad-hoc reviews are required to be conducted by respective personnel as per the policy devised at the enterprise level (ISACA, 2007). The ongoing revision is required to avoid common risk management pitfalls such as overlooking or overspending. Periodic assessment of internal controls is paramount to ensure operational efficiency, which in turn leads to less vulnerabilities and improved IS security management (Mishra, 2007).

### 2.2.5 IT Audit Risk

Whitman and Mattord (2004) state that IT risk should be managed while taking into account the whole business context. According to Westerman and Hunter (2007) IT risk is defined from business perspectives rather than assurance or compliance perspectives. The focus of this research is on risk based IT audit to obtain business value. However, there is a risk in the audit process itself that is required to be assessed, evaluated and managed (Wright et al., 2008). Eilifsen and Willekens (2008) refer to audit quality deficiencies that may result in 'audit failure' and state that "an audit failure occurs when the auditor fails to issue a modified report when appropriate". In another word, an audit failure may take place when an auditor fails to detect all material misstatement, over looked a risk or performs an inadequate risk analysis, or advises ineffective mitigating measures. Similarly, Hunton et al. (2004) indicate that audit risk is the likelihood that an IT auditor fails to uncover a material error or fraud. The authors add that audit risks is a combination of risks, it includes inherent risks, control risks and detection risks, as shown in Figure 2.17.

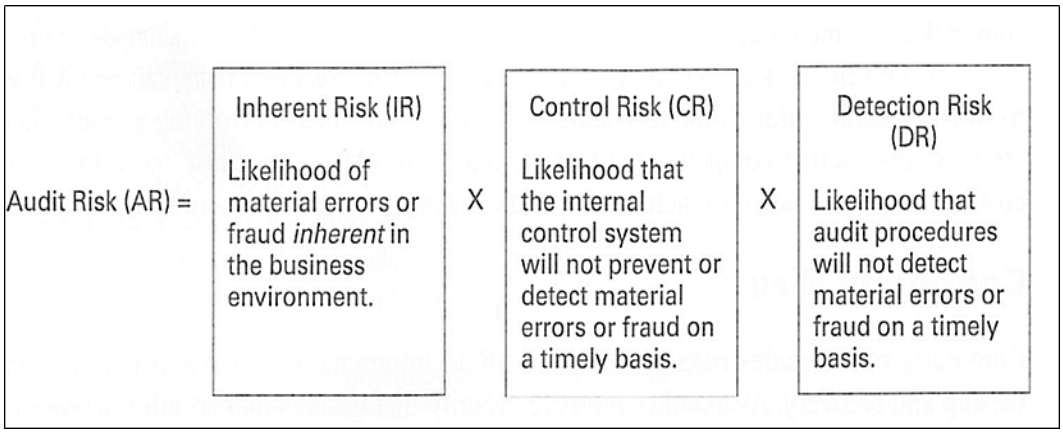


**Figure 2.17: The Audit Risk Model (Hunton et al., 2004, p. 49)**

Hall and Singleton (2005) state that auditors could reduce the level of control risk by testing internal controls. Merhout and Havelka (2008) stress that business changes for example processes, and roles of new and old personnel, would lead to a higher audit risk. While IT risk always exists to various degrees, organisations are better off managing the IT risk of high impact, as opposed to low impact IT risk. In addition, because no organisation can build all the hardware and software it needs, a great deal of attention is required to understand the dependency of all these systems, where most of IT risk issues reside (ISACA, 2009b).

While concluding this sub-section, it is imperative to indicate, what has been emphasised: that establishing an assurance program based on recognised frameworks and standards, enables an organisation audit their IT systems and processes systematically, and avoid the auditing deficiencies which would ensure quality audits (Merhout & Havelka, 2008).

### 2.2.6 Section Summary

In section 2.2 the following key points have contributed to achieving the chapter's objectives:

- Aspects of auditing and assurance were defined and examined
- IT controls objectives and categories, were defined;
- Role of the IT auditor in providing sought after assurance;
- IT audit process aspects were examined;
- Risk of IT audit and challenges were laid out.

## 2.3 REVIEW OF CONTROL FRAMEWORKS, STANDARDS AND BEST PRACTICE

This section encompasses summaries of the most recognised and utilised control frameworks for auditing, risk management standards and best practices in sub-sections 2.3.1 and 2.3.2 respectively. While sub-section 2.3.3 examines IT controls frameworks and best practices. Sub-section 2.3.4 explores project management methodologies, and sub-section 2.3.5 reviews some of the common compliance standards. Sub-section 2.3.6 summarises the key points of the section.

### 2.3.1 Review of Audit Standards and Guidelines

Throughout the years, several organisations have developed many auditing guidelines and standards. Some are for general auditing, with a supplement that covers IT or technical systems. A few of those were devised specifically for IT auditing, although their main objective remains to assure the business of the effectiveness and reliability of their IT systems.

This section is structured as follows: sub-section 2.3.1.1 to explore the Auditing Standard from PCAOB, while sub-section 2.3.1.2 reviews Statement Auditing Standards (SAS). Sub-section 2.3.1.3 is to review standards from the

Institute of Internal Auditors (IIA) Auditing Standards, while sub-section 2.3.1.4 explores Auditing Guideline from ISACA.

#### 2.3.1.1 Auditing Standard (AS)

According to Moeller (2008, p. 53) the PCAOB released auditing standard was called Auditing Standard No. 2 (AS2), a rule-based set of external auditing standards in 2007. AS2 rules mandate external auditors to take a conservative approach that they consider a very time and resource consuming subject that has no proportional value in return. Subsequently, PCAOB released AS5, a risk-based internal control auditing standards, with the objective to perform a quality audit tailored to the organisation's environment, in comparison to its predecessor AS2 (Moeller, 2008). In late 2010, the PCAOB released a set of seven new risk-based auditing standards, AS No. 8-14 (Moeller, 2011). The set of auditing standards provide direction on audit procedures from planning, evaluating and forming of audit opinion in the auditor's report (Moeller, 2011). While these auditing standards are not related to the enterprise risk management, however, they emphasise the necessity of performing risk based audit. In addition, ASs are for external auditors to produce financial statements but the same principles could be applied for IT auditi, which would be part of the overall external audit for that purpose.

#### 2.3.1.2 Statements on Auditing Standards (SAS)

Statements on Auditing Standards (SASs) are considered authoritative interpretation of Generally Accepted Auditing Standards (GAAS) (Hall & Singleton, 2005). In 1972 the first statement SAS 1, was released. Then AICPA released a number of SASs for example SAS 55, 78, 94 and 98 (Champlain, 2003, p. 227). Table 2.2 lists these SASs with a brief summary for each of them.

**Table 2.2: A Summary of Audit Statements on Internal Control and IS (Hunton et al., 2004, p. 57)**

| Statements on Auditing Standards | Summary |
|---|---|
| SAS No. 55, Consideration of Internal Control in a Financial Statement Audit. Issued in 1988. | Was the first auditing standard to address the need for auditors to understand internal control. Defined internal control and three components auditors must address. |
| SAS No. 78, Consideration of Internal | Revised SAS No. 55 to conform to COSO internal control definition and components. |

| Statements on Auditing Standards | Summary |
|---|---|
| Control in a Financial Statement Audit: An Amendment to SAS No. 55. Issued in 1996. | Required auditors to obtain a sufficient understanding of internal control. |
| SAS No. 94, The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit. Issued in 2001. | Recognised the pervasive use of IT and its effect on risk and control.<br>Required auditors to consider effect of IT on audit strategy.<br>Recognised the significant IT use may mean that audit evidence depends on controls over accuracy and completeness.<br>Explained that auditors should understand an organiation's manual and automated procedure used to prepare financial statements. |
| SAS No. 95, Omnibus Statement on Auditing Standards. Issued in 2002. | Issued in response to report of the Public Oversight Board Panel on Audit Effectiveness.<br>Required greater understanding of enterprise and its environment, including internal control.<br>Requires more rigorous risk assessment related to financial statement material misstatements<br>Improves relationship between risk assessment and audit procedures. |

According to Champlain (2003); Senft and Gallegos (2009) the SASs relate to the independent auditor's consideration of internal control in financial audit. SAS 55 used non-COSO internal control definition, as it was released before COSO, while SAS 78 included COSO's definition (Hunton et al., 2004). SAS 94 added the effect of IT on internal control, which was a significant amendment to SASs, claims (Champlain, 2003). In addition, Hunton et al. (2004) outlined SAS no. 70, which is primarily used by third party service providers (IT, Internet, Helpdesk), banks, data processing centers; to present to 'user organisation' as attestation of the existing and effectiveness of the internal controls in the organisation. In 2011, SAS no. 70 has been superseded by Statement on Standards for Attestation Engagements (SSAE) No. 16.

#### 2.3.1.3 Internal Audit Standard

Moeller (2011) indicates that the Institute of IIA maintains, and updates regularly, a set of standards: International Standards for the Professional of Internal Auditing, that all internal auditors are mandated to apply. The author further adds that the sets cover a wide range of audit activities, the standards refer on a number of occasions

for internal auditor's responsibilities to consider risk while planning and when performing the audits. In 1991, the IIA issued Systems Auditability and Control (SAC) as assistance to internal auditors on devising IT internal controls and IT audit (Senft & Gallegos, 2009).

#### 2.3.1.4 ISACA Audit Guidelines

According to Senft and Gallegos (2009) the first Control Objectives was issued in 1975 by EDP, the predecessor of ISACA. Subsequently, updated revisions were released and the organisation transitioned into ISACA. ISACA board of standards issues IT audit standards, guidelines and procedures (Hunton et al., 2004). Auditors accredited with Certified information systems auditors (CISA) certification are required to comply with ISACA's code of ethics and professional conduct described in those standards (Hunton et al., 2004).

### 2.3.2 Review of Risk Management Frameworks

Risk management frameworks based on the International Organisation for Standardisation (ISO) ISO-31000 and ISO-27001/2/5 standards or organisations like ISACA and NIST help practitioners build a systematic risk management process. Shortreed (2008) defines risk management framework as: "a set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organisation" (p 5). This section is structured as follows: sub-section 2.3.2.1 describes related standards and guidelines from ISO, while sub-section 2.3.2.2 explores Risk IT framework from ISACA. Sub-section 2.3.2.3 outlines some methods devised by other organisations like the COSO internal control framework. Sub-section 2.3.2.4 reviews COSO-ERM framework, while Sub-section 2.3.2.5 examines Basel II.

#### 2.3.2.1 International Organisation for Standardisation (ISO)

ISO has published a wide range of standards and guidelines to regulate and advise on good practice and to help organisations achieve outcomes of desirable quality. The focus of this sub-section is on a selection of the ISO published standards and guidelines for managing risk. The Implementation of risk management framework is based on ISO-31000 and ISO-27001/2 standards.

#### 2.3.2.1.1 AS/NZS ISO 31000:2009

AS/NZS ISO 31000:2009 - Risk management – Principles and guidelines, that have superseded AS/NZS 4360:2004, risk management standard (Moeller, 2011). According to Shortreed (2008) the guidelines consist of 11 principles and 5 attributes of excellence, and there objectives are driven within the context of the risk criteria. Cusack (2010) states "This standard is the parent of all risk based standards" (p. 43). Cusack (2010) further indicates that the guidelines define risk and the establishment of risk management process that has all the attributes that would ensure effective, efficient and current risk management framework. Although the guidelines are not specifically for IT risk management, the principles could be applied for IT systems and aligned that with business objectives, context, and risk in other business areas (Kouns & Minoli, 2007). According to Cusack (2010) the guidelines provide an Annex that details the attributes of enhanced risk management along with the relation to risk and governance structure.

#### 2.3.2.1.2 ISO 31010:2009

IEC/FDIS 31010 - Risk management- Risk assessment techniques. The standard details the different techniques to assess risk as part of the risk management process as described in ISO 31000 guidelines. The standard helps practitioners understand risks that could affect the achievement of business objectives. In addition, adequacy and effectiveness of devised mitigating controls could be assessed. Similarly to ISO 31000, ISO 31010 risk assessment techniques are not mandated and they are for risk management in general, however, they can be applied when managing IT risk.

#### 2.3.2.1.3 ISO 27001:2005

ISO 27001 is a risk based standard for an Information Security Management System (ISMS), formally known as BS7799-2 (Kouns & Minoli, 2007; Cusack, 2010). The standard consists of a set of mandatory sections that every organisation seeking accreditation to ISO-27001 standard, must comply with. In addition, there are optional sections that could be tailored to the organisation's context to ensure optimum security management is achieved. Risk management elements are included in the mandatory sections to ensure risk is identified, analysed and treated and continuously monitored (BSI, 2009). ISO 27001 incorporates Deming's Plan-

Do-Check-Act cycle (Kouns & Minoli, 2007) to ensure continuous improvement of the effectiveness of the risk based devised controls.

#### 2.3.2.1.4 ISO 27002:2005

ISO 27002 is a risk based standard (Security Techniques- The code of practice for information security management) formally ISO 17799 (Kouns & Minoli, 2007; Cusack, 2010). ISO 27002 provides a detailed description for security controls and implementation advice. The set of identified security controls (133 under 39 security objectives) are to address security information risk exposure. Applicable controls can be implemented at the Capability Maturity Model Integration (CMMI) level according to the feasibility and cost-effective analysis. Ames (2007a) indicates that devised controls in ISO 27002 should be tailored to the organisation's specific context and structure, in particular around identifying accountabilities.

### 2.3.2.2 Risk IT

RiskIT is an IT risk framework released by ISACA in 2009, which addresses IT risk management in a holistic manner. RiskIT framework leverages the activities, controls and processes relate to IT risks that are defined in other frameworks from ISACA-ITGI: COBIT and Val IT. The common controls and processes will be examined in the IT Control frameworks respective sections. RiskIT framework provides the how-to for managing IT risk as a business risk. The framework consists of three domains: Risk Governance, Risk Evaluation and Risk Response; each domain contains three processes (ISACA, 2009b).

### 2.3.2.3 COSO Internal Control Framework

According to Moeller (2011) an internal framework from Committee of Sponsoring Organisations (COSO) was first released in 1992 for building and measuring internal controls. Moeller added that the COSO framework for internal controls received worldwide recognition. The framework that Tarantino (2006) calls COSO I, uses a three-dimensional model to structure an internal control system for an enterprise. The COSO model can be described as a pyramid with five layers comprising the internal control system and how its components interact (Moeller, 2008; Moeller, 2011). Figure 2.18 illustrates the COSO framework from different perspectives, namely: the effectiveness and efficiency of operations, reliability of

financial reporting and compliance with law and regulations. The framework consists of five interrelated components: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring (Senft & Gallegos, 2009; Hunton, et al., 2004; Champlain, 2003; Mishra & Dhillon, 2008). Moeller (2008) stresses that, in order to arrive at factual control evaluation, auditors should assess internal controls on multilevel and multidimensional models that are shown in Figure 2.18. The COSO framework highlights the importance of a risk-based approach when assessing and building internal controls (Moeller, 2008; Mishra & Dhillon, 2008).

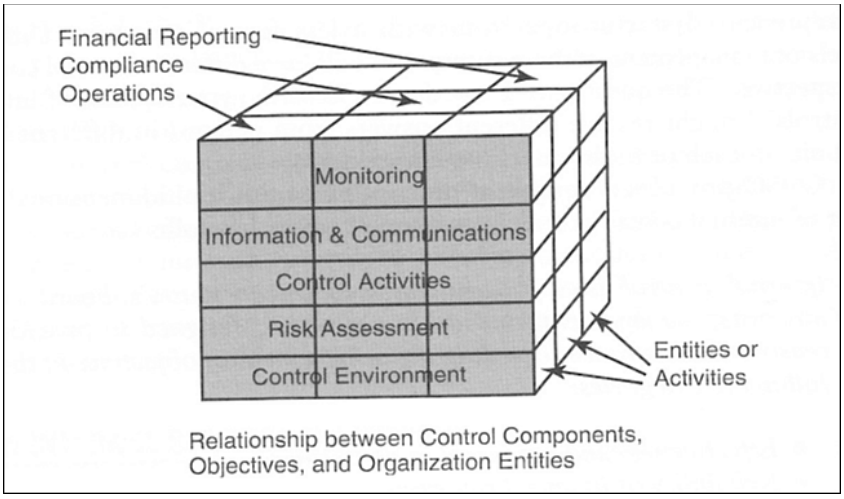


**Figure 2.18: COSO Internal Control Model (Moeller, 2008, p. 54)**

#### 2.3.2.4 COSO – Enterprise Risk Management (ERM)

According to (Moeller, 2008) there was an issue with the COSO internal control framework for having an inconsistent way in defining risks. COSO released COSO-ERM an enterprise risk management integrated framework, in 2004 (Tarantino, 2006; Moeller, 2011). COSO-ERM, which Tarantino (2006) calls COSO II, is considered an enhanced framework in building risk based internal controls for Sarbanes-Oxley (SOX) requirements. Also the principles adapted in the audit process help in auditing the enterprise risk management processes (Moeller, 2008). Figure 2.19 illustrates COSO-ERM frameworks with three-dimensional cube for strategic objectives of enterprise risk, risk components and entity units. Moeller (2008) claims that COSO-ERM should not be considered as just an improved version of COSO but as a much better solution for risk management. According to Tarantino (2006) COSO-ERM consists of eight components: Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control

Activities, Information and Communication, and Monitoring. Moeller (2011) indicates that COSO-ERM define 'control activities' like policies and procedures to ensure the identified risks are mitigated by those control activities. The author further stresses that these controls often overlap across multiple functions and units.

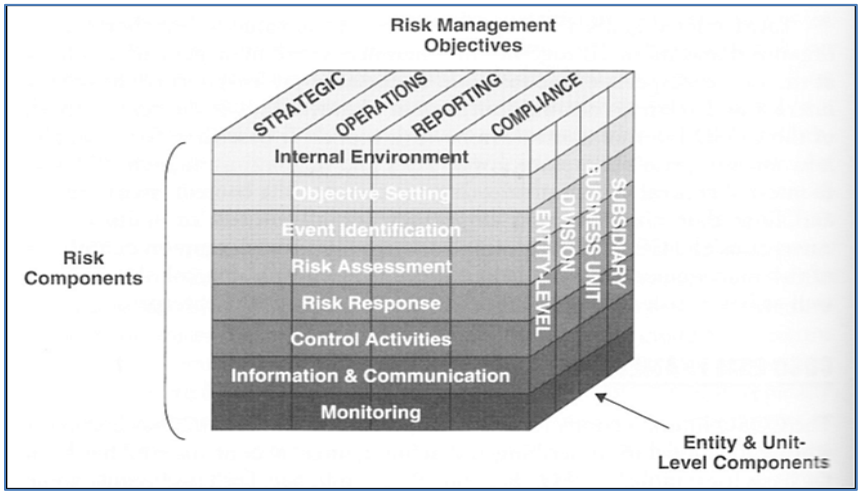


**Figure 2.19: COSO – ERM Framework (Moeller, 2011, p. 55)**

#### 2.3.2.5 Basel ll

In 2004, the Central Bank governors of Group Ten (G10) countries released a new framework for capital adequacy called The International Convergence of Capital Measurement and Capital Standards: A Revised Framework. The framework is known as Basel II, after the city name where the meeting took place in Basel, Switzerland (Tarantino, 2006). Basel II is a set of guidelines meant to protect banks' interests by managing market, credit and operational risks (Monahan, 2008). Tarantino (2006) claims that Basel II's 'Pillar 2' has many parallels to internal controls provisions of SOX section 404, and that both are built based on COSO internal control framework. The ultimate objective is to ensure the capital level at an individual bank is determined according to the bank's risk profile and the robustness of its enterprise risk management process and internal controls.

### 2.3.3 Review of IT Control Frameworks and Best Practices

Risk management frameworks based on ISO-31000 and ISO-27001/2/5 standards help organisations build a systematic risk management process. However, any organisation is required to respond to changes of the impacting factors in a timely fashion. That would deem necessary to re-work the risk assessment cycle, which is proved to be cost prohibitive in many occasions. It is a common scenario where a

risk profile is not current that could lead to an organisation has a false sense of assurance about their IT systems readiness. With an invalid risk profile, the probability for the management to make ill-fated decisions would be very high. To ensure their risk profile is up-to-date and they have the capacity to make informed decisions, many organisations have implemented forms of IT controls frameworks and best practices. For example Control Objectives for Information and related Technology (COBIT), Val IT, Microsoft Operations Framework (MOF) (Voon & Salido, 2009). In addition, known best practices like IT Infrastructure Library (ITIL) have been adapted to complement the COBIT-Val IT control based structure. In IT controls frameworks and best practices (COBIT, Val IT, ITIL) there are elements of risk management that either manage or contribute to managing risk in their respective areas.

This section is structured as follows: sub-sections 2.3.3.1, 2.3.3.2 and 2.3.3.3 examine ValIT, COBIT and ITIL, respectively.

#### 2.3.3.1 ValIT

Val IT is relatively a new IT governance framework developed by IT Governance Institute (ITGI) in 2005. The framework focuses on value delivery and ensures that IT-enabled investments are managed through their full economic life cycle (ISACA, 2009c). According to Haes and Van Grembergen (2005) the Val IT framework "starts from the premise that value creation out of IT investment is a business responsibility in the first place" (p. 183). IT investment is about enabling business change and if managed properly, can bring enormous returns. Thorp (2009, as cited in ISACA, 2009c) indicates, however, without effective governance and good management there is an equally significant risk to destroy values. Val IT defines and manages risk as part of risk and return management of a portfolio of IT investment (Barnier, 2009). Val IT is structured in 3 domains: Value Governance, Portfolio Management, and Investment Management. In addition, Haes and Van Grembergen (2005) describe Val IT as a complementary to COBIT 4.1 and it follows the same structure and templates.

#### 2.3.3.2 Control Objectives for Information and Related Technology (COBIT)

COBIT 4.1 is a framework for IT Governance developed by ITGI (Moeller, 2008). COBIT, was initially developed as an IT audit framework, and has evolved to become an IT Governance framework at version 4.1. A new version 5.0 has been released in 2012 that combines COBIT, ValIT, and RiskIT. COBIT 4.1 comprises of 34 processes structured in 4 domains: Plan and Organisation, Acquisition and Implementation, Delivery and Support, and Monitoring (Tarantino, 2006). Some of COBIT activities provide the "means" to facilitate risk management process (ISACA, 2009c), for example security controls that ensure the confidentiality, integrity and availability (CIA) of information. Similarly, identifying roles and responsibilities and ensuring appropriate segregations of roles and duties is another example (Moeller, 2008). Maintaining asset management and their business impact analysis (BIA) and feeding that into Business Continuity Plan (BRP) or Disaster Recovery Plan (DRP) and help in prioritising risks are other activities that COBIT provides. COBIT manages risk at the strategic, project, and, to some extent, operational levels.

Processes within the Monitor and Evaluate (ME) domain play a big role in ensuring risk management effectiveness and relevancy as noted by Brand and Boonen (2005). COBIT helps in conducting audit review at a lower cost and potential better value returns. COBIT helps in collaborating with other frameworks and/or best practices like Val IT, ITIL and ISO 27001/2 to achieve risk management process objectives, as part of the whole IT governance objectives (Kouns & Minoli, 2007; Champlain, 2003).

#### 2.3.3.3 IT Infrastructure Library (ITIL)

ITIL offers a systematic approach to the delivery of quality IT services (Jong, Kolthof, Pieper, Tjassing, Veen, & Verheijien, 2009; Moeller, 2008). ITIL helps in identifying risk implied in the service portfolio that consists of the list of services and underlying processes, capacities and capabilities required at various degrees. From the perspective of ITIL service portfolio, risk is categorised into: contract risk, design risk, operational risk and market risk (Jong et al., 2009). ITIL guidelines for setting incident management and problem management help in

recording incidents reports that can help in identifying threats and analysing their impact and frequency of occurrences (Kouns & Minoli, 2007). In addition, change and release management help in identifying vulnerabilities and corresponding threats and thence rectifying them at the design and implementation levels. ITIL manages outsourcing via different types of SLAs ensuring business requirements are met (Doughty, 2003). ITIL defines risk as "…an uncertain outcome, or in other words, a positive opportunity or a negative threat" (Jong et al., 2009, p. 21). Overall ITIL recognises risks of contract, design and operation.

### 2.3.4 Project Management

Project Management Institute (PMI), a project management professional organisation, released a wide range of project management guidance documentation (Moeller, 2011; Senft & Gallegos, 2009). PMI produced a standard-like document called *A Guide to the Project Management Book of Knowledge* (PMBOK Guide). Moeller (2011) describes the guide as a comprehensive guide that covers all aspects of project management. The PMBOK Guide-book identifies five basic process groups and nine knowledge areas for project management that almost all projects comprise (Moeller, 2011). PMI sponsors Project Management Professional (PMP) designation, for project managers who pass a test and demonstrate relevant work experience (Champlain, 2003).

### 2.3.5 Review of Compliance

There are increasing cases of financial fraud (Singleton, 2007), identity theft, and data leaks that result from intentional, or negligent actions that target IT systems and the hosted data. Furthermore, the vital role IT systems play in enabling businesses to be sustainable and resilient. In addition, the increasing complexity of IT systems have pressured governments and industrial agencies to enact and regulate through acts and standards for organisations to comply with.

This section is structured as follows: sub-section 2.3.5.1 explores Payment Card Industry (PCI), while sub-section 2.3.5.2 examines Sarbanes-Oxley (SOX), and sub-section 2.3.5.3 discusses Health Insurance Portability and Accountability Act (HIPAA).

#### 2.3.5.1 Payment Card Industry (PCI)

Payment Card Industry Data Security Standard (PCI DSS, or simply PCI), is the standard that companies are required to comply with, should they process, store or transmit payment cardholder data using credit cards. PCI is the authorised program of goals and associated security controls and processes to protect payment card data from exploitation (Thakar & Ramos, 2009). While PCI-DSS is the core standard, other sub-standards such as Payment Application Data Security Standard (PA DSS) and Personal Identification Number (PIN) Entry Device Security Requirement (PED) exist for other parties who develop applications or manufacture devices used at the point of sale. The PCI set of standards continue to evolve to accommodate the changing and evolving technologies and their associated risks. For example PCI DSS wireless guideline is an information supplement from PCI security standards council. PCI standards cover IT systems hardware and software that process, store or transmit payment card data (Woda, 2007). However, the PCI standard is an example of why meeting the compliance requirements at the design-level of the development cycle, is becoming increasingly important as that can reduce the overall compliance program costs (North, North, & North, 2009).

#### 2.3.5.2 Sarbanes-Oxley (SOX)

In the USA in July 2002 the Public Company Accounting Reform and Investor Protection Act (in the Senate) and Corporate and Auditing Accountability and Responsibility Act (in the House) were passed - more commonly called *Sarbanes–Oxley*, Sarbox or *SOX*. The act was part of an attempt to give the Securities and Exchange Commission more tools for the regulation of financial companies (Moeller, 2008). At its heart SOX is a set of rules for handling the privacy and security of financial records (North et al., 2009). SOX section 404, specifically, requires reporting and auditing of systems that handle financial data. This includes web servers and web applications (Bagranoff & Henry, 2005; Tarantino, 2006). In addition, the reporting must also include an attestation by an external auditor or management's internal control assessment. The SOX Act is mandatory for all organisations listed on the New York Stock Exchange in the United States, and is overseen by the Public Company Accounting Oversight Board (PCAOB).

Singleton (2007) indicates that many organisations have adapted SOX even though they are not required to comply with the Act.

#### 2.3.5.3 Health Insurance Portability and Accountability Act (HIPAA)

HIPAA deals with privacy of electronically stored medical records (North et al, 2009). The Act was enacted by US Congress in 1996. The high volume of electronic transactions involved in the health industry are the reasons behind HIPAA numerous regulations to assure the security and privacy of medical data (Jensen, Cline & Guynes, 2007). According to Senft and Gallegos (2009) HIPPA calls for stringent security measures for electronic health information in storage or in transient. HIPAA is structured in Title I and Title II, the latter is known as Administrative Simplification (AS) that requires the establishment of national standards to ensure security and privacy for medical data. Ogren (2009) indicates that the Healthcare industry is unique in storing and distributing health records among primary care, specialised clinics, and other health care and possibly insurance providers. That requires efficient data sharing systems to ensure patient privacy is intact and legitimate claims processing (Champlain, 2003). To comply with HIPAA, organisations must monitor their IT systems and the data they host and also must perform regular assessments to comply with the act requirements (Damore, 2009).

### 2.3.6 Section Summary

In section 2.3, various recognised frameworks and standards have been explored in the following categories:

- Controls frameworks and Standards for IT auditing;
- Frameworks and Standards for risk management;
- IT controls frameworks and best practices;
- IT Project management; and
- Compliance standards.

## 2.4 CONTROLS CONFIGURATIONS

Curry et al. (2006) refer to an organisation as a system that “in order to survive as a whole, a system needs to regulate its behaviour” (p.105). It has been established

that organisations operate within the wider business environment, which is dynamic and "it is important to remember that no organisation exists in a vacuum" (Curry et al., 2006, p. 34). External Factors that affect an organisation are illustrated in Figure 2.20. The level of complexity caused by a number of interrelating factors makes it very difficult to analyse the environment for planning and managing purposes (Curry et al., 2006).

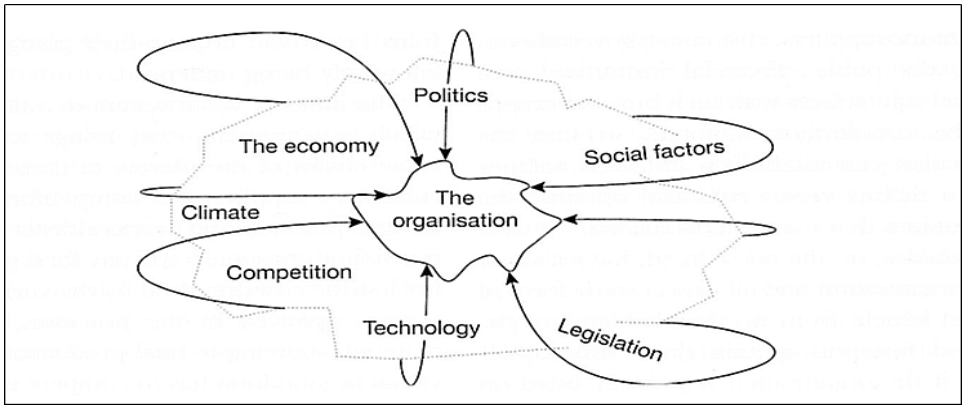


**Figure 2.20: The Organisational Environment (Curry et al., 2006, p. 35)**

The authors emphasise that the system should react to changes in its environment to ensure that it can cope with any threats or opportunities that present themselves. Furthermore, Curry et al. add that "different types of systems require different levels of controls in order to maintain their existence" (p. 97). System thinking as illustrated in Figure 2.21 provides a powerful tool for modeling large complex problems in a logical and practical way (Curry et al., 2006). While system approach doesn't guarantee a quality solution, it makes it possible to find such a solution as pointed out by Curry et al. (2006).

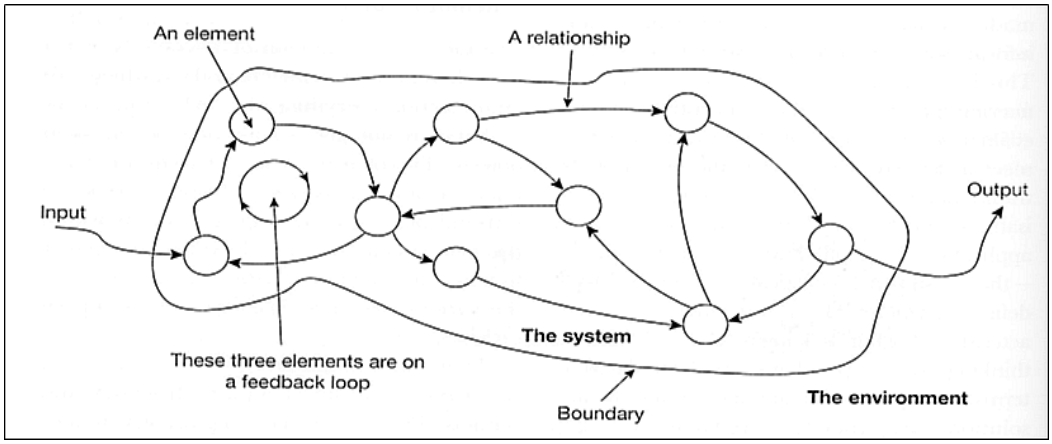


**Figure 2.21: Presentation of a System (Flood & Jackson, 1991, as cited in Curry et al., 2006, p. 100)**

Richmond (1994, as cited in Curry et al., 2006) states that “Systems thinking is the art and science of making reliable inferences about behaviour by developing an increasingly deep understanding of the underlying structure” (p. 101). Applying Systems Theory in analysing IT systems risks in relation to business context helps generate the required information with high accuracy. Subsequent analysis, planning, and management decisions would be based on actual data rather than estimated data, which is a key to an effective IT risk management process (Whitman & Mattord, 2004).

In section 2.1 and 2.2, IT risk management and IT assurance and auditing were reviewed, defined and discussed, respectively. Business requires effective, efficient and timely risk assessment. Subsequently, risk is managed proportionally by reducing the negative side of risk, the impact, while capitalising on its positive side, the corresponding opportunities. In addition, organisations are required to comply with various industry standards and regulatory requirements. Risks are managed via controls, which come in various types, levels of complexity and cost.

The IT assurance function provides the business with a reasonable assurance through IT audit reviews performed by internal or external auditors. IT auditors review and assess existing controls’ effectiveness, efficiency, and reliability, depending on the audit objectives. Several organisations specialised in accounting and auditing, produced a number of auditing standards and guidelines to formalise and assess audit process. The objective is to ensure methodical procedures are applied and adhered to by auditors, as outlined in section 2.3. Similarly, some organisations specilised in IT auditing, risk management, governance and security management have produced IT standards, guidelines, frameworks and best practices. Aiming at ensuring relevant IT functions are performed, risks are managed and resources are adequately utilised. As the IT systems role grew to be a business enabler, while technologies continually evolve and interact with other IT systems and business processes in various ways, it has become paramount to establish controls based IT environment. Al-Khazrajy (2012) conducted a qualitative case study research, which outlines a number of benefits an organisation would gain from a controls based IT environment, established through applying recognised frameworks, best practices and standards.

At the enterprise level, various internal control frameworks have been published, as outlined in section 2.3, COSO internal framework (COSO I), COSO-ERM (COSO II), and Basel II. Similarly, frameworks and best practices pertained to IT systems have been widely utilised by organisations of various sizes and in different industries, for example COBIT and ITIL (Singh, 2010). In Al-Khazrajy (2012) case study research, a number of interviewees indicated that while they agree on the benefits of implementing recognised frameworks and best practices. However, the interviewees didn't see a necessity in fully implementing all of these frameworks and best practices. Hence, practitioners chose to select a set of controls and processes that were found to be more relevant to their business environment. Similarly, a (ITGI, 2008) survey results show that "half of companies have implemented such frameworks, use them as a reference model" (Singh, 2010, p. 4). Furthermore, only one third of the surveyed organisations have strictly implemented those frameworks. Other researchers and papers convey similar view about ITIL and ISO 27001 (Wallhoff, 2004; Schlarman, 2007).

Hunton et al. (2004) indicate that an IT auditor is required, at the audit planning stage of the Audit process, to determine the inherited risks and understand the client's environment. In addition, it is imperative to identify the existing controls and their objectives, as outlined in sub-section 2.2.4.1. According to Abu-Musa (2008) an auditor has to understand risks, existing controls and relevant regulatory requirements along with the evolving technologies and business dynamics. In addition, Tongren (1997, as cited in Abu-Musa, 2008) indicates that advances in technologies render controls and procedures ineffective or obsolete. Abu-Musa (2008) further outlines the statement issued by the Public Oversight Board – POB (2000) which indicates its concerns about the auditor's ability to properly assess risks arising from the rapidly evolving information processing systems. Auditors will find it necessary to understand fully the risks associated with new and advanced business IS, and the controls that are needed to respond to those risks (Abu-Musa, 2008; Hunton et al., 2004; Merhout et al., 2008). In sub-section 2.1.4.1 risks interdependency was discussed and controls could mitigate many risks at different levels and interact with other controls in various ways. This increases the complexity level of the context an auditor is required to analyse, assess and

evaluate. Merhout and Havelka (2008) point out the necessity for the auditor to be able to assess and evaluate the risk holistically.

When auditors are able to identify risks and perform their audits focusing on high priority risks of the value-added projects and protecting most valuable assets, the audit process quality improves. In order to be able to identify risks from the business point of view, a controls-based structured environment helps achieve that with less effort and performed timely and holistically (Al-Khazrajy, 2012). Al-Khazrajy also indicates that establishing IT controls based environment through implementing recognised IT controls frameworks, is costly, but the benefits outweigh the cost. Recognised IT controls frameworks, like COBIT, ITIL, ISO 27001,ValIT have their applications in ITG, IT risk management, IT security management, IT services management and IT value management (Al-Khazrajy, 2012; Ramakrishnan, 2009).

Henczel (2001), further, points out that organisations have different environments, internal and external, and are subject to various regulatory requirements. As IT auditors have different resources at their disposal, hence, there is no single method of working through the audit process' stages. Henczel further indicates that it is imperative to tailor the audit process to the organisation's environment. For example, audit review scope, data collection method, analysis, and evaluation and communication strategies (Henczel, 2001). Hence even when a recognised framework is implemented an element of customisation is required to ensure the implemented controls and processes fit the environment.

According to Singh (2010) recognised IT controls frameworks and best practices like COBIT and ITIL have been widely accepted and implemented as ITG framework. However, evidence obtained from various research studies indicate that many organisations opted not to fully implementing those frameworks. Instead, a set of controls objectives or processes were elected and implemented. Singh (2010) argues that various reasons behind the partial implementation, among them: cost, level of complexity and the lack of comprehensive knowledge in customising those frameworks. In answering the question of what to select from those recognised frameworks and best practices, and on what basis, various data gathering methods were performed. For example, researchers (Debreceny & Gray, 2009; Kim, Phelps & Milne, 2006, as cited in Singh, 2010) have surveyed practitioners and IT

managers to obtain their opinions regarding controls set selection. The issue incites a need to establish a systemic way of selecting controls and processes from various recognised frameworks, standards and best practices. This is particularly true when the risk profile changes, as a result of business dynamics, and new technology or regulatory requirements.

This section is structured as follows: sub-section 2.4.1 defines a set of terms that pertain to controls configurations and frameworks. Sub-section 2.4.2 and sub-section 2.4.3 examine respectively, some examples and controls configurations. While Sub-section 2.4.4 discusses the value gained from selecting a set of controls configurations. The section is briefly summarised in sub-section 2.4.5.

### 2.4.1 Definitions

In this sub-section a number of existing definitions are explored, and some new definitions are formed or introduced, in sub-sections 2.4.1.1-2.4.1.11.

#### 2.4.1.1 Control Types and Mechanisms

As noted in the opening paragraph that different systems and their corresponding risks require different controls. Various authors (Pathak, 2005; ISACA, 2011) have defined controls types as preventive, detective and corrective controls. (Curry et al., 2006) describe two main forms of control mechanisms: feedback and feed-forward controls, these mechanisms could be utilised in a fashion that suits the environment. For example, feed-forward is used as preventative controls to deter some expected behaviour based on some information and calculation to predict the occurrence of such undesirable events and prevent them from recurring. However, not every control implementation approach is always feasible to apply because of cost or domain complexity and difficulty in collecting sufficient data (Leitch, 2008). Curry et al. (2006) indicate another attributes of a control, that's continuous vs. discontinuous. This is determined by the type of variable being controlled and by the nature of the control mechanism applied. For example a corrective control could only be triggered by a detective control to remedy a certain scenario when a risk materialises (Leitch, 2008). When the risk adverse impact ceases to exist the corrective control will be halted, while the detective control continues to operate (Whitman & Mattord, 2004). Leitch (2008) defines a concept of 'dynamic generation', as "controls generating other controls over time" (p. 23), which is

demonstrated in the Figure 2.22. In that view, Leitch (2008) argues the necessity to integrate internal controls and risk management.

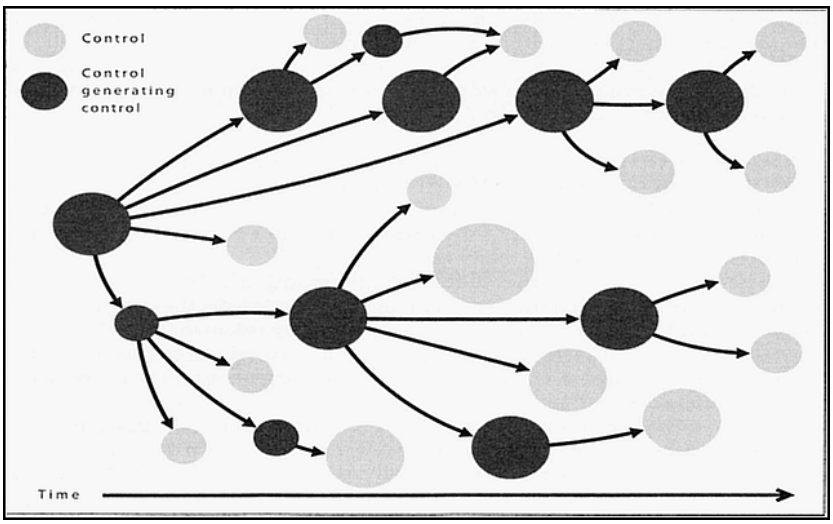


**Figure 2.22: A Self- Generating Risk Control System (Leitch, 2008, p. 24)**

Leitch (2008) elaborates on the 'dynamic generation' and sets an example where a security policy, is a control, stipulates a need to conduct a security risk assessment for a new project, which is another control. The security risk assessment requires other types of controls depending on the technology and business process the project touches or creates. It is possible to predict, some controls requirements, but for some controls, it is not possible to determine that until some events start to unfold (Leitch, 2008). The author indicates that "a well-designed control system should be self-sustaining, generating the actions that will keep it going and keep it up to date" (p. 24). Furthermore, the author points out that the idea of implementing 'intelligent internal controls', where risk based controls are designed by a different set of controls mechanisms (preventive, detective, corrective). Then they are carried out by people of various management roles. The latter statement in Leitch's definition of intelligent internal controls indicates the necessity for the management involving in performing control activities, while other parties would audit-review the execution process, which has been discussed in section 2.2.

#### 2.4.1.2 Controls Interdependency or Interaction

An important aspect of controls is that they interact with each other in various ways. Brand and Boonen (2005) refer to the following premise from COIBT framework: "In order to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped

processes" (p. 57). The authors further outline that controls defined by COIBT have differing degrees of impact on all of the information criteria defined by COIBT 4.1 framework (Reliability, Compliance, Availability, Integrity, Confidentiality, Efficiency, and Effectiveness). The risk model illustrated in Figure 2.22 from Leitch (2008) demonstrates controls interdependency. In addition, from the definition of controls mechanisms above, it could be inferred that some controls interact with each other in various ways, which is required to be considered when evaluating control's effectiveness and efficiency. In many circumstances, some controls could be structured in layers to provide most effective and efficient performance as noted by (Pathak, 2005; ISACA, 2007). Supporting this view, Leitch (2008) states that "control system should be multi-layered" (p. 72) to ensure that controls are not understated.

CICA (1998) explore the definitions of various control model types, as can be seen in Figure 2.15. In the technology control model, where various controls are designed to manage various technologies and systems, CICA indicate the necessity integrate all types of controls within the enterprise. In addition, Risk level controls should be designed to focus on business functions with high exposure. Ultimately, CICA state that as no size fits all, in most organisations a combination of those models are integrated to form a hybrid control model where balancing risks and their cost is a key factor in selecting and implementing required controls.

CICA (1998) further elaborate on the enterprise technology control model, where a combination of controls is required to be implemented at the various levels and functions- listed as: Data, Application Systems, General Computer Control, Accounting Control, Management and Administrative, and Corporate Governance. Figure 2.15 depicts the enterprise technology control model with its various types, which demonstrates the importance of data related controls that interact with general computing controls, accounting controls and application controls. The application controls, in turn, interact with each other along with the overarching corporate policy and administrative and management controls.

#### 2.4.1.3 Controls Classification

Pathak (2005) classifies IT controls into management and application controls. Management controls are "considered vertical in nature as they follow the hierarchical lines of the organisational structure" (p. 10). While application controls

are “considered horizontal in nature, as they go across lines of organizational authority and follow the data flow through the organisation” (p. 10) adds Pathak. Moreover, Hall and Singleton (2005) classify controls into two main categories, general controls and application controls. General controls (management controls) apply across the organisation’s IT environment, while application controls are specific to certain application, as noted by Pathak (2005).

Pathak indicates that it is imperative, from an audit efficiency point of view, for IT auditors to evaluate management controls first before delving into the detailed application controls. The author sets an example of a higher documentation control, if it is proved to be adequate, then there is no need to review all the application documentation controls. The absence or ineffective management controls should be a concern for an IT auditor, as management controls apply across the organisation (Pathak, 2005). In the same way, Moeller (2008) indicates that risk based audit stipulates that testing all controls is not necessary, rather, to focus on key controls, as the existing external audit standards require. Moeller indicates that it is imperative to test first, the higher level IT general controls, before focusing on the detail-level controls.

#### 2.4.1.4 Control and Risk Monitoring

Hunton et al. (2004) and Havelka and Merhout (2007) highlight the importance of continually monitoring risks and applied controls. As it was discussed in section 2.1, monitoring risks is part of risk management process. In addition, relevant controls must be reviewed depending on the type and design of the control. Hunton et al. (2004) argue that assessing internal controls involves constant monitoring of the internal control system. Hunton et al. further emphasise that “just because an organisation has created an adequate set of controls doesn’t mean that these controls are always working” (p. 63). IT controls framework COBIT, defines several control objectives related to control monitoring, which include monitoring the process, assessing internal control adequacy, obtaining independent assurance, and providing an independent audit (Hunton et al., 2004).

#### 2.4.1.5 Controls Frameworks

Hunton et al. (2004) outline the goal of internal controls frameworks and guidelines, and indicate that “various organisations have produced internal control

frameworks and guidelines to assist auditors and management in developing optimal control systems" (p. 53). Section 2.3 summarises a number of those frameworks, best practices and standards.

#### 2.4.1.6 Controls Evaluation

Pathak (2005) points out that IT auditor is in a unique position to holistically assess changes in IT systems, ensuring they are aligned with business objectives. In addition, IT auditors ensure that corresponding risks are assessed and appropriate controls are integrated within IT systems and processes at the design stage. The author further points out that controls activities are performed to manage risks to an acceptable level, and emphasises that "in most cases, it is cost-prohibitive to implement every type of control in an effort to eliminate all element of risk" (p. 99). Hence, it is imperative for the IT auditor to make a judicious use of the internal controls to ensure the benefits outweigh the cost and the business is able to capitalise on opportunities when they come into existence.

According to Pathak (2005) control value can be assessed in terms of its cost and its effect on reducing the expected losses, which could be made by reducing the probability or the amount of loss, should a risk materialise. Pathak (2005) states that "the objective of internal control is to reduce the potential loss by removing the causes of losses" (p. 11). It is the auditor's role to evaluate how effective the control is in achieving its objective, however, Pathak (2005) stresses that control evaluation is a complex task to perform.

#### 2.4.1.7 Controls and Risk Matrix

Leitch (2008) indicates that "matrix mapping of risks and controls is a useful format in any situation that requires the coverage provided by controls to be shown against risks" (p. 71). Leitch further outlines that risks and controls map in a many-to-many relationship. There are two common approaches, for risks-controls matrix, as illustrated in Tables 2.3 and 2.4. The issue with the first approach is that controls are listed more than once, which could lead to a cumbersome documentation. In addition, if an attempt is made to reduce control duplication, it might lead to inadequate risk-control coverage, missing a crucial attribute of multilayered control systems. The author argues that this approach could undermine the risk-control mapping as the control-coverage might not be fully tested.

**Table 2.3: Risk Control Table in Common Format (Leitch, 2008, p. 72)**

| *Risk/control objective* | *Controls* |
|---|---|
| Risk A | Control 1<br>Control 2<br>Control 3 |
| Risk B | Control 1<br>Control 4 |
| Risk C | Control 2<br>Control 3 |
| Risk D | Control 5 |
| etc. | etc. |

As for the second approach, depicted in Table 2.4, while it shows that lots of space will be wasted and a bulky document could be resulted if there were many risks. However, the author claims that that design is more suitable to mark all the corresponding risks and fits with the multi-layered nature of effective control system, as controls can be grouped under subheadings.

**Table 2.4: Risk Control Table Matrix Layout (Leitch, 2008, p. 73)**

| *Control* | *Risk A* | *Risk B* | *Risk C* | *Risk D* | *etc.* |
|---|---|---|---|---|---|
| Control 1 | | 1 | 1 | | |
| Control 2 | | | 1 | | 1 |
| Control 3 | 1 | | | | 1 |
| Control 4 | | | 1 | 1 | 1 |
| etc. | | | | | |

Pathak (2005) discusses control evaluation by internal and external auditors, and describes a conceptual form for a control matrix. In sub-section 2.2.2.2, a discussion was held, where controls are evaluated in terms of their effectiveness in reducing risks impact. Also, the controls reliability in accordance to control compliance testing is included in the evaluation. Pathak further elaborates on the types of control testing performed: column, row and global evaluation. The column and row evaluation is about control effectiveness performed before and after testing the controls for reliability purposes. Global evaluation, on the other hand, is about finding the optimal control set that suits the organisation in respect of the column and row evaluation. Pathak recognises that with regards to global evaluation and finding an optimal set, there are two more complicating factors. These are the costs and benefits of a control that are required to be considered when deciding the optimal controls set. Furthermore, Pathak points out that how these three evaluations performed are subject to further research and few professional auditing bodies have established standards in that regard.

#### 2.4.1.8 Control Capital

In an attempt to identify optimal controls set from COIBT 4.1 framework, Singh (2010) introduces 'Control Capital' a term driven from research in process capital and social capital analyses that have some applications in ITG and performance measurement. Singh defines control capital as a "measure of the level of control in an organisation's IT portfolio, in terms of how extensively it uses COIBT" (p. 3). To analyse and measure control capital, Singh utilises Network Analysis a known data analytics method for social network analysis.

Before delving into Singh's definition, it is worth mentioning some definitions of social capital and process capital and the analogy to control capital defined by Singh (2010). According to Coleman (1998, as cited in Mandarano, 2009) social capital is "a variety of entities with two characteristics in common: they all consist of some aspects of a social structure and they facilitate certain actions of individuals who are within the structure" (p. 246). Moreover, another definition that says "connections among individuals – social network" and "that enable participants to act more effectively to pursue shared objectives" (Putnam, 1995, as cited in Mandarano, 2009, p. 246). An analogy could be drawn from these definitions of social capital and social network to the power, weight or importance of various controls or processes that construct controls frameworks. In that context, controls and processes denotes the actors while recognised frameworks represent the network, which have common objectives of providing reasonable assurance by managing defined risks and capitalising on opportunities.

Fuhrer and Cucchi (2012) explored the relationship between social capital and ICT, and claim that knowledge of such a relationship is insufficient. Furthermore, the authors claim that while there are numerous research reports about ICT usage, however, there are a few that examine the network of exchange and actor's position within the network.

A recognised method in analysing and measuring social capital is social network analysis (SNA), which is defined as "an approach that considers society as a system of actors – individuals, groups, organisations – linked by a number of relationships" (Fuhrer & Cucchi, 2012, p. 17). The SNA relationships formed in various ways and the analysis comprises of a number of types determining the presence or absence of such relations noted (Tichy, 1981; Brass & Burkart, 1992,

as cited in Fuhrer & Cucchi, 2012). In addition, SNA describes the network relationships' structure and configuration. Fuhrer and Cucchi (2012) cited a number of authors (Tichy, 1981; Laumann & Pappi, 1976; Nohira, 1992) to support this point. Actors within the entity's network interact, among themselves and within a group like a team or department and within a larger group for example a company (Lamb & Kling, 2003; Reagans et al., 2004, as cited in Fuhrer & Cucchi, 2012).

One of the most studied concepts used by SNA is the Centrality, which requires the analysis of actor's position within the network and its engagement with other actors. Centrality reflects the importance of the actor within the network, claim the authors. In addition, the number of links, direct and indirect, an actor has with others within the network is a measure of the importance of the actor (Wasserman & Fasut, 1994, as cited in Fuhrer & Cucchi, 2012; Mandarano 2009). According to Mandarano (2009) density is an indicator of the community's social capital, which calculates the total number of actual ties to the possible connections. While, centrality is an indicator of each actor's social capital; it calculates each actor's network density. In Table 2.5 types of centrality measures summarised by Fuhrer and Cucchi (2012). According to Fuhrer and Cucchi (2012) social capital and social network concepts are closely linked, as both relate to the notion of a group of actors. Fuhrer and Cucchi further emphasise that SNA is an approach that considers any group of actors is a system of actors that interrelate to each other in various forms of relationships.

**Table 2.5: Centrality Measures Used (Fuhrer & Cucchi, 2012, p. 19)**

| | |
|---|---|
| Degree | A measure of the activity. The central actors have more relationships than other actors in the network. |
| In-degree | Oriented links of network members to the individual. |
| Out-degree | Oriented links of the individual to network members. |
| Eigenvector | Assessment of the centrality of an actor, considering that his centrality depends on the centrality of actors he is connected with. |
| Authority | For a weighted graph, we can add all the weights of relations from and to an individual. |
| Hub | Node having important degree and betweenness. |

Similarly, Jiang and Carroll (2009) point out that SNA has been used to study social capital and highlight that "focusing on social ties or network structure gives us computational power and superior visualisation to understand complex connections among social actors" (p. 51). The authors, further, claim that computational social network analysis is emerging and has been utilised in research domains like

information science, organisational and management studies. It is imperative to mention that the SNA approach focuses on the social network configuration, in which the network actors interrelate to measure its centrality, and density. Rather than looking at the underlying mechanisms of how these actors interact and build their ties among themselves.

As noted in the beginning of this definition, Singh (2010) indicates that both social capital and process capital have some analogy to control capital in the IT context. Singh utilises network analysis to prioritise COBIT 4.1 control objectives according to the highest connectivity with other control objectives. However, as noted in the control-risk matrix definition at the beginning of this section, that controls are designed to manage corresponding risks, and there is a many to many relationship between controls and risks. Therefore, it is imperative, when selecting a control, to take into account the corresponding risk(s). Also, factors like control types, for example preventive, detective and corrective as well as the level where the control operates (strategic, tactical and operational), are important to consider when assessing the best set of controls. Besides, the cost of controls implementation and value an organisation gains, should be considered, as noted in sub-section 2.1.3.

#### 2.4.1.9 Control Attributes

In order to asses and evaluate controls comprehensively, controls attributes could be defined to determine control's properties. Control attributes in summary comprise the following:

Control capital – as defined by Singh (2010) analysed and measured utilising SNA (Singh, 2010). Control capital will reflect control's interdependency as well as its weight within the implemented controls framework and best practices.

Control category – strategic, compliance, operational as noted in section 2.1.3. While controls may or may not be implemented depending on the cost-benefit analysis, see sub-section 2.1.2, however, strategic and compliance controls have high priority as they imply high value or cost for the business.

Control mechanism – mechanisms of controls (preventive, corrective, and detective) as noted in the control mechanism definition.

Control type – types of controls (administration, general, and application) some authors describe strategic as administration or management controls that apply across the organisation, as noted by (Pathak, 2005).

Control Cost – control implementation and maintenance cost (Whitman & Mattord, 2004).

**Table 2.6: Control Attributes**

| Control Attribute | Definition |
|---|---|
| Control Capital | Defined by Singh (2010) analysed and measured utilising SNA (Singh, 2010). |
| Control Category | Strategic, compliance, or operational, some authors describe strategic as administration or management controls that apply across the organisation. Strategic controls must be implemented, while operational controls may or may not be implemented depending on the cost-benefit analysis, see definition section. |
| Control Mechanism | Types of control mechanisms (preventive, detective and corrective) |
| Control Type | Types of controls (Administration, general, and application) |
| Control Cost | Cost of control implementation and maintenance |

#### 2.4.1.10 Risk Attributes

In similar fashion to controls, risk attributes should be defined to reflect contributing factors, so that risk is assessed holistically as it should, for full details on risk measurement see sub-section 2.1.4.1. Risk attributes should be defined as follows:

Risk Rank – as detailed in sub-section 2.1.4.1 and illustrated in Figures 2.8 and 2.9. While, Risk Interdependency – is a numerical value based on expert or practitioners estimates, where the estimate is increased by one for every defined risk interdependency.

**Table 2.7: Risk Attributes**

| Risk Attribute | Definition |
|---|---|
| Risk Rank | Defined in sub-section 2.1.4.1 and illustrated in Figures 2.8 and 2.9. (High, Medium, Low) |
| Risk Interdependency | A numerical value based on expert or practitioners estimates, where the estimate is increased by one for each defined interdependency. |

Reflecting on risk-control matrix depicted in Table 2.3 and Table 2.4 and the definition of control and risk attributes, a cube of model, as Figure 2.23 illustrates, where the controls and corresponding risks along with their attributes are identified and determined.

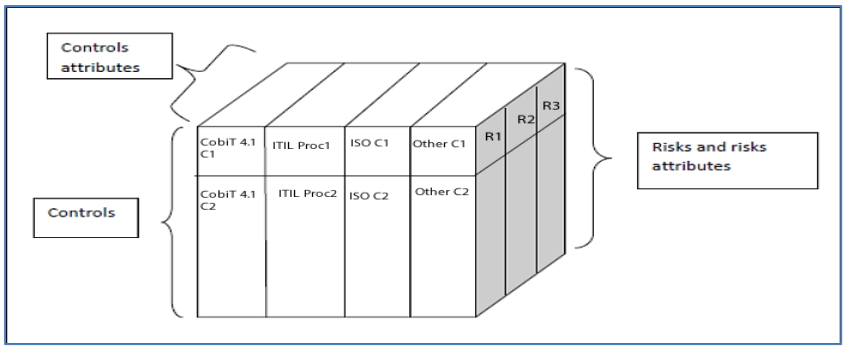


**Figure 2.23: Controls-Risks Matrix and their Attributes**

### 2.4.1.11 Cost and Benefit Criteria

Based on the risk analysis to determine proposed mitigating measures or controls, a cost-benefit analysis is undertaken where asset intrinsic value as well as business value are taking into account to estimate cost verses benefit or value return from implementing defined control/s to mitigate risk. For a full discussion see sub-section 2.1.4.2.

When control properties are estimated based on the defined attributes, an overall control rank (High, Medium, and Low), in terms of capital as a reflection of the control importance and weight, is derived. It is imperative to indicate that a control could correspond to one or more risks; in addition, some controls could collectively mitigate one or more risks. Similarly, when risk properties are estimated, an overall risk rank (High, Medium, and Low), in terms of impact severity, likelihood and uncertainty, is derived. In the same way, a ranking schema for cost-benefit evaluation (High cost, Even, and Low cost) is driven. With the three overall ranking for control, risk and cost-benefit, an informative decision-making facility will be readily available for concerned parties, for example: business managers, security and risk management practitioners, and certainly IT auditors. Figure 2.24 illustrates the proposed control, risk and cost-benefit model.

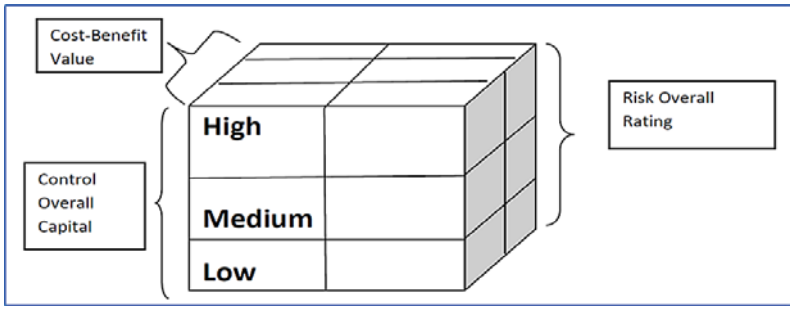


**Figure 2.24: Control, Risk and Cost-Benefit Conceptual Model**

### 2.4.2 Examples

Various authors have analysed or proposed numerous mixtures of IT controls frameworks, best practices and standards. The aim is to provide a comprehensive coverage of different controls and processes to effectively and efficiently manage defined risks, and achieve planned objectives. Datardina (2005) refers to PCAOB's Auditing Standards guidance regarding the use of frameworks, which indicates that: "Management is required to base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognised framework established by a body of experts that followed due-process procedures to develop the framework" (p. 4). Datardina further indicates that while PCAOB recommends the COSO framework, however, organisations are allowed to adopt other frameworks if they meet the PCAOB's guidance, and have similar elements as COSO does. For example, CICA's Criteria of Control Board or 'CoCo' for short. Mishra and Dhillon (2008) claim that "COSO and COBIT frameworks are widely used as guidelines for SOX compliance, systems audit in organisations and also for ITG purposes" (p. 6). However, Mishra and Dhillon do argue that COSO and COBIT are broad in nature and do not specifically handle detail security controls.

With regards to utilising recognised controls frameworks, Tabor (2009) states that "if existing frameworks help organisations achieve their goals, then valuable resources need not be used to reinvent proven process" (p. 2). Tabor (2009) further points out that to manage IT security, there is no single methodology or framework that comprehensively covers all required solutions. Rather, the author states "professionals consider, applying what is most needed and relevant to their organisation" (p. 2). Datardina (2005) indicates that "when selecting a control framework, management must ensure that the framework is sufficient, but also does not impose controls that create more costs than benefits" (p. 10). In addition, it is imperative to consider the familiarity of the audit community, management, and responsible staff with the selected control frameworks, to ensure better customisation is applied (Datardina, 2005). The author further points out that implementing recognised IT controls frameworks enables the management fulfill legal and business obligations and requirements by ensuring their IT systems are reliable, effective and efficient. However, Datardina (2005) further states that "management cannot simply 'cut and paste' just any framework into their

organisation" (p. 25). Frameworks should be selected, customised and adopted to add value by improving subject process, reducing cost, to name a few examples.

With regards to IT, COSO categorises IT controls into general and applications controls categories. However, these are high level controls and no details are provided. Datardina (2005) points out to the framework selection criteria devised by CICA that includes: relevance, reliability, neutrality, understandability and completeness. Among many IT controls frameworks, COBIT, has a global recognition and is well known to assurance and governance practitioners. Tabor (2009) conducted a survey as part of research, soliciting answers regarding frameworks and best practice adoption. The author further outlines the survey results that show 70% of the respondents indicated that increased efficiencies and process improvement when adapting the listed frameworks, best practices and standards. In addition, while COBIT was not in the initial list, 25% of the respondent referred to using COBIT as the 'Other' framework mainly by their internal assurance division. As noted by many authors, COBIT by itself is not enough to provide a holistic solution to all governance, risk and security management activities for IT systems; therefore, it must be accompanied by other frameworks and/or best practices. According to von Solms (2005a, as cited in Tabor, 2009) combining COBIT with ISO-27001 provides a broader base solution for IT security governance. Datardina (2005) states that ISO 17799, which superseded by ISO 27001, proves to be a companion framework for COBIT, covering IT security. Datardina (2005) indicates that COBIT and ISO 17799, superseded by ISO 27001, complement each other. COBIT specifies what needs to be done, and ISO 27001 details how to achieve the requirement. However, that complementary framework-relationship covers the IT security area only.

Likewise, Singh (2010) cites a number of authors who indicated that COBIT and ITIL have gained a wide recognition for ITG framework. Table 2.8 from (Singh, 2010) illustrates the usage of various IT control and perormance frameworks that have been utilised for the noted years.

**Table 2.8: Use of Different IT Control and Performance Frameworks (Singh, 2010)**

| | **2006** | **2005** | **2004** |
|---|---|---|---|
| Balanced Scorecard | 63.81% | 59.60% | 59.16% |
| Capability Maturity Model Integration | 30.00% | 29.40% | 18.85% |
| Capability Maturity Model for Software | 25.00% | 25.40% | 18.32% |

| | | | |
|---|---|---|---|
| Malcolm Baldrige Quality System | 9.29% | 11.20% | 6.54% |
| People Capability Maturity Model | 7.62% | 8.40% | 3.40% |
| Six Sigma | 41.19% | 38.20% | 35.86% |
| Lean Six Sigma | 29.76% | 19.80% | - |
| QPR Scorecard (Corporate Performance Management) | 14.29% | 14.60% | 7.33% |
| Business Activity Monitoring | 22.14% | 20.20% | 8.90% |
| IT Infrastructure Library (ITIL) | 50.71% | 38.40% | 6.02% |
| ISO 9000x | 40.95% | 43.80% | 35.60% |
| COBIT | 5.48% | 2.60% | 1.31% |
| Other | 6.19% | 8.00% | 24.35% |
| None | 23.10% | 18.00% | 12.30% |
| European Foundation for Quality Management | - | - | 2.09% |
| Software Acquisition Capability Maturity Model | - | - | 3.14% |
| System Engineering Capability Maturity Model | - | - | 5.24% |

Tabor (2009) indicates that the most common recognised frameworks and best practices are ISO 27001, COIBT and ITIL, however, there are other frameworks that are industry specific or common in the public sector. Schlarman (2007) outlines a number of factors that should be considered when selecting or integrating control frameworks. For example, the organisation's size, complexities of the business, whether it spans over many nations or it is an autonomous business unit. The author further states that frameworks provide support and the systematic approach to overcoming challenges and ensuring business operations are controlled in an environment to achieve desirable objectives. The IT controls structure comprised of ITIL, COIBT and ISO 17799 (ISO 27001) are strong candidates to consider for IT controls infrastructure. The three mentioned frameworks are widely accepted frameworks with a history of validation that provides much creditability from an executive perspective (Schlarman, 2007). While the best frameworks and best practices help organisations structure a control based IT environment, they lack the technical details to optimally configure and manage various IT systems resources. Schlarman (2007) refers to publications from other organisations that develop and publish technically detailed documents to manage and configure various IT systems aspects like operating systems, networking, web applications, and more. The various frameworks, standards and best practices, along with the specialised technical publications could be integrated to provide comprehensively controlled IT systems environment, as depicted in Figure 2.25.

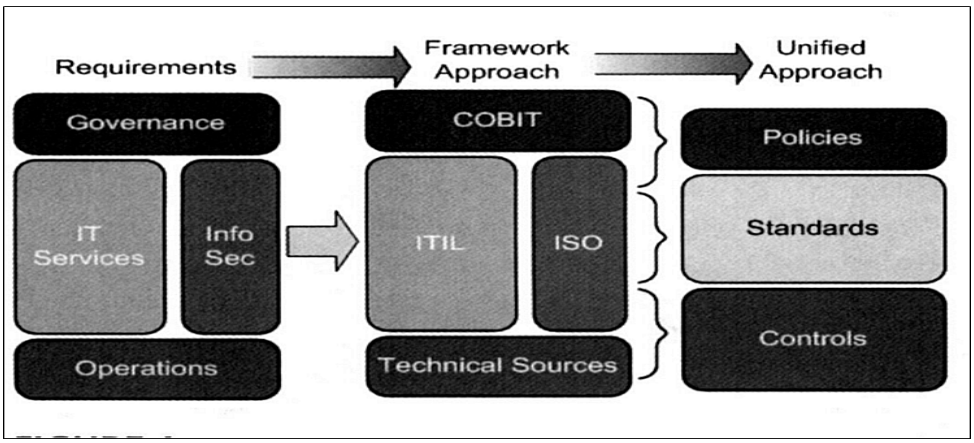


**Figure 2.25: The Evolution of Framework Adoption (Schlarman, 2007, p. 150)**

Similarly, Wallhoff (2004) points out to COIBT, ITIL and ISO 17799 as the widely recognised frameworks and best practices, with the known strengths and shortcomings of each. While COIBT operates at the strategic level and provides controls, guidance on 'what' is required. ITIL on the other hand is a process oriented and operates at the operational level and advises practitioners on the 'how' to design and run processes efficiently. However, ITIL lacks guidance on controls, and is not well versed with strategic planning and business alignment. Both COIBT and ITIL lack the detailed aspects of IT security that ISO 27001 describes and goes in depth on defining various controls pertaining to IT security (Wallhoff, 2004). Merhout and Havelka (2008) highlight another aspect of IT controls frameworks and indicate that Val IT and COIBT combined, enable organisations to direct IT investment on value-added business components. Furthermore, the authors cite(Schaafsma, Spangenberg & Williams, 2007) who conducted an empirical study on a large samples of IT projects and obtained evidence where recognised framework like COIBT is implemented, lead to the least instances of projects exceeding cost and time budgets. Merhout and Havelka (2008) also highlight the high quality audit can be delivered when a recognised IT audit methodology is followed, and control frameworks implemented where IT auditors require less effort to evaluate controls and processes and identify any gaps or redundancies.

Keeny (1992, as cited in Mishra & Dhillon, 2008) states "values are what we care about and they should be the driving force for our decision making" (p. 3). Furthermore, Catton (1952, as cited in Mishra & Dhillon, 2008) defines value as "value is not a property of an object but is a quality of relationship" (p. 108). Mishra and Dhillon (2008) performed a research on value driven internal controls, and

gathered that most of the respondents indicated that technical controls by themselves are not enough to ensure an information security governance structure. Leitch (2008) indicates the need to have a multi-layered controls model to ensure an optimum and factual assurance of a true sense of security, in addition to other objectives that ITG should achieve. Ramakrishnan (2009) also discusses various recognised methodologies that answer the common questions when assessing implemented controls and processes to develop controls based IT structure environment, as listed in Table 2.9.

**Table 2.9: Frameworks Alignment with Four Questions (Ramakrishnan, 2009, p. 300)**

| Four Questions | Methodologies |
|---|---|
| Are we doing the right things? | Val IT |
| Are we doing the right way? | The Open Group Architecture Framework (TOGAF), COBIT |
| Are we getting them done well? | COBIT, ITIL, CMMI, ISO/IEC 20000, Six Sigma, PRINCE2, PMBOK |
| Are we getting the benefits? | Val IT |

### 2.4.3 Controls Configurations

Tarantino (2006, p. 191) maps various control objectives in COIBT 4.1 to their corresponding controls and processes in COSO control framework (COSO I) and COSO-ERM (COSO II) as well as PCAOB. Leitch (2008) states that "risks and controls map in many-to-many way" (p. 71). When mapping risks to relevant controls, Leitch (2008) states that "control system should be multi-layered" (p. 72) to ensure that controls are not understated. As there are various types of controls that operate at different levels, strategic/operational, and designed based on different control mechanisms: preventive, detective and corrective. In addition, IT controls interact with each other and are interdependent in various ways. IT controls should be designed and implemented as a whole system, to ensure associated risks are managed holistically to avoid or reduce controls' risks.

In sub-section 2.4.2, it has been established that the adaptation of one or more recognised controls frameworks has a number of benefits. It has also been argued that given the domain complexity of IT systems and its interwoven relationship with business, no one framework suffices to establish a control based structured IT environment. A number of authors researched various mixtures of frameworks, best practices and standards, from COIBT, ISO 27001, ITIL, ValIT,

COSO I, COSO II. For a further list of examples see section 2.3.While integrating various IT controls and processes frameworks seems a promising solution, however, that comes at cost and increases the implementation complexity. (Al-Khazrajy, 2012).

Henczel (2001) emphasies that organisatons have different requirements and business context, and have various levels of resources. Hence, there is no single method of working through the audit process, in particular, when evaluating IT controls. To determine their effectiveness and whether to implement more compensating controls or removing unnecessary controls. As corresponding risk profile changes, because of the deployed technology or business dynamics, controls could become ineffective or redundant, (Champlain, 2003).

In this sub-section a discussion is undertaken to explore the practicality of adopting, COBIT, ITIL, ISO 27001 and ValIT, as a minimum set of controls and processes frameworks, best practices and standards. The aim is to establish an IT controls infrastructure, where risks are identified, and managed through a cost effective set of controls. As it has been noted (Datardina, 2005; Wallhoff, 2004) that selected frameworks must be customised to the business and IT systems environment, and take into consideration the legal and regulatory requirements. The controls configuration should be constructed with sufficient agility in order to accommodate business dynamics and its agile environment.

Enterprise Framework COSO and COSO-ERM are known as holistic frameworks for the enterprise risk management, but they don't provide details on the implementation (Hunton et al., 2004). Monahan (2008) argues that the COSO-ERM framework, defines enterprise risk management and its aspects, however, it "offers little guidance on how to design and execute an effective enterprise risk management framework" (p. 119). Moeller (2008) indicates that in order for internal controls to operate effectively they require strong processes to make sure required activities are executed. For example, IT changes are properly authorised, tested, and approved before implementing those changes into production. The author claims that ITIL best practices help an organisation to comply with SOX internal control requirements. On the other hand, audit standards, and guidelines, provide a methodical way for conducting effective audit process. But they do not answer the question on what is the best control combination an auditor could select.

In addition, those standards and guidelines, do not offer guidance on how to assess and evaluate risks, taking into account compound risks and risk interdependency.

From the recognised control frameworks, COIBT stands out as a good choice for IT as it is business driven. Moeller (2008) indicates that the COIBT framework although it is designated for IT, however, it has gained a broader reputation of being business oriented (Senft & Gallegos, 2009). In addition, it has been utilised by practitioners as a tool for documenting, reviewing, and understanding SOX internal controls (Moeller, 2008). Figure 2.26 depicts COIBT components and its relationships to business and IT. Furthermore, Hunton et al. (2004) point out that IT audit guidelines provided by ISACA as one of COIBT companion, which aid IT auditors to perform various IT audit reviews based on COIBT control objectives.

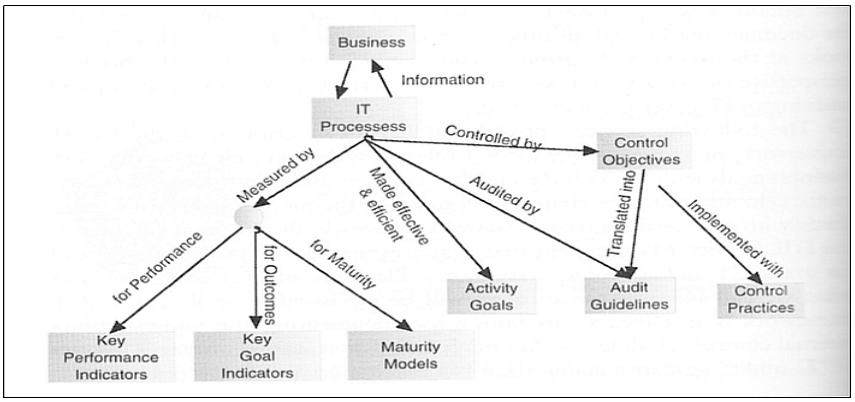


**Figure 2.26: COIBT Components Relationship (Moeller, 2008, p. 122)**

COIBT maps well to COSO, as noted in Figure 2.27, where COSO components are mapped to COIBT controls objectives.

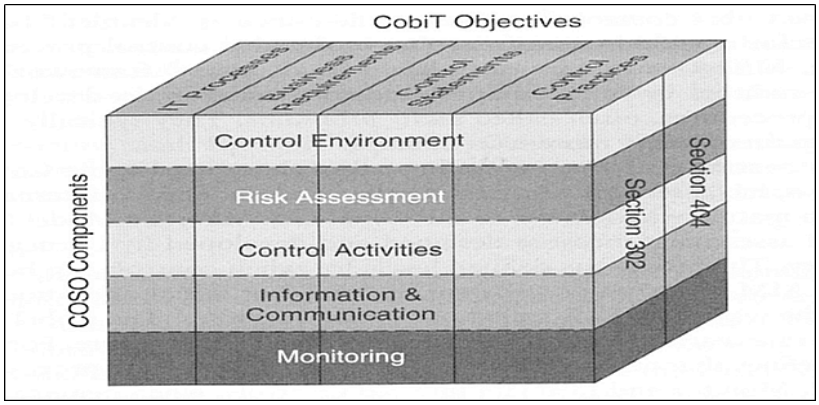


**Figure 2.27: COIBT – COSO Relationship (Moeller, 2008, p. 142)**

Furthermore, Datardina (2005) outlines common IT controls between COSO and COIBT as depicted in Table 2.10.

**Table 2.10: Relationship between COSO and COBIT (Datardina, 2005, p. 16)**

| | |
|---|---|
| ***COSO Non-IT Controls***<br>• Adequacy of employee retention procedures<br>• Fairness of employee assessments | |
| ***COSO IT Controls that are in COBIT***<br>• Application System Development and Maintenance Controls<br>• Access security | ***COBIT Controls that apply to COSO***<br>• Acquisition or development of application software<br>• Ensure systems security |
| ***COSO IT Controls that are not in COBIT***<br>• Application Controls<br>• Information Quality | ***Other IT Controls that apply to COSO but are not in COBIT***<br>• Application Controls<br>• Information Quality |
| | ***COBIT Controls that do not apply to COSO***<br>• Technological direction of the company<br>• Management of Investment in IT |

In addition, Datardina highlights another relationship between COIBT and PCAOB that was articulated by ITGI the ISACA's research arm and shown in Table 2.11. The mapping of the COIBT high level processes and control objectives to the enterprise level frameworks like COSO II and PCAOB, reflects COIBT's strength in integrating IT controls with the overall enterprise controls infrastructure. In addition, as it has been noted in sub-section 2.3.3.2 that COIBT was initially developed as an IT audit framework, and evolved to be an IT governance framework, that helps organisations manage their IT risk and compliance (Hunton et al., 2004; Wright et al., 2008).

**Table 2.11: ITGI's Mapping of COIBT to PCAOB Requirements (as cited in Datardina, 2005, p. 15)**

| **COBIT Control Objective Heading** | **PCAOB IT General Control Heading** | | | |
|---|---|---|---|---|
| | Program Development | Program Change | Computer Operations | Access to Programs and Data |
| 1. Acquire or develop application software. | ● | ● | ● | ● |
| 2. Acquire technology infrastructure. | ● | ● | ● | |
| 3. Develop and maintain policies and procedures. | ● | ● | ● | ● |
| 4. Install and test application software and technology infrastructure. | ● | ● | ● | ● |
| 5. Manage changes. | | ● | | ● |
| 6. Define and manage service levels. | ● | ● | ● | ● |
| 7. Manage third-party services. | ● | ● | ● | ● |
| 8. Ensure systems security. | | | ● | ● |
| 9. Manage the configuration. | | | ● | ● |

| COBIT Control Objective Heading | PCAOB IT General Control Heading | | | |
|---|---|---|---|---|
| | Program Development | Program Change | Computer Operations | Access to Programs and Data |
| 10. Manage problems and incidents | | | ● | |
| 11. Manage data. | | | ● | ● |
| 12. Manage operations. | | | ● | ● |

Furthermore, Moeller (2008) claims that there is a growing convergence between frameworks, best practices and compliance standards, like COIBT, ITIL and SOX. However, COIBT, as noted in the previous sub-section, lacks the detail on how to achieve its controls objectives (von Solms, 2005). Also COIBT doesn't operate at the operational level. However, ITGI the research arm of ISACA has developed and published a number of documents for mapping COIBT controls to various controls frameworks, best practices and standards, as depicted in Table 2.12.

**Table 2.12: Available COIBT 4.1 Mapping to other Frameworks from ISACA**

| |
|---|
| ISO 17799-2000/17799-2005, ISO 27002 |
| CMMI v1.2 |
| ITIL v3.0 |
| NIST SP800-53 Rev 1 |
| TOGAF 8.1 |
| ISO/IEC 20000 |

It should be noted that not all COIBT control objectives map to other controls and/or processes in the other frameworks or standards (von Solms, 2005). The author further indicates that the downside of this mapping is that it is in one direction only, from COIBT to other frameworks.

With regards to establishing a governance structure for information security, von Solms (2005) stresses the benefit of implementing a recognised framework and standards. The author further suggests that COIBT and ISO 17799, with its successor 27001, are complementary to each other and if "used together, they provide a synergy which can be very beneficial to companies" (p. 100). Wallhoff (2004) states that "what ITIL is for IT Management, COIBT is for IT-audit and ISO 17799 is for security management" (p. 1). As it has been noted in the previous section that ITIL is strong at the operational level, and it provides the 'How' to achieve control objectives and apply underpinning processes. While

COIBT and ITIL strengths are at different levels within IT systems. However, "ITIL and COIBTcomplemented with each other to a high degree" (Wallhoff, 2004, p. 3). Moreover, Wallahoff indicates that ITIL does not correspond to ISO 17799 in the same fashion it does to COIBT. Hence, it can be inferred that COIBT provides the overarching framework for other frameworks, best practices and standards (Datardina, 2005). Ultimately, a best combination of controls and process could be integrated seamlessly where overlapping controls are minimised and a comprehensive coverage is achieved (Schlarman, 2007). Wallhoff (2004) emphasises the necessity for not to fully implementing ITIL, COIBT and ISO 17799, in one go, as it is bound to fail. The author further outlines the difficulties in selecting the high priority controls based on the cost-benefit analysis and their risk mitigation capacity.

In section 2.2.3 the IT auditor's role has been discussed and it has been established that the IT auditor plays a big role in establishing an effective IT governance structure through the devised controls and processes. Afzali et al. (2010) debate the importance of IT governance structure to enable business realising the value of IT capabilities and activities. The authors discuss the necessity for the ITG to be shifted to Enterprise Governance of IT through integrating COIBT and Val IT control frameworks. Furthermore, Afzali et al. indicate that COIBT focuses on IT-related responsibilities, while Val IT focuses on business-related responsibilities. According to the authors, COIBT and Val IT can together provide an answer to the four questions on ITG structure listed in Table 2.9, as illustrated in Figure 2.28.

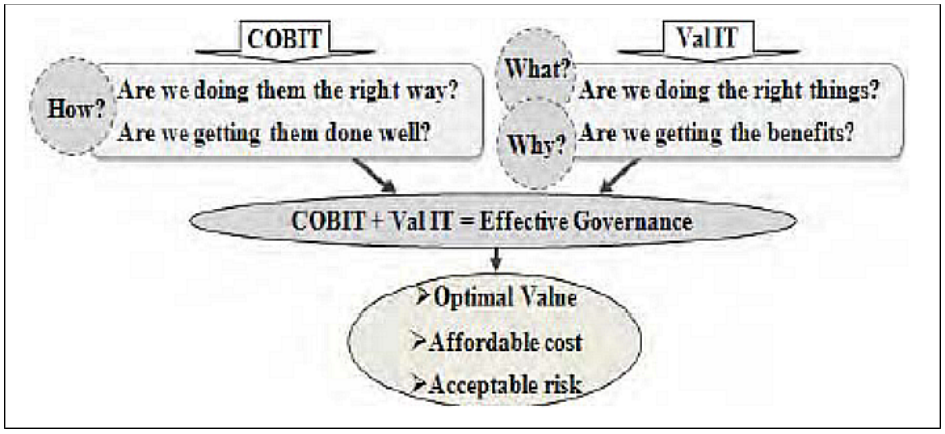


**Figure 2.28: Effective ITG through the Use of COIBT and Val IT (Afzali et al., 2010, p. 48)**

By integrating related controls and processes from both frameworks, they provide business and IT decision makers with a comprehensive framework for value creation from the delivery of high quality IT services (Afzali et al., 2010).

It can be concluded that integrating controls and processes from COIBT, ITIL, ISO 27001 and Val IT provides a comprehensive control infrastructure. Controls and processes however should be selected based on their merit to manage corresponding IT risks to ensure best value is delivered. To achieve that, controls are identified as per the control-risk cube model defined in configuration definition noted in sub-section 2.4.1, and illustrated in Figure 2.23. The aim is to develop control-risk (High, Medium, and Low) evaluation along with the cost benefit ranks as depicted in Figure 2.24. In order to build a decision-making model, where controls are mapped to associated defined risks, and controls and risks attributes are defined, accordingly controls cost-benefit analysis and figures are calculated. The model should provide a current status of the control-risk-cost-benefit at any given time as and when needed, to allow informed decision-making.

### 2.4.4 Value

Organisations constantly have to make decisions at all levels: strategic, tactical and operational. The goals for these decisions vary from responding to market demands, or meeting regulatory requirements, or simply to keep the business alive (Ames, 2007b). Changes do happen, risks materialise for different reasons and at different levels as outlined in section 2.1.2. When business management has confidence that their capacities and capabilities are reliable, well developed and wisely budgeted for, then the business is able to make informed business decisions (Whitman & Mattord, 2004). When organisations make decisions and respond to changes in business and technology in order to achieve planned goals, they invest in building solutions and subsequently expect a return on investment (ROI) (Ames, 2007a). It was stated by Barnier and Fischer (2010) that “To grow, an enterprise must take risks” (para. 9). To realise the value of responding to the various demands, organisations should make a dependable and informed decision (Whitman & Mattord, 2004). Stockman (1996) argues that “Under certain conditions, a rational guess is the expected value” (p. 535). Stockman’s statement could be rephrased without changing the balance of the premise and the conclusion by saying: “Under

certain conditions [where uncertainty or risk is managed], a rational [informed] guess is the expected value".

According to Leitch (2008) who states that "Control objectives are the flip side of risks" (p. 76), by implementing cost-effective controls, risk is managed and desirable value is obtained (Al-Khazrajy, 2012). Furthermore, Leitch (2008) states that "Controls designed as an integrated system rather than piecemeal can be more efficient and effective. This is particularly so, if special skill is applied and the focus is on value rather than just risk coverage" (p. 29). As IT systems underpin all business activities, IT risk exists wherever IT systems are planned, implemented, operated and managed (Murphy, 2002).

Organisations must design, develop and maintain secure and reliable IT systems (Whitman & Mattord, 2004). To ensure IT systems are secure and reliable, IT risk has to be assessed and managed; however, a balance should be struck between managing the perceived risks and opportunities. Managing IT risk within business context requires considerable effort to accommodate many changing factors (Murphy, 2002). To manage IT risks, it has been established that utilising recognised methodologies in developing controls and processes infrastructure provides many benefits to the organisation. Ramirez (2008) indicates that having a standardised methodology for risk management would allow practitioners to simplify their approach and provide mechanisms for continual improvement. In addition, implementing recognised frameworks ensures a systematic solution to the complex domain of business-IT of risk and value. The discussion explored in the previous sub-section leads to the necessity of selecting a set of controls from the recognised framework COBIT, mixed with processes from ITIL, and controls from ISO 27001 and Val IT. However, to achieve that, immense time and effort are required that could increase the cost of managing the risk to a level it becomes cost-prohibitive (ISACA, 2007).

IT auditors face a daunting task in evaluating controls and selecting adequate controls. Furthermore, IT auditor has to assess and determine the most important risks and to resolve the interdependency of the various controls from numerous frameworks, standards and best practices. Hunton et al. (2004, p. 208) indicate that the IT auditor is required to determine inherited risks and understand business context. In addition, it is imperative to identify existing controls and their

objectives, as outlined in sub-section 2.2.4.1. Abu-Musa (2008) points out that the International Standard on Auditing 401 – Auditing in Computer Information Systems Environment – states that auditing process for both internal and external have been rapidly changing. Abu-Musa further indicates that factors causing these changes include: "the globalisation of business, advances in technology, demands for value-added audits, and the organisational structure of the client's computerised information systems (CIS) activities" (p. 440). In addition, Tongren (1997, as cited in Abu-Musa, 2008) indicates that advances in IT continuously could render control procedures obsolete, and the 'value' of traditional internal audit has become seriously questioned.

In sub-section 2.1.4.1 risk interdependency was discussed as one of the challenges that management or practitioners face with when evaluating risks. In addition, controls could attenuate many risks at different levels and interact with other controls in various ways. Resulting in increasing the complexity level of the context an auditor is required to analyse, assess and evaluate. Merhout and Havelka (2008) highlight the necessity for the auditor to be able to see the 'big picture', so that risks are adequately evaluated. Auditors will find it necessary to understand fully the risks associated with new and advanced business IS, and the controls that are required to mitigate those risks (Abu-Musa, 2008; Hunton et al., 2004; Merhout et al., 2008).When auditors are able to identify risks and perform their audits focusing on high priority risks, the audit process quality improves. Merhout and Havelka (2008) stress that a quality audit process adds value by performing risk based audit, utilising resources efficiently, focusing on the more value added projects and protecting most valuable assets.

One direct benefit of IT control based frameworks is ensuring the economy of the operation before risk materialises, and survival afterwards (Abram, 2009). IT risk management framework at a higher level in the capability maturity model (CMMI) would have efficient control self-assurance (CSA) and be embedded within the enterprise's culture (Doughty & O`Driscoll, 2002). Managing IT risk holistically would help leverage processes and activities performed as part of IT governance structure, for example Business Impact analysis (BIA) which is part of Business Continuity Planning (BCP). Other ITG framework activities examples are: assets management, security management, incident management, change and

configuration management, project management, research and development (R&D), software testing and quality assurance (QA), internal audit review, external audit review, and awareness programs. A framework that is implemented as an integral part of the enterprise IT governance structure (COBIT, Val IT, ITIL, RISK IT) would provide a holistic approach in managing IT risk (Fischer, 2008).

In order to be able to identify risks from the business point of view, a controls based structured environment helps achieve that with less effort and is performed timely and holistically (Al-Khazrajy, 2012). Al-Khazrajy further points out that establishing a control based environment through implementing recognised frameworks, best practice and standards, while it is costly, however the benefits outweigh the cost. Establishing a controls-based environment in such a fashion ensures the assessing and evaluating of IT risks, and the monitoring of the associated controls are among the benefits an organisation could gain. Recognised frameworks, like COIBT, ITIL, ISO 27001, ValIT have their applications in ITG, IT risk management, IT security management, IT services management and IT value management (Al-Khazrajy, 2012; Ramakrishnan, 2009). By establishing those recognised methodologies, an organisation benefits immensely from the aforementioned practices, as well as, reducing the cost of the assurance function (Abu-Musa, 2008; Al-Khazrajy, 2012; Merhout & Havelka, 2008).

According to Bunker (2003, as cited in Mishra, 2007) for information assurance purposes audit teams should form a close work-relationship with the IT security team. Mishra (2007) describes an efficient internal audit process to provide assurance on the organisation's ITG structure and the security of their IT systems. To be able to play such a vital role, audit teams as well as IT governance and security teams, should have a common language and a framework where they could coordinate their effort to obtain desirable outcomes (Abu-Musa, 2008). Mishra (2007) cites a number of researchers (Flowerday & Solms, 2005; Rezmierski et al., 2002; Whitman, 2003) who indicate that achieving compliance with standards and regulatory requirements, requires, regular periodic assessment of internal controls, which leads to more efficient operations and better security. Similarly, Henczel (2001) highlights that reasonable assurance and compliance status is obtained via different types of auditing, for example, Finance, Process and Technical or IT.

Henczel (2001, p. 197) discusses first and second audit generations, where the first audit generation is conducted initially across the entire organisation. Subsequent audit reviews that follow are called $N^{th}$ degree audit generations, where auditors focus on business units, process or assets with high value or anticipated vulnerability. According to Henczel (2001) the key factor in moving from one audit generation to the next is "the ability to use the historical data already captured and the framework developed in previous audits" (p. 197). Establishing an internal controls framework based on recognised methodologies facilitates subsequent audit generations with a focus on high value/risk control, process, function and assets. The risk based, cost effective and value adding best set of controls, will aid management to govern their IT systems, manage their IT risk and obtain best value. Also, will contribute to the audit process quality and ultimately the business gains all facets of values, tangible and intangible.

### 2.4.5 Section Summary

The below key points summarise the contribution of section 2.4:

- Some key controls definitions: types, mechanisms, classifications, were outlined;
- Combining controls from various frameworks examples were examined and analysed;
- Controls configurations, causality, objectives and challenges were highlighted
- Ensuring values of controls via effective IT auditing, security and risk management.

## 2.5 POTENTIAL ISSUES FOR RESEARCH

This section outlines a number of issues and challenges as well as gaps that have been highlighted throughout the various sections that have reviewed in this chapter.

### 2.5.1 Issues and Challenges in Managing IT Risks

The IT risk management process, as depicted in Figure 2.3, shows it is imperative to ensure effective communication with all stakeholders. Furthermore, messages should be crafted with the right terminology and tone to the targeted audience. By

conducting the ‘Monitor and Review’ part of the process it ensures the risk management process is continuous, dynamic and responsive to changing threats and vulnerabilities in a timely fashion. Figure 2.4 shows the interwoven relationship between IT and business, to gain the anticipated value from IT systems as illustrated in Figure 2.5. IT systems must be secured, and associated risks are managed. IT Risk, however, is not simply a probability of loss, it is multilayered, and hence managing risk is potentially a complex task that requires comparable effort to be discharged to arrive at planned outcomes. IT risk should not be managed in isolation from the business processes and activities that correspond to the IT assets where the potential risk exists. To achieve desirable assurance, an IT risk governance structure is required to oversee all the efforts executed in a concerted way and aligned with the business’ objectives, at all levels: strategic, tactical and operational.

One key factor and quite challenging task of IT risk governance is developing a risk awareness culture. This is where all stakeholders are aware, of their roles and responsibilities to monitor, interpret, document, report and take action when required. That requires an adequate and well-designed educational and training activity, as part of the overall IT risk management program aligned with the business objectives. Establishing such a program is quite a challenging undertaking that requires not only a budget in time and resources, but also, skillful personnel who would be able to design and execute an effective and efficient program activities.

Figure 2.6 illustrates a crucial relationship between managing IT risk and capitalizing on IT opportunities. All organisations seek to have IT as a value enabler. That happens when a business establishes an effective structure of controls and processes in a robust setting that could sustain the impact when potential risks materialise. The structure would have to be agile enough to enable the business react in line with the business dynamics and changes in internal and external environments. To be able to manage IT risk adequately, going through the stages shown in Figure 2.3, a key factor is arriving at a risk rating that reflects the true assessment of the risk, as discussed in sub-section 2.1.4.1. However, IT risk in its nature, is largely qualitative, and it is estimated often via consulting stakeholders that results in a subjective estimate. Subsequently, that leads to an element of

uncertainty and/or inefficiency in the devised risk treatment decision. Furthermore, as IT risks impacts various systems differently, it is required to be managed holistically, which further compounds the complexity of the risk assessment.

In sub-section 2.1.4.2, it was discussed that when estimating IT risk, the business value of related assets should be identified as well, but this has been argued as another dimension to the already complex issue. Figure 2.10 illustrates a vital presentation of risk and value. This has been referenced as a multidimensional concept, tangible and intangible, that is hard to express in a simple number. When evaluating IT risk, attention should be made to how an IT asset impacts business processes and how it enables the business in achieving its strategic objectives.

Business contexts, both internal and external, are subject to change and accordingly the risk profile also changes. New assets could be introduced, their business value and impact must be evaluated and included in the risk assessment. In addition, vulnerabilities and associated threats evolve and quite possibly new types are introduced by new and existing assets. Therefore, the risk profile must be maintained current and the corresponding controls that have been implemented must be reviewed for their effectiveness and efficiency as well as ensuring the business value outcomes are produced.

### 2.5.2 Issues and Challenges in IT Assurance

In sub-section 2.2.1.2 it has been discussed that organisations are required to have a satisfactory level of assurance and their risks are to be managed adequately as and when required. Issues such as ITG, E-commerce, security and privacy and control of public and enterprise information have driven the need for self-reviewing and self-assuring. Auditing is about managing risk. The objective of auditing is to act as a management means to measure and report risks, which should allow the management to make an informed decision. It is imperative to indicate the necessity of audit independence so it could add value to the organisation. Auditing is an independent examination of an organisation’s management that must follow a set of guidelines and standards published by an external sanctioning body.

An effective IT governance structure for an organsiation denotes secure IT systems, anticipated IT risks are managed, and business-IT objectives are aligned. While it is the IT senior management’s responsibility to undertake developing such

a structured environment. IT auditors play a vital role in providing the management with adequate advice and recommendations to ensure defined objectives are met. Furthermore, IT auditors have a vantage point to holistically assess and evaluate risks and their corresponding controls. This is a vital aspect in managing IT risks and designing adequate controls. In addition, IT auditors perform auditing reviews to manage compliance of IT systems with applicable regulatory and standard requirements. Depending on the compliance requirements, some reviews are required to be more frequent to ensure a valid compliance status and the risk profile along with the corresponding controls are current. The audit reviews proved to be a resources intensive task to perform, which forces many organisations to perform shallow reviews within the available budget. Following a systematic method by implementing recognised frameworks and best practices, provides a guaranteed solution.

As IT audit should be risk based, hence, risk management methodologies apply and form essential aspects in conducting an effective audit. While IT risk assessment evaluates the use of technology to identify risk and design compensating controls, when required. IT auditing evaluates the compliance and adequacy of the implemented controls, and the applied methodology.

The business management is responsible for the effectiveness of the implemented internal controls. An auditor examines the subject systems, controls, processes and generates a report about the assurance status of the reviewed systems, controls and processes. Internal audit plays an important role in assessing internal controls for the organisation as well as compliance and assurance activities. IT auditing is a process that examines how well the organisation's information requirements and deliverables connect to the organistional mission, goals and objectives that is illustrated in Figure 2.14. The objectives are ensuring IT systems are protected and information is timely and reliable and any deviations from the organisation's defined policies and controls are detected and corrected in a timely fashion.

In sub-section 2.2.2.1, it has been highlighted that controls should be designed to achieve the organisation's objectives. While the technology role is a key enabler, it is important to emphasis that control should be primarily driven by business, rather than technical, requirements.

In sub-section 2.2.3 the IT auditor's role was examined and highlighted how it has evolved to advising management on matters related to IT governance, risk management, internal controls, and best practices. The auditor role's traditional aspect is of verifying internal controls and adherence to the organisation's policies. IT auditors must keep abreast and acquire more knowledge and practical experience in the noted aspects, in order for IT auditors to play effective role in providing the business with a reasonable assurance of its IT systems. In addition to the changing and evolving technologies that require IT auditors to acquire new knowledge to be able to determine the effectiveness of the conducted risk management activities.

Auditing of complex technologies comprises of various IT systems and communication protocols. For example different types of applications, networks and infrastructure. As security and privacy compliance have gained so much attention, in overall IT systems assurance, it is important for the IT auditor to understand security controls and measurement techniques to ensure adequate auditing of the implemented controls and processes. Figure 2.16 shows the IT audit process, which is required to be continually executed. Business context and the corresponding risk profile change, hence the IT audit process is executed to ensure the business and IT objectives are aligned and achieved.

In section 2.2.5 risk of IT audit is examined, and depicted in Figure 2.17, which is the likelihood of an IT auditor fails to uncover a material error. Audit risk is required to be assessed, evaluated and managed. As risk profile changes for the various reasons that have been discussed in a number of occasions in this research, the likelihood of IT audit risk to occur increases. It has been argued that establishing an assurance program based on recognised IT controls frameworks, best practice and standards that enables the organisation to follow a systematic way in auditing their IT systems, would improve the IT audit process quality. IT auditors face a daunting task in holistically assessing IT risks and evaluating existing controls effectiveness and reliability. IT controls should be tested and evaluated to ensure they remedy the associated risks. IT risks could be interdependent of each other; similarly, controls could be interdependent on other controls. IT controls could lead or trigger other controls, and often they are constructed in layers to ensure optimum coverage and controls risk is minimised.

### 2.5.3 Issues and Challenges in Frameworks, Standards and Best Practices

Organisations are required to respond to changes of the impacting factors in a timely fashion. That would deem necessary to re-work the risk assessment cycle, which is proved to be cost prohibitive in many occasions. It is a common scenario where risk profile is not current that could lead to organisations having a false sense of assurance about their IT systems readiness. With an invalid risk profile, the probability for the management to make ill-fated decisions would become very likely. To ensure their risk profile is up-to-date and they have the capacity to make informed decisions, many organisations have implemented forms of IT controls frameworks and best practices

To establish internal controls infrastructure where the IT is governed, IT risks are managed, and IT assets are secured, this allows the assurance division to perform IT audit reviews with ease and objectivity. A number of standards and methods have been published by reputed institutions, for example: COSO, ISACA, ISO, NIST, and IIA. Those standards and best practices give guidance on effective controls implementation and application. The explored number of standards, guidelines, best practices and frameworks represent a small portion of the real number of published materials. In addition, the explored recognised standards and frameworks have evolved and many of them have several versions that have been released to rectify a reported shortcoming or just an upgrade to provide coverage for new used technology.

Organisations, practitioners, and auditors, are obliged to invest in time and money to acquire adequate knowledge in the new releases of those frameworks and standards, to be able to comply with them, or at least to adopt what is applicable. It is a challenging undertaking, and could put off organisations as well as practitioners from benefiting from those frameworks and best practices.

### 2.5.4 Issues and Challenges in Forming Controls Configurations

To ensure IT risks are identified and managed adequately, organisations establish infrastructure of controls and processes to meet desirable objectives. IT controls are subject to change as their corresponding risks and business contexts change. IT controls must be tested and evaluated to ensure their effectiveness, reliability and efficiency are current. In addition, it is imperative to ensure those controls and are

communicated and adhered to by stakeholders. Organisations operate within a wider business environment, internal and external, as it was illustrated in Figure 2.20. Both environments aspects are dynamic and changing. It has been argued, that the level of complexity caused by a number of interrelating factors makes it difficult to analyse the environment for planning and managing purposes and to be able to manage associated risks of those changes.

Businesse management requires effective, efficient and timely risk assessment and subsequently identified risk is managed proportionally by reducing the negative side of the risk impact. While capitalising on the risk positive side, the corresponding opportunities. In addition, organisations are required to comply with various standards and regulatory requirements. Achieving compliance with standards and regulatory requirements requires periodic assessments of the internal controls, which leads to more efficient operations and better security. IT assurance function provides the business with a reasonable assurance through IT audit reviews performed by internal or external auditors, who review and assess existing controls' effectiveness, efficiency, and reliability, depending on the audit objectives. A number of auditing standards and guidelines have been produced to formalise and assess the auditing process to ensure methodical procedures are applied and adhered to by auditors, as outlined in section 2.3. Likewise, organisations specialized in IT audit, risk management, IT governance and security management, have produced IT related standards, frameworks and best practices to ensure relevant IT functions are performed, risks are managed and resources are adequately utilised. When the IT systems role evolves to be a business enabler it has become paramount to establish a controls based structured IT environment.

In sub-section 2.2.4.1 it has been outlined the importance of identifying the existing controls and their objectives. The point to highlight here is the daunting tasks an auditor faces to understand risks, identify existing controls and relevant regulatory requirements. In addition, IT auditors need to consider the effect of the evolving technologies and business dynamics, and the demand for value-adding audits. As controls could impact many risks at different levels and interact with other controls in various ways, this increases the complexity level of the context that an auditor is required to analyse, assess and evaluate. Controls designed as an integrated system a more efficient and effective. This is particularly so if the focus

is on value rather than just risk coverage. Figure 2.22 depicts a suggested system of intelligently constructed controls, where not all controls are active simultaneously, but rather, some controls would trigger other controls to operate within certain conditions. This is to ensure the efficiency of the implemented controls and processes. Hence, it could be inferred that some controls interact with each other in various ways, which necessitates taking into account the controls' interaction, when evaluating control's effectiveness and efficiency.

Control value can be assessed in terms of its cost and its effect on reducing the expected losses, which could be made by reducing the probability or the amount of the loss, should a risk materialise. As indicated earlier control evaluation is a complex task to perform. A control could correspond to one or more risks; in addition, some controls could collectively mitigate one or more risks.When auditors are able to identify risks and perform their audits focusing on high priority risks, the audit process quality improves. A quality audit adds value by performing risk-based audit, utilising resources efficiently, focusing on the more value-adding processes and protecting most valuable assets. It has been argued, in order to be able to identify risks from business point of view, a control based structured environment helps achieve that with less effort and better efficiency.

Establishing a controls-based structured environment via recognised frameworks, standards and best practices, albeit it comes at cost, but it provides a solution. However, even when a recognised framework is implemented an element of customisation is required to ensure the implemented controls and processes are adequate to the environment. In line with the view on utilising recognised controls frameworks, the fact that there is no single methodology or framework that comprehensively covers all required solutions, rather professionals consider, applying what is most needed and relevant to their business' context. Implementing recognised IT controls frameworks enable the management to fulfill legal and business obligations and requirements by ensuring their IT systems are reliable, effective and efficient. However, it has been argued that, implementing recognised frameworks, is not by simply 'cut and paste' any framework into their organisation. Frameworks should be selected, customised and adopted to add value by improving the subject processes, reducing cost, and eliminating duplication. It has also been argued that given the domain complexity of IT systems and its interwoven

relationship with business, no one framework suffices to establish a control based structured IT environment.

In section 2.3, a review of various internal control frameworks that have been developed for the enterprise level such as the COSO internal framework (COSO I), COSO-ERM (COSO II), and Basel II. Similarly, frameworks and best practices pertained to IT systems have been widely utilised by various sizes of organisations and in different industries, for example COBIT, ValIT, ISO 27001/2 and ITIL. Evidence obtained from various research studies indicates that many organisations opted not to fully implement those frameworks. Instead, a set of control objectives or processes were elected and implemented. This begs the need to establishing a systemic way of selecting controls and processes from various recognised frameworks, standards and best practices, when the risk profile changes.

While integrating various controls and processes frameworks seems a promising solution, however, that could increase the cost and the implementation complexity. Increasing the cost, could render the integration business prohibitive. While the implementation complexity, could lead to users rejecting the implemented controls.

Selected frameworks must be customised to the business and IT systems environment, along with the legal and regulatory requirements. The controls configuration should be constructed with sufficient agility in order to accommodate business dynamics and its agile environment. Frameworks customisation requires skilled practitioners who understand those frameworks and standards thoroughly, and have considerable experience in the subject business. Audit standards and guidelines provide a methodical way of conducting an effective audit process, but they do not answer the question of what best controls combinations an auditor should select. In addition, those standards and guidelines, do not offer guidance on how to assess and evaluate risks, nor take into account compound risks and risk interdependency.

Selecting best control configurations to facilitate IT assurance in order to ensure that IT risk is managed and value is obtained, faces many challenges. For example business dynamics, emerging technologies, and regulatory demands. On the other hand, implementing an integrated IT control framework faces many hurdles such as lack of top management sponsorship and lack of local expertise in

implementing these frameworks. Organisations are challenged by the need to realise the value from implementing resource-intensive and costly frameworks.

## 2.6 CONCLUSION

The reviewed literature has established the duality of risk and value that can be achieved through implementing cost-effective and reliable controls. To implement control environments, organisations must take risk when responding to strategic and operational demands. The risk must be managed to help organisations make informed and trustworthy decisions to ensure the return of business value. As IT systems underpin various business functions and processes at all levels, managing IT risk has become paramount to the business existence. Managing IT risk, however, should not be performed in isolation from managing the business risk. The effective and efficient IT risk management is achieved when IT risk is defined from the business perspectives. The IT risk management process is illustrated in Figure 2.1, and shows the elements of effective IT risk management.

In the following Chapter 3 the information and issues presented in this Chapter are analysed to identify key problem areas that can lead to research and knowledge growth for control environments. In Chapter 4 a research methodology will be defined to systematically select one researchable problem, the relevant questions and a way of researching the problem.

# Chapter 3

# Literature Analysis: Problem Scope

## 3.0 INTRODUCTION

Chapter 2 has identified key issues arising from the literature review focused on IT control environments. These issues suggest that there are underlying problems that worth investigating and addressing. The key issues are discussed in section 2.5. It was emphasised by Moeller (2011) that "Risk Management should be part of a decision-making process and be tailored in a systematic and structured manner" (p. 26). Furthermore, assurance is a professional service, is usually performed by IT auditors and assurance consultants. It is aimed at providing business with quality information that helps decision-making to be more effective and reliable (Hall & Singleton, 2005). Therefore, practitioners could play a crucial advising role to the management of an organisation for decision-making. IT auditors play a vital role in establishing an effective IT governance structure, controls and IS security, through various audit reviews (Senft & Gallegos, 2009; Hall & Singleton, 2005).

Auditors would utilise their judgment to determine the controls materiality, which is, according to Hall and Singleton (2005) in an IT environment, a difficult decision to make because of the technology complexity and sophisticated internal control structure. It is a common scenario where a risk profile is not current that leads to an organisation has a false sense of assurance of their IT systems readiness. With an out of date risk profile, the probability for the management to make ill-fated decisions becomes rather high. To ensure up-to-date risk profile and having the capability to make informed decisions, many organisations have implemented forms of IT controls frameworks and best practices. For example, Control Objectives for Information and related Technology (COBIT), Val IT, and the Microsoft Operations Framework (MOF) (Voon & Salido, 2009). In addition, known best practices like the IT Infrastructure Library (ITIL) have been adapted to complement the COBIT-Val IT control-based structure. In IT controls frameworks and best practices (COBIT, Val IT, ITIL) there are elements of risk management that either manage or contribute to managing risk in their respective areas. According to Keeny (1992, as cited in Mishra & Dhillon, 2008) "values are what

we care about and they should be the driving force for our decision making" (p. 3). Modern IT auditing is risk based. The objective of auditing is to act as a management means to measure and report identified risks, which allows the management to make an informed decision.

In this chapter the problems associated with IT control environments are identified in section 3.1. In section 3.2 a reasoned feasibility analysis is undertaken to select a researchable problem that is appropriate for the resources and scope of a PhD study. In section 3.3 Decision Support Systems are defined and in section 3.4 Game Theory is explored as a possible way for conceptualising events in IT controlled environments. Section 3.5 reviews specific research papers that provide insight into how to research the selected problem. Chapter 4 then specifies research questions and a methodology for doing the research.



## 3.1 PROBLEMS IDENTIFICATION

In Chapter 2, section 2.5 a number of issues and challenges have been highlighted as discussed in the respective four sections in Chapter 2. A number of researchable problems are going to be driven from the discussed issues and challenges. According to Creswell (2011) a researchable problem should introduce learning opportunities, either by confirming or refuting an existing, documented study. The author further adds that such a problem should contribute to the community of business and practitioners in the researched domain. This view is shared by Berndtsson et al. (2008) who also indicate that such a problem should have the potential to suggest alternatives for further research. According to Berndtsson et al. (2008) researchable problems "are of general interest, or which can be generalized or applied" (p. 30). Furthermore, while ensuring it takes ethical considerations a researchable problem should not be biased and have possible answers. A researchable problem must be: active, has an impact and no adequate solution is

available (Ellis & Levy, 2008). Similarly, Oates (2006) indicates what a potential researchable problem should be. It is to be driven from the requirement to add new knowledge and there has to be enough resources to research the problem within an allowed time frame. Considering what the aforementioned authors have argued the number of criteria a researchable problem should meet, the researcher has devised a list of criteria listed in Table 3.1, including their definition and justifications.

**Table 3.1: Criteria for Selecting Researchable Problems**

| Criterion | Description |
|---|---|
| Value adding | Solving the problem would add value, by a means of adding new knowledge or advancing existing knowledge. For example providing a new business model. |
| Generalisability | Outcomes of the research could potentially answer or aide in resolving relevant researchable problems. |
| Literature or research gap | There is a notable gap in the literature and/or it is not addressed sufficiently by the relevant literature. |
| Testable | Developed artefacts, resulting from researching the problem, are testable, and relevant data could be collected, to be able to provide validated outcomes. |
| Invite more research | Resulting outcomes provide directions for further research. |
| Ethical | Researching the problem does not violate any ethical aspects. |
| Researchable | It is possible to find an answer within a permissible time and resource requirement. |
| Clarity | The problem is clearly identified and an adequate statement is producible. |

Based on the issues outlined in Chapter 2, section 2.5, a number of researchable problems are identified and as listed below:

- High cost and complexity of integrating frameworks, standards and best practice.
- Subjectivity in evaluating assets values and associated risk which impacts selecting the adequate controls and their associated capability maturity levels.
- Complexity of implementing an effective and efficient IT assurance program in a changing context.
- Changes and new releases of standards, frameworks, and best practices.
- Lack of local expertise in implementing effective IT control-based structured environments.

- Demonstrating business value of governing IT in control-based structured environments through an assurance program.
- Selecting the best set of IT controls configurations in any situation for the highest business value outcomes**.**

This section elaborates on the seven problems in more detail in the respective sub-sections: 3.1.1-3.1.7.

### 3.1.1 Research Problem One

**High cost and complexity of integrating frameworks, standards and best practice**.

It has been argued that implementing a cost-effective IT control based structure, to manage IT risks and to capitalise on the opportunities, while it is rewarding, it is costly at the same time. It has also been argued that no one recognised framework or best practice provides a comprehensive structure from strategic to operational levels. Frameworks like COBIT and best practices like ITIL, while they provide some coverage to IS security aspects, but not to the extent that the ISO 27001 standard does. The wide range of IT risks necessitates the importance of integrating a number of recognised frameworks and best practices. Implementing an integrated framework of standards and best practices is a challenging task. If it is not planned and executed professionally, the new structure could complicate the environment and incur unnecessary cost. Furthermore, complexity could discourage operators from adhering to the devised controls and processes. That would defeat the purpose of establishing such a framework.

Frameworks, best practices and standards, are structured differently, in terms of the layers and grouping of controls and/or processes. Also the objectives of the controls and processes of one framework are not identically aligned with relevant ones in the other utilised frameworks. That causes overlaps among the implemented controls and processes. In turn, that incurs cost and adds to the complexity of the controls settings, and renders the framework to be business prohibitive. Furthermore, this could render the controls structure, very difficult and costly to maintain; should a need arise to re-assess and re-design the controls structure, when risk profile changes.

### 3.1.2 Research Problem Two

**Subjectivity in evaluating assets values and associated risk which impacts selecting the adequate controls and their associated capability maturity levels.**

In Chapter 2, section 2.1.2 explores various stages of the IT risk management process. When identifying asset value, it is imperative to identify the business value rather than the asset intrinsic value. However, this is not a straightforward exercise, as there is an expected percentage of uncertainty when applying a best-judgment and experience. Similarly, when analysing risk, starting with vulnerabilities and threats assessment, an element of subjectivity is present that would affect the overall risk assessment. The risk evaluation stage where qualitative, and/or quantitative approaches are utilised. The qualitative approach is common in evaluating IT risks, as it is easier to facilitate. However, it is subjective as there will be different views on the risk evaluation's attributes (Impact and Likelihood). Although risk management practitioners have advised a more granular qualitative approach based on estimation of likelihood and impact, however, the outcome remains subjective. In a business context, value propositions are demonstrated in monetary figures, leading to the question: how could qualitative risk be monitised?

The other alternative is quantifying IT risks. However, that proves to be a challenging task to accomplish. While some types of IT risks can be quantified, such as those related to software licenses or hardware assets, however, other types of IT risks are more difficult to quantify. Furthermore, as it was argued that risks impact business units or functions at various levels. Also it has been argued that risks have an interdependency on each other in their existing mesh, which compound the complexity when attempt to quantify IT risks.

### 3.1.3 Research Problem Three

**Complexity of implementing an effective and efficient IT assurance program in a changing context.**

In Chapter 2, sub-section 2.1.2 that explores risk management process and sub-section 2.2.4, which examines audit process. Various aspects were discussed outlining the challenges in conducting an effective and efficient risk based IT audit reviews. Audit reviews aim at achieving various objectives, among them ensuring alignment of business and IT objectives from strategic to operational levels.

Furthermore, compliance with business and regulatory requirements is another objective of adequate audit reviews. To ensure objectives are achieved, it is imperative to establish an effective assurance program, which would include a set of activities, like business continuity planning, and operational functions. For example, incident management, release and test management, security management, to name a few functions.

Implementing a current, effective, efficient and mature IT control-based structure, faces a number of challenges. The context of IT risk changes over time for a number of reasons. Business and regulatory requirements change and new technologies are introduced all requiring reassessment of the IT risk profile. As it was noted in section 2.2.4 that explores IT audit process, re-assessing risk should be done in a timely fashion to ensure an actual sense of assurance. Establishing IT risk management processes in control-based structured environments would generate new controls and processes. Evaluating existing controls for effectiveness, reliability and efficiency is a daunting task that IT auditors face. Controls and their cost-effective analysis are subject to the same subjectivity issue, which is also associated with IT risk assessment.

A key measure of the effectiveness of an IT controls infrastructure that is based on recognised frameworks is when risk awareness is embedded within the orgnisation's culture. Developing such a culture requires educating staff and management through a well-designed program undertaken by highly trained practitioners. Involving stakeholders through a series of workshops would help in that regard, although initially it would consume resources and time. IT auditors are required to have various skills to be able to play their vital consulting role to help organisations build an effective and value adding controls infrastructure. In addition, newly created controls and processes should be communicated to respective stakeholders through an effective training program and ensure they are adhered to. Inadequately implemented or poorly communicated controls and processes could be rejected by staff, which could cause delays and affect the outcomes quality.

### 3.1.4 Research Problem Four

**Changes and new releases of standards, frameworks, and best practices.**

Frameworks, standards and best practices are subject to change, for example ITIL v.2, v.3 and 2011 edition; Val IT v.1 and v.2; and COBIT, which has evolved from being an IT auditing framework to a governance framework. Furthermore, COBIT v.5.0, has been released in late 2012, which, according to the publishing authority, includes COBIT 4.1, Val IT v.2, and Risk IT. In similar fashion, the ISO 31000, and 27000 series were preceded by another set of guidelines and are constantly updated to reflect relevant changes in their domains. An established framework or compliance structure would certainly need to be updated to accommodate new changes. For example, when ISO 27001 was released it didn't contain controls for wireless or RFID devices. Organisations would have to find relevant controls from other sources to ensure their systems and processes are adequately controlled. Similarly, the Payment Card Industry (PCI) Security Standards Council released an information supplementary for wireless networks, which was added to the first edition of the PCI standard. Organisations now have to adopt the new amendments in order to retain their PCI compliance status.

Problem one, which is about the high cost and complexity of integrating frameworks, standards and best practice, is compounded by the changing nature of frameworks identified in Problem Four. When new frameworks versions are released, practitioners must stay abreast with those changes, to be able to accommodate those changes. That surely requires time and comes at cost, which business has to budget for.

## 3.15 Research Problem Five

**Lack of local expertise in implementing effective IT control-based structured environments.**

Recognised frameworks and best practices are not designed as a 'one size fits all'. Hence they require a level of customisation that suits each business context to achieve the desirable outcomes. Establishing a framework and adapting a set of standards and best practices, requires the availability of local expertise in those standards, frameworks and an understanding of the business context itself. In the absence of local expertise in those recognised frameworks, many organisations opt to use a third party to close that gap. However, that would increase the cost and the risk of lacking the knowledge of the local environment and business rules, resulting

in inadequate implementation of those frameworks. Developing internal capabilities to carry out such activities is costly in time and resources. Furthermore, the problem is compounded by staff turnover.

Implementing an integrated frameworks standards and best practices is a challenging task. If it is not planned and executed professionally, the new structure could complicate the environment and incur unnecessary cost or risk. That could also discourage stakeholders from adhering to the devised controls and processes, which could render the framework to be business prohibitive.

### 3.1.6 Research Problem Six

**Demonstrating business value of governing IT in control-based structured environments through an assurance program.**

As indicated in Problem 5, implementing a current, effective, efficient and mature IT controls infrastructure, comes at a cost. Demonstrating business value not only helps in gaining executive management support, but also helps in gaining staff's support and buy-in. The latter plays a vital role in embedding the risk management concepts and aspects into the organisation's culture, which is a key measure of the effectiveness of an IT risk management framework. Various business value perceptions for IT systems roles and IT risk management were explored in section 2.1.3, and 2.4.4. However, with different perceptions for business values such as tangible (financial) and intangible (reputational), demonstrating the business value remains a challenging task. How could a business realise the value of implementing risk based controls configurations that is integrated within the organisation's IT governance structure? When business value forms are identified, then measuring criteria could be modelled to help organisations realise the benefits and thence they could make informed decisions to seize opportunities as and when they arise. However, this seems to be one of the most challenging tasks that organisations and professionals face with because of the dynamic and complicated nature of the domain.

### 3.1.7 Research Problem Seven

**Selecting the best set of IT controls configurations in any situation for the highest business value outcomes.**

Problem seven (7) is about identifying the best set of controls configuration from a selected number of recognised controls frameworks, best practices and standards. Every aspect of business has elements of uncertainty; hence risk is inherent in business. Organisations must have the capability to seize opportunities when they arise, as it has been argued that to grow, organisations must take risk. In that view, risk represents value for business. Risk, however, needs to be analysed, identified, and managed to reduce its impact, which is the negative side of risk. The ever increasing of business reliance on IT systems and the parallel of the increasing complexity of utilised technologies have made it paramount for organisations to ensure the reliability of their IT systems.

One of the discussed challenges is demonstrating business value through managing IT risk. To facilitate that, implementing a risk-based IT assurance program through integrated control frameworks, best practice and standards, is required. The integration should generate best IT controls configurations that lead to establishing an effective and efficient risk based IT governance to gain the highest business value outcomes.

Finding the best set of controls from a myriad of recognised frameworks is a daunting task that entails a high percentage of uncertainty stemmed from various causes as discussed in Chapter 2, section 2.5. Furthermore, the cost in time and resources this type of exercise consumes makes it impractical to run as often as the risk profile changes. As a result, implemented controls and processes could render ineffective if not tested on a regular basis. Organisations would have a false sense of assurance, and their implemented controls become a liability for no return. Practitioners need a mechanism that allows them to re-assess the risk profile and the corresponding controls, timely, at a reasonable cost.

Researching this problem and finding a solution by building a model of controls-risks along with their cost and gained benefits to determine the best set of controls would enable practitioners to conduct this arduous exercise in a timely fashion. Furthermore, it would provide stakeholders a means to evaluate controls based on their associated risks as, and when, a risk profile changes. Which in turn leads to having a realistic sense of assurance of how trusted the IS environment is.

## 3.2 PROBLEMS SELECTION

The identification of problems arising from reviewing the relevant literature presents a challenge in itself. Not all problems are researchable and some problems are too costly or insignificant to pursue. In this section an evaluation and feasibility analysis of the seven problems listed in Table 3.2 are conducted to select the research focus problem. The selected problem that can be beneficial to research and attempt to solve for a better understanding of IT control environments. The resulting outcomes of researching the problem could benefit audience in academia as well as in business.

Sub-section 3.2.1 discusses the evaluation of the identified problems, while in sub-section 3.2.2 a discussion of the selected problem and a scoping of its potential researchable attributes is made.

### 3.2.1 Evaluation of the Problems

As noted in section 3.1 the introduction paragraph; researchable problems should meet certain criteria which are listed in Table 3.1. Identified problems as tabulated in Table 3.2, for a quick reference, will be evaluated against those criteria to determine the focus problem of this research.

**Table 3.2: Summary of the Identified Problems**

| Problem No. | Description |
|---|---|
| 1. | High cost and complexity of integrating frameworks, standards and best practice. |
| 2. | Subjectivity in evaluating assets values and associated risk which impacts selecting the adequate controls and their associated capability maturity levels. |
| 3. | Complexity of implementing an effective and efficient IT assurance program in a changing context. |
| 4. | Changes and new releases of standards, frameworks, and best practices. |
| 5. | Lack of local expertise in implementing effective IT control-based structured environments |
| 6. | Demonstrating business value of governing IT in control-based structured environments through an assurance program. |
| 7. | Selecting the best set of IT controls configurations in any situation for the highest business value outcomes. |

Despite the fact that the evaluation criteria have been identified, however, it is anticipated that the identified problems have to meet the listed criteria to various degrees. To evaluate those problems, objectively, it is imperative to measure them against a defined scale or scoring system. According to Flynn and Goldsmith (1999) who argued that, to evaluate consumer behavior, it is imperative to evaluate consumer subjective knowledge. Flynn and Goldsmith claim that they have developed and validated a short but reliable self-report measure of subjective knowledge that is applicable to various data collection methods. While the intention is not to explore that self-report measure, but rather, to emphasise the significance of objectivity of measuring subjective knowledge. According to Robinson, Shaver and Wrightsman (1991) it is imperative to define a scale for selection and evaluation to ensure reliable and consistent outcomes. The National Institute of Health (NIH), in the US ("Scoring Guidance", 2016) designed a scoring system to evaluate applications in a health system, to ensure objective evaluation. Consequently, reviewers would be able to identify and communicate the scientific impact of their evaluation. According to NIH, the scoring system uses a 9-point rating (1= Exceptional; 9= Poor) for overall Impact and Criterion Strength scores (High, Medium and Low) for all applications, as depicted in Table 3.3.

**Table 3.3: NIH Evaluation Scoring System ("Scoring Guidance", 2016)**

| Overall Impact or Criterion Strength | Score | Descriptor | Description |
|---|---|---|---|
| High | 1 | Exceptional | Exceptionally strong with essentially no weakness. |
| | 2 | Outstanding | Extremely strong with negligible weaknesses. |
| | 3 | Excellent | Very strong with only some minor weaknesses. |
| Medium | 4 | Very Good | Strong but with numerous minor weaknesses. |
| | 5 | Good | Strong but with at least one moderate weakness. |
| | 6 | Satisfactory | Some strengths but also some moderate weaknesses. |
| Low | 7 | Fair | Some strengths but with at least one major weakness. |
| | 8 | Marginal | A few strengths and a few major weaknesses |
| | 9 | Poor | Very few strengths and numerous major weaknesses. |

For the purpose of the doctoral research in this thesis, the researcher chose to adopt the NIH scoring system to evaluate the identified problems. The overall rating scale of (High, Medium and Low) will be used to denote the compliance degree of those problems with the evaluation criteria listed in Table 3.1. For each of the seven problems a table is created outlining the compliance rating and the rationale for the scoring.

**Table 3.4: Problem 1 Evaluation**

| **1- High cost and complexity of integrating IT frameworks, standards and best practice.** | | |
|---|---|---|
| **Criterion** | **Compliance Rating** | **Rationale** |
| Value adding | High | Finding out how to manage the cost and increase the understanding of how to integrate various IT controls frameworks, would aid researchers and practitioners facilitate the implementation of those frameworks |
| Generalisability | Low | Finding of researching this problem would be of low relevance to the other identified problems. |
| Literature or research gap | High | The importance of integrating frameworks has been observed and reported in the literature, however, few publications are available. |
| Testable | Low | To test this kind of problem, it requires empirical data from real-world cases, which is hard to find. |
| Invite more research | High | Adding new or extending the existing knowledge, would enable researchers to utilise the findings and do further research. |
| Ethical | High | No ethical issues could be caused by resolving this problem. |
| Researchable | Medium | The problem needs to be broken into sub-problems so it can be managed within the allowed time for the research. |
| Clarity | High | The problem statement is clearly articulated. |

**Table 3.5: Problem 2 Evaluation**

| **2- Subjectivity in evaluating assets values and associated risk which impacts selecting the adequate controls and their associated capability maturity levels.** | | |
|---|---|---|
| **Criterion** | **Compliance Rating** | **Rationale** |
| Value adding | High | Reducing subjectivity in assessing IT risk or mitigate that in practical terms would have a great value in finding the true impact of |

| 2- Subjectivity in evaluating assets values and associated risk which impacts selecting the adequate controls and their associated capability maturity levels. | | |
|---|---|---|
| **Criterion** | **Compliance Rating** | **Rationale** |
| | | defined risk, leading into selecting more adequate mitigating measures. |
| Generalisability | Medium | Resulting outcomes of researching this problem would contribute to researching problem 1, 6 and 7. |
| Literature or research gap | Medium | A noted gap in the published literature, however, published research is more on non–IT risk, for example finance, and insurance. |
| Testable | Low | As in the first problem, empirical data is required to test and validate any proposed model theorized, which would be hard to obtain. |
| Invite more research | Medium | If testing this problem proved to be feasible, then its findings could lead to further research. |
| Ethical | High | No issues with ethical aspects. |
| Researchable | Medium | Some of IT risks could be quantified, to reduce the subjectivity, but it is hard to generalise across other IT risks, however, reducing subjectivity of some IT risks still viable, but it requires time to achieve. |
| Clarity | High | The statement is clearly articulated. |

**Table 3.6: Problem 3 Evaluation**

| 3- Complexity of implementing an effective and efficient IT assurance program in a changing context. | | |
|---|---|---|
| **Criterion** | **Compliance Rating** | **Rationale** |
| Value adding | High | Understanding the aspects of establishing effective assurance program, would certainly add a great value to wherever IT systems are deployed, in every aspects of life. |
| Generalisability | Medium | Finding answers to this problem, could contribute to problems 1, and 6, but not so much for the other identified problems. |
| Literature or research gap | High | Establishing an effective assurance program is identified as a challenging issue and relevant research is scarce. |
| Testable | Medium | Empirical data could be obtained by conducting a case study, however, the challenge would be in finding a real-world case. Only corporate business would establish such an assurance program. |

| 3- Complexity of implementing an effective and efficient IT assurance program in a changing context. | | |
|---|---|---|
| **Criterion** | **Compliance Rating** | **Rationale** |
| Invite more research | Medium | The outcomes of researching this problem would possibly provide opportunity for further research. |
| Ethical | High | No issues with ethical aspects. |
| Researchable | Medium | It is viable, but requires a longitude case study to arrive at the most valuable findings. |
| Clarity | High | The statement is clearly articulated. |

**Table 3.7: Problem 4 Evaluation**

| 4- Changes and new releases of standards, frameworks, and best practices. | | |
|---|---|---|
| **Criterion** | **Compliance Rating** | **Rationale** |
| Value adding | High | New frameworks and standards are continually produced; existing ones are updated regularly to accommodate new technology, changes. Researching this problem, would provide a great value. |
| Generalisability | Medium | Findings of researching this problem, could contribute to problem 1, 3 and 7. |
| Literature or research gap | High | In similar fashion to the other problems, a noted gap in the literature is identified. |
| Testable | Low | It is a bit challenging to obtain empirical data for this kind of problem, which would hinder testing and evaluating any theorized model. |
| Invite more research | High | Findings would highly encourage more research. |
| Ethical | Medium | No issues with ethical aspects. |
| Researchable | Medium | To some extent, if the problem focuses on one standard or framework, for example, ISO 27001/2 from edition 2005 to 2013, or COIBT 3, 4.0, 4.1 and 5.0, but it would be a bit challenging to extend that to other frameworks or best practice, like ITIL, TOGAF, SABAS, as those have different architecture. |
| Clarity | High | The statement is clearly articulated. |

**Table 3.8: Problem 5 Evaluation**

| 5- Lack of local expertise in implementing effective IT control-based structured environments. | | |
|---|---|---|
| **Criterion** | **Compliance Rating** | **Rationale** |
| Value adding | Medium | Some value will be gained from researching this problem. |

| 5- Lack of local expertise in implementing effective IT control-based structured environments. | | |
|---|---|---|
| **Criterion** | **Compliance Rating** | **Rationale** |
| Generalisability | Low | Findings of researching this problem, would not contribute much to the other listed problems. |
| Literature or research gap | High | Yes, a noted gap is in the literature. |
| Testable | Medium | Case studies could be conducted to obtain firsthand data. |
| Invite more research | Medium | Yes |
| Ethical | High | No issues with ethical aspects. |
| Researchable | Medium | Yes |
| Clarity | Medium | The statement is clearly articulated. |

**Table 3.9: Problem 6 Evaluation**

| 6- Demonstrating business value of governing IT in control-based structured environments through an assurance program. | | |
|---|---|---|
| **Criterion** | **Compliance Rating** | **Rationale** |
| Value adding | High | Identifying business value is a very challenging task to achieve. Many stakeholders would benefit from the outcome of resolving such a problem. |
| Generalisability | Medium | This problem would contribute immensely to resolving problem 1, 3 and 7. |
| Literature or research gap | High | A noticeable gap in the literature and it is very scarce with little conducted and published research in this area. |
| Testable | Low | It is very challenging to obtain real-world data. |
| Invite more research | High | Any attempts to do research demonstrating the value of governing IT in a controlled environment, would surely pave the way for further research. |
| Ethical | High | No issues with ethical aspects. |
| Researchable | Low | This problem must be divided in two sub-problems, each conducted in a sequential manner. |
| Clarity | High | The statement is clearly articulated. |

**Table 3.10: Problem 7 Evaluation**

| **7- Selecting the best set of IT controls configurations in any situation for the highest business value outcomes.** | | |
|---|---|---|
| **Criterion** | **Compliance Rating** | **Rationale** |
| Value adding | High | Without a doubt this problem would add and/or expand existing knowledge. |
| Generalisability | High | Finding validated outcomes to this problem would contribute to the other defined problems, as it would reduce the cost and complexity noted in problem 1, as well as problem 3, as it facilitates combining controls and processes from different frameworks. As for problem 5 and 6, finding answers to problem 7, would reduce the impact of the underline causes of those problems. In Problem 2, the subjectivity would remain an issue, but finding the answer to problem 7, would help manage the impact to an acceptable level. |
| Literature or research gap | High | It has been highlighted in the literature, that no one framework provides a comprehensive coverage for all IT areas, governance, risk, security and operations management. Including bridging business with IT objectives at strategic and operational levels, has scarce relevant publications. |
| Testable | High | Many organisations have implemented many frameworks, in addition, many practitioners have accumulated wealth of knowledge and work experience in implementing various frameworks and standards, so that the theorized aspects could be put to test and practical data obtained for analysis. |
| Invite more research | High | Researching this problem methodically, and if communicated adequately, would certainly provide a ground for further research. |
| Ethical | High | No issues with ethical aspects. |
| Researchable | High | The problem could be researched in a systematic way, however, a balance should be maintained between theorising a model and testing and validating the proposed theory. |
| Clarity | High | The statement is clearly articulated. |

In summary, it has been argued that implementing a control-structured environment based on recognised controls frameworks, best practices and standards, potentially provides a solution to the other identified problems, by managing IT risk

holistically. While this approach has its benefits, but it also entails many challenges, as outlined in the problems (1), (2) and (3). Furthermore problems (4) and (5) outline the other challenges when the selected recognised frameworks change, requires developing adequate in-house sets of capabilities. Subsequently, organisations are able to customise and apply those newly released controls in a most cost-effective fashion. On the other hand problem (6) pinpoints the challenge of demonstrating business value out of applying the costly recognised frameworks and best practices. While enduring all the cost of developing in-house capabilities and conducting the resource intense exercises to re-assess the risk profile and verifying effectiveness of the associated controls and processes.

The evaluation of the identified problems is shown in their respective tables. Evidently, problem 7, is the focus of this research as it scores the highest in the defined evaluation criteria. Table 3.11 summarises the problems compliance ratings. In the section that follows, the research problem 7 is further discussed justifying the selection to be the research focus problem.

**Table 3.11: Summary of Problems Evaluation**

| Criterion | Compliance Rating | | | | | | |
|---|---|---|---|---|---|---|---|
| | P1 | P2 | P3 | P4 | P5 | P6 | P7 |
| **Value adding** | High | High | High | High | Medium | High | High |
| **Generalisability** | Low | Medium | Medium | Medium | Low | Medium | High |
| **Literature or research gap** | High | Medium | High | High | High | High | High |
| **Testable** | Low | Low | Medium | Low | Medium | Low | High |
| **Invite more research** | High | Medium | Medium | High | Medium | High | High |
| **Ethical** | High | High | High | Medium | High | High | High |
| **Researchable** | Medium | Medium | Medium | Medium | Medium | Low | High |
| **Clarity** | High | High | High | High | Medium | High | High |

### 3.2.2 The Focus Problem

The focus of the doctoral research in this thesis sits around problem no. 7 with the challenge of identifying the best set of controls configurations from a selected

number of recognised controls frameworks, best practices and standards. Researching this problem and attempting to find a solution by identifying associated risks and corresponding controls will provide practitioners a useful means to evaluate controls based on their associated risks and cost-benefit analysis. Implementing a cost-effective IT controls infrastructure, to manage IT risks and capitalise on opportunities, is rewarding and costly at the same time. It has been indicated that establishing an effective IT risk management process that encompasses the whole organisation, is an extensive time-consuming, costly and a challenging undertaking (see Chapter 2, section 2.2). It has been argued that managing IT risk in a holistic approach provides a solution to this issue. To ensure the holistic approach is applied, some recognised control frameworks, best practices and standards could be implemented and adapted. While this approach has some challenges, it also leverages activities performed for other processes. Additionally, this approach ensures managing IT risk is done in a timely manner and not in isolation from the rest of the business risks.

It was indicated that establishing IT controls infrastructure based on integrated recognised frameworks is rewarding, but requires a pragmatic approach by selecting controls and processes cost-effectively. Selecting an optimum set of control configurations based on cost effective analysis of the high risk/value assets/processes helps organisations realise business value of governing IT in control-based structured environments through an assurance program.

*How could organisations benefit from implementing IT controls infrastructure that meets business objectives and comply with its requirements?* When business value perceptions are identified, measuring means can be modelled that could help organisations realise the benefits and thence make informed decisions. In addition, the necessity of articulating the gained business value from implementing the framework remains high and it plays a vital role in earning top management support.

When problem (7) aspects are researched and resolved, the findings would pave the way to solve problems (1) and (3) by implementing an effective IS assurance program through integrated recognised IT controls frameworks. As with the problem of subjectivity in assessing the risk outlined in problem (2), being able to find the best controls configuration would reduce the impact of the uncertainty

in assessing the risk and associated controls; which is achieved by providing a persistent way in evaluating the identified risks. Similarly, when best controls configurations selection criteria are identified, the challenges noted in problem (4) are addressed when new frameworks' versions are released. Lastly, reviewing and verifying the effectiveness and efficiency of existing controls and processes, would enable the organisation develop a mature environment from a CMMI perspective. Which would enable the organsiation to measure and realise the value from implementing IS assurance program, which was discussed in problem (6).

A defined process ensures selecting the best set of controls, is based on analysing the associated risks; taking into account the cost of risks and the implementation of the controls and processes. This would facilitate achieving the desired objectives within a manageable cost and time. It would also provide a means where knowledge and expertise of experienced practitioners are captured in a knowledgebase. Which can benefit less experienced and/or novice practitioners. Furthermore, such a knowledge base could be used by a third party. For example, external auditors and consultants that many organisations resort to, to overcome the issue noted in problem (5). Which is regarding the lack of local expertise to review and verify the effectiveness of existing controls and processes.

In Chapter 2, sections 2.5, discussed the importance of identifying best controls configurations that generates the best business value outcomes in managing IT risk, also noted the difficulties and challenges of the implementation. Research about integrating recognised IT control frameworks and best practices in relation to business-IT value is scarce. Moreover, described by researchers as either limited or lacking empirical data. Reputed researchers have chosen field work to gather practitioners' perception in order to analyse and obtain factual data to bridge the gaps in this domain. The researcher is persuaded to research this problem and present the findings to contribute to this part of the academic literature and to further ongoing research. Outcomes of this research would benefit organisations and practitioners in applying guidelines to enable businesses realise high business value outcomes.

## 3.3 DECISION SUPPORT SYSTEMS (DSS)

To secure IT assets that enable various business processes and functions to produce anticipated outcomes, a risk based approach is being argued to determine cost-effective IT controls and processes. Practitioners face a daunting task to undertake challenging activities to ensure quality outcomes of the assurance process, by finding a best set of controls to manage the continually changing risk profile. To aid practitioners, and ultimately the business, achieve their objectives, a decision support system is typically required. The decision system facilitates the selection process of the best set of controls and processes from recognised IT controls frameworks, best practices and standards.

This section is structured as follows: the sub-section 3.3.1 outlines the DSS concepts and types that relate to the research. In sub-section 3.3.2 the DSS phases are discussed, while in sub-section 3.3.3 the DSS architecture is outlined. Lastly, sub-section 3.3.4 discusses the DSS development.

### 3.3.1 DSS

Successful business management depends on quality performance of managerial functions such as planning, organising, directing and controlling (Turban & Aronson, 2001; El-Najdawi & Stylianou, 1993). Furthermore, managers, have considered, for years, that management is a pure art, and a talent acquired throughout years of work experience. This approach is based, often on “creativity, judgment, intuition and experience rather than on systematic quantitative methods grounded in a scientific approach” (Turban & Aronson, 2001, p. 6). In the current business environment, business, technology, regulatory requirements are rapidly changing and increasing in complexity. This dynamic environment requires adequate and equally complex decision making systems that are capable of correlating various variables and impacting factors and producing adequate decisions in timely fashion. Senior management and their staff need to monitor, digest, and understand a volume of data. Hence a Decision Support Systems (DSS), which is classified as a class of information systems that support organisations, professionals, in decision-making process is a logical solution (King, 1992/1993). King states “This flood of data has heightened the desire for computerised

assistance with decision-making and problem-solving processes" (p. 137). Udo and Guimaraes (1994), as cited in Turban and Aronson (2001) outline the perceived benefits of DSS as "higher decision quality, improved communication, reduced cost, time savings, increased productivity and customer and employee satisfaction" (p. 14).

DSS first appeared in the 1970s, according to Sprague and Watson (1993); Turban and Aronson (2001), although it had been researched in academia in mid 1960s (Power, 2008). In addition, Sprague and McNurlin (1986/1993) indicate that DSS was both an evolution and a departure from previous types of computer support for decision making. For example, the management information systems (MIS), which provided scheduled report for predefined requirements. MIS employ mathematical models to better analyse and understand problems, but lacked, handling of data and use of analytic aids, or interaction between the user and the system (Sprague & McNurlin, 1986/1993). The DSS definition evolved to become, according to Sprague and Carlson (1980), as cited in Sprague (1980/1993): interactive computer based systems that help decision makers, confront ill-structured or semi-structured problems through direct interaction with data and analysis models. Sprague and Carlson emphasised that DSS must be comprised of three sets of capabilities: dialogue, data and modeling and that a balance should be struck among them to ensure most effective DSS (Turban & Watkins, 1986). Furthermore, according to El-Najdawi and Stylianou (1993), DSS emphsise flexibility and adaptability. The authors point out that "to qualify for help from DSS, a problem must have a quantifiable dimension that can provide criteria for evaluation of alternative solutions" (p. 56).

A number of limitations impact DSS, though. For example DSS are useful for managing a sub-set of all possible defined semi-structured problems. Moreover, the DSS role in the problem-solving process is limited to evaluation of possible alternatives (El-Najdawi & Stylianou, 1993). The authors further add that DSS do not relieve the user from making the actual decision. In addition, the structure of the problem and evaluation criteria should be defined by the 'user', the decision maker. Despite these attributes are described as limitations of DSS, however, reflecting on the research focus problem, which requires practitioners utilising their expertise in assessing the risks and devising adequate mitigating measures from the

IT controls frameworks. Also, as the business context and risk profile change for various reasons, experts would have to apply due diligence to select the best options from the viable alternatives. Therefore, the indicated DSS limitations are in fact advantages, and confirm that DSS have a great potential to solve the research problem.

Another form of computerised systems that aid in decision making is Expert Systems (ES). According to El-Najdawi and Stylianou (1993) who describe them as intelligent systems. Expert systems techniques can be utilised to preserve expertise to be used by various parties who do not possess that level of knowledge (Luconi, Malone & Scott Morton, 1986/1993; Turban & Watkins, 1986). Similarly, Turban and Aronson (2001) emphasise "that many unstructured and even semi-structured problems are so complex that they require expertise for their solution" (p. 107).

### 3.3.2 Decision Making Process Phases

Turban and Aronson (2001) state that there are three phases for decision-making process: Intelligence Phase, Design Phase and Choice Phase. The first phase identifies the goals and objectives of the process and impacting factors of the environment of the problem. While the design phase "involves finding or developing and anlysing possible courses of action. These include understanding the problem and testing solutions for feasibility" (Turban & Aronson, 2001, p. 45). Modelling is a method of analysing the influencing factors; fixed factors are called parameters, if they vary, they are called variables (Holsapple, 2008). Models can be normative or descriptive. According to Turban and Aronson (2001) the normative model examines all possible options to reach the optimal solution. Moreover, the descriptive model is extremely useful in DSS for investigating processing various configurations and the resulting consequences under different conditions. The analytic model attempts a set of alternatives but not all. Therefore, the solution is not guaranteed to be the optimal, rather is good enough or a satisfying solution. According to Simon (1977), as cited in Turban and Aronson (2001), organisations and individuals are often willing to accept a satisfactory solution. The common reasons for accepting satisfying system are: time pressure, as decisions may lose value over time. Also, feasibility in achieving an optimal solution in cost

effective manner (Turban & Aronson, 2001). The third phase of the decision-making process is the choice phase, where the actual decision is made and certain courses of actions are to be followed.

### 3.3.3 DSS and ES Architectures

There are many DSS architectures and types (Holsapple, 2008), however, the one of interest to this research is conceptually, could comprise of: the User who makes the decision; the Dialog between the user and the system; the Data that support the system, and the Model that provides the analysis capability (Watson & Sprague, 1992/1993). Figure 3.1 depicts the components defined by the noted authors.

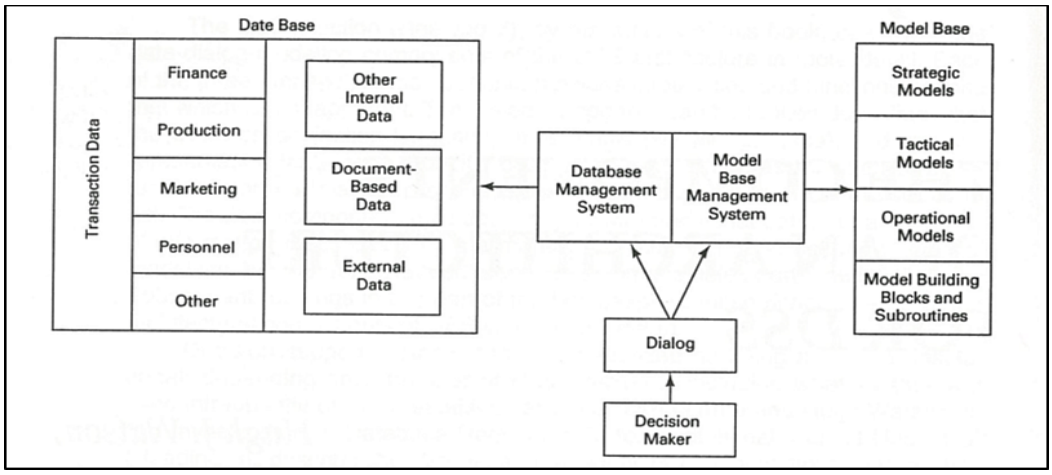


**Figure 3.1: The Components of a DSS (Watson & Sprague, 1992/1993, p. 100)**

The dialog acts as the interface between the system and the user, who inputs the requirements. The user could also feed some information, as the user's expertise in the domain along with the system's own data base, could be processed by the model. The dialog stage, presents the output to the user, who should understand and/or able to interpret the outcomes and act upon them. The Data source, as depicted in Figure 3.1, is becoming increasingly critical for the DSS. Furthermore, the concept requires expansion to Information base, rather than just data. In that view decision making process requires the input of a subject matter expert, for example IT auditors, Risk and Security professionals. Those professionals have the knowledge of the business as well as the IT systems they are reviewing and/or managing. They are also experienced in analysing the associated risks, and should be familiar with the IT controls, which they would require to implement to mitigate the defined risks. Reflecting on the subject domain of this research, the Data

component would include information about the applied recognised IT controls frameworks, risk evaluation and treatment options and returned value.

Lastly, the Model component, where a mathematical representation of the problem, and algorithmic processes are utilised to generate information for the decision making. Different types of models are employed in various ways, to accommodate the DSS purpose. The two main categories are optimisations or description. In the former, the model identifies the point of maximisation or minimization. For example: high risk, high value, minimum cost. A descriptive model on the other hand, describes the behavior of a system (Watson & Sprague, 1992/1993). It is imperative to highlight that Watson and Sprague point out that "nearly all systems are probabilistic. That is the behavior of the system cannot be predicted with certainty because of a degree of randomness is present" (p. 106). DSS could be constructed of several models, each representing a different part of the decision-making problem (King, 1992/1993; Turban & Aronson, 2001; Holsapple, 2008). As mentioned in the introductory paragraph that important attributes of DSS are to provide flexibility and adaptability. Which are crucial to enabling DSS to accommodate 'cognitive' and 'environment' variables (El-Najdawi & Stylianou, 1993).

Expert Systems (ES) have, "A unique feature of an expert system is its ability to reason (think)" (Turban & Aronson, 2001, p. 409). Beside the other components, the user interface, the data source and the model, ES conventionally comprise of a set of reasoning methods or an 'inference engine' according to Luconi et al. (1986/1993). Similarly, Turban and Aronson (2001) call it a 'control program'. An Inference engine utilises a stored knowledge base that could be constructed based on defined set of rules of type 'If ..Then..' scenarios to produce an outcome. A decision tree or semantic network is another method of constructing relational knowledge (Luconi, et al., 1986/1993; Turban & Aronson, 2001). The inference engine or control program directs the search through the knowledge base and decides which alternative to eliminate and which ones to favour. Table 3.12 summarises reasoning or inferencing methods. In that table, of interest to this discussion, is procedural (numeric) reasoning, where a mathematical model or simulation (model based or qualitative reasoning) is utilised. In a model based expert system, the reasoning process is based on a model of the objects in the

application and the specific operations that act on those objects (Wu, Hu & Ho, 1990).

**Table 3.12: Reasoning Methods (Turban & Aronson, 2001, p. 511)**

| *Method* | *Description* |
|---|---|
| Deductive reasoning | Move from a general principle to a specific inference. A general principle is composed of two or more premises. |
| Inductive reasoning | Move from some established facts to draw general conclusions. |
| **Analogical reasoning** | Derive an answer to a question by known analogy. It is a verbalization of internalized learning process (Owen, 1990). Use of similar past experiences. |
| Formal reasoning | Syntactic manipulation of a data structure to deduce new facts following prescribed rules of inferences (such as predicate calculus). |
| **Procedural (numeric) reasoning** | Use of mathematical models or simulation (such as model-based reasoning, qualitative reasoning, and **temporal reasoning,** or the ability to reason about the time relationships between events). |
| Metalevel reasoning | Knowledge about what is known (e.g., about the importance and relevance of certain facts and rules). |

Turban and Aronson (2001) indicate that "Model-based ES can overcome difficulties of rule-based ES" (p. 520). The authors further state that often model-based reasoning is combined with other forms of inferencing methods. An interesting attribute of a model-based ES is its 'transportability', where the knowledge of one expert could be made use of by other users of the system that do not possess the same expertise (Turban & Aronson, 2001; Luconi et al., 1986/1993).

### 3.3.4 Developing and Selecting a DSS

In order to develop a DSS, it is imperative to analyse the environment or the affecting factors of the decision making (Turban & Aronson, 2001). The authors further state "No decision is made in vacuum" (p.168). When developing DSS, it must be custom-designed, developed and implemented for each specific application/environment. Organisations don't have to build a mega-enterprise DSS, rather, initially, build small, specialised solution that resolves the pressing problem (Holsapple, 2008; Turban & Aronson 2001). Sometimes it is not possible or feasible to quantify the resulting value, so the developer relies on fuzzy and qualitative evaluation until hard facts become available. According to Turban and Aronson (2001) Evaluation is an integral part of DSS development process as it is the control mechanism for the entire iterative design process of DSS. The authors

outline that a prototype is ideally a small but usable system for decision maker. As the system evolves, it must be evaluated continuously. In addition, add the authors, most DSS are developed with the prototyping methodology, as it allows developers to get a partial but going system, relatively fast and at low cost. The system, through the iterative processes, evolves in complexity and encompassing more aspects of the domain subject to decision making. Reasons for prototyping: stakeholders are involved in every phase and iteration. Learning is integrated into the design process to devise a suitable system.

Turban and Aronson (2001), indicate that model based DSS uses mostly quantitative models, while Expert Systems use qualitative, knowledge based models in their applications, a view also noted by Turban and Watkins (1986; El-Najdawi & Stylianou, 1993). The determination of an optimal solution to a complex problem could not be possible considering the cost and time (Turban & Aronson, 2001). Hence, add the authors, under these conditions it is possible to obtain 'satisfactory' solutions in a more pragmatic approach using 'heuristics', to find out the best solution among a number of alternatives. However, the downside to this method is it could produce a poor solution. Models can be integrated with other models, and could also be multidimensional. In reflection on the research subject, a system could be developed where the knowledge of senior practitioners is captured, that could help novice practitioners in mitigating IT risks. Also, inexperienced users do not need to spend many years developing the required expertise to be able to select the best set of controls that returns the best value.

Expert systems are widely used by large and medium sized organisations as an important tool in decision making process to improve the quality and productivity, according to Turban and Watkins (1986; El-Najdawi & Stylianou, 1993). Turban and Watkins also indicate that expert systems are used in strategic decisions and business process reengineering.

El-Najdawi and Stylianou (1993), suggest that integrating DSS and ES to utilise the advantages of both systems, resulting into what the authors call Expert Support Systems (ESS). Sprague and Watson (1993) point out that ESS, while share with expert systems the use of the same technique, however, the former help 'people' solve a wider range or problems. Constructing expert support systems from expert systems is done by pairing the human with the expert system. While

the expert system provides the reasoning and some of the knowledge, the user provides an over-all problem solving direction. Users could lend their expertise in the field, when dealing with qualitative data and subjective interpretation is inevitable (Holsapple, 2008). The author suggests that expert support systems should be developed to support expert users rather than replacing them. They emphasise the importance of the scarce resources of talent and the expertise those users have that would enhance the decision making outcomes.

## 3.4 GAME THEORY

"Game theory is the study of how individuals interact in situations involving move and countermove in which the objective is mutually exclusive or mutually beneficial" (Webster, 2009, p. 2). Webster adds "Game theory is the study of strategic behaviour" (p. 2) and indicates that life is basically made up of actions and decisions that affect and are affected by others' decisions. Watson (2002) describes games "are formal descriptions of strategic settings", and further states that "game theory is a methodology of formally studying situations of interdependence. By 'formal; I mean a mathematically precise and logically consistent structure" (p. 5). Similarly, Bierman and Fernandez (1998) indicate that game theory is about players' decision-making knowing that their actions affect each other. For example, in a Chess game, players need to take into consideration past and expected opponent's moves (Webster, 2009). The author, further outlines that many think of a game as an activity where two or more players involved in a recreational activity like chess, or a sporting event like football, the objective is to win the game. This is a view shared by Bierman and Fernandez (1998); and (Watson, 2002). In addition, Webster (2009) also points out that in business, a winning party is the one that makes the biggest profit over their rivals. In that process, each party must take into account what the others will do (Gibbons, 1992).

While this review is not fully examining game theory, however, it explores some aspects of the game theory, leading to establishing the relevance of game theory and its application to this research. The sub-section is organised as follows: sub-section 3.4.1 outlines definitions and some examples, while sub-section 3.4.2 highlights game theory relevance to this research, and lastly, sub-section 3.4.3 discusses Model based DSS.

### 3.4.1 Short History, Definitions, Examples

As indicated at the beginning of this sub-section, that Game Theory is the study of strategic behaviour. Watson (2002) claims that hundreds of years ago, mathematicians began studying parlor games in an attempt to formulate optimal strategy, and further indicates, in 1713, James Waldegrave communicated a card game. Early analysis of strategic behavior may be attributed to Augustin Cournot (1838) according to Watson (2002). Webster (2009) indicates that, Cournot's work, five decades later, was modified by Joseph Bertrand (1883) who emphasised the role of strategic behaviour in pricing of products. Von Neumann and Oskar Morgenstern teamed up and capitalised on work done in early 1920s, and devised modern game theory in their 1944 work, *Theory of Games and Economic Behavior* (von Neumann & Morgenstern, 1944). Furthermore, mathematician John Forbes Nash, in his dissertation and several papers published in1950s, demonstrated that in non-cooperative games with a known outcome could have what he called a 'fixed point' equilibrium, which occurs, where a rational player adopts a strategy that would return the best outcome based on the expected best strategy a rival takes. Since the 1970s, game theory catapulted a revolution in economic thoughts, and in 1990s, its applications expanded to mobile telecommunications services (Webster, 2009).

The following definitions are adopted into this doctoral thesis:

**Strategic behavior**, according to Webster (2009) "Strategic behavior involves any situation in which the decision of competing individuals or groups are mutually interdependence." (pp. 2-8). In this context, the author adds, the decision-making process is mutually interdependent. Bierman and Fernandez (1998) point out that "This interdependency among decision makers is the essence of a game" (p. 3).

**Player,** a decision maker in a game

**Payoffs,** is the gain or loss to a player at the conclusion of a game; one payoff for each player (Bierman & Fernandez, 1998). Figure 3.2, shows numerals payoffs for each player in parentheses. Watson (2002) argues the importance of considering payoff uncertainty as players usually care about if they were exposed to risk.

**Simultaneous-move game** is a game in which players move at the same time, while, **Sequential-move game**, a game in which players take turns.

**Static game**, is a game in which the players are ignorant of their rivals' decisions until all moves have been made. A simultaneous-move game is an example of a static game; Gibbons (1992) gives a detailed example: a sealed-bid auction, where bidders have no idea what each other's bid, and they submit their bids simultaneously. Bierman and Fernandez (1998) point out that, in static games, players have no interest in players' future actions. In contrary, a **Dynamic (multistage) game** is the same thing as a sequential-move game. In this type of game, chronological time is quite important as future payoffs must be taken into account when choosing best strategy (Bierman & Fernandez, 1998). According to Gibbons (1992) in dynamic games, players would have perfect information of all the steps that have been taken thus far.

**One-time game** is a game that is played once, whereas, a **Repeated game** is a game that is played often.

**Rational behaviour,** when players try to optimise their payoffs

**Strategy**, is a decision rule that defines a player's moves. It is a complete description of a player's decisions and/or a contingent plan at each stage of a game.

**Strategy profile,** a list of strategies, one for each player, in text found in parentheses () or curly brackets {}, for example (Attack, Attack), {Silent, Confess}, (Bierman & Fernandez, 1998).

**Pure strategy** is a complete and nonrandom game plan, in comparison to a **Mixed strategy**, which is a game plan that involves randomly mixing pure strategies.

**Strictly dominant strategy** is a strategy that strictly dominates every other strategy. It is a strategy that results in the best payoff given the strategies adopted by the other players. According to Bierman and Fernandez (1998) a rational player will never adopt such a strategy nor expect a rational opponent to do so.

**Nash equilibrium**, when each player adopts a strategy that is the best response to the strategies adopted by the rivals. A strategy profile is a Nash equilibrium when no player can improve his or her payoff by switching strategies. It is named in the honor of John Forbes Nash Jr., who along with John Harsanyi and Reinhard Selten were awarded the 1994 Nobel Prize for their pioneering work in Game Theory (Bierman & Fernandez, 1998; Webster, 2009). According to Bierman and Fernandez (1998) the Nash equilibrium is considered a controversial solution for games, as it is often not unique. Bierman and Fernandez, claim that in

circumstances when there is more than one Nash equilibrium, it is difficult to predict the chosen strategy with complete information about the context, players, and domain.

**Strictly dominant strategy equilibrium** is a Nash equilibrium that results when each player has, and adopts, a strictly dominant strategy. While, a **Non-dominant strategy**, a strategy that is neither strictly nor weakly dominant. A player's best strategy depends on what he or she believes is the strategy adopted by a rival.

One of the most common games explored in almost every game-theory literature is the Prisoner's Dilemma (Gibbons, 1992; Bierman & Fernandez, 1998; Webster, 2009). This game is a two-player, non-cooperative, simultaneous-move, one time game. In this game both players have a strictly dominant strategy, which happens when the game results in the best payoff regardless of the other player's strategy.

| | | Suspect *B* | |
|---|---|---|---|
| | | *Silent* | *Confess* |
| **Suspect *A*** | *Silent* | (–½, –½) | (–10, 0) |
| | *Confess* | (0, –10) | **(–5, –5)** |

Payoffs in years: (Suspect *A*, Suspect *B*)

**Figure 3.2: Prisoner's Dilemma (Webster, 2009, p. 8)**

**Three-Player Games**; according to Webster (2009), increasing the number of players, increases, exponentially, the analyses difficulty. Webster adds, analysing more than three-player games requires advanced mathematics. Figure 3.3 exhibits a 3-Player static game. To determine, the best strategy players could have, it requires, normalisation, before solving the game.

Three-Player Static Oil-Drilling Game

| | | COEXCO | | | |
|---|---|---|---|---|---|
| | | *Narrow* | | *Wide* | |
| | | GLOMAR | | GLOMAR | |
| | | *Narrow* | *Wide* | *Narrow* | *Wide* |
| PETROX | *Narrow* | **(25, 25, 25)** | (**12**, 24, **12**) | (**12**, **12**, 24) | (**4**, 8, 8) |
| | *Wide* | (24, **12**, **12**) | (8, 8, **4**) | (8, **4**, 8) | (3, 3, 3) |

Payoffs: (PETROX, GLOMAR, COEXCO)

**Figure 3.3: Three-Player Static Game (Webster, 2009, p. 49)**

**Focal-Point Equilibrium,** Webster (2009) discusses the concept of focal-point equilibrium, in a coordination game, which would have a multiple Nash equilibrium strategy profiles, a view shared by Bierman and Fernandez (1998). Players' common background, shared culture, life experience, will contribute to their understanding of the circumstance. Which would therefore impact the strategies the players would adapt, this underlies the concept of a focal-point equilibrium add the authors. Furthermore, Webster (2009) examines this concept by analysing a cold war game, where superpowers would have to choose between First Strike or Second Strike strategy. The latter strategy is selected as the superpower would retaliate if attacked. However, if First Strike strategy is selected by either superpower would lead to retaliation by the other superpower, resulting in total annihilation of both superpowers. However, the author, emphsises, if cooperation is possible, it would be in the interest of both superpowers' interest to negotiate a treaty to retain their interest. Hence both parties would gain the best payoff out of this game. The author claims that even if cooperation is not viable, a common understanding of the problem, would lead to both sides selecting the strategy that would return the best payoff, which is the Nash equilibrium of the game. Webster (2009) states that "Rationality can be an important selection criterion when identifying a focal-point equilibrium" (p. 75).

**Issues with game theory:** Halpern (2008/2010) claims that game theory has focused on relatively small games, 2-3 player games, which are easy to describe, and analyse. As for a larger number of players' game, to resolve more practical problem, as Halpern (2008/2010) emphasises, it becomes imperative to find an efficient analytical method to describe, analyse and compute the various viable strategies.

**Role of Knowledge in Games;** Haprlen (2008/2010) points out to the importance of knowledge in games since Aumann's publication in 1976, which initiated a substantial work in attempt to understand and evaluate the role of knowledge in games.

**Cooperative Games;** Bowles and Gintis (2010) indicate that "Cooperation is said to occur when two or more individuals engage in joint actions that result in mutual benefits" (p. 66). The authors further give some examples for that, like mutually beneficial exchange of goods, taxes payment for public goods, and team

production. In this research, an analogy could be made to various IT controls and processes from different recognised IT controls frameworks to manage IT risks. Also capitalising on their positive side, while keeping their negative part within an acceptable level, and keeping IT risks within the risk appetite boundaries.

Cooperation in game theory has been developed in model based games (Shubik, 1959; Taylor, 1976; Axelrod & Hamilton, 1981, as cited in Bowles & Gintis, 2010). This is where a repeat of social interactions, could eventually lead to players adhering to social norms to avoid retaliation, reaching a Nash Equilibrium. Bowles and Gintis (2010) claim that when the model-game is repeated sufficiently, and players are sufficiently patient, a cooperative equilibrium can be reached and sustained. According to Watson (2002) business rivals would compete in various ways to outsmart each other and dominate their respective market. The author further indicates that in either form of interaction, players' behaviour affects each other, and the term interdependency applies. In addition, Watson (2002) further outlines that these scenarios of interdependence are called: Strategic, as one player's decision is formed considering the other player's action. However, the author indicates that not all the settings are, or could be considered as, non-cooperative. Watson (2002) argues that it is imperative to keep in mind that conflict and cooperation overlap. In addition, in social structures people interact constantly, in a cooperative way like business partners, successfully running their business affair. For example, two managers in a firm working on a new product, while their individual activities affects each other. In this situation, the setting involves an interdependence, however, there would not be a winner and a loser. They would cooperate to capitalise on each other's strategy to make the best outcomes for both.

### 3.4.2 Game Theory Relevance to the Research

Game theory has many applications in Economics, Insurance, and various other fields, even Politics. Furthermore, many researchers and practitioners in risk management and decision making established the relevance of game theory. This sub-section explores some of those instances, where a game theory model is built to help decide best strategy in managing risk, be it general risk or IT risk.

Rajbhandari and Snekkenes (2011) argue that obtaining probabilities in classic risk management approach in estimating risk is guessed, and no guarantees

on how accurate those probabilities are. On the other hand, they claim that applying game theory to "obtain representative data on how stakeholders assess the value of the outcomes of events/incidents" (p. 147) would render more actual probabilities, which would lead to devising more effective risk mitigation measures. As game theory based model is taking into considerations the players' incentives, underlying motives and other interaction behaviour aspects, game theory helps in exploring the behaviour of real-world adversaries (Rajbhandari & Snekkenes, 2011). In the same way, game theory can be utilised to improve antagonistic risk analyses.

Rajbhandari and Snekkenes reference QuERIES model, a quantitative cybersecurity risk assessment approach, using Game Theory for attack or protect modeling. Pang and Li (2013) outline the importance of integrating internal controls and risk management process within an enterprise, which has been argued in this literature review. Furthermore, the authors claim that utilising game theory in analysing the complex settings of incomplete contracts reduces the impact of uncertainty in managing property rights.

Cox (2009) raises a question of why not use game theory in analysing risk, and makes an analogy to managing terrorist's attacks as an attacker-defender game. In this model, Cox further elaborates: the defender first chooses and applies defending measures to protect key assets/potential targets. While the attacker, knowing what, to some extent, the defender has done, then decides which target is best to attack. Cox (2009) claims that "risk analysis and game theory are also deeply complementary" (p. 1062).

Aliahmadi, Sadjadi, and Jafari-Eskandari (2011) designed a three-player model to manage risks of design, construction and operation of a tunnel project. In their model the researchers, utilised cooperative-game concept in building an interactive decision making structure. In their model, three players represent: taskmasters, advisors and contractors. The aim is to strike a balance between the impacting factors in making decisions for selecting the best strategy to manage risks and to obtain the best possible outcome utilising the available resources. In this model, the Expert System concept are adapted to solicit experts' opinion on evaluating the risk and determining the best results in a collaborative fashion by applying the most effective mitigating measures.

### 3.4.3 Model Based DSS

From this brief review of game theory and its application in managing IT risk and deciding a best strategy to mitigate defined risks. An n-player model, can be envisaged, to determine the most cost effective way of managing the risks. In the model, each player represents one of the recognised IT control frameworks: COBIT, ITIL, ISO 27001, ValIT, RiskIT and so on, to select the best set of relevant controls and processes for risk mitigation. Controls and processes from those frameworks and best practices contribute to managing the identified IT risks aiming at reducing overlap whenever is possible. The aim is to produce the most effective and cost effective mitigating measures. The players would compete, based on their controls and processes' merits, to reach a strategy that would generate the best outcomes balancing cost vs benefits. The n-player setting is structured in a competitive game that resembles a model for an interactive DSS for decision making process.

The DSS outlined in the previous paragraph would enable experts like IT auditors, IT risk and security managers, utilise their expertise in the subject domain. Including business dynamics, assessing the ever changing risk profile, and the internal and external environments where an organisation operates. The experts are responsible for managing IT risk in general or specific security risks, via implementing various IT controls from recognised IT controls frameworks. The practitioners utilising their expertise and knowledge of the mentioned IT control frameworks, and of the subject domain to analyse the risk and estimate the cost vs benefits. Hence, experts play a crucial role in defining the payoffs of each possible decision or strategy in the game theory terminology. As outlined in the previous paragraph the best strategy would be calculated utilising a 3-player model built using the described game model. The resulting best strategy would comprise a set of various controls and processes relevant to the defined risks.

The interactive DSS and its game theory based model allows users to accumulate their knowledge of using the system iteratively. Should the risk profile change, then users would need to work out the payoff matrix again and feed that into the model. As argued previously, this accumulated experience could be used by other users who do not have the same level of knowledge, and use the system to work out the best control configurations in a timely fashion. Similarly, should any player, in this setting change when one of the recognised frameworks, is updated

or replaced. For example COIBT 4.1, to COIBT 5, and ITIL 3.0 to ITIL 2011 edition, then replacing the controls and processes should take far less effort to update the model. Furthermore, if the environment requires another framework to the game, for example, CoSo-ERM, ISO 31000. While it would initially require some preparation work for example identifying relevant controls and processes and the payoff matrix by some experts in those new frameworks. However, the system could be used by other practitioners with less effort.

Webster (2009) indicates that the complexity of analysing static games increases exponentially as the number of players increases. Furthermore, the author points out that analyising games with more than 3 players would require advanced mathematic techniques. However, that doesn't mean it is not possible to do so. So in this research a 3-player model is to be designed. The three players are: COIBT, ITIL, and ISO 27001. The selected recognised frameworks, best practices and standards will manage IT risks with the most cost effective controls configuration. It has been discussed and justified at length in Chapter 2, sub-section 2.4.3. Subsequent analysis, planning, and management decisions would be based on actual data rather than estimated data, which is a key to an effective IT risk management process (Whitman & Mattord, 2004).

## 3.5 REVIEWING RELEVANT RESEARCH

Various research projects are reviewed on utilising decision support systems DSS and game theory in developing an interactive DSS system, to enable stakeholders reach most cost-effective mitigation measures to manage identified risks. The research projects utilise various research methodologies, for example case studies, that involve using a software application used by practitioners. It also uses interviews and conducts surveys and collects documents to gather data; and, to test proposed hypotheses and/or to validate a proposed framework. The following three sub-sections review a selection of published papers. The aim is to analyse the selected paper and identify the research methods used by the contributing researchers, addressing similar research topics. The purpose is to find the analogies of research methodology, theory, solution approach and techniques that found applicable to this research.

### 3.5.1 Risk Management and Game Theoretical Approaches

Rajbhandari and Snekkenes (2011) presented a paper where they demonstrated applying game theory principles in managing IT risks. The authors argue that traditionally probabilities are used to work out the risk's impact and likelihood. However, the probability is not something practitioners are well acquainted with and "history may not be always be a very good teacher". On the contrary, "game theory puts emphasis on collecting representative data on how stakeholders assess the value of the outcome of incident scenarios" (p. 147). In their effort to demonstrate the point the authors map risk management processes described in ISO/IEC 27005 to corresponding game theory aspects. ISO/IEC 27005 standard was selected, among a number of similar standards: NIST 800-30, RiskIT and CORAS. The selection was justified by the authors, as this standard clearly articulates risk management process stages and terminologies. The authors indicate that while there are many published papers discussing application of game theory in various domains, but it is not known to the authors of any published work similar to their security risk paper.

The authors initially describe the classical risk management and indicate that it is based on a single player's perspective (individual, system, etc) when analysing risk. As in an example utilising Probabilistic Risk Analysis (PRA), people's action/reaction are not considered important. Furthermore, the authors argue that in the classical risk assessment approach is subjective, because estimating the probabilities values is either assumed or driven from historical data. A reference is made to incidents known as Black Swan, where predictions were not possible to obtain using historical data. On the other hand, in game theory, the authors claim, players' incentive is taken into account as it is important to understand their underlying motive of the players' action. A reference is made to an incentive-based modeling approach devised by Liu and Zang (2003, as cited in Rajbhandari & Snekkenes, 2011). Furthermore, a reference is made to the QuERIES model, which is a game theory based quantitative cyber-security risk assessment approach, for constructing and evaluating attack/protect models.

The authors proceed and highlight the outcomes of a top level comparison between the two approaches. Figure 3.4 depicts, on the left side, the steps of risk management process according to ISO/IEC 2005, while the right side outlines the

game theoretical steps. As it has been discussed in Chapter 2, sub-section 2.1.2, the risk management process stages are iterated until satisfactory results are obtained. Furthermore, the process is triggered all over again, when the underlying risk factors change. Similarly, game theoretical steps are performed by the respective player/s for the same purpose until desirable objectives are achieved.

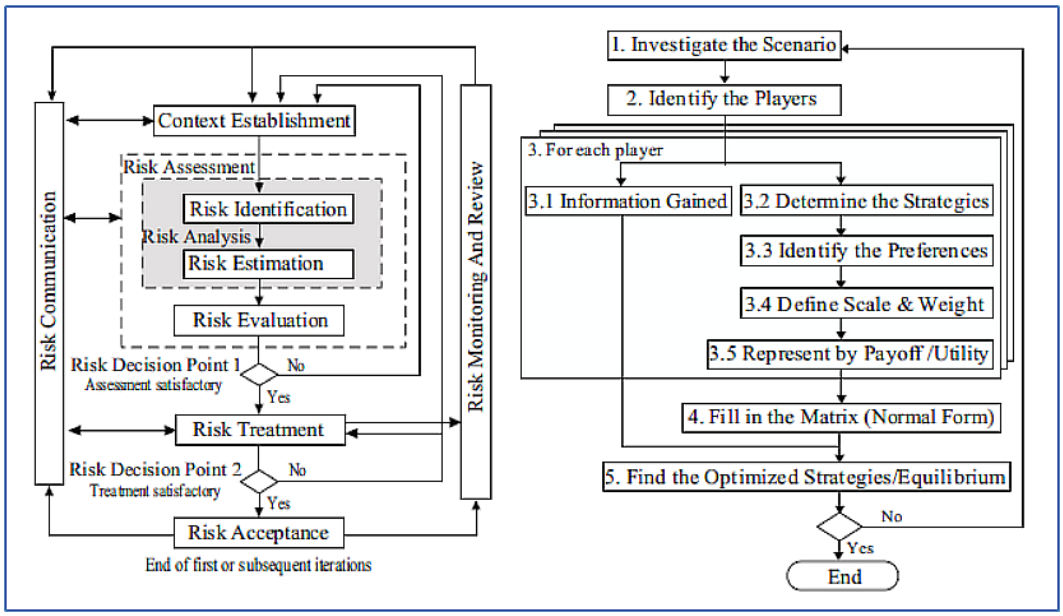


**Figure 3.4: ISM Process Mapping to Game Theoretical Steps (Rajbhandari & Snekkenes, 2011, p. 149)**

The authors further elaborate on the game theoretical steps and outline in detail the inputs, the process step details and the output, as illustrated in Figure 3.5. It shows the conventional risk management process steps of defining risk context, identifying vulnerabilities/threats as well as game theory aspects in utilising players' knowledge and expertise of the subject. The Figure also outlines the players' ability in determining the strategies and corresponding payoffs, resulting in a matrix of; Players, Strategies, Payoffs/Utilities, taking into account the players' preferences and evaluation of scale and weight of those aspects.

In conclusion the authors point out the benefits of utilising game theory for risk management as follows:

- The quality of collected data is likely to be better, as no actuarial data is required.
- Players' incentives, capabilities and experience are made use of, rather than asking an expert for historically based probabilities.

- Experts' judgment on collected data can be further validated and audited, to identify what information was available.

Despite the listed above benefits, the game theory based approach has some limitations that relate to the players' knowledge level and their personal traits and the overall uncertainty of the expected outcomes.

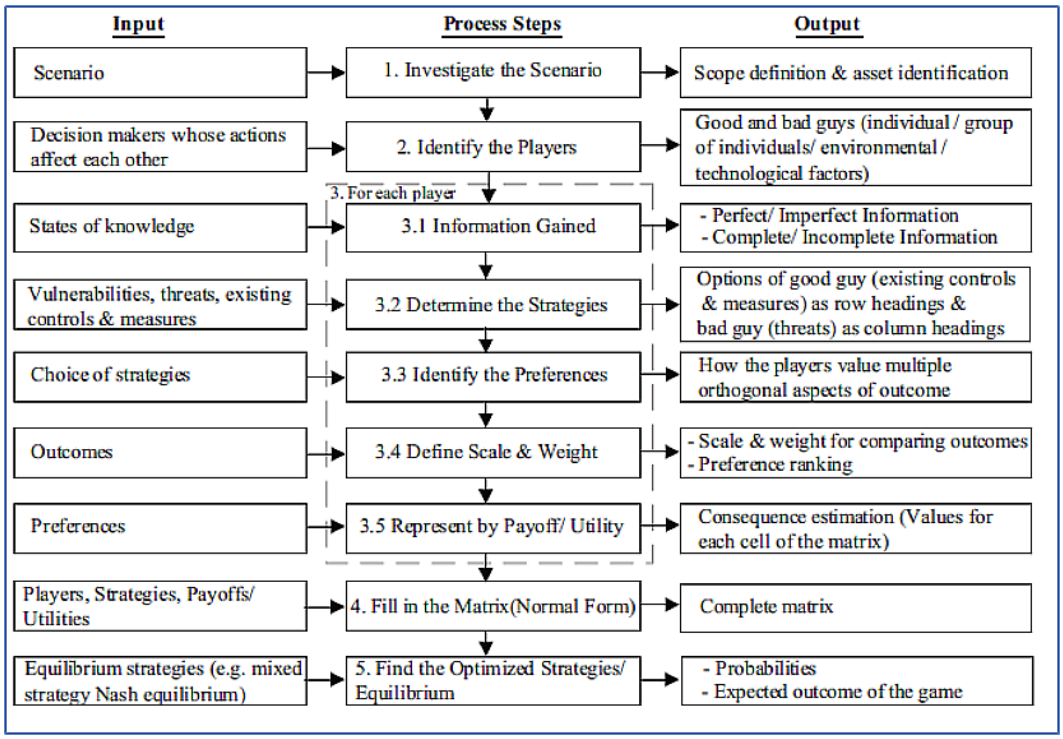


**Figure 3.5: I/O for Game Theoretical Steps (Rajbhandari & Snekkenes, 2011, p. 150)**

### 3.5.2 Expert Decision Making Design Using Game Theory

A case study conducted by Aliahmadi et al. (2011) detailed what the authors developed an interactive expert DSS using game theory and fuzzy logic. The system is to manage risks in design, construction and operation of a tunnel project. The proposed game theory model is constructed of a 3-player cooperative game integrated with an interactive fuzzy analytical hierarchy process. The designed system is used to balance actions and a selected strategy for each player, according to the authors. The authors further point out that that settings result in a collaborative strategy with the best payoffs for all stakeholders. Figure 3.6 depicts the 3-palyer model along with fuzzy logic based DSS.

Aliahmadi et al. (2011) initially explore traditional decision making issues caused by various reasons, for example: complexity of environment, conflicting

systems of logic, uncertainty and imprecise knowledge. With regards to the complexity, the authors indicate the various types of risks (tendering, the contract negotiation, construction, strategic options and strategic decisions) in the tunnel project that could potentially exist at its various stages.

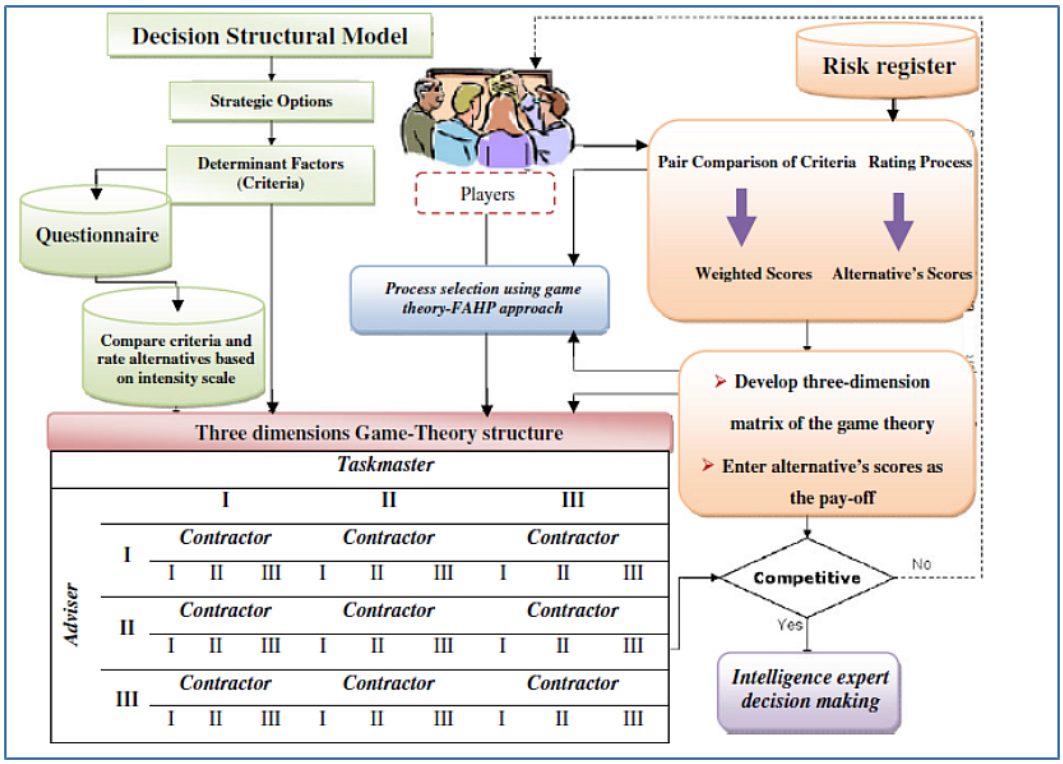


**Figure 3.6: Fuzzy DSS in Risk Management Using Game Theory and Fuzzy Logic (Aliahmadi et al., 2011, p. 795)**

To manage those risks, a number of managers with specific set of skills are assigned to manage those risks. The focus of the authors is to aid the three players: Taskmaster, Advisor, and Contractor, to comprehensively manage the potential risks at each stage. A survey of managing such risks in a traditional way revealed that risk assessment is conducted in two phases. The first is evaluating the risk, where the likelihood and impact are quantified utilising the expert's judgment and knowledge of the risk factors and the subject domain. The first phase results in a number of strategic plans. In the second phase the aim is to identify the strategy plan with the best outcomes, in a collaborative game setting. In collaborative games, players would need to communicate with each other and repeat the game time and again to arrive at the best strategy, state Aliahmadi et al. (2011). The results of risks assessment and evaluation, along with the outcomes of tenders' evaluation where project risks and cost are taken into account, are passed to the decision makers in tabulation form of total estimated risks cost of each tender. From

previous project's reports, the authors further derive possible Threats (T1-T5) and Opportunities (O1-O5) along with their Extent (Impact) and Probability of occurrence (Likelihood) as shown in Figure 3.7. The evaluation of those threats and opportunities outlines the risk space of the project.

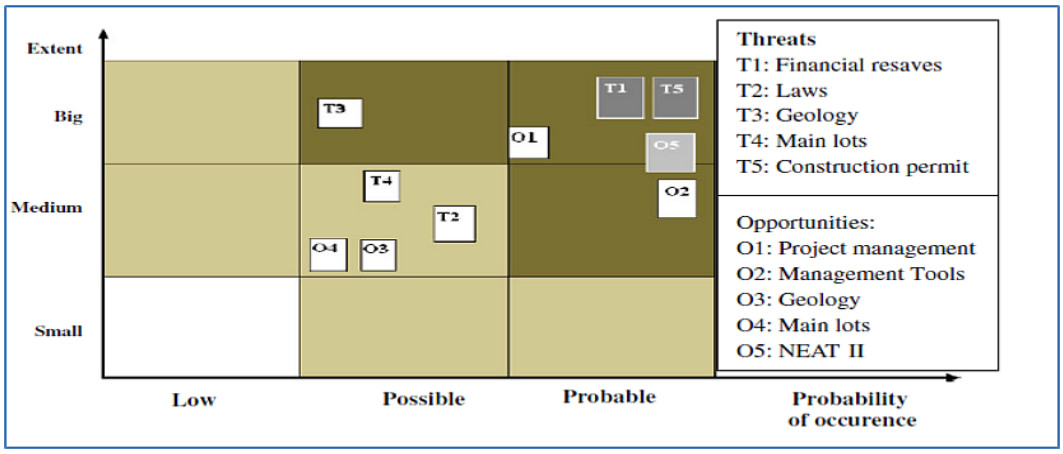


**Figure 3.7: Risk Situation in the Overall Project (Aliahmadi et al., 2011, p. 792)**

Aiding in assessing the risk impact and likelihood, Table 3.13 outlines the used metrics along with the associated cost.

**Table 3.13: Applied Valuation Matrix (Aliahmadi et al., 2011, p. 793)**

| | 1 | 2 | 3 |
|---|---|---|---|
| Probability of occurrence (*P*) | Low (not expected) | Possible (cannot be excluded) | Probable (occurrence assumed) |
| Extent of damage/benefit (*E*) | | | |
| Costs | Low (melow CHF 1 Mio.) | Medium (CHF 1–10 Mio.) | High (over CHF 10 Mio.) |
| Schedule | Low (below12 months) | Medium (12–18 months) | High (over 15 months) |

As and when risks are assessed and evaluated, along with their associated cost and gain, the results are fed in the expert system which uses the information, to select the best strategy, utilising stakeholders or players' knowledge and expertise in the field. Figure 3.8 depicts the aforementioned described decision support system.

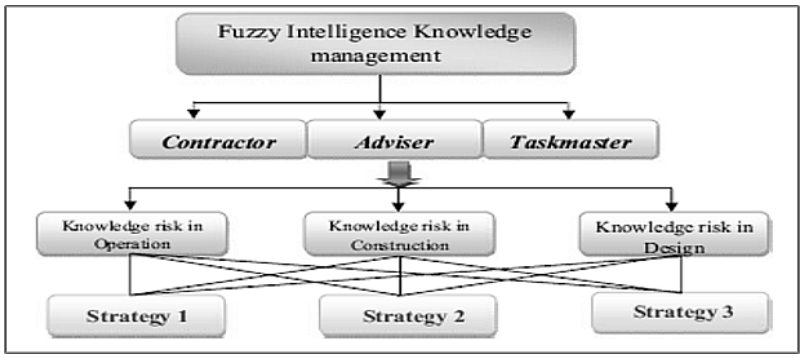


**Figure 3.8: Knowledge Management, Fuzzy Rule-Based Model (Aliahmadi et al., 2011, p. 794)**

The paper utilises multi-stage DSS, where artefacts are prepared and provided aiding practitioners, to find the best strategy, by applying fuzzy logic to infer the work outcome of the DSS.

### 3.5.3 A Design Science Research Project Approach to DSS

Vaishnavi and Kuechler (2008) selected an example to demonstrate the application of Design Science (DS) research methodology. The authors utilised DS in developing a computrised decision support system DSS for nuclear reactors. One of the authors, Vaishnavi, was one of the senior project team members of the software engineering group who became aware of a national awareness to the problem of safe operation of a nuclear power plant, and the director was interested in developing an IS based rule-based DSS. The previous paragraph constructs the first stage of the design science methodology where the problem is defined and its awareness is raised. The authors further elaborate on the problem when an attempt is made to develop a rule-based decision support system using the language Prolog. They indicated that it is nearly impossible to develop such a DSS of thousands procedures, and if developed, it would not be viable to maintain. They outlined the project problem as "continuously changing requirements and the complexity inherent in several thousand rule-based interlocking procedures" (p. 22).

The authors proceeds in exploring possible suggestions to resolve the problem, and highlighted that some alternatives were discarded, while new insights into the problem continued to emerge. One key insight, according to the authors, was system complexity resided primarily in control of the system. Various cycles of discussion, reading and individual deliberation that depicts design science research aspects lead ultimately to a successful path to the development of the solution. In that process, the phase of raising the awareness of the problem was revisited; as any of the design research method phases can be revisited (Vaishnavi and Kuechler, 2008). While revisiting previous phases has some difficulties in backtracking, to make the necessary changes, design science makes it possible. In this example the problem statement was changed to a sub-goal of the original problem statement. The authors stress that this sort of 'drilling-down' into the problem or re-scoping is one of the key aspects and advantages of the design science research methodology.

As the problem statement and its sub-goal got refined and expected artefacts are adjusted accordingly, proceeding to the development phase was the next expected stage. The authors claim that developing artefacts can be straightforward; however, it was not the case for this project. Constructing the artefacts was conceptual and required some discovery-iterations through trial and error of suggested rules. Those iterations resulted in a final conceptual model comprising of two sets of rules. The resulting design/development model should be put to test and evaluated. Vaishnavi and Kuechler (2008) claim that in a design process evaluating every design decision outcome is an on-going activity resulting in a large number of micro-evaluations. However, they elaborated on the formal evaluation that requires taking place when the design reaches a mature and stable stage. It is crucial to determine the type of tests that would yield credible outcomes that the design is a logically correct system. The authors indicate that during the final evaluation, on several occasions, some minor design artefacts changes were deemed necessary. Those redesign occurrences are common in design science research (Vaishnavi & Kuechler, 2008). At the end of the evaluation phase, the model was adjudged a success by the design team.

As for the last two stages of DS were 'Conclusion' and 'Communication'. For the former, desirable artefacts were produced: codification of the problem, design basis in prior work and the design itself and the result were documented in the researcher's dissertation in 1991. The work was successfully defended and obtained the approval of the judging panel. As for the latter phase, a collaborative work based on the research project was submitted to IEEE *Transactions on Data and Knowledge Engineering (TKDE)* (Vaishnavi & Kuechler, 2008). The research aspects and findings were further reviewed in another paper by Vaishnavi et al. (1997, as cited in Vaishnavi & Kuechler, 2008).

## 3.6 CONCLUSION

In this chapter the issues and challenges that have been highlighted in Chapter 2, section 2.5, were revisited and seven researchable problems have been identified. It is imperative to evaluate the identified problems to ensure that they are valid and researchable problems. Thence evaluation criteria were argued and listed, to ensure objective evaluation has been carried out. A scoring system has been adopted, and

the seven problems were evaluated against those criteria. A separate table for each problem evaluation outcome has been created. The evaluation provided the evidence for selecting the research focus problem, which resulted in choosing problem (7) for its merits in adding value to academia and business. The selected research problem, if resolved, can contribute to resolving the other highlighted problems.

In Chapter 4 the research questions are to be developed for the research problem. A research methodology is also to be explored and justified to assist the build of a decision support system that can assist practitioners make better decisions regarding the IT control configurations. The Design Science methodology is to be adopted.

# Chapter 4

# Methodology

## 4.0 INTRODUCTION

Chapter 2 and 3 reviewed the literature that is relevant to the IT control environment and selected the researchable problem of identifying the best set of controls configurations from a selected number of recognised controls frameworks, best practices and standards. The problem impacts both Information Systems (IS) theory and practice, and requires solutions that give better efficiencies in practice than are currently attainable. The Chapter 3 problem analysis suggests that the selection of control configurations impacts system outcomes and can determine the benefit of a system to stakeholders. The Chapter 3 literature review also suggests that a DSS provides a potential solution to the context for assisting efficient decision making and that other researchers have used the Design Science (DS) methodology to develop DSS. In this chapter the challenge of developing and selecting researchable questions to the problem is taken up. The task of developing a DSS is then framed by the DS method and a plan presented for building and evaluating the artefact.

In section 4.1 the outcomes of chapter 3 are brought forward to shape the context for problem and question development and the hypothesis construction. In section 4.2 the research methodology selection is justified. In section 4.3 the DS methodology is elaborated on in some depth to identify ways to apply it to the research question. Section 4.4 specifies the data and evaluation requirements, section 4.5 reports the research progress, and section 4.6 evaluates the limitations of the research methodology. Section 4.7 forecasts the expected outcomes of the research. Chapter 5 then reports findings of the first iteration of the artefacts development and their evaluation.

## 4.1 PROBLEM REVIEW

In Chapter 3, section 3.1, seven problems have been discussed, evaluated and prioritised. It was concluded that problem (7) is the research focus problem. This section outlines a number of questions arising from the identified problems, in sub-section 4.1.1. The research main question is outlined in sub-section 4.1.2, while in sub-section 4.1.3 the research sub-questions along with a number of hypotheses are presented.

### 4.1.1 Questions from the Problem Context

Research questions present the ideas to be researched (Haber, 2006). Berndtsson et al. (2008) add that questions at the start of the research are more general and open, as the research progresses the questions are refined and articulated. According to Haber (2006) research questions should be driven from critical appraisal of relevant literature and reflect a refinement of the initial thinking.

In this sub-section the research problems discussed in chapter 3, are revisited, outlining a number of questions stemmed from the identified problems.
In Problem 1, it was indicated the importance of integrating recognised IT controls frameworks, standards and best practices, which entails high cost and complexity. That is so, to achieve best outcomes and ensuring IT risks are managed in a cost effective way and business objectives are met. That leads to a number of questions:

- What is the integrating basis for those frameworks, standards and best practices?
- Are the resulting integrated structures of controls and processes performing according to a desirable quality?
- Are the integrated frameworks effective and efficient in achieving the anticipated goals?

In Problem 2, the subjectivity of identifying asset value, and the corresponding risks was highlighted as a problem, as it is not a straightforward exercise, because certain errors are expected when applying best-judgment and experience. This also applies when analysing risk by identified vulnerability and a threat assessment, which

affects the residual risk retained within the asset. Furthermore, there are two approaches to evaluate IT risks: Qualitative, and Quantitative. The Qualitative approach is common, as it is easier to estimate, however, it is subjective as there will be different views in evaluating the risk. In the business context, value proposition are demonstrated in monetary figures. The following questions are interesting to ask:

- How is the subjectivity in analysing and assessing IT risks compensated to arrive at factual outcomes?
- How is qualitative risk monitised, when possible?
- How are cost-effective mitigating measures devised based on qualitative assessment?

In Problem 3, the issues and challenges of managing the ever changing risk profile of the IT risk as the context changes over time. Furthermore, business and regulatory requirements change and new technologies are introduced. This requires re-assessing the risk profile. Section 2.2.4 explores IT audit process, it was indicated that re-assessing risk should be done in a timely fashion to ensure an acceptable level of assurance. Evaluating existing controls for effectiveness, reliability and efficiency is a daunting task that all IT auditors face.

A key measure for the effectiveness of an IT controls infrastructure based on recognised frameworks is when risk awareness is embedded within the organisation's culture. That would require educating staff and management through a well-designed program, undertaken by highly trained practitioners. IT auditors are required to have various skills to be able to play their vital consulting role to help organisations build an effective and value adding controls infrastructure. That stems a number of questions:

- What comprises an effective IT assurance program?
- How can effective and efficient risk based auditing reviews be ensured?
- How IT auditors are kept abreast with new technologies and changes in regulatory requirements?
- How are IT risk management aspects embedded within the organisation's culture?

Problem 4 explored the frameworks, standards and best practices that have been elaborated in Chapter 2, section 2.3, which are subject to change, for example ITIL,

Val IT, ISO 27001/2 and other ISO series related to IT, COBIT, RiskIT and SAS. Also industry standards like Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) are often amended and expanded to include new technologies and/or business models. Established framework or compliance structures have to be updated to accommodate the new changes. Relevant controls have to be found to ensure the systems and processes are effectively controlled.

- How do the established IT risk management, IT assurance program and compliance structure incorporate the new changes in timely fashion?
- What level of knowledge and expertise do the practitioners need to acquire to ensure their competence accommodates the changes in those standards?

In Problem 5, the complexity of implementing and integrating frameworks standards and best practices was discussed along with the challenges it entails. If the integration is not planned and executed professionally, the new structure could complicate the environment. In addition, it could incur unnecessary cost, which would render the framework to be business prohibitive. Moreover, integrating frameworks and adapting best practices, requires the availability of local expertise in those frameworks and the business context itself. Should an organisation opt to utilise a third party, then that would increase the cost and the risk of inadequate assessment of the local environment and business context.

- How is the complexity of integrating and customising many standards and frameworks managed without impacting the business?
- How is the balance maintained between developing local expertise and utilising third party in customising the required frameworks and standards?

In Problem 6, the issues of demonstrating business value in implementing costly IT controls and processes from recognised frameworks and standards, were explored and a relevant problem statement was formed. How could a business realise the value of implementing risk based controls configurations that are integrated within the organisation.

- How is the business value from IT controls frameworks measured?
- How can an organisation realise the value of implementing IT controls frameworks?

Problem 7 was selected as the research focus problem. It was argued that finding the best set of controls from a myriad of recognised frameworks entails numerous challenges. Resolving this problem of the seven identified problems would potentially contribute to the most improved business value outcomes. Practitioners require a mechanism that allows them to evaluate controls configurations in a timely manner and with less effort when a risk profile changes or the controls framework changes itself.

Researching this problem and attempting to find a solution by building a model of controls-risks along with their cost and gained benefits to determine the best set of controls. The desired outcome would enable practitioners to conduct the arduous exercise of control selection in a timely fashion and with less effort. Furthermore, it would provide stakeholders with a means to evaluate controls based on their associated risks and to have a realistic sense of assurance of how trustworthy an IS environment is at any given point in time.

- What are the criteria for selecting the most effective and efficient controls configurations for the best business value outcome?
- How are the controls and processes from different frameworks, standards and best practices, combined?
- What are the evaluation criteria of the resulting configuration of controls and processes?
- How are the continual effectiveness and efficiencies of the resulting controls configuration ensured?

### 4.1.2 The Research Question

As problem 7 has been selected as the research focus problem, as detailed in Chapter 3 section 3.2 and sub-section 3.2.2, subsequently corresponding questions are formed for this problem. The following question has been formed as the research question:

**What are the criteria for selecting the most effective and efficient controls configurations for the best business value outcomes?**

As some controls and processes could overlap and not all are required to mitigate the same risks, this aspect of overlap could cause overwork and incur unnecessary cost. It is imperative to define selection criteria for controls from the myriad of

recognised frameworks, best practices and standards. Each consists of tens of controls and processes. The key aspect in finding adequate IT controls and processes is to assess the corresponding IT risks, which requires a holistic risk assessment. Such an assessment would take into consideration the business context and all the challenges that were explored at length in Chapter 2. For example, IT risks and associated controls and processes have a many to many relationship. Furthermore, risks impact different IT assets at various degrees. Moreover, it was argued that when assessing IT risk the intrinsic business value of the underpinning assets must be taken into account.

As indicated in Chapter 3, sub-section 3.1.7, finding a solution or solutions to the highlighted problem would also contribute to solving aspects of the other identified problems in this research. Answering the research formed question relates to this problem would in turn contribute to answering the other defined questions.

### 4.1.3 The Research Sub-Questions and Hypotheses

According to Berndtsson et al. (2008) “research questions state what you want to learn”, while “Hypotheses, in contrast, are statements of your tentative answers to these questions” (p. 11). To supplement the research question, a set of sub-questions are devised below that aid in gathering the data needed to answer the research question:

1- What is the minimal set of recognised IT controls/process Frameworks, Best Practices and Standards that could be integrated to provide a comprehensive structure of controls configurations?

There are many applicable IT controls frameworks, COBIT, ITIL, ISO 27001/2, TOGAF, SABSA, PMI, Prince2, ISO 31000 and many more. In addition there are enterprise frameworks such as the COSO ERM, so there is a need to search and find an answer for such a question.

2- What are the criteria for selecting a recognised IT controls Frameworks, Best Practices and Standards?

For example, a framework helps an organisation to comply with regulatory requirements such as Privacy Act, or industrial standards such as PCI. Other

frameworks help in IT strategic planning, business and IT objectives alignment, Business Continuity Planning (BCP).

3- How is the business value assessed in managing IT risk in a control-based structured environment that is established through implementing recognised frameworks?
4- Once an IT controls configuration is selected, it is imperative to validate the controls configuration. What are the validation criteria?

Validating the selected set of IT controls is important to ensure that IT objectives are serving the business goals. Additionally, validation runs a quality check to ensure elected controls are not conflicting with other controls. This question has 2 further sub-questions: how and when to validate the selected IT controls configurations? Is this completed before or after implementing the controls? Furthermore, there is an issue of cost and feasibility of performing the validation process, which is necessary to answer.

Answering those sub-questions would contribute to answering the main research question, which is about finding what framework to elect and how to assess the business value deliverables out of the selected controls and processes to mitigate the defined risk. Also validating the resulting controls configuration would ensure the selected set of controls mitigates the risks effectively. To attempt answering the noted questions, a conceptual model has been theorised as noted in Chapter 2, section 2.4, regarding controls configurations. In Chapter 3, section 3.4.3, which outlines the model based DSS. As noted in the introductory paragraph the hypotheses speculate answers to the raised questions. Hypotheses are considered a means to validate the theorised model and put it into testing (Haber, 2006). Figure 4.1 illustrates the conceptual map of the research stages and the role of questions and hypotheses in directing the research activities to achieve the research's goals. Oates (2006) points out that when research theory is developed, that leads to form statements based on the theory that can be tested. Oates further states that "this statement is of the form 'Factor A causes B', and is known as a hypothesis" (p. 127).

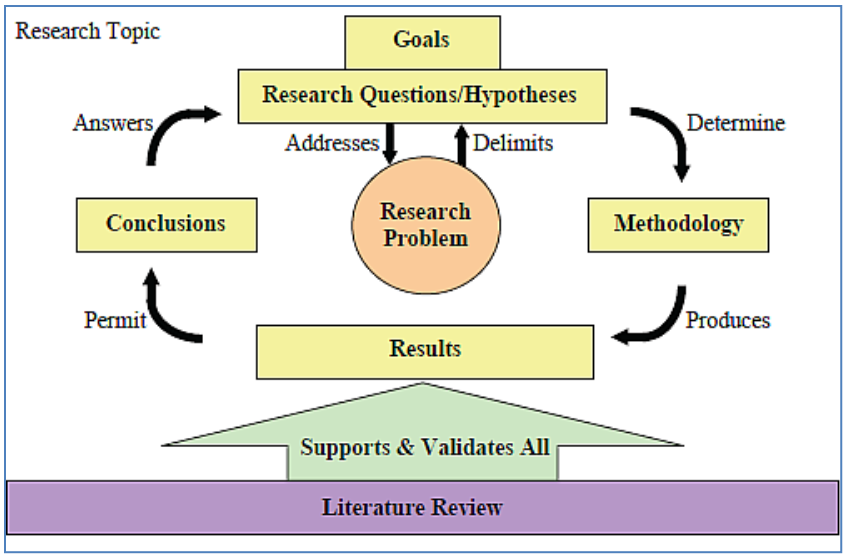


**Figure 4.1: Conceptual Map of the Problem-Based Research Cycle (Ellis & Levy, 2008, p. 19)**

In managing IT risks in control-based structured IT environments established via implementing recognised IT controls frameworks, best practices and standards, the following hypotheses are to be asserted when attempting to answer the research question:

**H1** - Establishing a risk-based effective IT-assurance program ensures business-IT value.

**H2** - Assessing IT risks holistically results in obtaining factual risk assessment.

**H3** – Structuring IT controls and processes in a framework ensures business's overall objectives are achieved.

**H4** – Regularly evaluating IT controls' effectiveness and efficiency ensures management of IT risks is cost-effective and current.

**H5** – Integrating IT controls and processes from recognised IT controls frameworks in a complementary fashion is a key to establishing an effective IT assurance program.

## 4.2 RESEARCH METHODOLOGY

Vaishnavi and Kuechler (2008) define 'research' "as an activity that contributes to the understanding of a phenomenon" (p. 7). Similarly, Berndtsson et al. (2008) define 'research' in an academic context as "the activity of a diligent and systematic inquiry or investigation in an area, with the objective of discovering or revising

facts, theories, applications etc" (p. 10). Berndtsson et al. indicate that the goal is to "disseminate the new knowledge" (p. 10). To ensure the defined problem is researched in a systematic way, a methodology has to be defined and applied, to enable researcher obtain relevant data and analyse it accordingly. According to Peffers et al. (2007) a methodology is "a system of principles, practices, and procedures applied to a specific branch of knowledge" (p. 5). The selection of an appropriate, systematic method is important for the research project to succeed (Berndtsson et al., 2008).

To select a research methodology that suits the subject domain of this research the general context of research is explored in this section. In sub-section 4.2.1 research philosophies and paradigms are explored and in sub-section 4.2.2 qualitative and quantitative methods are reviewed.

### 4.2.1 Research Philosophy and Paradigms

According to Nicho (2008) when discussing 'research' it is imperative to also indicate the research philosophy. Bryan (1966) defines 'research philosophy "as the underlying theory which places research activities in perspective with man's existence in the universe" (p. 69). Understanding the philosophical aspects of the research is crucial in choosing the research method that suits the research subject emphasised Bryan (1966). Similarly, Oates (2006) states that researchers can select a research method that suits the research subject so long it is defined. In addition an evaluation means is available to assess how the research has been carried out and at what quality. Identifying evaluation criteria is important because research methods have different underlying 'philosophical paradigms'. Oates (2006) defines a paradigm as "a set of shared assumptions or ways of thinking about some aspects of the world", and further indicates that "shared thinking is about how to do research and gain or create knowledge" (p. 282). Similarly, a paradigm is defined as "a set of beliefs about the nature of social reality, that is, the nature of the 'world' and the individual's place in it" (Shanks, Rouse & Arnott, 1993, as cited in Shanks, 2002, p. 76). A view shared by Vaishnavi and Kuechler (2008) who also indicate that some research domains are bound into a category where sets of phenomena of interest overlap in methods of investigation for which 'multi-paradigmatic' based research methodology is required.

Vaishnavi and Kuechler (2008) outline definitions relating to philosophical research paradigms:

- **Ontology** "is the study that describes the nature of reality. For example what is real and what is not, what is fundamental and what is derivative?"
- **Epistemology** "is the study that explores the nature of knowledge. For example on what does knowledge depend, and how can be certain of what we know?"
- **Axiology** "is the study of values. What values does an individual or group hold, and why?" (p. 16).

Proctor (1998) highlights similar interest in the above terms and adds 'Methodological' as "how can the researcher discover what she or he can be known?" (p. 74). Similarly, Oates (2006) defines Ontology and Epistemology; and refers to the fact that in IS "a wide range of research strategies, with different underlying philosophical paradigms, that have been used to understand the use of information systems by people" (p. 282). Gregor (2006) published a research essay about "structural nature of theory in IS" (p. 611), in which a taxanomy is devised to classify IS theories from four perspectives: analysis, explanation, prediction and prescription. Gregor further defines five IS theory classifications: theory for analysing, theory for explaining, theory for predicting, theory for explaining and predicting, and theory for desing and action.

According to Guba and Lincoln (1994) there are four underlying research paradigms namely: positivism, post-positivism, critical theory and constructivism. Oates (2006); Orlikowski and Baroudi (2002) refer to three paradigms positivist, interpretivist, and critical. Orlikowski and Baroudi examine the three noted paradigms outlining the various aspects of them and arguing their relevance and applicability to various research domains. Furthermore, Nicho (2008) in his attempt to argue the best paradigm for his PhD research, summarised two perspectives of Myers (1997) and Orlikowski and Baroudi (2002). In Table 4.2 these views are summarised and the shaded area shows the fit of his research study in measuring IS controls and CMMI level based on a combination of COBIT and Goal Question Model (GQM) methods. In Table 4.1, Nicho (2008) demonstrates the suitability of the positivist paradigm to the research in IS, which is argued as well by Shanks (2002). However, according to Oates (2006), the positivist paradigm is the oldest

among the three paradigms. It underlies a scientific method and indicates its application in the natural sciences such as physics, chemistry and biology. However, it is less suited to research domains of the social world where people, orgnistaions and technology are interacting within particular settings. According to Lee (2001) as cited in Berndtsson et al. (2008) the field of IS "is connected with the interaction between social and technological issues" (p. 9). Berndtsson et al. further elaborate and indicate that the interactions between IS (technical and otherwise) and social aspects within an organisation are critical.

**Table 4.1: Research Paradigm Summary (Nicho, 2008, p. 85)**

| Ref. | Positivist | Interpretive | Critical |
|---|---|---|---|
| (Orlikowski & Baroudi, 2002) | (1)Premised on the existence of a priori fixed relationships within phenomenon which are typically investigated with structured instrumentation | Assume that people create and associate their own subjective and inter-subjective meanings as they interact with the world around them | Aim to critique the status quo, through the exposure of what is believed to be deep seated structural contradictions within social systems. |
| | (2)Serves to test theory in an attempt to increase predictive understanding of the phenomenon | Attempt to understand the phenomena through the meanings that participants assign to them | A critical stance taken towards taken-for-granted assumptions about organisations and information systems |
| | (3)Evidence of formal propositions, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about a phenomenon | Reject the possibility of an 'objective' or 'factual' account of events and situation | N / a |
| | N / a | Generalization from the setting to a population is not sought as the idea is to understand the deeper structure of the phenomenon | N / a |
| (M. Myers, 1997) | (4)Positivists assume that reality is objectively given and can be described by measurable properties which are independent of the observer and the instruments | Assume that access to reality is only through social constructions such as language, consciousness and shared meanings | Assume that social reality is historically constituted and that it is produced and reproduced by people |
| | N / a | (5)Does not predefine dependent or independent variables, but focuses on the full complexity of human sense making as the situation emerges | Recognize that the ability of people to change their social and economic setting is constrained by various forms of social,, cultural and political domination |

Oates (2006) critique of the three paradigms highlights that 'interpretivist' is better suited to IS research. For example, IS studies do not prove or disapprove hypotheses as is the case in 'positivist' research. Rather, IS studies "try to identify, explore and explain how all the factors in particular social setting are related and interdependent" (p.292). The interpretive research goal is for plausibility, rather than finding a proof, as is the case in positivist research (Oates, 2006). Interpretivist publications in IS research are increasing in number and are becoming more

accepted by IS researchers. On the other hand, the 'critical theory' paradigm focuses on the conflict and contradiction in a researched setting, enlarging the scope to discover where interpretations and understanding are not enough (Oates, 2006).

Before concluding this sub-section it is crucial to indicate that Oates points out that some researchers have argued and favoured one paradigm over another with their underlying strategies being adapted to IS research. Oates (2006) states that "to resolve this, some have suggested that the different paradigms can be combined as a compromise solution" (p. 114), for which, researchers must justify the need for such an approach. The complexity of IS and the fact that it crosses multi and different disciplines, stems the need to adopt multi-paradigm research methodologies (Vaishnavi & Kuechler, 2008; Berndtsson et al., 2008).

### 4.2.2 Qualitative and Quantitative Research Methods in IS/IT

Research in IT systems in general has been conducted by both qualitative and quantitative methods as indicated by Nicho (2008). According to Berndtsson et al. (2008) qualitative methods relate to social sciences and are mainly concerned with exploring how to improve the understanding of a domain rather than explaining it. A qualitative method is defined by Myers (1997) as that "which involves the use of qualitative data, such as interview, document, and participant observation data, to understand and explain social phenomena" (p. 241). On the other hand, Berndtsson et al. (2008) argue that quantitative methods have their roots in natural sciences. A quantitative method as described by Myers (1997) "assumes that reality is objectively given and can be described by measurable properties which are independent of the observer" (p. 241). Quantitative method is underlined by positivist paradigm where asserted hypotheses and propositions are tested (Taylor & Bogdan, 1998). Data collection methods utilised in a quantitative approach are mainly through conducting surveys. Surveys are used to obtain facts or causes and to filter out the subjective statistics of individuals (Taylor & Bogdan, 1998). However, depending on the researched domain-complexity quantifying research elements might not be at all feasible (Yin, 1984).

Taylor and Bogdan (1998) assert that qualitative methods suit complex domains that involve a high level of subjectivity. Qualitative research methods suit researching complex domains where contributing factors are dynamic in nature and

the researcher would have to holistically examine the environment and gather factual insights within a context (Taylor & Bogdan, 1998). It has been established (see Chapter 2 sections 2.1-3) that the domain of managing IT risk holistically through an effective IS assurance program is a complex and dynamic domain. The fact that the subject of this research depends on its context makes it imperative to obtain empirical data besides the theoretical data from the literature to answer the research question. The research question in itself is about integrating recognised IT controls frameworks, best practices and standards. The justifications as will be discussed in section 4.3.2.1, would lead the researcher to believe that the best approach to achieve the research objectives is to adapt the DS method and its framework derived by Peffers et al. (2007). A DS investigation is an exploratory study where artefacts are produced, reviewed and evaluated, and re-designed if deemed necessary. The proposed artefacts are evaluated with a data collection method. Proposed hypotheses are verified, using the analysed qualitative data applying quasi-judicial method, where a rational argument is used to interpret the data (Collis & Hussey, 2009).

Qualitative and quantitative research methods have been utilised for researching various topics in IT and IS. Each method has specific advantages and disadvantages depending on the researched domain and available resources. It has been established that the domain subject of this research is subjective and complex and that a qualitative method allows investigating the subject holistically to obtain qualitative data. In addition, relevant research publications are few, and that led many authoritative researchers to conduct exploratory studies for the investigation of subjects within the domain of this research topic. Some of those publications were examined to determine what methods they have utilised and what were the selection criteria. In Chapter 3, section 3.5 a number of relevant papers were reviewed where, among them a paper in which DS methodology has been adopted to develop a DSS to solve an identified business problem. Given the time and available resources for this research it can be concluded that exploratory study where artefacts are developed and evaluated by experts along with critical reflection, is the most suitable approach to research the question of this study.

## 4.3 DESIGN SCIENCE (DS)

The term ‘design’ in industry and research has been widely discussed (Oates 2006; Vaishnavi & Kuechler, 2008; Hevner & Chatterjee, 2010; Offermann, Levina, Schonherr & Bub, 2009). Vaishnavi and Kuechler (2008) pose a question: “Can Design be Research” (p. 9). They argue the applicability of Design Science in research, which will be examined in the next sub-section. Oates (2006) examines ‘design and creation’ as a research strategy, but claims it focuses on developing IT products, or ‘artefacts’. Oates argues that design and creation research could be based on any of the three aforementioned paradigms (positivist, interpretivist, and critical). However, many IS design research projects are unknowingly based on positivism. The rationale for that is “the designer is an objective, dispassionate outsider who uses rational thinking, and tools and methods that are based on mathematics and logic, rather than human intuition or politics” (Oates, 2006, p. 302). However, other authors provide plausible grounds for utilising ‘design’ and ‘design and creation’ in IS research in the academia context; as explored further in the next sub-section. This section is structured as follows: in sub-section 4.3.1the ‘Design Science’ (DS) as a research paradigm is demonstrated. While sub-section 4.3.2 argues the relevance of DS to IS research along with a methodology that suits this research. While DS guidelines, framework and roadmap’s various stages are explored and examined in sub-section 4.3.3. Lastly, sub-section 4.3.4 discusses the importance of evaluating research developed artefacts.

### 4.3.1 Design Science (DS) Methodology

Simon (1996); Vaishnavi and Kuechler (2008) refer to a clear distinction between ‘natural science’ and ‘science of the artificial’. The former relates to “objects or phenomena in the world (nature or society) that describes and explains how they behave and interact with each other”. While the ‘science of the artificial’ is about “artificial (man-made) objects and phenomena designed to meet certain desired goals” indicate Vaishnavi and Kuechler (2008, p. 8).

Oates (2006) describes ‘design and creation’ as a research strategy utilised in developing IT products or ‘artefacts’. The author’s view comes from the position that IT artefacts are marketable products produced by designers for a requesting stakeholder, which is justifiable. However, in academia, the context is not the same.

In fact, Oates elaborates further on ‘design and creation’ and describes the stages of ‘design and creation’ labeled as ‘learning via making’ in four stages, namely: Awareness of the problem, Suggestion, Development, Evaluation and Conclusion. These stages, are similar to the stages of what other authors call ‘Design Science’ based research (Vaishnavi & Kuechler, 2008; Hevner & Chatterjee, 2010; Hevner, March, Park & Ram, 2004; Peffers et al., 2007; Offermann et al., 2009). These authors emphasise that those steps (6 steps of Design Science) are not to be followed in a rigid fashion, but rather in a fluid and iterative cycle. The aim is enhancing the artefacts, in that way, “the researcher using design and creation strategy learns through making”, states Oates (2006, p. 112). An advantage of this approach is producing a tentative solution without having full understanding of the whole system (Oates, 2006; Vaishnavi & Kuechler, 2008; Offermann, et al., 2009). The context is true for IS researchers, who in many cases are involved with complex systems where technologies, people and organisations are interconnected and are required to comply with, and conform to, various rules and regulations (Berndtsson, et al., 2008; Vaishnavi & Kuechler, 2008).

Oates (2006) claims that ‘design and creation’, or ‘design science’ as branded by Vaishnavi and Kuechler (2008); Hevner and Chatterjee (2010); and, Offermann et al. (2009) can be used in IS research. However, it is imperative while iterating DS cycles to enhance the required artefacts, researchers must clearly document how the final artefacts have emerged (Oates, 2006). In that view, Oates (2006) further elaborates and indicates that ‘design and creation’ can be used as a research strategy. However, that is not for demonstrating technical skills but rather to demonstrate “academic qualities such as analysis, explanation, argument, justification and critical evaluation and it must also create some new knowledge” (p. 114). A key concept that Oates (2006) refers to is “Often in typical industry-based design and creation projects, the less that is learned, the more successful the project is considered to be” (p.114). Because, if everything goes well according to the plan there will not be much backtracking, re-thinking and re-designing. A similar view is noted by Vaishnavi and Kuechler (2008) who also state “in industry design effort, a new product (artefact) is produced; but in most cases, the more successful the project is considered to be, the less is learned” (p. 26). On the other hand, IS research projects, following ‘learning via making’ steps, backtracking and

revisiting analyses and design are common and encouraged (Oates, 2006). Although backtracking in DS has many challenges, which involves re-analysing that leads to re-scoping and re-designing of the research artefacts, however, it is an effective part of the DS method (Vaishnavi & Kuechler, 2008).

In industry-based projects uncertain areas and risks are identified and deliberately avoided by practitioners. While in research projects a researcher would focus on those areas as that would lead to a new knowledge through the iteration cycles of 'design and creation' (Oates, 2006). Vaishnavi and Kuechler (2008) assert that understanding the philosophical grounding of an adapted research methodology is really important. Vaishnavi and Kuechler compiled Table 4.2 based on Gregg et al. (2001), as cited in Vaishnavi and Kuechler (2008), in which, Gregg adds a meta-level assumption to design science, which they term as 'socio-technologist/developmentalist approach', contrasting the positivist and interpretive contribution to design research.

**Table 4.2: A Philosophical Assumptions of the Three Perspectives (Vaishnavi & Kuechler, 2008, p. 17)**

| Research Perspective | | | |
|---|---|---|---|
| **Basic Belief** | **Positivist** | **Interpretive** | **Design** |
| Ontology | A single reality Knowable, probabilistic | Multiple realities, socially constructed | Multiple, contextually situated alternative world-state Socio-Technologically enabled |
| Epistemology | Objective; dispassionate Detached observer of truth | Subjective (i.e., values and knowledge emerge from the researcher-participant interaction) | Knowing through making: objectively constrained construction within a context iterative circumscription reveals meaning |
| Methodology | Observation; quantitative, statistical | Participation; qualitative, Hermeneutical, dialectical | Developmental Measure artefactual impacts on the composite system |
| Axiology: what is of value | Truth: universal and beautiful; prediction | Understanding: situated and description | Control; creation; progress (i.e., improvement understanding |

In Table 4.2 Vaishnavi and Kuechler (2008) summarise the philosophical assumptions of three perspectives. In the multiple contexts of ontology, epistemology, and methodology the ways of knowing through making and iterative circumscription are elaborated. Artefacts are refined and adjusted. In addition,

Vaishnavi and Kuechler added Axiology as defined in sub-section 4.3.1, which refers to the study of values (utility) anticipated by researchers adapting the DS paradigm-research methodology; so a researcher could gain more knowledge progressively. According to Vaishnavi and Kuechler (2008) "the end result of a design science research effort maybe very poorly understood and still be considered a success by the community" (p. 18).

The DS researcher is a pragmatist according to Vaishnavi and Kuechler (2008). Vaishnavi and Kuechler emphasise that DS is multi-paradigmatic, and claim that "the philosophical perspective of the design science research changes as progress is iteratively made through the phases" (p. 19). Similarly, according to Bunge (1984) who suggests that design science research is most effective when practitioners shift between pragmatic and theoretic perspectives and are guided by a pragmatic assessment of progress in the research stages.

Lau (1997) indicates that 'action research' is a type of research methodology, and claims "that it has been used in the field of social science since the 1940s as a research strategy that integrates theory and practice through change and reflection", citing (Argyris, Putnam & Smith, 1985; Lewin 1947; Reason 1993a, as cited in Lau, 1997, p. 32). The applicability of 'action research' in IS research is established, since IS research has adopted multiple research paradigms and methodologies. The reasoning for that is outlined in further elaboration about the epistemology of 'action research', in which the use of an inquiry strategy is undisputed. However, the use of 'action research' as a research paradigm is in question, because of various views of many researchers (Lau, 1997). A key aspect of 'action research' is whether 'action research' is used as a research strategy or a theory of social science, in "the characteristics of being change-focused, collaborative and an iterative process" Lau (1997, p. 34). That is similar to what Oates (2006) has argued about 'design and creation' as a research strategy, discussed in the introduction of sub-section 4.3.

According to Lau (1997, p. 34) the most comprehensive definition of action research was provided by Hult and Lennung (1978):

> Action research simultaneously assists in practical problem-solving and expands scientific knowledge, as well as enhances the competencies of the respective actors, being performed

> collaboratively in an immediate situation using data feedback in a cyclical process aiming at an increased understanding of a given social situation, primarily applicable for the understanding of change processes in social systems and undertaken within a mutually acceptable ethical framework (p. 247).

Lau further explores a number of IS research areas where the 'action research' has been utilised. For example: analysis, design, development and implementation of IS and DSS; collaboration between users and developers when designing complex systems. Gregor (2006) supports Lau's view on the use of 'action research' in IS research, to produce IS research, covring "the areas of analysis, design, development, and implementation" (p. 629). Lau (1997) points out that using 'action research' in IS is rewarding, however, it entails many challenges at the same time. It is evident that what Lau is referring to as 'action research' is what (Vaishnavi & Kuechler, 2008; Hevner & Chatterjee, 2010; Hevner, March, Park & Ram, 2004; Peffers et al., 2007; Offermann et al., 2009) have called 'design science' paradigm.

### 4.3.2 Design Science in IS Research

Peffers et al. (2007) claim that the use of interpretive research paradigm has been accepted in IS research. However, the authors indicate that "the resulting research outcome is mostly exploratory and, it could be argued, not often applicable to the solution of the problem encountered" (p. 1). On the contrary, "design, the act of creating an explicitly applicable solution to the problem" has been accepted as a research paradigm in faculties such as engineering. Several researchers have been utilising DS as research paradigm (Peffers et al., 2007), however, "DS research has been slow to diffuse into the mainstream of IS research" (p. 2).

Hevner and Chatterjee (2010) point out the high relevance of DS research paradigm to IS research, mainly because it addresses two key issues of IS: the role of IT artefacts and scarce IS research. The authors indicate to what Simon (1996) has conceptualised DS paradigm and described it as a pragmatic research paradigm as it appeals for creating innovative artefacts to solve an identified problem. However, there has been a reluctance to adapt DS in IS research, as it was considered for more technical disciplines like Computer Science and Engineering

(Hevner & Chatterjee, 2010). The authors further add that DS has been progressively accepted by IS researchers since 1990s, to improve effectiveness and utility of the produced IT artefacts. A view is shared and emphasised by Alturki, Gable, and Bandara, (2011a).

IS research involves a mixture of technology, people and organisations, (Lee, 1999). According to Vaishnavi and Kuechler (2008) who argue that design science research is applicable to IS because of the types of research questions that are naturally formed. In addition, the interaction of many functions/processes with other non-IS related functions/processes. The authors further state that "human-computer information producing and processing systems are, by their nature, complex and grounded in multiple disciplines" (p. 2). The questions arise are often have little or nonexistent theoretical background, where research by 'exploring by building' or 'learn through making' is where design science excels.

Furthermore, IS have significant impacts on people's lives and businesses, however, many unanticipated and/or poorly understood events occur (Berndtsson, et al., 2008; Vaishnavi & Kuechler, 2008). Vaishnavi and Kuechler (2008) state that Information Systems is a perfect example of a multi-paradigmatic field. Vaishnavi and Kuechler (2008) further claim that the dynamic nature of IS and multi-paradigmatic of design science, through exploration, allows better understanding of how IS operates and interacts with internal and external environments. Furthermore, the authors stress that "even in the absence of a strong theoretical grounding that design science research DSR is the paradigm of choice" (p. 4).

### 4.3.3 Design Science – Guidelines, Framework and Roadmap

According to Hevner et al. (2004) a researcher adapting DS must further the existing knowledge to help resolve the identified problem. Also to develop and communicate "knowledge concerning both the management of information technology and the use of information technology for managerial and organisational purposes." according to Zmud (1997, as cited in Hevner et al., 2004). However, adding new knowledge through developing validated artefacts is not an easy exercise to undertake (Hevner et al., 2004). Furthermore, Hevner et al. state

"designing useful artefacts is complex due to the need for creative advances in domain areas in which existing theory is often insufficient" (p.76).

Hevner et al. (2004) argue that adding new knowledge requires two distinct but complementary paradigms, of behavioral and design science. The behavioral sciences are rooted in natural science, while DS has its root in Engineering (Simon, 1996; Hevner et al., 2004; Alturki et al., 2011a). Hevner et al. indicate that technology and behavior are not dichotomous in IS, they are in fact joined at the hip.

As for the IT artefacts, according to March and Smith (1995); Nunamaker, Chen and Purdin (1991), they are defined as:

- **Constructs** (vocabulary and symbols), the conceptual terms of references of the problem and solution domain that evolves and refined throughout the design phase (March & Smith, 1995).
- **Models** (abstractions and representations), according to Vaishnav and Kuechler (2008) "the model is a set of propositions or statements expressing relationships among constructs" (p. 13). From DS perspective, the model focus is on utility while for natural science traditionally focuses on truth.
- **Methods** (algorithms and practices), which according to March and Smith (1995) are used to perform a task with a goal to manipulate the constructs to realise the solution statement.
- **Instantiations** (implemented and prototype systems), represent the research resulting outcomes (March & Smith, 1995).

Hevner et al. (2004) emphasise that artefacts help researchers analyse and address the identified problem through developing adequate systems when they are implemented successfully. In order to explain the phenomena with respect to the artefact's use, usefulness, and impact on individuals as well as the organisation, quality and dependency. IT artefacts developed and implemented in an organisation context, require, often, behavioural-science research validation aspects (DeLone & McLean, 1992, 2003; Seddon, 1997). Newly developed artefacts resulting from DS based research could require quantitative analyses. Furthermore, and depending on the subject and level of interaction between people, technology and organisation, the new artefacts could require qualitative assessment to interpret the phenomena adequately for problem-solving or theory development (Klein & Meyers, 1999).

In DS “design is both a process (set of activities) and a product (artefact) – a verb and a noun” state Walls, Widmeyer, and El Sawy (1992, p. 36). The design process entails a series of activities producing innovative product, i.e. the design artefact. Artefact will be tested to evaluate its efficacy to provide further understanding and/or to improve the quality of the design itself. The design process of a build-and-evaluate loop is done in an iterative fashion until a final artefact is produced (Markus, Majchrzak, & Gasser, 2002). It is imperative for the researcher to have a thorough understanding of how the artefacts are evolving from inception to the final shape (Hevner et al., 2004). “The goal of behavioural-science research is truth. The goal of design-science research is utility” state Hevner et al. (2004, p. 80). Hevner et al. indicate that an artefact may have utility (value), but yet to be proved if relevant truth is discovered. On the other hand, “a theory is yet to be developed to the point where its truth can be incorporated into deign” (p. 80). Furthermore, Hevner et al. assert “A justified theory that is not useful for the environment contributes as little to the IS literature as an artefact that solves a nonexistent problem” (p. 81).

Hevner et al. (2004) developed a set of guidelines depicted in Table 4.3. The principles outlined in the table emphasise what the authors have been theorising around DS aspects, the design process, artefacts and the iterative nature of the process. The produced artefacts are meant to serve an objective, so artefacts “must yield utility for the specified problem” (p. 82). The utility (value) will be verified when the artefacts are evaluated. Artefacts must be novel and a new knowledge must be added to the domain. The research outcomes must be communicated to the adequate audience of technical as well as business management. Hevner et al. (2004) indicate that they developed the guidelines to help researchers and reviewers follow a systematic method in conducting DS based research and evaluate the resulting artefacts accordingly.

**Table 4.3: Design Science Research Guidelines (Hevner et al., 2004, p. 83)**

| Guideline | Description |
|---|---|
| Guideline 1: Design as an Artifact | Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation. |
| Guideline 2: Problem Relevance | The objective of design-science research is to develop technology-based solutions to important relevant business problems. |

| Guideline | Description |
|---|---|
| Guideline 3: Design Evaluation | The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods. |
| Guideline 4: Research Contributions | Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies. |
| Guideline 5: Research Rigor | Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact. |
| Guideline 6: Design as a Search Process | The search for an effective artifact requires utilising available means to reach desired ends while satisfying laws in the problem environment. |
| Guideline 7: Communication of Research | Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences. |

Hevner and Chatterjee (2010) address some of the highlighted issues in the published work of Hevner et al. (2004) and point out the importance of differentiating between professional design and DS design. The former aims at creating applications of existing knowledge, while DS design addresses un-resolved problems in an innovative way. DS design adds quality and tested additions to the knowledge base. Knowledge is generated through design could come in various forms: constructs, models, methods, and instantiations (March & Smith, 1995). The results of DS research conducted in a specific context, once evaluated and its applicability is approved, then another project could take place to generalise the research outcomes into a wider context. Based on Hevner et al. (2004) guidelines, listed in Table 4.3, Hevner (2007) highlight three DS research processes in Figure 4.2. The three processes: 'Relevance', 'Design' and 'Rigor'.

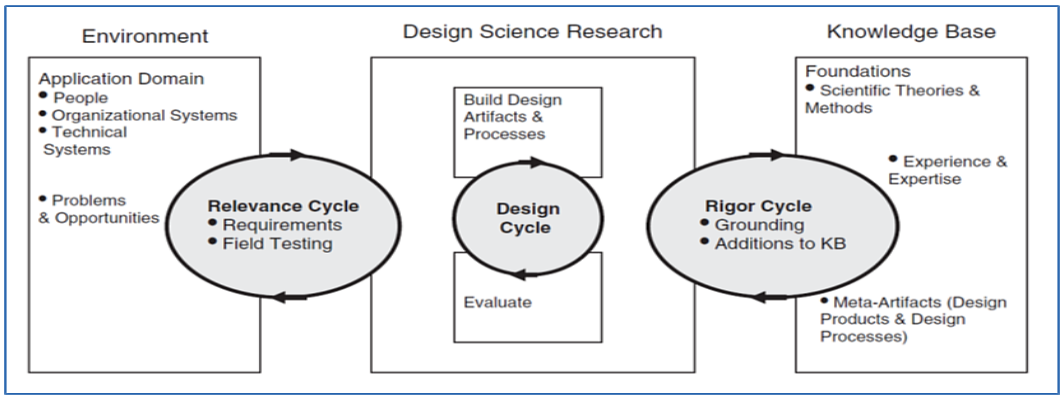


**Figure 4.2: Design Science Research Cycles (Hevner, 2007, p. 2)**

The research environment context is bridged with the DS activities through the first cycle. While the design cycle is done iteratively between the core activities from identifying the problem to designing and evaluating the proposed artefacts. Lastly, the third cycle that connects the DS activities with the existing knowledge, expertise relate to the identified problem and evaluated and finalised the solution, aiming at adding new or refining existing knowledge. Hevner and Chatterjee (2010) stress that "these three cycles must be present and clearly identifiable in a design science research" (p. 17).

Peffers et al. (2007) developed DS research methodology (DSRM) along with a framework based on the DS guidelines developed by Hevner et al. (2004). Figure 4.3 depicts the DS framework; the objective is to aid researchers in conducting DS based IS research systematically.

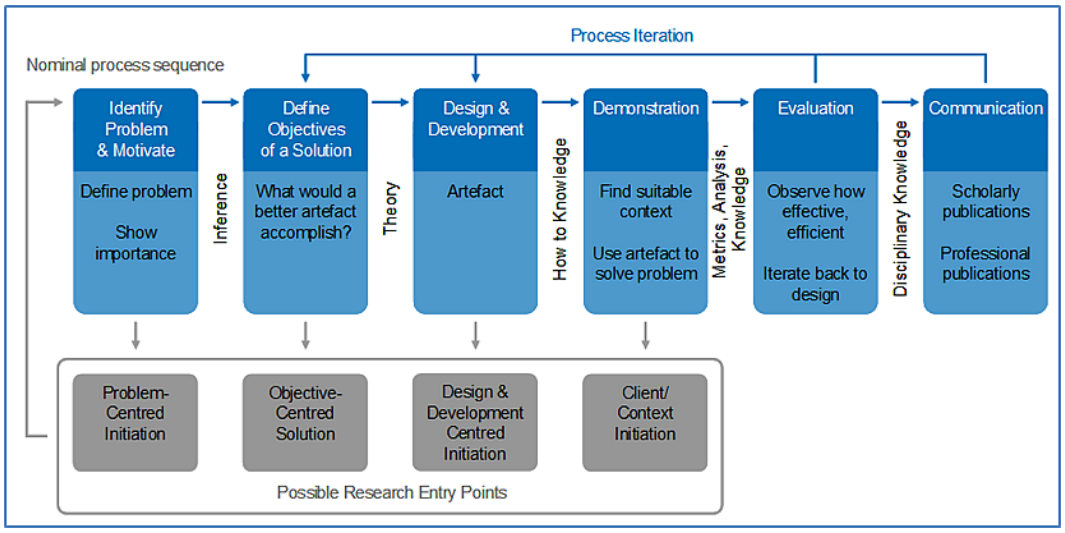


**Figure 4.3: Design Science Research Methodology Process Model (Peffers et al., 2007, p. 54)**

The framework comprises nominal process stages, with possible entry points or initiation that could trigger the process iteration. In addition, it can be noted the iterative aspect where the resulting outcomes are evaluated to ensure their applicability and anticipated utility.

Vaishnav and Kuechler (2008) indicated that DS based research requires six stages starting with the 'Awareness of a Problem', and 'Suggestions' to resolve the identified problem that are driven to some extent from existing knowledge. According to Peffers et al. (2007) the "identified problems do not necessarily translate directly into objectives for the artefact because the process of design is necessarily one of partial and incremental solutions" (p. 12). Furthermore, the

‘development’ where a design is made, partially or fully, is awaiting the ‘evaluation’ outcomes. The authors stress that the Development, Evaluation and Suggestions stages are often repeated until satisfying outcomes are obtained, in which the stage is called ‘Conclusion’. However, Vaishnav and Kuechler (2008) point out the challenge of the iterative aspect of DS, as it is not always easy to pin point in retrospect where the change should be made. Lastly, the ‘Communication’ stage is when the newly found knowledge or refined theory is reported to the target audience. The basis of the iteration, is according to Vaishnav and Kuechler (2008) “the flow from partial completion of the cycle back to the ‘Awareness of Problem’” (p. 12), to adjust the artefacts. In DS even the problem statement is subject to change (Vaishnav & Kuechler, 2008; Offermann et al., 2009) as the research progresses through the iterative process. This view is aligned with Peffers et al. (2007) DS framework depicted in Figure 4.3. To aid practitioners in conducting DS research (DSR), Hevner and Chatterjee (2010) developed a set of questions depicted in Table 4.4 based on (Hevner et al., 2004) DS guidelines. A researcher could use the guidelines and the set of questions, to check the research progress.

**Table 4.4: DS Research Checklist (Hevner & Chatterjee, 2010, p. 20)**

| No. | Questions | Answers |
|---|---|---|
| 1. | What is the research question (design requirements)? | |
| 2. | What is the artefact? How is the artefact represented? | |
| 3. | What design processes (search heuristics) will be used to build the artefacts? | |
| 4. | How are the artefacts and the design processes grounded by the knowledge base? What, if any, theories support the artefacts design and the design process? | |
| 5. | What evaluations are performed during the internal design cycles? What design improvements are identified during each design cycle? | |
| 6. | How is the artefact introduced into the application environment and how is it field tested? What metrics are used to demonstrate artefact utility and improvement over previous artefacts? | |
| 7. | What new knowledge is added to the knowledge base and in what form (e.g. peer-reviewed literature, meta-artefacts, new theory, and new method)? | |
| 8. | Has the research question been satisfactorily addressed? | |

Furthermore, Hevner and Chatterjee (2010) align the three DS research processes: 'Relevance', 'Design' and 'Rigor', with the DS checklist of 8-questions, listed in Table 4.4, as illustrated in Figure 4.4.

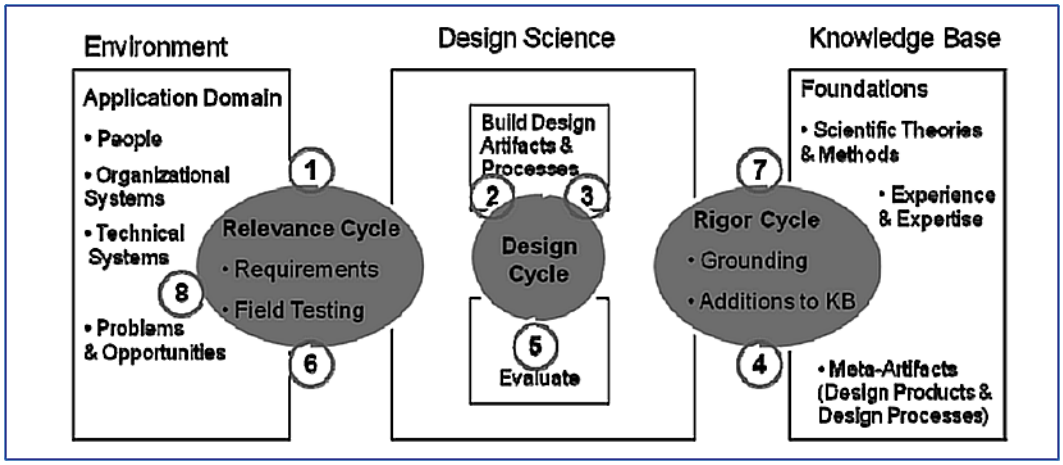


**Figure 4.4: Questions Mapped to DS 3 Cycles (Hevner & Chatterjee, 2010, p. 20)**

However, some authors argued that the DS guidelines and the questions as well as the mapping of the three DC cycles with the produced checklist questions, shown in Figure 4.4, are deemed too abstract. New practitioners to DS, could find it too high level and generic to follow (Peffers et al., 2007; Alturki et al., 2011a). In addition, DR abstract guidelines, while they enable researchers to adopt the guidelines for many types of research, the guidelines lack of specificity that causes another conflicting issue (Alturki et al., 2011a; Alturki, Gable, & Bandara, 2013). To streamline tasks and activities at each of the stages Alturki et al. (2011a) have developed a roadmap and further refined the roadmap as depicted in Figure 4.5, which is aligned with the three DS cycles.

Alturki et al. (2013) indicate that the DSR roadmap (Alturki et al., 2011b) is still evolving despite being evaluated and refined. The authors indicate that the DSR roadmap adopts IS Design Theory (ISDT) and includes a Central Design Repository (CDR) to document all the details of a DS research project, as it progresses. The authors further describe the roadmap, from the top view, in its centre to the left the Environment and to the right the Knowledge base sections. It contains four main interrelated components: (A) DS research cycles, (B) DS research output, (C) DS risk management, and (D) Central Design Repository (CDS). As illustrated in Figure 4.5, component A feeds and reads from component D, which in turn, feeds into component B. The two components D and B, contribute to the two sections: Environment and Knowledge base. In the centre, the roadmap

contains detailed tasks and activities that are defined at each of the three cycles. While it still appears generic and high level, the roadmap tasks drill down further from the DS guidelines shown in Table 4.3. A full discussion on the content of the DSR roadmap depicted in Figure 4.5 and summarised with the defined tasks headings in a table in sub-section 4.3.4. A detailed discussion of the roadmap contents can be found in the cited published paper.

The roadmap designed by Alturki et al. (2011a) and refined by Alturki et al. (2011b) as noted above. While it is still evolving, however, it has been influenced by the aspects discussed in many papers by various authors in DS. Hence, in this research the roadmap along with the three cycles and the checklist questions defined by Hevner and Chatterjee (2010), have been adopted.

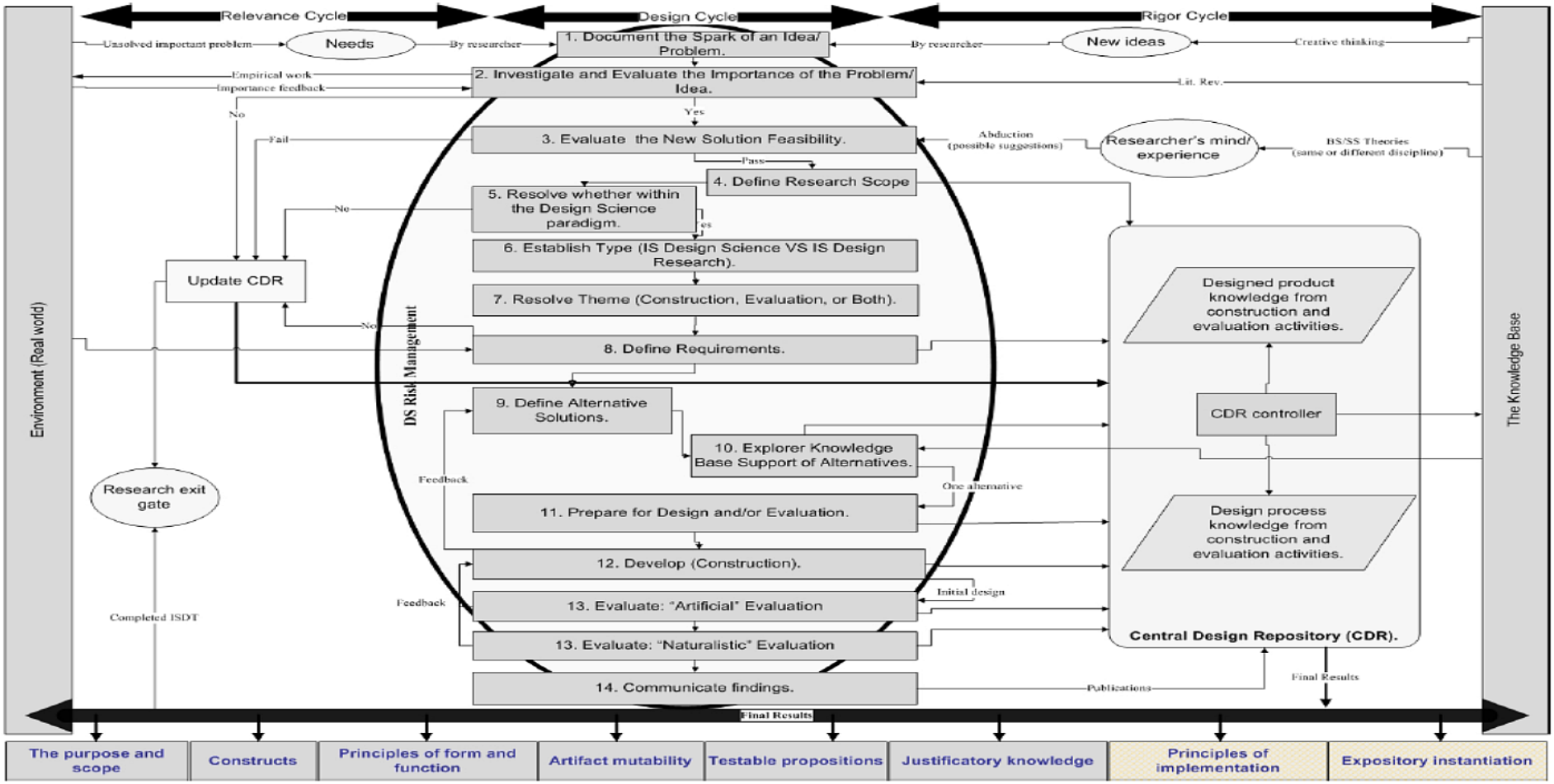


**Figure 4.5: The Overall Design Science Research Roadmap (Alturki et al., 2011b, p. 6)**

### 4.3.4 Design Science – Research and Artefact Evaluation

According to Alturki et al. (2011a) it is not enough to have an important un-resolved problem to initiate DS based research; rather, the question is "Is it possible to produce a new solution?" (p. 111). Markus (1997) puts a great emphasis on evaluation aspects for practical research, and indicates the necessity of validating the solution empirically. In sub-section 4.3.3 a detailed discussion has been conducted and tables and figures outlined the DS guideline and roadmap, to evaluate the DS research as a whole. This is to ensure a systematic approach of conducting the research and to detect any issues and correct the course of action, if warranted.

Moreover, resulting artefacts from DS research also require a thorough evaluation that is to be designed according to the type of the produced artefacts. According to Offermann et al. (2009); Vaishnav and Kuechler (2008) when solution artefacts reach an acceptable stage, they can be evaluated against some defined criteria. The evaluation criteria themselves could evolve from one evaluation cycle to another. In the same way Oates (2006) states that artefacts must be evaluated, and suggests examples of evaluation criteria, such as: functionality, completeness, consistency, accuracy, performance, reliability, accessibility, and fit with organisation. It is imperative, according to Vaishnav and Kuechler (2008) any detected deviation "must be tentatively explained" (p. 21). In this phase hypotheses are made about the behavior of the produced artefacts. It demonstrates a distinction from positivist based research, where hypotheses are tested and either proved or not. In addition, Offermann et al. (2009) claim that it is challenging to evaluate the general research hypotheses as a whole, rather, they suggest the hypothesis is refined by 'smaller' hypotheses. According to Vaishnav and Kuechler (2008) detected deviations in DS research present interesting findings to interpret and to find an explanation, which would lead to new or refined knowledge.

According to Oates (2006) many researchers tend to evaluate the artefacts with an objective of show 'proof of concept' rather than evaluating the artefacts in real-life context. Furthermore, artefacts should be evaluated from functional perspective, rather than the details of how the artefacts are constructed and/or organised (Vaishnav & Kuechler, 2008). Offermann et al. (2009) indicate that evaluation could be accomplished via a case study, action research by

demonstrating the applicability in practice, surveying experts in the field, or by laboratory experiment. Similarly, Oates (2006) indicates that some of the data generation methods such as critical reflection, observations, questionnaires and documents, could be deployed.

Hevner and Chatterjee (2010) point out that according to a pragmatic philosophy, which "argues that truth (justified theory) and utility (artefacts that are effective) are two sides of the same coin and that scientific research should be evaluated in light of its practical implications" (p. 12). In that view, evaluating the research artefacts applicability is equally important to how the research is executed to achieve its planned objectives. Hence, in the DS guidelines shown in Table 4.3; guideline no. 3 – Design Evaluation, the design artefacts utility, quality and efficacy are verified through an adequately executed evaluation plan. It is imperative to balance the efforts spent on building and evaluating the design artefacts (Hevner & Chatterjee, 2010).

According to Venable (2006) produced artefacts are to be evaluated in two stages, or types: Artificial and Naturalistic evaluation. The former, is defined as "the design solution or artefact is tested in a stilted way where it pass on to external evaluation or return to the design step for refinement before entering the same loop again" (p. 23). As for the Naturalistic type, which is "the 'real' test where the invented designed solution or artefact is tested in an actual organisation to check the how good or bad it is" (Venable, 2006, p. 23). The two types of evaluations are adopted in the DSR roadmap devised by Alturki et al. (2011b) and shown in Figure 4.5. Ostrowski and Helfert (2012) refer to them as Internal and External evaluation that aim at ensuring the quality of the produced artefacts.

When evaluating artefacts it is imperative to do that with defined criteria based on the requirements of the context for which the artefacts are developed (Peffers, Rothenberger, Tuunanen & Vaezi, 2012). Various authors have indicated evaluation criteria, around efficacy, effectiveness, performance, and applicability. Prat, Comyn-Wattiau, and Akoka (2014) conducted an interesting study; researching, analysing and evaluating what a number of authors have published. Prat et al. (2014) produced a comprehensive artefacts evaluation criteria framework, shown in Figure 4.6. Prat et al. indicated that "DSR in IS lacks a systematic list of evaluation criteria for artefacts and an associated set of evaluation

methods" (p. 23). The essence of the framework is considering "IS artefacts as systems to be evaluated" (p. 23), hence the authors apply general systems theory in the framework they developed. This is aligned with what has been discussed in Chapter 2, section 2.4, in which it has been argued that to manage organisation's IT risks, system thinking is required to find an effective solution.

Prat et al. (2014) indicate that their evaluation criteria framework outlined in Figure 4.6 accommodate the five fundamental dimensions of systems: goal, environment, structure, activity and evolution.

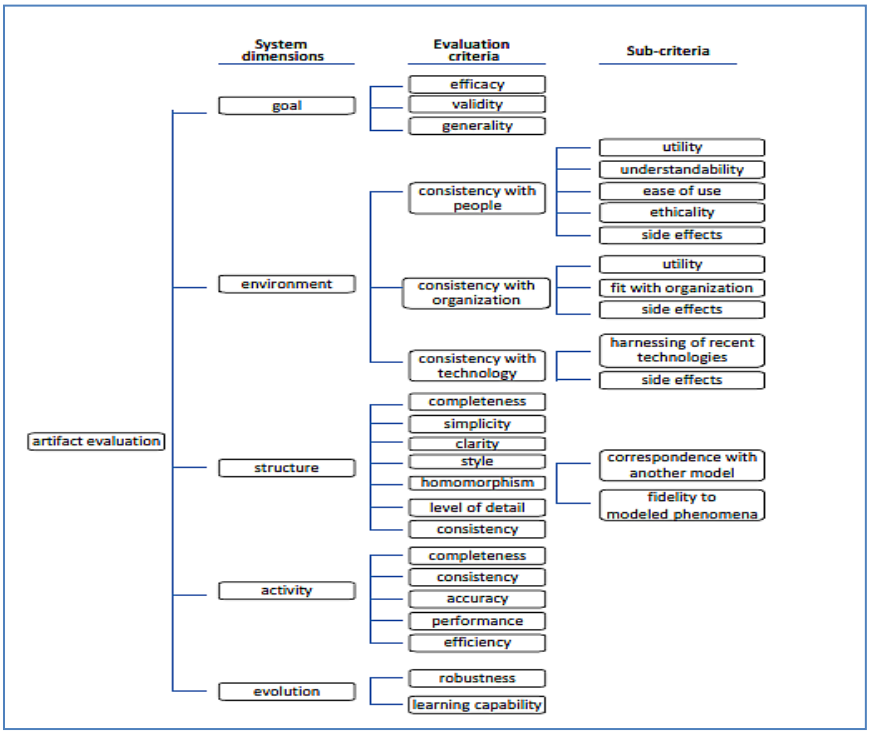


**Figure 4.6: Hierarchy of Criteria for Artefacts Evaluation (Prat et al., 2014, p. 29)**

## 4.4 DATA AND EVALUATION REQUIREMENTS

The DS research requires data to evaluate the artefact. Figure 4.7 summarises the relationship between the research question and the data requirements. The research data plan comprises of gathering experts' evaluation and feedback in written and oral forms, after using the developed solution. The collected evaluation-data is analysed, critically reflected upon, and the research findings are articulated. The objective is to answer the research question and sub-questions, and to provide the anticipated research outcomes - which are the controls and processes selection criteria and potential mechanisms to ensure their effectiveness and efficiency.

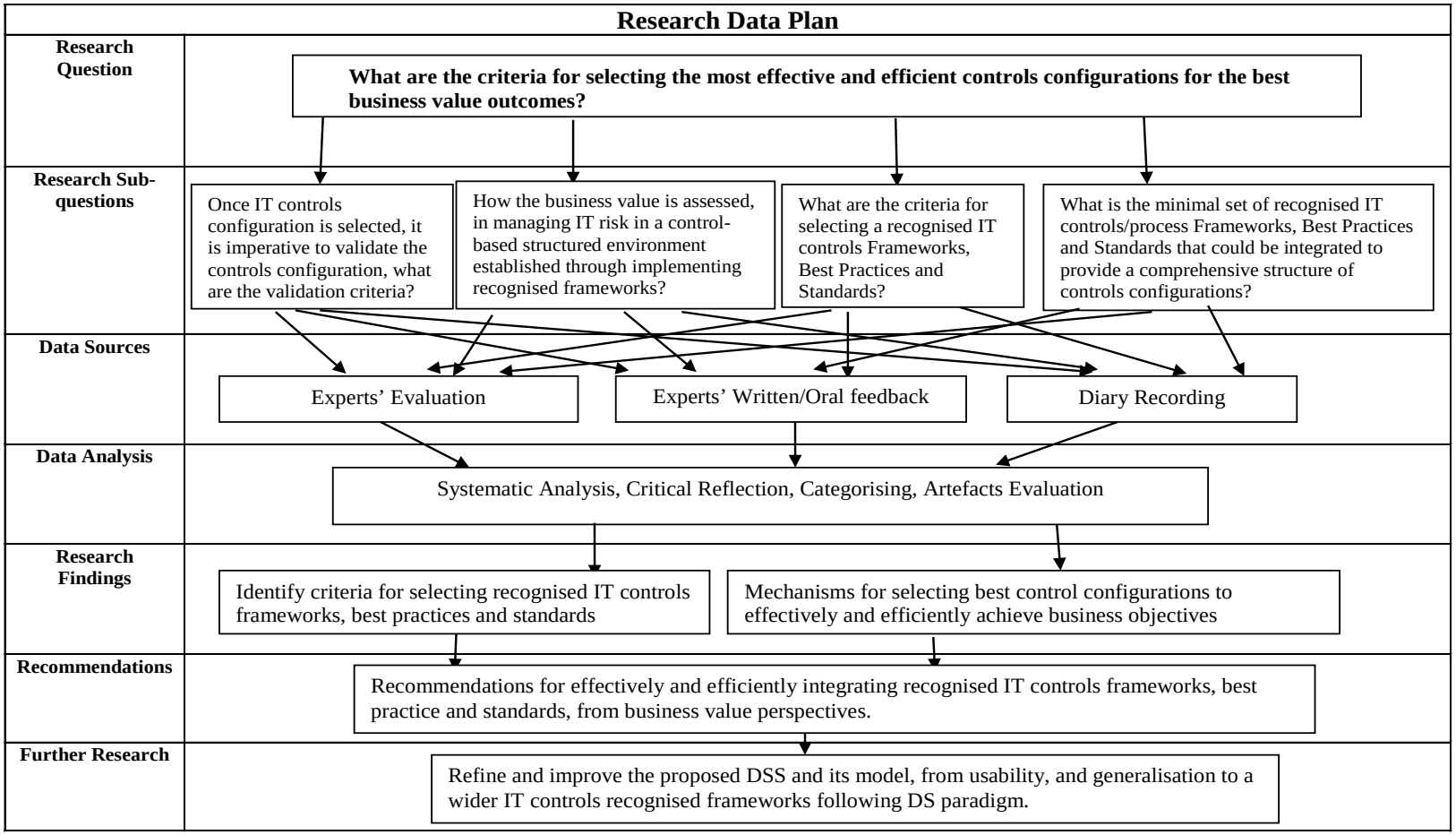


**Figure 4.7: The Research Data Plan**

The DS methodology allows continuous improvement of the artefacts by going through sequences of revisions. It is planned to complete two evaluation cycles in the available time and to deliver recommendations for further improvement. DS does not provide a true or perfect outcome but rather it delivers utility value and quality improvement recommendations for further development and research.

This section outlines the data requirements based on the DS research methodology for ensuring quality artefacts are produced. The section is structured as follows: sub-section 4.4.1 reviews the data collection methods deployed in the research. While sub-section 4.4.2 explores data analysis, and sub-section 4.4.3 examines data visualisation options. Lastly, sub-section 4.4.4 outlines the developed artefacts for the research.

### 4.4.1 Data Collection Methods

The DS paradigm is adapted in this research. The approach, as it has been argued by a number of scholars that DS is a multi-paradigmatic framework. Following the DS research framework by Peffers et al. (2007), guidelines and roadmap by Hevner et al. (2004) and Alturki et al. (2011b) respectively, the adoption is well-positioned. Data gathered from expert opinion evaluation will be interpreted to aid in determining the validity of the produced artefacts. Collis and Hussey (2009) describe qualitative data as “normally transient, understood within context” (p. 143). They argued that since qualitative data need to be understood within the context, it is imperative to gather data about the subject background, which is defined as ‘contextualisation’. Collecting data is one of the hardest parts (Yin, 1984). Yin adds that to gather data the investigator needs to have a set of skills, for example: be able to ask good questions; be a good listener, flexible and adaptive, and knows the subject very well and to be unbiased.

However, data collection should be controlled to some extent to avoid having uninterpretable data, which is one of the deficiencies noted by Yin (1984). Various data collection methods will be utilised to validate the gathered data in a form of ‘triangulation’ (Taylor & Bogdan, 1998). Data will be processed, analysed to test and evaluate the produced artefacts, and make any changes deemed necessary. Furthermore, the resulting analysis can be used to assert hypotheses and to draw inferences (Yin, 1984). Analysed data can be presented in various forms

and facilitated by using software for analysing qualitative data (Gibbs, 2002), and/or in any other form found necessary.

Data will be collected from three sources: Expert opinion evaluations of the produced artefacts (DSS design and utilisation of the developed model), and critical reflection and feedback, archival records and diary recording (Yin, 1984). According to Collis and Hussey (2009) experts and archival records are common data collection. While other forms of data collection are possible, for example, a survey, however, this has been ruled out because of time constraints.

Experts' feedback will be gained from participants from internal audit, IT audit, IT security and risk management, IT division manager, and business unit management. Also academic experts will be consulted for feedback.

#### 4.4.1.1 Experts Evaluation

The evaluation phase of DS based research is vital to assess the solution design, as it has been outlined in sub-section 4.3.4. According to Peffers et al. (2012) experts' evaluation that utilises 'logical arguments' is part of the evaluation method classifications, where artefacts are evaluated by one or more experts. It is anticipated that the evaluation method is driven by the type and nature of artefacts (Peffers et al., 2012). Alturki et al. (2011a) point out the importance of preparation of functional specifications, metrics or criteria to evaluate the various aspects of the developed artefacts. According to March and Smith (1995) metrics should be defined before commencing the evaluation, as they play vital role in the evaluation process. To ensure quality evaluation is conducted, Alturki et al. (2011a) indicate that attention should be paid, when selecting an environment and experts who evaluate the artefacts.

Experts' feedback (IS/IT auditors, IS security and risk managers, IT line managers) evaluation is planned to take place in two stages (Internal/Artificial and External/Naturalistic) (Venable, 2006; Alturki et al., 2011a; Ostrowski & Helfert, 2012). The first stage is to be conducted by 2-3 practitioners to obtain initial assessment of the designed DSS structure; analyse the data gathered at that stage and make any adjustment to the design, if required. That would involve asking experts for their opinion about the designed model as well as some questions and sub-questions as noted in sections 4.1.2 and 4.1.3. The second stage will be repeated with another 4-6 experts, to test the artefacts in the real environment, excluding the

first practitioners involved in the initial evaluation. Similar data gathering and analysis procedures will be followed.

According to Mantelaers (1997) selected Experts must have many years of relevant experience in the field, in order to be acknowledged as an expert in the field. The researcher has carefully examined the background of the nominated experts in order to obtain credible evaluation of the developed artefacts. Mantelaers (1997) indicates the importance of knowledge elicitation in gathering expert opinion in various possible ways, so that data will be analysed and modelled, to form practical guidelines to address the identified problem. However, eliciting expert opinion cannot be observed directly according to Wijers (1991, as cited in Mantelaers, 1997) who points out the challenges of data gathering from experts and outlines some types of data gathering. For example, written and oral feedback are the most common methods as they encourage experts to outline their explanation and make clarification. In addition, protocols such as 'Think Aloud' and 'Introspection' can be utilised to obtain expert views on problem solving, and thinking about artificial problems. Those protocols have advantages and disadvantages, but can be utilised to gather quality data from the experts, when the cons are mitigated.

#### 4.4.1.2 Diary Recording

In DS based research, continually thinking about the effectiveness of the produced artefacts, is essential. It is widely known that the diary recording method is used by people to record daily events or issues for different purposes. The researcher will be using this method to record any issues and/or observations that may arise during the research in relation to the artefact build and use. Trauth (1997) highlights the importance of diary recording. Collis and Hussey (2009) point out that diary recording is a good method for collecting qualitative data. Berndtsson et al. (2008) suggest recording researcher observations would help validate the research results. Diary recording may also be used to record informal observations during evaluation as indicated by Tavalea (2008).

### 4.4.2 Data Analysis

As noted in section 4.4.1.1, expert written and oral feedback could be obtained and collated for analysis. Data analysis methods are either qualitative or quantitative.

However, it is necessary to emphasise that IS research adopting DS research methods offers the possibility to combine qualitative and quantitative materials. Some artefacts may vary from software, formal logic, and rigorous mathematics to informal and natural language descriptions (Hevner et al., 2004). While mathematical basis artefacts would require quantitative analysis methods, other types of artefacts that relate to organisational context would require empirical and qualitative methods. As the collected data for this research is qualitative data the focus of this discussion is on qualitative analysis methods. Yin (1984) points out the difficulties of data analysis, to filter out the noise and avoid bias and subjectivity, which are common to qualitative data.

After collecting data from the experts, data will be processed by tabulating. Berndtsson et al. (2008) point out that once data is obtained then data sets are systematically analysed; the analysis, means "you evaluate the data against the objectives of the project" (p. 73). The researcher will be conducting critical reflection on the gathered data resulting from the experts' evaluation of the DSS and its core model. As shown in Table 4.6, in sub-section 4.4.5, the artefacts evaluation criteria and corresponding questions will be used to benchmark the artefacts experts' evaluation and feedback.

### 4.4.3 Data Visualisation

In DS based research communicating the outcomes is crucial to ensure repeatability and to aid practitioners benefit from the produced artefacts (Hevner et al., 2004). In addition, it helps build an accumulative knowledge base for further extension and evaluation. When expert evaluation and other data are collected and systematically analysed, data sets are formed in various forms that allow inferences to be drawn and/or action taken (Denzin & Lincoln, 1998). The process entails reduction in the data set based on the coding that should have taken place at an earlier stage. Bailey (2007) describes visual representation "as a means by which the researcher can literally show the results to an audience" (p. 152). Denzin and Lincoln (1998) list some examples of those visual representations, such as structured summaries and synopses. Bailey (2007) also state that visual presentation could be resembled visually or textually in the final manuscript. Bailey (2007) refers to a set of examples of presentation forms: drawings, conceptual maps, matrices, tables, and

charts. These forms “would serve not only as visual presentation of what one has learned through analysis but also as generative, analytical techniques” (p. 151).

### 4.4.4 Developed Artefacts

In Chapter 3 sub-section 3.4.3, it has been discussed that an interactive DSS with a model in its core will be developed to aid practitioners work out the best set of controls is the focus of this research. The artefacts would aid practitioners to mitigate the defined risks. Such DSS would enable practitioners utilise their expertise in the subject domain, and also be able to change, at ease, the risk parameters and corresponding controls cost. The gained value could also be altered as circumstances change so that selected controls are current and cost effectively mitigate the defined risk.

In order to develop a DSS, it is imperative to analyse the environment or the affecting factors on the decision making. When developing DSS it must be custom-designed, developed and implemented for each specific application/environment. Organisations don’t have to build a mega-enterprise DSS but rather building first a small, specialised solution that solves the identified problem. As it has been discussed in section 3.4.3, evaluation is an integral part of DSS development process as it is the control mechanism for the entire iterative design process of DSS. Hence a prototype is ideally a small but usable system for a decision maker. As the system evolves, however, it must be evaluated continuously. The DSS system, through the iterative process, evolves in complexity and encompassing more aspects of the domain subjectivity. Prototyping has advantages such as that the stakeholders are involved in every phase and iteration and learning is integrated into the design process to devise a suitable system.

In Chapter 3, section 3.3, it has been emphasised that attempting to resolve complex systems problems, requires suitable level of expertise to find quality solutions. The expertise could be provided by a DSS equipped with a knowledge base component, and/or a means to capture knowledge and experience of senior practitioners. In reflection on the research subject, a system where the knowledge of senior practitioners (IT auditors, security and risk management specialists) in applying controls from recognised IT controls frameworks could be utilised to help novice practitioners in mitigating IT risks. This would come without the need for

novice practitioiners to spend many years developing the required expertise. Subsquently, those inexperienced practitioners would be able to select the best set of controls that returns the best value. Table 4.5 outlines the proposed DSS and its components.

**Table 4.5: DSS Components**

| DSS Component | Description | Implementation |
|---|---|---|
| Interface – Input / Output | Currently only Input is developed for assessing IT risks. | Provided in the Risk Register spreadsheet with risk analysis attributes of Impact and Likelihood. |
| Data | IT General Controls (ITGC) and associated risks. Selected Access Management as a sample of Security controls part of ITGC. | Provided in the Risk Register |
| Knowledge Base | COBIT 4.1, ITIL 3.0, ISO 27001/2 mapping documents. | Extracted relevant controls and process from publicly available documents and |
| Model | A model based on cumulative impact distribution analysis. More details are provided in Chapter 5. | In a spreadsheet. |

The DSS Tool is constructed to analyse risk impacts and likelihood of the risk. The Risk definition, analysis, assessment and evaluation for a resulting overall risk rating could be done in a conventional risk register by simply using a spreadsheet. For this research 'Access Management' (AM) has been selected, as a sub-set of the IT General Controls (ITGC), as AM has strategic, security, project and operational risks.

Three high level AM Risks have been identified:

- Unauthorised access (Accounts, Systems, Applications)
- Unauthorised changes (Accounts, Systems, Applications)
- Data Leakage (Industrial Espionage, Compliance and Privacy issues)

Corresponding mitigating measures have also been identified utilising publicly available documents that map COBIT 4.1 to ITIL v3.0 and ISO 27001/2.

### 4.4.5 Artefacts Evaluation Criteria

As it has been discussed that two kinds of evaluation will be carried out (Internal/Artificial) and (External/Naturalistic) (Venable, 2006; Alturki et al., 2011a; Ostrowski & Helfert, 2012). Artefacts evaluation criteria based on a system approach derived by Prat et al. (2014) as noted in Table 4.6 are to be used with the criteria and possible questions devised by the researcher.

**Table 4.6: Artefacts Evaluation Criteria - Questions**

| System dimensions | Evaluation criteria | Sub-criteria | Questions |
|---|---|---|---|
| Goal | Efficacy | | Q1. How effective is the proposed DSS in managing the defined IT risks. |
| | Validity | | Q1. How reliable the DSS outcomes are?<br>Q2. Is the risk assessment adequate? |
| | Generality | | Q1. How easy is it to update the included frameworks in the DSS? E.g. replace ITIL 3.0 with ITIL 2011, ISO 27001-2005 with 27001/2013.<br><br>Q2. Is DSS capable of including all ITGC risks?<br><br>Q3. Could the DSS include other frameworks, e.g. ValIT, COSO_ERM? |
| Environment | Consistency with people | Utility | Q1. What is the total gained value, from practitioner's perspective? |
| | | Understand-ability | Q1. Is the DSS intuitive? |
| | | Ease of use | Q1. Is the DSS easy to use? |
| | | Ethicality | Q1. Does using the DSS have or could cause any ethical issue? |
| | | Side effects | Q1. Does the DSS or model produce new risks and/or incur further cost? |
| | Consistency with organisation | Utility | Q1. What is the total gained value, from organisation's perspective? |
| | | Fit with Organisation | Q1. Is the DSS (Risk Register, selected frameworks, model) adequately fit the organisation's Internal/External environment? |
| | | Side effects | Q1. Any issues caused by using this DSS? E.g. incurring further cost, complicating the environment. |
| | Consistency with technology | Harnessing of recent technologies | Q1. How effective and easy it is to accommodate new technology by the DSS? |

| System dimensions | Evaluation criteria | Sub-criteria | Questions |
|---|---|---|---|
| | | Side effects | Q1. Any issues, this DSS could cause? E.g. introducing new risks, overusing/underutilising resources, etc. |
| Structure (Static, the artefact's construct) | Completeness | | Q1. How complete the DSS is?<br>Q2. Any area of improvement? |
| | Simplicity | | Q1. How simple the DSS is structured? |
| | Clarity | | Q1. Are the DSS components clear |
| | Style | | N/A- Not to be enquired about. |
| | Homomorphism | Corresponds with another model | Q1. Does the DSS map well to other Enterprise settings if any, for example IT Governance, Enterprise Risk Management, Internal Audit, Business/IT Strategic plan? |
| | | Fidelity to modelled phenomena | Q1. Does the designed DSS align with the theorised solution design and meet fidelity criteria exhibiting least deficiency (redundancy, incompleteness, excess, and overload)? |
| | Level of detail | | Q1. Does the DSS provide enough details and instructions on use? |
| | Consistency | | Q1. Are the DSS components developed in (spreadsheets, word, other applications) consistent? |
| Activity (Dynamic, the operations and functionality of the artefact) | Completeness | | Q1. Does the DSS have the right set of functions? |
| | Consistency | | Q1. Does the DSS operate consistently? |
| | Accuracy | | Q1. How accurate the DSS functionalities are? |
| | Performance | | Q1. Any issues with performance? |
| | Efficiency | | Q1. How efficient the DSS is in terms the utilised time/resource and the obtained outcomes? |
| Evolution | Robustness | | Q1. Does the DSS accommodate changes in internal/external environments? E.g. business dynamics, regulatory requirements, that requires assessing risks on timely fashion. |
| | Learning capability | | Q1. Could the DSS – knowledge base – component enhanced with use?<br>Q2. Could practitioners add more knowledge as they use the DSS? |

## 4.5 RESEARCH PROGRESS

The DSR guidelines, process model and roadmap have been outlined in Table 4.3, Figure 4.3 and Figure 4.5 respectively. Therefore, it is helpful to review the research progress. For that purpose a matrix is presented that combines the three cycles by Hevner (2007) and the set of questions as defined in Figure 4.2 and Table 4.4 devised by Hevner and Chatterjee (2010) and the number of tasks devised in the DSR roadmap developed by Alturki et al. (2011b), as shown in Appendix B, Table B-1. Answers to the noted questions along with taken actions are documented as shown.

It can be seen that the 'Relevance' cycle requirements, apart from answering the research question, have been achieved through the noted activities as documented in Chapter 2, 3 and 4 this far.

## 4.6 RESEARCH METHODOLOGY LIMITATIONS

The selected method for this research has been designed to provide reliability and a means to collect and analyse data. This would lead to answer the outlined questions and finding a solution to the research focus problem. However, Berndtsson et al. (2008) claim that "a method is only valid and reliable within a certain range of uses" (p. 56). As any research methodology, the selected DS methodology has limitations (Oates, 2006; Hevner et al., 2004; Vaishnav & Kuechler, 2008). Hevner and Chatterjee (2010) and, Oates (2006) indicate it is difficult to differentiate between DS research versus professional design. In addition, Oates (2006) points out a number of disadvantages that a DS researcher could face such as proving that an innovative outcome has been achieved. Also it can be difficult to generalise the research outcomes to a wider setting, and a researcher needs to have necessary technical and/or artistic skills. Simply being enthusiastic is not enough. Moreover, the research outcomes could be invalidated by rapidly evolving technologies that could render the artefacts inapplicable and/or obsolete.

Trauth (1997) indicates that qualitative methods, while they have their strengths, they also have some limitations and issues that could hinder the research effort. For example, the education of IS professionals involved in the research

(Trauth, 1997). In another words, the educational background and experience level of the selected expert opinion to evaluate the research artefacts would evidently present a level of discrepancy from one expert view to another.

This section discusses those limitations, their potential impacts on the research and viable mitigating measures to reduce the impact to a manageable level. A reasoned explanation is provided. Sub-section 4.6.1 explores reliability, while sub-section 4.6.2 examines validity, and lastly, sub-section 4.6.3 discusses generalisation.

### 4.6.1 Reliability

Reliability is the accuracy of the selected research method in measuring or developing a proposed model. Stated differently, how adequate is the method in meeting the planned research objectives (Berndtsson et al., 2008). Another definition of reliability is, according to Collis and Hussey (2009) "refers to the absence of differences in the results if the research were repeated" (p. 64). That is, if another party attempts to conduct the same research, would they get similar results? A view shared by Trauth (1997) who emphasises the importance of being able to produce trustworthy results and institute meaningful findings and of interest to the audience. Most importantly, the results can be re-produced, should another researcher attempt to conduct and follow the same research procedure. The level of reliability influences the decision of whether to trust the findings of the research or not. It also affects other researchers to use the proposed research methodology in conducting similar research. Yin (1984) and Simones (2009) recommend documenting the research procedure so that it can be re-performed again following the same steps that have been done in the first run. The aim is to minimise the errors and biases in a study, argue Yin (1984) and Simones (2009). Similarly, Trauth, (1997) suggests that being aware of this issue would aid a researcher to put that into perspective to limit the impact.

Collis and Hussey (2009) claim that reliability mostly concerns positivist studies, while under the interpretive paradigm reliability is of little importance. Collis and Hussey further add "The qualitative measures do not need to be reliable in the positivist sense" (p. 53). While this research is designed to be conducted under DS paradigm, and as indicated, the collected data are qualitative data via

qualitative data gathering means. Trauth (1997) indicates that qualitative methods, while they have their strengths, however, they have some limitations and issues that could hinder the research effort. For example, the education of IS professionals involved in the research (Trauth, 1997). However, the DS three processes devised by Hevner (2007) see Figure 4.6, (Relevance, Design and Rigor cycles) along with the repetitive aspect of the processes, provides self-detection and enables researchers applying necessary changes when necessary. Furthermore, the framework developed by Peffers et al. (2007) based on the Hevner et al. (2004) guidelines, would ensure an adequate documentation of the research procedures as the research progresses. This would provide another cycle of assurance to mitigate the outlined limitations concerning reliability.

Data analysis will be performed using quasi-judicial method, where "a rational argument is used to interpret qualitative data" (Collis & Hussey, 2009, p. 174). Collis and Hussey further indicate that quasi-judicial method, drawn from legal profession is adequate to interpret empirical data. In addition, the method focuses on the nature and source of the data, and data analysis is not kept until the end of the study. Collis and Hussey (2009) indicate that for interpreting qualitative data, defined procedures and protocol would ensure authenticated results. Eriksson and Kovalainen, (2008) have a similar view on the need for high reliability for quantitative data but not so much for qualitative data.

In the researcher's view, this measure is viable and would mitigate the risk indicated in this type of limitation. The research design has been argued and documented at all levels, as demonstrated in the research design section. Furthermore, the artefatcs evaluation types have been planned to be conducted on due course. Artefacts evaluation criteria have been adapted to assess the artefacts when data is collected. This to ensure the evaluation is conducted methodically and documented procedures would ensure repeatability.

### 4.6.2 Validity

According to Berndtsson et al. (2008) validity is the relationship between what a researcher intends to measure or develop and what it is actually measured or developed. Validity is of a particular concern for qualitative researches. Collis and Hussey (2009) define validity as "the extent to which the research findings

accurately reflect the phenomena under study" (p. 65). That is, how accurate the findings and the drawn conclusions of what have been investigated are and what evidence have been provided to ascertain the results (Eriksson & Kovalainen, 2008). Construct validation is a term used that is of importance to business research. Collis and Hussey (2009) indicate that validity is demonstrated in an interpretive paradigm analysing qualitative data, and the positivist paradigm has to have a high reliability to reproduce similar results. Kvale (1996) shares the same view stating that "qualitative research can, in principle, lead to valid scientific knowledge" (p. 238). In line with that DS based research utilising qualitative means would utilise the strength of qualitative data gathering and analyses and manage the weaknesses to an acceptable level, without jeopardising the research objectives.

Yin (1984) refers to this limitation as construct validation and indicates that there is a high level of 'subjectivity' in data collection. A view shared by Berndtsson et al. (2008), who also refers to subjectivity in, conducting interviews, preparing surveys and questionnaires and analysing the data. In the same way according to Trauth (1997), one important aspect of any qualitative research project is the 'subjectivity' of the expert opinions. When they evaluate the artefacts and provide their feedback, subjectivity is involved. Also the researcher's view would play a part, as the researcher would be conducting the interaction and analysing the data. However, Simones (2009) argues that in qualitative research subjectivity is not a negative thing. In addition, subjectivity cannot be totally eliminated. Trauth (1997) claims that in qualitative research, it can never be completely objective and judgment free, although reducing the subjectivity level would help in gaining more credibility in the research results. To reduce its impact a form of triangulation can be used that collects various forms of data from different resources and cross checking the outcomes (Yin, 1984). Trauth (1997) refers to triangulation of the collected data, which can be utilised to build confidence in the interpretation and understanding of any anomalies, should any discrepancy occur. The researcher's observation of the research participants' reactions, plays a part in triangulating collected data should any contradiction be witnessed and/or data are collected through others means.

In this doctoral research the data collection methods of expert evaluation, critical reflection, document collection and diary recording should help in the

triangulation of the collected data. Obtained feedback will be analysed as more data is gathered, considering the experts' background and depth of experience in the relevant fields. Experts' perspectives will be analysed, compared and reflected upon to identify any patterns or anomalies in the adapted approach or developed artefacts. Also, the researcher's observations noted in the diary recordings are reviewed regularly. Trauth, (1997) suggests that being aware of the existing issue of subjectivity would aid a researcher to put that into perspective when gathering and analysing the collected data. However, as it is only the researcher who works on the research, there will be a level of subjectivity in analysing and justifying the outcomes. The researcher would endeavour to provide as much evidence as possible to ascertain the inferred conclusions. Data collection methods are outlined in Figure 4.7, which depicts the research data plan, to facilitate the stated objective.

### 4.6.3 Generalisation

Generalisation, or external validity in the Yin (1984) definition, is the ability to apply the research findings into a wider setting. Generalisation has been recognised as a limitation in any research. Oates (2006) highlights a number of difficulties in DS based research and refers to the generalisation limitation as "it can be difficult to generalise settings from the use of an IT artefact in a single situation" (p. 122). With the results of DS research conducted in a specific context, once evaluated and its applicability is approved, then another project could take place to generalise the research outcomes into a wider context (Hevner & Chatterjee, 2010). Evaluating applicability is of high importance in DS based research. In addition, key objectives of DS based research are, developing innovative artefacts, which would comprise valuable utility, and adding new knowledge, that would help a better understanding of the complex domain.

In addition, similar critiques of other types of research are made. For example, case studies are helpful, however, Yin (1984) refers to critics of generalised findings of one case study to the universe. Yin (1984) argues that the critics are inadequate as they implicitly make analogy to survey research. Survey research is based on statistical generalisation, while case study research is based on analytical generalisation. According to Kvale (1996) analytical generalisation

"involves a reasoned judgment about the extent to which the findings from one study can be used as guide to might occur in another situation" (p. 233).

Generalisation, however, does not take place automatically argues (Yin, 1984) and asserts that "a theory must be tested through replication of the findings in a second or even a third neighbourhood" (p. 44), or another setting. That highlights the importance of communicating the research outcomes in meaningful ways (Hevner et al., 2004; Hevner & Chatterjee, 2010). The communication of the research findings is the last guideline (see Figure 4.5). Hevner et al. (2004) emphasise the importance of presenting the outcomes to both technical and management audiences. The level of technical details provided would enable practitioners to re-evaluate the outcomes, extend the scope and replicate in different settings, which would facilitate generalisation of the research. As this research is following the DS guidelines by Hevner et al.(2004) and the framework articulated by Peffers et al. (2007), along with DS roadmap by Alturki et al. (2011b) evaluating the adherence to the outlined activities of DS framework, would ensure the research objectives are met and the solution design mitigates the impact of this limitation.

## 4.7 FORECASTED RESEARCH OUTCOMES

By conducting this research the researcher aims to find quality improvement solutions to a difficult problem. The answers help identify the criteria for selecting the best performing IT controls configurations that would return the highest business value outcomes. The literature review showed business value comes in many forms and at different stages within an organisation's business and IT interaction: strategic, financial, and operational activities. Furthermore, it was argued that the interdependency of IT risks and their many-to-many relation to controls and processes. An anticipated outcome is to provide insight to help practitioners understand the complex relationship between risks and corresponding controls and processes. That insight could help in making better decisions when selecting the best set of controls without causing further risks or incurring addition cost

The key anticipated outcomes are to identify the selection criteria of the recognised IT controls and processes frameworks, best practices and standards. As there are many of such recognised settings, and they continue to increase, defining

selection criteria would be paramount to ensuring a selected framework would return the best business value. Identifying best controls configurations and frameworks selection criteria, would contribute to address other problems raised in the literature review. For example, best practice in keeping efficient and sufficient IT risk management process that underpins an up-to-date IT risk program, to ensure secure and reliable IT systems.

Further research is required into many aspects of this project and the DS methodology can manage this risk. It is anticipated that new knowledge will be generated about constructing effective control configurations processes, process improvement and the challenges facing the user acceptability of the proposed design solution.

## 4.8 CONCLUSION

The review and analysis of the problems identified in the literature review helped to choose a focus problem in this research. One researchable problem has been selected and in this chapter questions and hypotheses developed to guide the research. The research question is:

**What are the criteria for selecting the most effective and efficient controls configurations for the best business value outcomes?**

The question is to be answered by building a decision support system to improve the efficiency of IT control use in business environments.

The DS methodology has been selected and evaluation criteria for the artefact utility adopted. Data will be collected in various ways: expert evaluation, critical reflection, document collection and diary recording. In chapter 5 the build of the DSS model and the first evaluation are reported. The outcome of the first evaluation will then feed into the quality improvement cycle of the DSS and its second evaluation reported in chapter 6.

# Chapter 5

# Results and First Evaluation

## 5.0 INTRODUCTION

In Chapter 4 the research methodology based on the Design Science (DS) methodology has been explored, demonstrating its suitability to achieve the research objectives. The research methodology aspects were discussed and outlined based on the DS research guidelines (Hevner et al., 2004), DS process three cycles (Hevner, 2007) and set of questions (Hevner & Chaterjee, 2010), and the DS roadmap driven by Alturki et al.(2011b) as depicted in Fig 4.5. In Chapter 3 it has been argued that developing an interactive DSS, to enable the researcher find an answer to the raised question. The answer, is about the selection of controls and the computation of their relative business value impact. The DSS model would also assist practitioners in selecting the most effective control configurations from frameworks, best practices and standards. Based on the defined risks that associated with IT assets and processes such a tool will be a valuable instrument in business decision-making.

In this chapter, the developed interactive DSS components are outlined, and a first attempt is made to compute business impacts from risk mitigation assessments. Further to what has been indicated in Chapter 4, the C-Model is detailed in this chapter, and an experiment is conducted using the C-Model. While in Chapter 6 the G-Model is detailed and its evaluation outcomes are reported. A crucial activity in the DS research path is evaluating the developed artefacts.

This chapter is structured as follows: section 5.1 reviews the artefacts design and development. Section 5.2 outlines artefacts evaluation, focusing on the initial experts' evaluation for the proposed model. Section 5.3 contains a discussion and rationale for the next move based on the outcomes of the artefact evaluation. In section 5.4, a review of the research progress according to the DSR roadmap tasks and activities is made. This indicates what changes, updates and additions are implied by the artefacts evaluation and outcome statements. The chapter is concluded in section 5.5.

| Structure of Chapter 5 | |
|---|---|
| **Section** | **Page no.** |


## 5.1 ARTEFACTS DESIGN, DEVELOPMENT

In Chapter 4 sub-section 4.4.4, it has been discussed that an interactive DSS with a model component in its core for the calculation of the best set of controls would be the focus of this research. It can assist practitioners in finding the best controls combinations to mitigate defined IT risks. Such a DSS would enable practitioners to utilise their expertise in the subject domain. Also to change, at ease, the risk parameters and corresponding controls costs and gained value as circumstances change. The proposed DSS would aid in selecting controls that are current and cost effectively mitigate the defined IT risks.

The emphasis of this section however is on documenting the developed artefacts, the proposed interactive DSS and its model. This section is structured as follows: sub-section 5.1.1 outlines the DSS, while sub-section 5.1.2 details the selected IT risks and corresponding controls and processes. Sub-section 5.1.3 describes the C-Model.

### 5.1.1 DSS

In Chapter 3 section 3.3, it has been stated that problem resolution in complex systems can be facilitated by a DSS when potential solutions are required for decision-making issues. An interactive DSS equipped with an interface that provides the input-output component, as well as a knowledge base and data components is a potential solution. In chapter 4 sub-section 4.4.4, Table 4.5 was formulated depicting the details of the four components of a DSS: the Input/output, the Data, the Knowledge Base and the Model. As it is noted in Table 4.5, a risk register in a spreadsheet is prepared where the defined IT risks details are captured. and a risk assessment rating matrix, for the risk impact and likelihood. Furthermore, as noted in Table 4.5, corresponding controls and processes from recognised IT controls frameworks can be selected utilising publicly available documents. In

addition, the practitioner's expertise and knowledge in the domain can be utilised. The DSS tool was constructed to analyse risk impacts and likelihood by generating a cumulative impact distribution of the risks, by utilising a model. The model for the DSS is a central component in the research and the artefact built.

With regards to the interface, currently only Input was developed for assessing IT risks. As for the Data, a number of Access Management (AM) related risks were identified as part of the security related risks. For the Knowledge base, controls and processes from recognised frameworks and best practices were selected. Lastly, the Model, which is based on cumulative probabilities analysis, is to be elaborated on and outcomes demonstrated in this chapter. The evaluation will also show its limitations and the necessity for further investigation in a further round of DS development.

### 5.1.2 IT Risks and Controls

As discussed in Chapter 2, organisations can have various IT risks within the many IT functions, systems, applications and data. For the purpose of testing the model, it would be beneficial to select an area, as an example, that touches as many of noted IT aspects. As noted in Chapter 4, section 4.4.4, for this research 'Access Management' (AM) IT risks, have been selected. AM is a good representative of IT risks, as AM has strategic, security, project and operational risks. Aspects of AM require policy, process and procedure to implement. Also to review and revoke access rights for operating systems, file systems, applications and data for ordinary and privileged user rights. For the sake of simplicity, three high level AM Risks have been identified as follows:

- Unauthorised access (Accounts, Systems, Applications)
- Unauthorised changes (Accounts, Systems, Applications)
- Data Leakage (Industrial Espionage, Compliance and Privacy issues)

Corresponding mitigating measures have also been identified utilising publicly available documents that map COBIT 4.1 to ITIL v3.0 and ISO 27001/2.

- COBIT 4.1: DS5.3 – "Identification of all users (internal, external and temporary) and their activity".
- ITIL 3.0: SO 4.5 "Access management".

- ISO 27001/1-2: a number of relevant controls: 11.2.3 “User password management”, 11.3.1 “Password use”, 11.4.1 “Policy on use of network services”, 11.5.1 “Secure logon procedures”, 11.5.2 “User identification and authentication”, 11.5.3 “Password management system”, 11.5.5 “Session time-out”, 11.5.6 “Limitation of connection time”, 11.6.1 “Information access restriction”.

### 5.1.3 C-Model

This section outlines the core component of the DSS, which includes a model to aid practitioners decide the best controls configuration that mitigates the defined risks cost-effectively. The model, C-Model, was developed in Excel to simulate the cumulative impact distribution of the defined risks in relation to the associated controls configurations. The model name comes from the word Cumulative, as the model is based on Cumulative Probability Analysis. A cumulative probability refers to the probability that the value of a random variable falls within a specified range (Vose, 2008). Frequently, cumulative probabilities refer to the probability that a random variable is less than or equal to a specified value.

To present the cumulative frequency distribution as a continuous mathematical equation instead of a discrete set of data, a researcher may fit the cumulative frequency distribution to a known cumulative probability distribution. Any equation that gives the value 1 when integrated from a lower limit to an upper limit in the data range can be used as a probability distribution for fitting. A sample of probability distributions that may be used can be found in probability tables. Probability distributions can be fitted by the parametric method, determining the parameters such as the mean and the standard deviation from the data using a method of moments, the maximum likelihood method and the method of probability weighted moments.

**Table 5.1: Risks Analysis and Associated Controls Configurations Data Entry**

| | | R1 | r1L | r1M | r1H | | | R2 | r2L | r2M | r2H | | | R3 | r3L | r3M | r3H | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C0 | 10 | | | | | | | | | | | | | | | | | |
| 1 | | pr | 0.20 | 0.40 | 0.50 | 1.1 | | pr | 1.00 | 3.00 | 2.00 | 6.0 | | pr | 1.00 | 2.00 | 1.00 | 4.0 |
| 2 | | pr adj | 0.18 | 0.36 | 0.45 | 1.0 | | pr adj | 0.17 | 0.50 | 0.33 | 1.0 | | pr adj | 0.25 | 0.50 | 0.25 | 1.0 |
| 3 | | impact | 3 | 4 | 5 | | | impact | 1 | 3 | 5 | | | impact | 2 | 3 | 4 | |
| C1 | 15 | cost | | | | | | | | | | | | | | | | |
| 1 | | pr | 0.20 | **0.50** | **0.20** | 0.9 | | pr | 1.00 | **2.00** | **0.50** | 3.5 | | pr | **1.50** | 2.00 | | 3.5 |
| 2 | | pr adj | **0.22** | **0.56** | **0.22** | 1.0 | | pr adj | **0.29** | **0.57** | **0.14** | 1.0 | | pr adj | **0.43** | **0.57** | | 1.0 |
| 3 | | impact | **1** | **3** | **4** | | | impact | | **2** | **4** | | | impact | **1** | **2** | 4 | |
| C2 | 25 | | | | | | | | | | | | | | | | | |
| 1 | | pr | **0.40** | 0.40 | **0.20** | 1.0 | | pr | 1.00 | 3.00 | **1.00** | 5.0 | | pr | **3.00** | 2.00 | 1.00 | 6.0 |
| 2 | | pr adj | **0.40** | **0.40** | **0.20** | 1.0 | | pr adj | **0.20** | **0.60** | **0.20** | 1.0 | | pr adj | **0.50** | **0.33** | **0.17** | 1.0 |
| 3 | | impact | **1** | **3** | **4** | | | impact | 1 | **2** | **3** | | | impact | 2 | 3 | 4 | |

In Table 5.1the first panel of C-Model that describes the distribution for the cumulative impact risks (R1, R2 and R3) along with controls configurations (C0, C1, and C2). Where C0 is a set of COBIT 4.1 Controls, while C1 is a set of combined controls/processes from COBIT4.1 and ITIL, and lastly C2 comprises controls/processes from COBIT 4.1, ITIL and ISO 27001.As shown in Table 5.1, there are three risks R1, R2 and R3, and the likelihood rating of these risks can be L (low), medium (M) or high (H).

For a given control configuration Cn: **a**. the probability distribution for risk R1 are possible values of R1 and the assumed probabilities (likelihood) e.g. pr(R1=L)=0.1, pr(R1=M)=0.4, pr(R1=H)=0.5.

**b**. there is a set of assumed impact levels categorised as 0, 1, 2, 3, 4 or 5 where low is good. The impact levels are obtained from detailed analysis and are a summary of the results of that analysis.

The estimated analysis for **control configuration C0** are in the adjacent three rows from the top in Table 5.1.The cost of implementing C0 control configuration is 10 as shown in the cell (raw-column: 2-2).There are two rows for probabilities as shown (pr and pr adj). It can be seen that values of 1, 2, 1 to set to the likelihood rate M is twice as likely as L or H. Assumed probabilities (likelihood) ratings are entered in row 1 of each noted risk. The second probability row (pr adj) adjusts the entered numbers so that the set of probabilities all adds to 1.The impact of each risk level for each risk is entered in row 3 of each risk e.g. if R1 is L the impact is 3, if R1 is M the impact is 4 and if R1 is H the impact is 5. The impact levels can only enter integers between 0 and 5, this could change however, as and

when estimates deem it necessary. Similarly, for **C1control configuration** that represents controls from two recognised frameworks: COBIT4.1 and ITIL. The cost, probability and impact information is entered in respective rows. If a probability or impact differs from that entered for C0 the entry is automatically reported in bold so a comparison can be made.

In the same fashion, data for **C2control configuration** that represents controls from three recognised frameworks, standards: COBIT 4.1, ITIL and ISO 27001, are fed in respective rows. Referring again to Table 5.1, the total impact is the sum of the impacts so it is an integer between 0 and 15. It is imperative to indicate that the C-Model assumes independence of the three risk assessments. Hence, probability (R2=M) is the same whether R1=L or R1=M or R1=H. If the distribution of R2 was dependent on the level of R1, it would require the entering of three assumed probability distributions for R2. Similarly, for all other risks the assumptions are declared and the estimates qualified. For a larger number of variables the calculation of formula would look more complicated (as the numbers are being picked up from more entries) but the calculations would be the same.

#### 5.1.3.1 Calculations

When risks (R1, R2, and R3) impact and likelihood assessments are entered as noted previously, the totals are calculated for the three risk possible impact occurrences, as noted in Table 5.2.

**Table 5.2: Risks Likelihood and Impact Calculations**

| Risk Dependency | | | Risk Likelihood = probabilities Calculation | | | | Impact Calculation | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | PR1 | PR2 | PR3 | Total | IR1 | IR2 | IR3 | Total |
| r1L | r2L | r3L | 0.18 | 0.17 | 0.25 | 0.008 | 3 | 1 | 2 | 6.00 |
| r1L | r2L | r3M | 0.18 | 0.17 | 0.50 | 0.015 | 3 | 1 | 3 | 7.00 |
| r1L | r2L | r3H | 0.18 | 0.17 | 0.25 | 0.008 | 3 | 1 | 4 | 8.00 |
| r1L | r2M | r3L | 0.18 | 0.50 | 0.25 | 0.023 | 3 | 3 | 2 | 8.00 |
| r1L | r2M | r3M | 0.18 | 0.50 | 0.50 | 0.045 | 3 | 3 | 3 | 9.00 |
| r1L | r2M | r3H | 0.18 | 0.50 | 0.25 | 0.023 | 3 | 3 | 4 | 10.00 |
| r1L | r2H | r3L | 0.18 | 0.33 | 0.25 | 0.015 | 3 | 5 | 2 | 10.00 |
| r1L | r2H | r3M | 0.18 | 0.33 | 0.50 | 0.030 | 3 | 5 | 3 | 11.00 |
| r1L | r2H | r3H | 0.18 | 0.33 | 0.25 | 0.015 | 3 | 5 | 4 | 12.00 |
| r1M | r2L | r3L | 0.36 | 0.17 | 0.25 | 0.015 | 4 | 1 | 2 | 7.00 |
| r1M | r2L | r3M | 0.36 | 0.17 | 0.50 | 0.030 | 4 | 1 | 3 | 8.00 |
| r1M | r2L | r3H | 0.36 | 0.17 | 0.25 | 0.015 | 4 | 1 | 4 | 9.00 |
| r1M | r2M | r3L | 0.36 | 0.50 | 0.25 | 0.045 | 4 | 3 | 2 | 9.00 |
| r1M | r2M | r3M | 0.36 | 0.50 | 0.50 | 0.091 | 4 | 3 | 3 | 10.00 |
| r1M | r2M | r3H | 0.36 | 0.50 | 0.25 | 0.045 | 4 | 3 | 4 | 11.00 |
| r1M | r2H | r3L | 0.36 | 0.33 | 0.25 | 0.030 | 4 | 5 | 2 | 11.00 |
| r1M | r2H | r3M | 0.36 | 0.33 | 0.50 | 0.061 | 4 | 5 | 3 | 12.00 |
| r1M | r2H | r3H | 0.36 | 0.33 | 0.25 | 0.030 | 4 | 5 | 4 | 13.00 |
| r1H | r2L | r3L | 0.45 | 0.17 | 0.25 | 0.019 | 5 | 1 | 2 | 8.00 |
| r1H | r2L | r3M | 0.45 | 0.17 | 0.50 | 0.038 | 5 | 1 | 3 | 9.00 |
| r1H | r2L | r3H | 0.45 | 0.17 | 0.25 | 0.019 | 5 | 1 | 4 | 10.00 |
| r1H | r2M | r3L | 0.45 | 0.50 | 0.25 | 0.057 | 5 | 3 | 2 | 10.00 |
| r1H | r2M | r3M | 0.45 | 0.50 | 0.50 | 0.114 | 5 | 3 | 3 | 11.00 |
| r1H | r2M | r3H | 0.45 | 0.50 | 0.25 | 0.057 | 5 | 3 | 4 | 12.00 |
| r1H | r2H | r3L | 0.45 | 0.33 | 0.25 | 0.038 | 5 | 5 | 2 | 12.00 |
| r1H | r2H | r3M | 0.45 | 0.33 | 0.50 | 0.076 | 5 | 5 | 3 | 13.00 |
| r1H | r2H | r3H | 0.45 | 0.33 | 0.25 | 0.038 | 5 | 5 | 4 | 14.00 |

In Figure 5.1, shows the estimate of the impact population equation.

$$\mu_R = \mathrm{E}[R] = \sum_{k=1}^{n} r_k p_k$$

**Figure 5.1: Estimate of Impact Population**

In Figure 5.2 the standard deviation of the risk impact formula is shown.

$$\sigma_R = \mathrm{SD}[R] = \sqrt{\sum_{k=1}^{n} (r_k - \mu_R)^2 p_k} = \sqrt{\sum_{k=1}^{n} r_k^2 p_k - \mu_R^2}$$

**Figure 5.2: Standard Deviation of Risk Impact**

The impact and cumulative impact probabilities are calculated, and the results are tabulated in Table 5.3, for C0. Similar tables are generated for the other controls configurations: C1 and C2.

**Table 5.3: Impact and Cumulative Impact Calculation**

| Impact Value | Cumulative Impact | Impact Levels |
|---|---|---|
| 0.00 | 0.00 | 1 |
| 0.00 | 0.00 | 2 |
| 0.00 | 0.00 | 3 |
| 0.00 | 0.00 | 4 |
| 0.00 | 0.00 | 5 |
| 0.01 | 0.01 | 6 |
| 0.03 | 0.04 | 7 |
| 0.08 | 0.12 | 8 |
| 0.14 | 0.26 | 9 |
| 0.20 | 0.47 | 10 |
| 0.22 | 0.69 | 11 |
| 0.17 | 0.86 | 12 |
| 0.11 | 0.96 | 13 |
| 0.04 | 1.00 | 14 |
| 0.00 | 1.00 | 15 |

Subsequently, the distribution and the cumulative impact are shown in Figure 5.3, which has two charts within that show the distribution and the cumulative impact respectively. In chart 1 the risk and realisation are shown to cluster and imprint around a central value. The chart 2 reports the cumulative impact distribution and shows the risk range for which the treatment is most effective. To generalise the result it is anticipated to show the effectiveness of each control and where overlapping control impacts can be resolved to treat a risk economically.

The distribution impact of C0 is expected to be found from other controls and from controls in other control frameworks, but in each instance the distribution is forecasted to be different. The difference may be as great as independence and as close as similarity. In one control framework such as ISO 27001 it is expected the overlap between related controls is minimal. As a network or framework of controls then the overall impact distribution ought to cover the scope of a risk context evaluation and provide information so that an informed decision can be made. The type of decisions would include a trade of costs, risk appetites, and the forecast of an expected financial return. The tool can hence optimise the number and type of controls selected to meet outcome expectations and budget expenditure. In the case of controls being selected from multiple frameworks then Table 5.3 and Figure 5.3, shows similarities between controls in terms of the treatment of risk. Consequently, the question of financial optimisation can be addressed again by eliminating a similar treatment for the same risk and selecting a single control and one cost for the forecasted return.

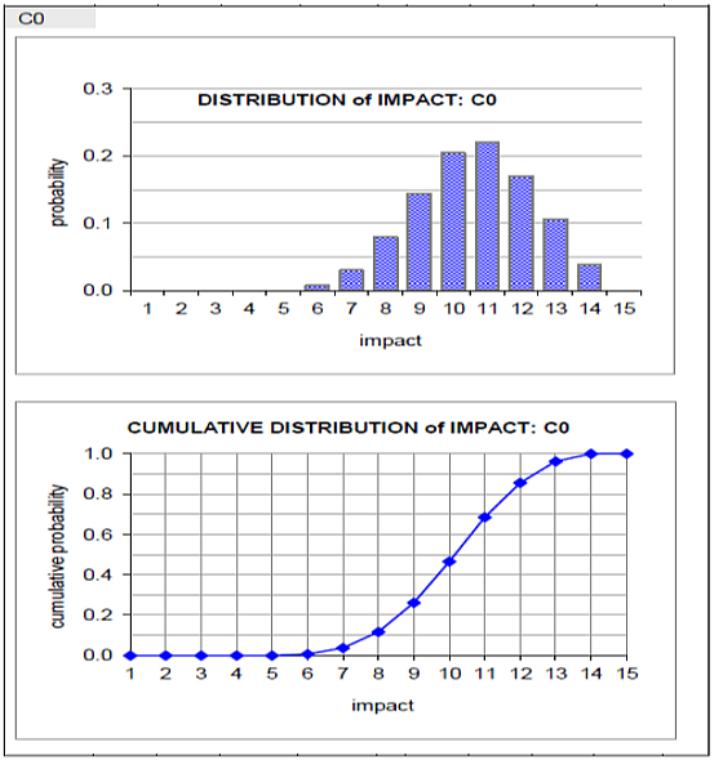


**Figure 5.3: Distribution of Impact and Cumulative Distribution of Impact Output**

Similarly, calculations for C1 and C2 control configurations and the associated risks are produced by analyses and results in charts that are generated in similar fashion.

## 5.2 ARTEFACTS EVALUATION

In chapter 4, subsection 4.3.4, an emphasis has been put on the evaluation aspects for practical research, and the necessity of validating the theoretical design solution empirically. When solution artefacts reach an acceptable stage, they can be evaluated against defined criteria. Any detected deviations are analysed, discussed and if any necessary changes are accommodated. However, it is imperative to balance the effort spent on building and evaluating the design artefacts with the intended deliverables.

It has also been indicated that the evaluation of the artefacts in the first development has the objective of 'proof of concept' rather than evaluating the artefacts in our real-life context. Furthermore, artefacts should be evaluated from a functional perspective, rather than focusing on the details of how the artefacts are constructed and/or organised. The artefacts should be evaluated in the light of their practical implications. This is equally important with how the research is executed to achieve its planned objectives.

The two types of evaluations are adopted in the DSR roadmap devised by Alturki et al. (2011b) and shown in Figure 4.5. These are noted by some authors as Internal and External evaluation, which has the aim of ensuring the quality of the produced artefacts. A number of evaluation criteria based on the system approach articulated by Prat et al. (2014) and corresponding questions have been shown in Table 4.6.

In this section the artificial evaluation outcomes are reported in sub-section 5.2.1. Based on the evaluation outcomes, C-Model is assessed in sub-section 5.2.2, and a critical reflection is conducted in sub-section 5.2.3. Subsequently, the naturalistic evaluation is halted, a justification for that is articulated in sub-section 5.2.4.

### 5.2.1 Artificial Evaluation

In chapter 4, sub-section 4.3.4, it is stated that Artificial evaluation could involve laboratory and field experiments, simulation, criteria-based analysis, theoretical argument and mathematical proof; with the purpose to evaluate the artefacts in non-realistic way. Therefore, an experiment is conducted with C-Model to identify the

best controls configuration to mitigate the three identified risks (R1, R2 and R3) from the outlined controls and processes as detailed in sub-section 5.1.2.

In Chapter 4, sub-section 4.4.1.1, it has been discussed the importance to obtain expert assessment of the produced artefacts and to conduct evaluation activities. Hence, the outcomes of the experirment were presented to some experts to obtain their feedback and initial assessment of the solution design. As noted in Chapter 4, sub-section 4.4.5, evaluating artefacts should be against defined criteria, which have been explored in that sub-section. A number of questions have been devised accordingly to bench mark the developed model (as shown in Table 4.6).

The experiment will be detailed in sub-section 5.2.1.1, and the expert evaluation will be reported in sub-section 5.2.1.2.

#### 5.2.1.1 Experiment

A pilot test was conducted with the proto-type C-Model that describes the distribution for the cumulative impact risks (R1, R2 and R3) and controls configurations (C0, C1, and C2). Shown in Table 5.4, there are three risks R1, R2 and R3, with the likelihood rating of these risks can be L (low), medium (M) or high (H).

**Table 5.4: C-Model Experiment Data Entry**

| | | R1 | r1L | r1M | r1H | | | R2 | r2L | r2M | r2H | | | R3 | r3L | r3M | r3H | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | |
| C0 | 10 | | | | | | | | | | | | | | | | | |
| 1 | | pr | 0.10 | 0.40 | 0.50 | 1.0 | | pr | 1.00 | 3.00 | 2.00 | 6.0 | | pr | 1.00 | 2.00 | 1.00 | 4.0 |
| 2 | | pr adj | 0.10 | 0.40 | 0.50 | 1.0 | | pr adj | 0.17 | 0.50 | 0.33 | 1.0 | | pr adj | 0.25 | 0.50 | 0.25 | 1.0 |
| 3 | | impact | 2 | 3 | 5 | | | impact | 1 | 3 | 5 | | | impact | 2 | 3 | 4 | |
| | | | | | | | | | | | | | | | | | | |
| C1 | 15 | | | | | | | | | | | | | | | | | |
| 1 | | pr | 0.20 | 0.50 | 0.20 | 0.9 | | pr | 1.00 | 2.00 | 0.50 | 3.5 | | pr | 1.50 | 2.00 | 0.50 | 4.0 |
| 2 | | pr adj | 0.22 | 0.56 | 0.22 | 1.0 | | pr adj | 0.29 | 0.57 | 0.14 | 1.0 | | pr adj | 0.38 | 0.50 | 0.13 | 1.0 |
| 3 | | impact | 1 | 3 | 4 | | | impact | 1 | 2 | 4 | | | impact | 2 | 3 | 3 | |
| | | | | | | | | | | | | | | | | | | |
| C2 | 25 | | | | | | | | | | | | | | | | | |
| 1 | | pr | 0.40 | 0.40 | 0.20 | 1.0 | | pr | 1.00 | 3.00 | 1.00 | 5.0 | | pr | 3.00 | 2.00 | 1.00 | 6.0 |
| 2 | | pr adj | 0.40 | 0.40 | 0.20 | 1.0 | | pr adj | 0.20 | 0.60 | 0.20 | 1.0 | | pr adj | 0.50 | 0.33 | 0.17 | 1.0 |
| 3 | | impact | 1 | 3 | 4 | | | impact | 1 | 2 | 3 | | | impact | 1 | 2 | 3 | |

For C0, the calculations and results are depicted in Table 5.5. There is a distribution of impact i.e. a list of possible impacts and their associated probabilities for risks R1, R2, R3 and control configuration C0. In Table 5.5 the risk likelihood and impact probabilities calculations are listed.

**Table 5.5: C0 - Risks Likelihood and Impact Calculations**

| Risk Dependency | | | Risk Likelihood = probabilities Calculation | | | | Impact Calculation | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | PR1 | PR2 | PR3 | Total | IR1 | IR2 | IR3 | Total |
| r1L | r2L | r3L | 0.10 | 0.17 | 0.25 | 0.004 | 2 | 1 | 2 | 5.00 |
| r1L | r2L | r3M | 0.10 | 0.17 | 0.50 | 0.008 | 2 | 1 | 3 | 6.00 |
| r1L | r2L | r3H | 0.10 | 0.17 | 0.25 | 0.004 | 2 | 1 | 4 | 7.00 |
| r1L | r2M | r3L | 0.10 | 0.50 | 0.25 | 0.013 | 2 | 3 | 2 | 7.00 |
| r1L | r2M | r3M | 0.10 | 0.50 | 0.50 | 0.025 | 2 | 3 | 3 | 8.00 |
| r1L | r2M | r3H | 0.10 | 0.50 | 0.25 | 0.013 | 2 | 3 | 4 | 9.00 |
| r1L | r2H | r3L | 0.10 | 0.33 | 0.25 | 0.008 | 2 | 5 | 2 | 9.00 |
| r1L | r2H | r3M | 0.10 | 0.33 | 0.50 | 0.017 | 2 | 5 | 3 | 10.00 |
| r1L | r2H | r3H | 0.10 | 0.33 | 0.25 | 0.008 | 2 | 5 | 4 | 11.00 |
| r1M | r2L | r3L | 0.40 | 0.17 | 0.25 | 0.017 | 3 | 1 | 2 | 6.00 |
| r1M | r2L | r3M | 0.40 | 0.17 | 0.50 | 0.033 | 3 | 1 | 3 | 7.00 |
| r1M | r2L | r3H | 0.40 | 0.17 | 0.25 | 0.017 | 3 | 1 | 4 | 8.00 |
| r1M | r2M | r3L | 0.40 | 0.50 | 0.25 | 0.050 | 3 | 3 | 2 | 8.00 |
| r1M | r2M | r3M | 0.40 | 0.50 | 0.50 | 0.100 | 3 | 3 | 3 | 9.00 |
| r1M | r2M | r3H | 0.40 | 0.50 | 0.25 | 0.050 | 3 | 3 | 4 | 10.00 |
| r1M | r2H | r3L | 0.40 | 0.33 | 0.25 | 0.033 | 3 | 5 | 2 | 10.00 |
| r1M | r2H | r3M | 0.40 | 0.33 | 0.50 | 0.067 | 3 | 5 | 3 | 11.00 |
| r1M | r2H | r3H | 0.40 | 0.33 | 0.25 | 0.033 | 3 | 5 | 4 | 12.00 |
| r1H | r2L | r3L | 0.50 | 0.17 | 0.25 | 0.021 | 5 | 1 | 2 | 8.00 |
| r1H | r2L | r3M | 0.50 | 0.17 | 0.50 | 0.042 | 5 | 1 | 3 | 9.00 |
| r1H | r2L | r3H | 0.50 | 0.17 | 0.25 | 0.021 | 5 | 1 | 4 | 10.00 |
| r1H | r2M | r3L | 0.50 | 0.50 | 0.25 | 0.063 | 5 | 3 | 2 | 10.00 |
| r1H | r2M | r3M | 0.50 | 0.50 | 0.50 | 0.125 | 5 | 3 | 3 | 11.00 |
| r1H | r2M | r3H | 0.50 | 0.50 | 0.25 | 0.063 | 5 | 3 | 4 | 12.00 |
| r1H | r2H | r3L | 0.50 | 0.33 | 0.25 | 0.042 | 5 | 5 | 2 | 12.00 |
| r1H | r2H | r3M | 0.50 | 0.33 | 0.50 | 0.083 | 5 | 5 | 3 | 13.00 |
| r1H | r2H | r3H | 0.50 | 0.33 | 0.25 | 0.042 | 5 | 5 | 4 | 14.00 |
| | | | | | | 1.000 | | | | |

While Table 5.6 shows the C0 impact and cumulative impact calculation.

**Table 5.6: C0 - Impact and Cumulative Impact Calculation**

| Impact Value | Cumulative Impact | Impact Levels |
|---|---|---|
| | | 1.00 |
| | | 2.00 |
| | | 3.00 |
| | | 4.00 |
| 0.004 | 0.004 | 5.00 |
| 0.025 | 0.029 | 6.00 |
| 0.050 | 0.079 | 7.00 |
| 0.113 | 0.192 | 8.00 |
| 0.163 | 0.354 | 9.00 |
| 0.183 | 0.538 | 10.00 |
| 0.200 | 0.738 | 11.00 |
| 0.138 | 0.875 | 12.00 |
| 0.083 | 0.958 | 13.00 |
| 0.042 | 1.000 | 14.00 |
| | 1.000 | 15.00 |
| 1.000 | | |

Figure 5.4 shows the impact and the cumulative probability distribution.

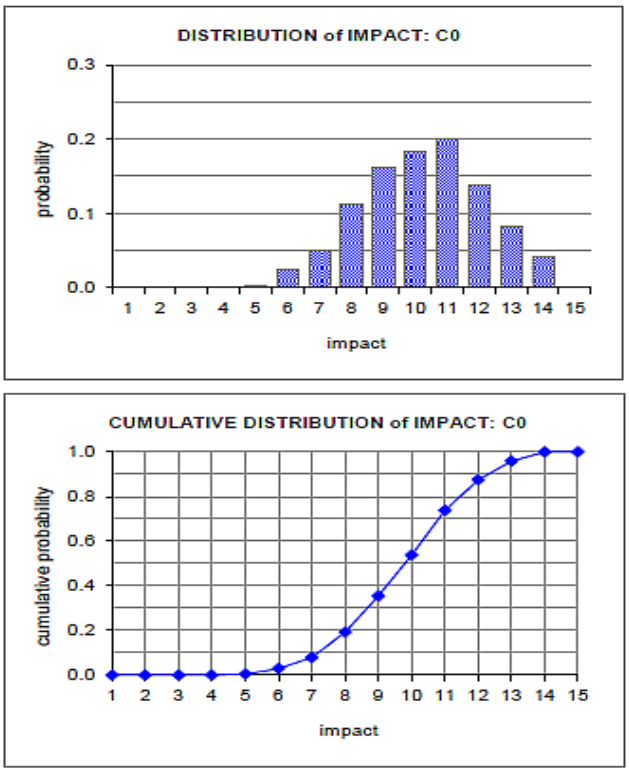


**Figure 5.4: C0 - Impact and Cumulative Probability Distribution**

**Table 5.7: C1 - Risks Likelihood and Impact Calculation**

| Risk Dependency | | | Risk Likelihood = probabilities Calculation | | | | Impact Calculation | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | PR1 | PR2 | PR3 | Total | IR1 | IR2 | IR3 | Total |
| r1L | r2L | r3L | 0.22 | 0.29 | 0.38 | 0.024 | 1 | 1 | 2 | 4.00 |
| r1L | r2L | r3M | 0.22 | 0.29 | 0.50 | 0.032 | 1 | 1 | 3 | 5.00 |
| r1L | r2L | r3H | 0.22 | 0.29 | 0.13 | 0.008 | 1 | 1 | 3 | 5.00 |
| r1L | r2M | r3L | 0.22 | 0.57 | 0.38 | 0.048 | 1 | 2 | 2 | 5.00 |
| r1L | r2M | r3M | 0.22 | 0.57 | 0.50 | 0.063 | 1 | 2 | 3 | 6.00 |
| r1L | r2M | r3H | 0.22 | 0.57 | 0.13 | 0.016 | 1 | 2 | 3 | 6.00 |
| r1L | r2H | r3L | 0.22 | 0.14 | 0.38 | 0.012 | 1 | 4 | 2 | 7.00 |
| r1L | r2H | r3M | 0.22 | 0.14 | 0.50 | 0.016 | 1 | 4 | 3 | 8.00 |
| r1L | r2H | r3H | 0.22 | 0.14 | 0.13 | 0.004 | 1 | 4 | 3 | 8.00 |
| r1M | r2L | r3L | 0.56 | 0.29 | 0.38 | 0.060 | 3 | 1 | 2 | 6.00 |
| r1M | r2L | r3M | 0.56 | 0.29 | 0.50 | 0.079 | 3 | 1 | 3 | 7.00 |
| r1M | r2L | r3H | 0.56 | 0.29 | 0.13 | 0.020 | 3 | 1 | 3 | 7.00 |
| r1M | r2M | r3L | 0.56 | 0.57 | 0.38 | 0.119 | 3 | 2 | 2 | 7.00 |
| r1M | r2M | r3M | 0.56 | 0.57 | 0.50 | 0.159 | 3 | 2 | 3 | 8.00 |
| r1M | r2M | r3H | 0.56 | 0.57 | 0.13 | 0.040 | 3 | 2 | 3 | 8.00 |
| r1M | r2H | r3L | 0.56 | 0.14 | 0.38 | 0.030 | 3 | 4 | 2 | 9.00 |
| r1M | r2H | r3M | 0.56 | 0.14 | 0.50 | 0.040 | 3 | 4 | 3 | 10.00 |
| r1M | r2H | r3H | 0.56 | 0.14 | 0.13 | 0.010 | 3 | 4 | 3 | 10.00 |
| r1H | r2L | r3L | 0.22 | 0.29 | 0.38 | 0.024 | 4 | 1 | 2 | 7.00 |
| r1H | r2L | r3M | 0.22 | 0.29 | 0.50 | 0.032 | 4 | 1 | 3 | 8.00 |
| r1H | r2L | r3H | 0.22 | 0.29 | 0.13 | 0.008 | 4 | 1 | 3 | 8.00 |
| r1H | r2M | r3L | 0.22 | 0.57 | 0.38 | 0.048 | 4 | 2 | 2 | 8.00 |
| r1H | r2M | r3M | 0.22 | 0.57 | 0.50 | 0.063 | 4 | 2 | 3 | 9.00 |
| r1H | r2M | r3H | 0.22 | 0.57 | 0.13 | 0.016 | 4 | 2 | 3 | 9.00 |
| r1H | r2H | r3L | 0.22 | 0.14 | 0.38 | 0.012 | 4 | 4 | 2 | 10.00 |
| r1H | r2H | r3M | 0.22 | 0.14 | 0.50 | 0.016 | 4 | 4 | 3 | 11.00 |
| r1H | r2H | r3H | 0.22 | 0.14 | 0.13 | 0.004 | 4 | 4 | 3 | 11.00 |
| | | | | | | 1.000 | | | | |

Calculations for C1 control configurations and the associated risk analysis and charts are generated in similar fashion, which are shown in Tables 5.7, 5.8 and Figure 5.5, respectively

**Table 5.8: C1 - Impact and Cumulative Impact Calculation**

| Impact Value | Cumulative Impact | Impact Levels |
|---|---|---|
| | | 1.00 |
| | | 2.00 |
| | | 3.00 |
| 0.024 | 0.024 | 4.00 |
| 0.087 | 0.111 | 5.00 |
| 0.139 | 0.250 | 6.00 |
| 0.254 | 0.504 | 7.00 |
| 0.306 | 0.810 | 8.00 |
| 0.109 | 0.919 | 9.00 |
| 0.062 | 0.980 | 10.00 |
| 0.020 | 1.000 | 11.00 |
| | 1.000 | 12.00 |
| | 1.000 | 13.00 |
| | 1.000 | 14.00 |
| | 1.000 | 15.00 |
| 1.000 | | |

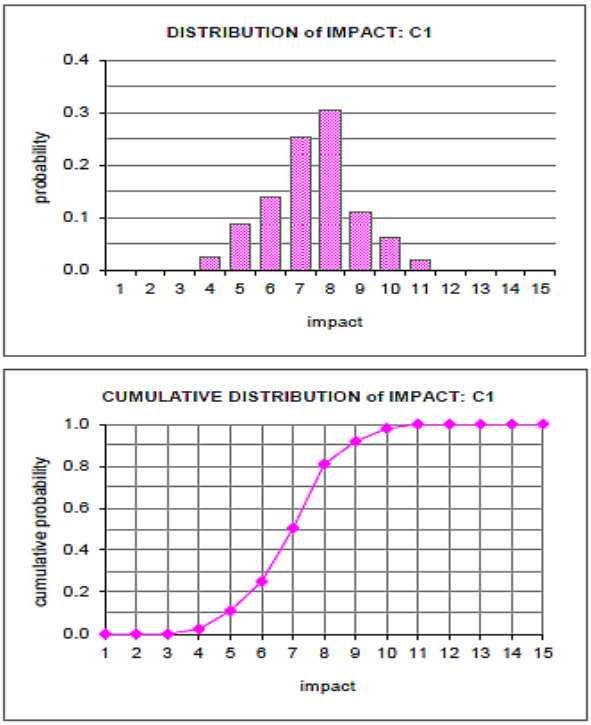


**Figure 5.5: C1 - Impact and Cumulative Probability Distribution**

In similar fashion calculations and results for C2 are depicted in Tables 5.9 and 5.10 and Figure 5.6 following.

**Table 5.9: C2 - Risks Likelihood and Impact Calculation**

| Risk Dependency | | | Risk Likelihood = probabilities Calculation | | | | Impact Calculation | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | PR1 | PR2 | PR3 | Total | IR1 | IR2 | IR3 | Total |
| r1L | r2L | r3L | 0.40 | 0.20 | 0.50 | 0.040 | 1 | 1 | 1 | 3.00 |
| r1L | r2L | r3M | 0.40 | 0.20 | 0.33 | 0.027 | 1 | 1 | 2 | 4.00 |
| r1L | r2L | r3H | 0.40 | 0.20 | 0.17 | 0.013 | 1 | 1 | 3 | 5.00 |
| r1L | r2M | r3L | 0.40 | 0.60 | 0.50 | 0.120 | 1 | 2 | 1 | 4.00 |
| r1L | r2M | r3M | 0.40 | 0.60 | 0.33 | 0.080 | 1 | 2 | 2 | 5.00 |
| r1L | r2M | r3H | 0.40 | 0.60 | 0.17 | 0.040 | 1 | 2 | 3 | 6.00 |
| r1L | r2H | r3L | 0.40 | 0.20 | 0.50 | 0.040 | 1 | 3 | 1 | 5.00 |
| r1L | r2H | r3M | 0.40 | 0.20 | 0.33 | 0.027 | 1 | 3 | 2 | 6.00 |
| r1L | r2H | r3H | 0.40 | 0.20 | 0.17 | 0.013 | 1 | 3 | 3 | 7.00 |
| r1M | r2L | r3L | 0.40 | 0.20 | 0.50 | 0.040 | 3 | 1 | 1 | 5.00 |
| r1M | r2L | r3M | 0.40 | 0.20 | 0.33 | 0.027 | 3 | 1 | 2 | 6.00 |
| r1M | r2L | r3H | 0.40 | 0.20 | 0.17 | 0.013 | 3 | 1 | 3 | 7.00 |
| r1M | r2M | r3L | 0.40 | 0.60 | 0.50 | 0.120 | 3 | 2 | 1 | 6.00 |
| r1M | r2M | r3M | 0.40 | 0.60 | 0.33 | 0.080 | 3 | 2 | 2 | 7.00 |
| r1M | r2M | r3H | 0.40 | 0.60 | 0.17 | 0.040 | 3 | 2 | 3 | 8.00 |
| r1M | r2H | r3L | 0.40 | 0.20 | 0.50 | 0.040 | 3 | 3 | 1 | 7.00 |
| r1M | r2H | r3M | 0.40 | 0.20 | 0.33 | 0.027 | 3 | 3 | 2 | 8.00 |
| r1M | r2H | r3H | 0.40 | 0.20 | 0.17 | 0.013 | 3 | 3 | 3 | 9.00 |
| r1H | r2L | r3L | 0.20 | 0.20 | 0.50 | 0.020 | 4 | 1 | 1 | 6.00 |
| r1H | r2L | r3M | 0.20 | 0.20 | 0.33 | 0.013 | 4 | 1 | 2 | 7.00 |
| r1H | r2L | r3H | 0.20 | 0.20 | 0.17 | 0.007 | 4 | 1 | 3 | 8.00 |
| r1H | r2M | r3L | 0.20 | 0.60 | 0.50 | 0.060 | 4 | 2 | 1 | 7.00 |
| r1H | r2M | r3M | 0.20 | 0.60 | 0.33 | 0.040 | 4 | 2 | 2 | 8.00 |
| r1H | r2M | r3H | 0.20 | 0.60 | 0.17 | 0.020 | 4 | 2 | 3 | 9.00 |
| r1H | r2H | r3L | 0.20 | 0.20 | 0.50 | 0.020 | 4 | 3 | 1 | 8.00 |
| r1H | r2H | r3M | 0.20 | 0.20 | 0.33 | 0.013 | 4 | 3 | 2 | 9.00 |
| r1H | r2H | r3H | 0.20 | 0.20 | 0.17 | 0.007 | 4 | 3 | 3 | 10.00 |
| | | | | | | 1.000 | | | | |

**Table 5.10: C2 - Impact and Cumulative Impact Calculation**

| Impact Value | Cumulative Impact | Impact Levels |
|---|---|---|
| | | 1.00 |
| | | 2.00 |
| 0.040 | 0.040 | 3.00 |
| 0.147 | 0.187 | 4.00 |
| 0.173 | 0.360 | 5.00 |
| 0.233 | 0.593 | 6.00 |
| 0.220 | 0.813 | 7.00 |
| 0.133 | 0.947 | 8.00 |
| 0.047 | 0.993 | 9.00 |
| 0.007 | 1.000 | 10.00 |
| | 1.000 | 11.00 |
| | 1.000 | 12.00 |
| | 1.000 | 13.00 |
| | 1.000 | 14.00 |
| | 1.000 | 15.00 |
| 1.000 | | |

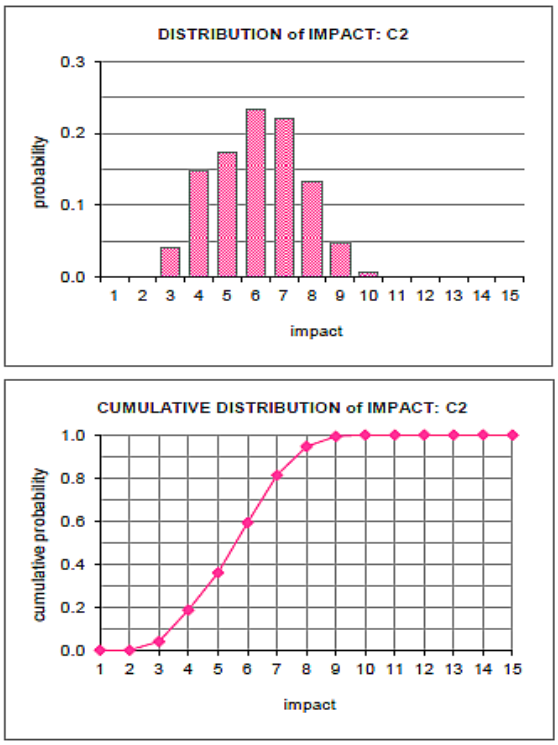


**Figure 5.6: C2 - Impact and Cumulative Probability Distribution**

#### 5.2.1.2 Expert Evaluation

With regards to experts' evaluation where artefacts are evaluated by one or more experts, that utilises 'logical arguments' plays a big part of the evaluation classifications. The evaluation method is driven by the type and nature of the artefacts. Furthermore, to ensure a quality evaluation, attention should be paid to the context, when selecting an environment and experts to evaluate the artefacts. Gathering experts' evaluation and collecting resulting data must follow AUT Ethics Committee procedures and its requirements, for details please see Appendix A.

Selected Experts must have relevant experience and qualifications in the field, to provide reliable assessment. For this research and as C-Model is still in its rudimentary stage, the approached experts are: a mathematician and the two supervisors of the thesis. Oral feedback has been provided by the selected experts about the design solution and experiment results. Feedback and answers are tabulated and used to populate Table 5.11.The proposed C-Model is assessed and results are discussed to outline the viable further development paths and to identify any issues that could hinder the development of the proposed model. The focus is mainly on the C-Model aspects as it is the core of the DSS.

**Table 5.11: Artefacts Evaluation Results**

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| **Goal** | **Efficacy** | | Q1. How effective is the proposed DSS in managing the defined IT risks. | While it has some merit with the provided defined risks and corresponding controls, however the C-Model has a number of limitations. Input is limited to the number of risks and controls configurations. The output should be in an easily interpreted form. Practitioners need to view controls and risks holistically, while currently the mode doesn't provide that.<br>The model should have a better way of representing the domain to allow holistic view on evaluating IT risks along with associated business/IT value, and interaction between risks and controls and processes, to allow practitioners make a trustworthy decision when selecting controls and processes.<br>Frameworks and best practices have a different architecture and could change over time. It requires the DSS and its model to be scalable to accommodate changes in those frameworks. |
| | **Validity** | | Q1. How reliable the DSS outcomes are?<br>Q2. Is the risk assessment adequate? | 1. It was not possible to determine the various controls interaction. Hence, it was not possible to fully validate the C-Model outcomes.<br>2. The risk assessment is adequate, as it is commonly utilised methodology. |
| | **Generality** | | Q1. How easy is it to update the included frameworks in the DSS? E.g. replace ITIL 3.0 with | 1. Updating utilised frameworks depends on the changes made to those frameworks. If the change doesn't affect the framework architecture as is the case in ITIL 3.0 to 2011 edition, and ISO27001-2005 to ISO27001-2013, it |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | | ITIL 2011, ISO 27001-2005 with 27001/2013.<br><br>Q2. Is DSS capable of including all ITGC risks?<br><br>Q3. Could the DSS include other frameworks, e.g. ValIT, COSO_ERM? | is reasonably easy, however, changing COBIT 4.1 to COBIT 5, requires considerably effort, as COBIT 5 is architecturally different than COBIT 4.1.<br><br>2. It is possible to add more risk into the risk register, however, adding more risks (more than 3 risks) to the C-Model, is difficult and hence, the C-Model scalability is a concern.<br><br>3. While including another framework to the DSS possible controls and processes, however, adding more controls to the C-Model requires re-investigating the calculation algorithm to ensure all possible controls configurations are adequately represented. |
| **Environment** | **Consistency with people** | **Utility** | Q1. What is the total gained value, from practitioner's perspective? | At this stage it is not clear and/or possible to obtain practitioners view on the potential gained value. |
| | | **Understand-ability** | Q1. Is the DSS intuitive? | This note relates to C-Model rather than the whole DSS. With the provided instructions, a user with knowledge of risk management could follow the instructions and enter the risk parameters and controls cost values. However, the output is not easily interpreted. |
| | | **Ease of use** | Q1. Is the DSS easy to use? | This note relates to C-Model rather than the whole DSS. With the provided instructions, a user with knowledge of risk management could follow the instructions and enter the risk parameters and controls cost values.<br>The output figures are calculated when the corresponding input data change. |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | **Ethicality** | Q1. Does using the DSS have or could cause any ethical issue? | No ethical issue noted. |
| | | **Side effects** | Q1. Does the DSS or model produce new risks and/or incur further cost? | No new risk, but the C-Model could potentially incur further cost, as practitioners would go through a learning curve to get used to the DSS and C-Model. |
| | **Consistency with organisation** | **Utility** | Q1. What is the total gained value, from organisation's perspective? | At this stage it is not clear and/or possible to obtain practitioners view on the potential gained value. |
| | | **Fit with Organisation** | Q1. Is the DSS (Risk Register, selected frameworks, model) adequately fit the organisation's Internal/External environment? | This could be obtained from External/Naturalistic evaluation, where artefacts are tested in a real environment, rather than an internal environment. |
| | | **Side effects** | Q1. Any issues caused by using this DSS? E.g. incurring further cost, complicating the environment. | No new risk, but the C-Model could potentially incur further cost of implementing with overlapping controls and processes. |
| | **Consistency with technology** | **Harnessing of recent technologies** | Q1. How effective and easy it is to accommodate new technology by the DSS? | The potential new risk introduced by new technology could be added to the list of possible risks, however, the C-Model limitation could hinder. The point has been highlighted in the answer to Goal-Efficacy-Q1 |
| | | **Side effects** | Q1. Any issues, this DSS could cause? E.g. introducing new risks, overusing/underutilising resources, etc. | No issues or new risks could be caused. |
| **Structure** | **Completeness** | | Q1. How complete the DSS is?<br>Q2. Any area of improvement? | 1. As the focus is on evaluating C-Model, and the whole DSS is in a rudimentary stage, it is not appropriate to judge the DSS from this perspective. |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| **(Static, the artefact's construct)** | | | | 2. First and foremost, C-Model limitations must be thought through, and if possible re-designed for the solution. Furthermore, C-Model requires to be integrated with the DSS and provide an output interface that is easily interpreted by practitioners rather than the currently 'Impact' and 'Cumulative probability distribution' charts, as depicted in Figure 5.1 |
| | **Simplicity** | | Q1. How simple the DSS is structured? | DSS comprises of a risk register and C-Model, although it is not fully integrated, but it is sufficient for the purpose of evaluation at this stage. |
| | **Clarity** | | Q1. Are the DSS components clear | Yes they are clearly distinguished |
| | **Style** | | N/A- Not to be enquired about. | N/A |
| | **Homomorphism** | **Correspondent with another model** | Q1. Does the DSS map well to other Enterprise settings if any, for example IT Governance, Enterprise Risk Management, Internal Audit, Business/IT Strategic plan? | While developing an interactive DSS is not new, however, utilising cumulative impact probability based model in managing IT risks, is new. The used concepts in defining risks, and devising mitigating measures from IT controls frameworks, are common to professional practice in enterprise settings. |
| | | **Fidelity to modelled phenomena** | Q1. Does the designed DSS align with the theorised solution design and meet fidelity criteria exhibiting least deficiency (redundancy, incompleteness, excess, and overload)? | 1. The DSS risk register including defined risks, controls and risk assessment matrix are professionally developed and used repeatedly for many years. |
| | **Level of detail** | | Q1. Does the DSS provide enough detail and instructions on use? | The provided instructions, at this stage, relate to C-Model only, as this is the focus of the artificial evaluation. |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | **Consistency** | | Q1. Are the DSS components developed in (spreadsheets, MS-word documents, and other applications) consistent? | All DSS components are consistent. |
| **Activity (Dynamic, the operations and functionality of the artefact)** | **Completeness** | | Q1. Does the DSS have the right set of functions? | All DSS components are functioning properly, apart from the output, which is still to be developed, as indicated earlier, |
| | **Consistency** | | Q1. Does the DSS operate consistently? | The DSS, in particular, C-Model operates, consistently with the expected outcomes, |
| | **Accuracy** | | Q1. How accurate the DSS functionalities are? | While the input, data and knowledge base component of the DSS provide adequate risk assessment and suggest relevant controls and processes, however, C-Model has a number of limitations and the outcomes are not meeting the expectations. |
| | **Performance** | | Q1. Any issues with performance? | No performance issues have been reported. |
| | **Efficiency** | | Q1. How efficient the DSS is in terms the utilised time/resource and the obtained outcomes? | As the C-Model resulting outcomes are not providing the expected aid in determining the best controls configurations, the C-Model is considered inefficient. |
| **Evolution** | **Robustness** | | Q1. Does the DSS accommodate changes in internal/external environments? E.g. business dynamics, regulatory requirements, that requires assessing risks on timely fashion. | This question requires external or naturalistic evaluation in a real life environment by practitioners. |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | **Learning capability** | | Q1. Could the DSS – knowledge base – component enhanced with use?<br>Q2. Could practitioners add more knowledge as they use the DSS? | This question requires external or naturalistic evaluation in a real life environment by practitioners. |

### 5.2.2 C-Model Assessment

The justification for designing C-Model in the current form is that controls are selected from recognised frameworks and it is possible to estimate the implementation costs. Controls cost does not vary often and when it does, it can be approximated. For example, increased antivirus application, licensing fees, the cost of extra firewall appliances, or the hiring of another system administrator to join the network team. However, IT risks assessment outcomes could change over time as business and technology change more frequently and in unpredictable patterns. A changing risk profile requires costly re-assessment to be carried out and the adoption of new cost-effective controls. Therefore the model is structured around the combined probability of risk impact levels, defined as Low, Medium and High, should the risk materialise. The cumulative impact probability distribution alongside with the control cost for the three sets (C0, C1, and C2) provides insight for the decision-making process. The aim is to decide what would be the best set of controls to select from numerous controls and processes that comprise the recognised frameworks.

However, it was anticipated that the initial model will be further developed to include a presentation layer that is easy for practitioners' understanding and interpretation. For example, outputs are related to the inputs in a heat map form. This output form will improve the model's readiness for external evaluation. In a real environment outputs that are related to the inputs would assist to obtain experts' feedback on the effectiveness of the risks evaluation and corresponding controls configurations. In addition, the model is required to authenticate controls as inputs to determine their relevance to the defined risks. The authentication will also include validating the selected attributes of the selected frameworks and controls and associated estimates.

### 5.2.3 Critical Reflection

Initially the C-Model was developed to combine a number of risks that any function or area within IT could potentially have. Then, produce the distribution of cumulative probability of those risks, in the hope to show the impact of all related risks. Furthermore, it was indicated, that further development would be undertaken.

Firstly, to include the input controls various context and consideration of how that would influence the risk analysis outcomes. Secondly, to present the model's outputs in a form that is easily understandable by practitioners so it can be interpreted accordingly. However, further analysis to the research domain and the observed limitations of the proposed model's, showed a number of deficiencies that would render the model too cumbersome for serious practical use.

C-Model was constructed by creating three sets of risk analyses along with three controls sets: C0, C1, and C2, where each set is comprised of controls to be selected from elected recognised control frameworks: COBIT, ITIL and ISO 27001. As it was outlined, C0 comprises controls from COBIT, and C1 combines controls and processes elected from COBIT and ITIL. While C2 is constructed with controls from the three noted frameworks, best practices and standards. It implies that should a practitioner opt to combine controls from COBIT and ISO 27001, or ITIL and ISO 27001, they would not be able to utilise C1 of the model. Similarly, C0 could only be used for COBIT controls. Alternatively, another controls configurations could be created, which would require changing the calculation and output diagrams.

On the other hand, introducing input and control context to the model would require too many assumptions to be made to simplify the model to a workable stage, which would return little value for the invested effort. For example, the mitigating effect of the applied controls is required to be analysed and a set of probability distributions to be generated and applied on the initial risks cumulative probability distributions. That would imply combining the overall mitigating effect of all the applied controls, limiting the practitioner's ability to view each control's mitigating power on the identified risks. Stated differently, it is known that controls and processes from various selected frameworks and best practices could mitigate the same risk to a different level. Therefore, it is imperative for a practitioner to be able to view each control's effect, whether it is applied individually or combined with other controls. Controls do overlap with each other in mitigating some risks. When selecting the best controls configuration, one of the key aspects to determine is to reduce the overlap between various controls, in order to ensure the best mitigating controls configuration is selected.

Lastly, as it was proposed that the model's output should be presented in an interpretable form by practitioners, which implies further research and development are required to transfer the cumulative probability distribution output into a meaningful form, for example, into a heat map or traffic light graphs. Producing outputs in a meaningful form should only be done after ensuring the underlying process design is adequate and functioning acceptably by practitioners. In this case, it seemed that the C-Model had a number of limitations that even if the proposed improvements were developed, it would still be incapable of producing the expected deliverables.

**Table 5.12: C-Model Assessment Summary**

| Merits | Limitations | Further Development |
|---|---|---|
| - Based on risk cumulative impact analysis<br>- Doesn't incur further risk or cost | - Input is limited to the defined number of risks; adding more risks (more than 3 risks) to the C-Model, is difficult and hence, the C-Model shows a scalability issue.<br>- Does not provide holistic view<br>- Does not fully cover all possible controls configurations combinations<br>- Controls context not comprehensively considered | - Interface output layer, like heat map<br>- Evaluate input context<br>- Add more risks and controls combinations |

Table 5.12 lists C-Model's merits and limitations and required further development. For the above stated reasons it can be stated that the proposed C-Model while it has some merits, however, with its noted limitations, the model would not be effective in finding the best controls configuration. Based on the newly discovered understanding, form the C-Model evaluation, the researcher began to theorise and explore other alternatives, which will be outlined in sub-section 5.3.1.

### 5.2.4 Terminating the Naturalistic Evaluation Stage

C-Model was due next to undergo the Naturalistic Evaluation as detailed in Chapter 4, sub-section 4.3.4, where the produced artefacts are required to be evaluated in two stages (Venable, 2006; Alturki et al., 2011a; Ostrowski & Helfert, 2012). The second stage, which is described often as the 'real' test, where the invented designed solution or artefact is tested in an actual organisation to check how effective the designed solution is. Naturalistic Evaluation was terminated based on the feedback from the experts and the expectation that little would be gained by perusing this research stage at the time.

As C-Model is the core of the devised DSS it was considered incomplete and inefficient in producing the expected outcomes, hence it was not considered ready enough to be evaluated externally. Testing the artefacts in a real environment by practitioners in the subject field requires the artefacts to be sufficiently developed to some respect. For example, functionality, usability, and validity, so that experts would use and evaluate the artefacts in a practical way. Subsequently, experts would provide feedback and recommendations on the use of the design solution that could be analysed and reported to motivate further improvement.

As noted in Chapter 4, expert evaluation is crucial for the DS research, initially it was planned to invite 5-6 experts to conduct a naturalistic evaluation once the model reaches an acceptable standard for their critique. Hence the outcome of the first evaluation is to recommend that the DSS development cycle is used to gain a better level of maturity before subjecting the model to an external evaluation. Experts in the subject domain, such as IT auditors, security and risk managers, business and IT operation managers, are usually very busy people and it is always a challenge to enlist their expertise in evaluating the proposed design. Approaching those experts, while the artefacts are considered insufficiently developed, was deemed impractical and would waste the experts and the researcher's time. Furthermore, asking experts at this stage could potentially jeopardise the involvement of the intended pool of experts, and obtained data would provide little value for the study.

## 5.3 NEXT MOVE – FURTHER MODEL DEVELOPMENT

In Chapter 4, sub-section 4.3.3 the DS research guidelines are listed in Table 4.3, which shows guideline 3: Design Evaluation. The design solution artefacts were subjected to expert evaluation, which has been undertaken and reported in this chapter. Furthermore, the DS research three cycles: Relevance, Design and Rigor, have been reviewed outlining the key aspects and the DS research process in the devised framework that has been illustrated in Figure 4.3. In the DS framework, the research process iterations and possible feedback to the various previous stages are available to undergo any remediation that deemed necessary. For example, the output of the Evaluation stage could feedback to the Define Objectives of a Solution and Design and Development stages. This feedback enables a researcher to re-assess the produced outputs of each of those stages, which could lead to adjusting the stated problems, and/or the designed solution itself and all the produced artefacts. Also the set of questions that are listed in Table 4.4, in which question 5 asks about the performed evaluation and design improvements that have been identified, arising from the evaluation activity. In the same way the DS research roadmap designed by Alturki et al. (2011b) is referenced in Figure 4.5, in Task 13, for Artificial and Naturalistic evaluations. In Figure 4.5, it shows a feedback loop from Task 13 into Task 12 - Develop, which in turn feeds into previous tasks. The feedback triggered exploring the knowledge base and finding another alternative and/or designing new artefacts, and re-executing the tasks that follow.

As the outcomes of the artefacts evaluation reported in section 5.2, were not satisfactory as outlined in Table 5.11 and discussed in sub-section 5.2.3. The researcher was bound to re-assess the research problem and the corresponding design solution. The revision resulted in retaining the identified stated problems and also developing an interactive DSS remains as the conceptually selected solution. However, the model on which the DSS is based, required reviewing and re-thinking. This led the researcher to further explore other theories, and the evaluation of their applications with the possibility of forming a new model based on critical appraisal and the feedback from the experts. Prior to developing C-Model, Monte-Carlo simulation was explored. Also, the concept of developing a model based on cube model that was introduced in Chapter 2, sub-section 2.4.1.11, both options were overruled as they show similar limitations of the C-Model. While

attempting to improve C-Model in particular adding the interface output layer, game theory was explored to investigate its applicability in forming such a layer. Subsequently, it was found that a game theory based model could potentially be developed replacing the C-Model and overcoming its limitations.

Sub-section 5.3.1 revisits game theory and game theory applications that have been discussed in detail in Chapter 3, section 3.4. It also briefly outlines, what has been discussed at length in Chapter 3, section 3.5, from the published papers about game theory applications in IT risk management, and interactive DSS.

### 5.3.1 Game Theory Model

In Chapter 3, section 3.4, game theory was explored as a potential contributor to an IT risk DSS model, outlining its history, concepts and some definitions. In sub-section 3.4.3, the application of the game theory based model in an interactive DSS to aid practitioners' decision making processes, was outlined. It showed how to select IT risks mitigating measures and illustrated that an n-player model could be designed to determine the most cost effective way of managing the risks. In the model, each player would represents one of the recognised IT control frameworks: COBIT, ITIL, ISO 27001, ValIT , RiskIT and the like, to select the best set of relevant controls and processes from those recognised frameworks.

The DSS based on a game theory model was subsequently proposed that would enable experts like IT auditors, IT risk and security managers, utilise their expertise in the subject domain, business dynamics, and to assess a changing risk profile efficiently. The experts are responsible for managing IT risk in general and specifically security risks, via implementing various IT controls from recognised IT controls frameworks. The complexity of analysing static games increases exponentially as the number of players increases. Furthermore, it is noted that analyising and resolving a game with more than 3 players requires advanced mathematic techniques. However, that doesn't mean it is not possible to do so. In this research a 3-player model is to be designed, where the three players are: COBIT 4.1, ITIL v3.0, and ISO 27001 edition 2005.

In Chapter 3, section 3.5, a number of published papers about utilising game theory in managing IT risk, and developing a DSS with a game theory based model were presented. In the first paper, Rajbhandari and Snekkenes (2011) demonstrated

applying game theory principles in managing IT risks. It was argued that traditionally probabilities are used to assess IT risk, however, cumulative impact probability analysis is not something practitioners are well acquainted with or use. On the contrary, “game theory puts and emphasis on collecting representative data on how stakeholders assess the value of the outcome of incident scenarios” (p. 147). In their effort to demonstrate the application of game theory the authors map risk management processes described in ISO/IEC 27005 to the corresponding game theory aspects. The ISO/IEC 27005 standard was selected, among a number of similar standards, such as NIST 800-30, RiskIT and CORAS. As for the second paper, a case study conducted by Aliahmadi et al. (2011) detailed an interactive expert DSS using game theory and fuzzy logic. The goal was of the DSS was to manage risk in design, construction and operation of a tunnel project. The proposed game theory model was constructed of a 3-player non-cooperative game integrated with an interactive fuzzy analytical hierarchy process. The objective was to balance actions and a selected strategy for each player.

In summary a number of important aspects have been discovered about using cumulative impact probability analysis as a model basis for the DSS. However the limitations meant that the C-Model was considered unfit for purpose. A new approach for modeling the DSS based on game theory is investigated and its development and evaluation will be described in the following Chapter 6. The changes to the research progress and roadmap are described in the next section 5.4.

## 5.4 DS RESEARCH PROGRESS FOLLOWING C-MODEL EVALUATION

In Chapter 4, sub-section 4.3.3, Hevner (2007) the three DS research processes: ‘Relevance’, ‘Design’ and ‘Rigor’, shown in Figure 4.2. Also, the set of questions developed by Hevner and Chatterjee (2010), and a DS research roadmap proposed by Alturki et al. (2011a, 2011b) illustrated in Figure 4.5. In section 5.3, the reviewing of research activities as per the DSR roadmap, resulted in retaining the identified problem, and the interactive DSS as the potential design solution. However, the C-Model was deemed inadequate to provide a solution to the identified problem. In this section the activities according to the various and relevant stages of the DS roadmap for the developing of artefacts and the resulting

changes are outlined. For example, what has been developed, tested, changes made and what are the justifications for that, also any further anticipated changes. The aim of this section is not to evaluate the full research progress. Rather the aim is to review the cause and effects that relate to the DS Design cycle: Evaluation outcomes, Changes to the Artefacts, and Additions to the DS Repository. In Chapter 4, it was indicated that the research progress is outlined in Table B-1, which is constructed in Appendix B. The table comprised of the DS three cycles based on the DS guidelines and DSR roadmap tasks and populated with taken action up to that stage. The table is amended with updates and additions resulted from the conducted activites in Chapter 5, which are prefixed with "Chapter 5 (C-Model) Amendments".

Table B-1 satisfies that the Relevance Cycle has been completed with the stated problem, and research question established. As for the Design Cycle, it was still in progress, and the potential solution had been designed and proposed artefacts had been developed and an internal model evaluation conducted. A number of changes deemed necessary were introduced to the design of the proposed artefacts. A new game theory based model has been explored to be included in the proposed interactive DSS and is to be included in the next development cycle. As for the Rigorous Cycle, this was considered unnecessary for the C-Model implementation and to be completed after the two evaluation cycles are completed, and the research outcomes are concluded, which will be reported in chapter 6 and chapter 7, respectively.

## 5.5 CONCLUSION

In this chapter the developed artefacts were described. They comprised a model based interactive DSS. Initially, the first model, was based on calculating risks from cumulative impact probability distributions, and was called C-Model. An internal experiment was conducted using C-Model. The model and the results were evaluated by three experts. Oral feedback was obtained, and reported against the evaluation criteria and corresponding questions. The aim was to get the experts' evaluation for using the DSS model and to obtain their recommended changes to further improve the model if deemed necessary. The evaluation results were examined and a justification has been argued that C-Model would not return a value

proportionate to the anticipated development efforts that the model requires. Thence, a game-theory has been explored seeking an alternative model to base the DSS upon. The progress of the research and the developed artefacts and the various conducted activities according to the DSR roadmap, have been examined and reported ensuring research objectives are achieved systematically.

The next Chapter will report the development of a new game theory based model, called G-Model. External experts' evaluation are documented and discussed to complete the evaluation cycle.

# Chapter 6

# Results and Second Evaluation

## 6.0 INTRODUCTION

In Chapter 5, the design and development of the research artefacts comprising of an interactive DSS and C-Model, were reported. An initial evaluation was conducted and outcomes were reported. The C-Model artificial evaluation results indicated a number of significant limitations for the designed C-Model. That necessitated further research and subsequently, game theory application was chosen as an option for developing a new model for the DSS.

In this chapter, the developed interactive DSS components are further detailed, and the newly proposed game theory based G-Model is outlined. A number of software applications to build game theory environments are examined, and an application is selected and used to design and construct a 3-player model. A crucial activity in the DS research path is evaluating the developed artefacts, which is the focus of this chapter. Artificial evaluation is done by two experts in the field, who ensure the developed artefacts meet the specified criteria. If the developed artefacts are deemed ready, and at an adequate capability maturity level, the artefacts are passed on to external experts, to be evaluated, naturalistically. This has been the case, and the artefacts have been further evaluated by five experts in IT audit, IT governance, security and risk management, and IT operation and Business Continuous Planning (BCP) management, respectively. The results of both evaluations are analysed, critiqued and bench-marked against the devised criteria and corresponding questions, to draw conclusions.

This chapter is structured as follows: section 6.1 reviews the newly proposed artefacts design and development. Section 6.2 outlines the artefacts evaluation, as the artificial and naturalistic experts' evaluation for the interactive DSS and G-Model. Section 6.3 contains other analyses available in the Gambit software and the framework application to design and build a game theory based model. In section 6.4, a review of the research progress according to the DSR roadmap tasks and activities is made, indicating what changes, updates and

additions are caused by the artefacts evaluation outcomes. The chapter is concluded in section 6.5.



## 6.1 ARTEFACTS DESIGN, DEVELOPMENT

In Chapter 5, evaluation of the artefacts were reported and discussed in section 5.2, and further detailed in sub-section 5.3.1. It concluded that C-Model was deemed not fit for purpose. It was decided that the rest of the proposed DSS components could remain the same. With regards to IT risks and Access Management (AM) risk were still included. However, as will be detailed in sub-section 6.2.1, the risks are detailed at a granular level than used in the C-Model. The risk mitigation measures, controls and processes are to be selected from the same recognised IT controls frameworks, best practice and standard: COBIT, ITIL and ISO 27001/2.

In Chapter 3, section 3.4, and briefly iterated in Chapter 5, sub-section 5.3.1, it was stated that Game-Theory modeling could be utilised to build a model for a DSS. The purpose of the DSS is to aid practitioners in their decision-making process for selecting the best controls. In this section the game theory based model is defined along with the guidelines on how to calculate the game's strategies payoff values. To develop a game theory based model and provide full analysis of the selected type of a game required a solid background in mathematics. The objective of this research is not to investigate game theory principles and validate its mathematical aspects, rather to investigate its applicability for addressing the research problem. The objective was therefore to investigate the application of a game theory based model, to find the best controls configuration to manage IT risks in a cost effective manner.

A number of developed software applications have been explored that provide a framework for constructing game settings. The goal was to find an adequate application to build a 3-player game setting where COBIT 4.1, ITIL v3.0 and ISO 27001/2 are the players representing the respective frameworks that can

compete to mitigate defined IT risks. This section is structured as follows, sub-section 6.1.1 explores some of the available game theory based applications. While sub-section 6.1.2 outlines the G-Model rules and guidance, and sub-section 6.1.3 the development of G-Model using Gambit14.1.0 is outlined.

### 6.1.1 Game Theory Software Applications

The following game theory software applications were explored to choose one of them to build the proposed IT-risk oriented game setting.

**GamePlan** is a game theory framework run under Microsoft Windows. When installing GamePlan users have an automatic trial period of 21 days and comprehensive documentation and help is provided along with a Tutorial. The tutorial uses the Example Library provided in the installation program. A good way to learn how to use GamePlan is to follow the tutorial as it explores some examples of the library. Figure 6.1depicts the layout of the initial display of GamePlan.

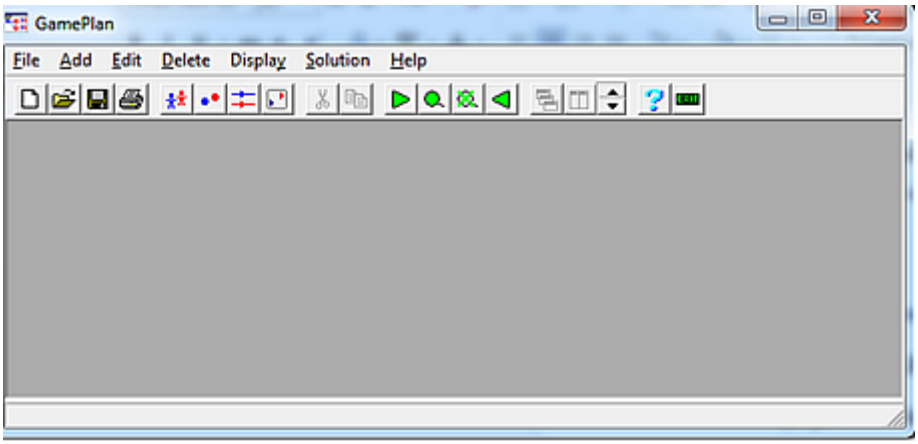


**Figure 6.1: GamePlan Display**

**Gambit** is an open-source collection of tools for creating 'Extensive' and 'Strategic' 'Normal' games and for doing computation in game theory. Gambit has an intuitive GUI to create games of multiple players, define and associate strategies for the players. Also it has a command-line for using Python scripting and an API is available. Gambit is available for Microsoft Windows, Mac OS X, and Linux operating systems. The framework facilitates computing one or all the Nash equilibria of the game, and other computational options.

The tool was developed by McKelvey, Richard D., McLennan, Andrew M., and Turocy, Theodore L. (2014). Gambit is a software tool for game theory, and version 14.1.0 is found at http://www.gambit-project.org.

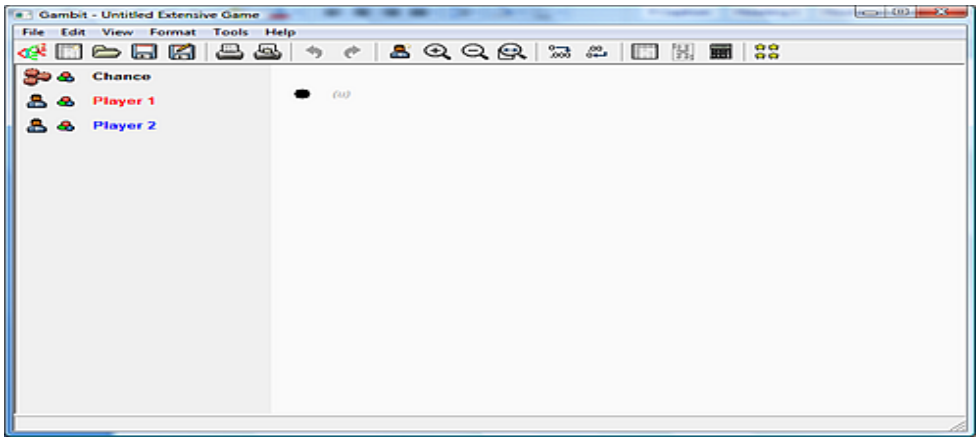


**Figure 6.2: Gambit Initial Display**

Figure 6.2 shows the initial display of Gambit, while Figure 6.3 depicts an extensive type of game found in Gambit.

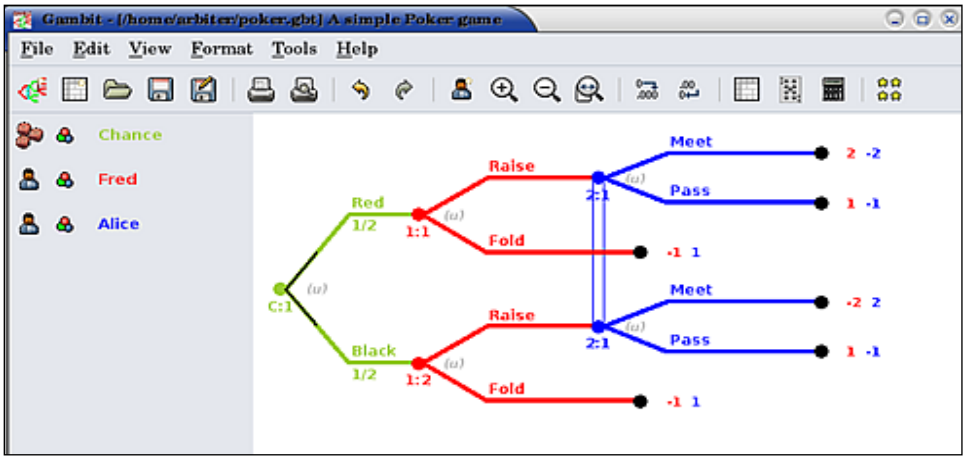


**Figure 6.3: Gambit Extensive Game Layout**

Figure 6.4 illustrates Strategic or a Normal form of game in Gambit, when payoff values are populated, Nash equilibria are calculated and dominant strategies are identified. The latter are marked in Crosses, as shown in Figure 6.4.

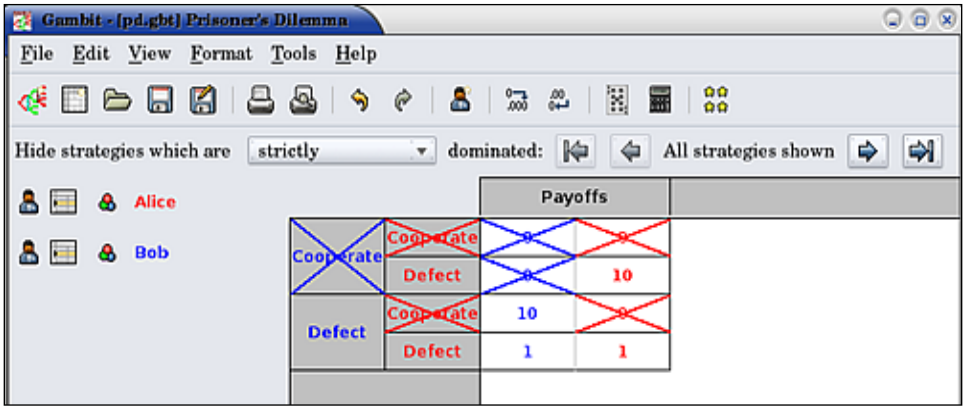


**Figure 6.4: Gambit Strategic Game**

**Game Theory Explorer (GTE)** is a web based software application developed where various types of games can be constructed in the framework. GTE is a software tool to create and analyse games as models of strategic interaction. An extensive or strategic-form of game can be created and displayed with a web based graphical user interface as shown in Figure 6.5. It will compute one or all Nash equilibria of the game. It is found at http://www.gametheoryexplorer.org/ .

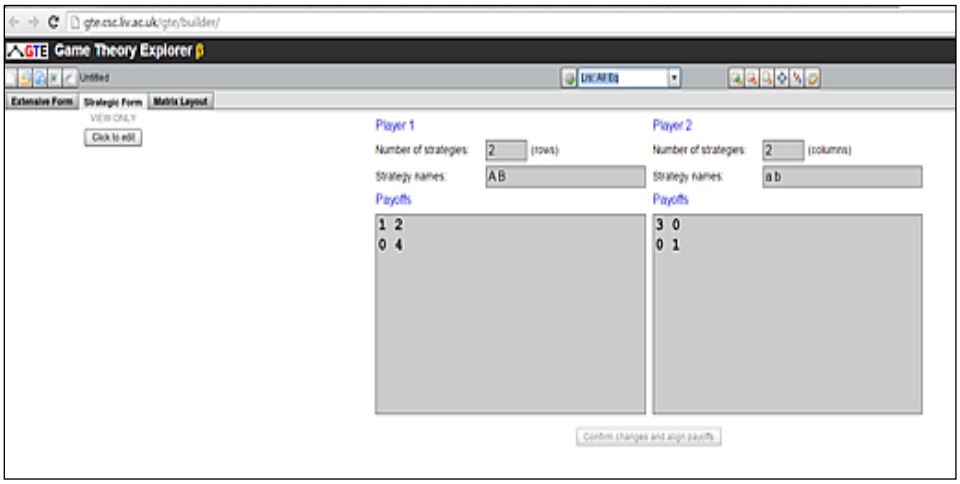


**Figure 6.5: Game Theory Explorer GTE- Strategic Game**

After spending sometime evaluating these applications, it has been found that GamePlan has some good features, documentation and a tutorial is provided, however, it is not free. On the other hand, Game Theory Explorer is not so intuitive, and the documentation is not thorough. On the contrary, Gambit is found to have a very good documentation and various games could be constructed in Extensive and Strategic forms. Gambit seemed to be more intuitive and has by far many more functions; hence the decision was made to use the Gambit software application to develop the proposed game theory based model.

### 6.1.2 G-Model Definitions and Guidance

The model is branded as G-Model denoting game-theory modeling. G-Model is built as a three player game with the players: COBIT 4.1, ITIL v3.0 and ISO 27001/2 2005. Each player has two strategies: Implement and Not-Implement, as depicted in Figure 6.6, which shows examples of payoff values for each player's strategy in the parentheses.

| | | COBIT 4.1 | | | |
|---|---|---|---|---|---|
| | | Not_Implement | | Implement | |
| | | ISO 27001/2 | | ISO 27001/2 | |
| | | Not_Implement | Implement | Not_Implement | Implement |
| ITIL V3.0 | Not_Implement | (0,-1,-2) | (0,0,-1) | (0,-1,1) | (0,0,1) |
| | Implement | (1,-1,-1) | (1,0,-1) | (1,-1,1) | (1,1,2) |

**Figure 6.6: 3-Player Game Model**

The type of the game that G-Model is based on a non-collaborative game setting where actions are executed in an order that best suits the environment. However, some overlap might take place in the players' selected strategies; i.e. mitigating similar risks or part of it, which should be considered when payoff values are determined. The game is to be played as and when a practitioner requires decision-making. The information is accumulated, and is reflected in the payoff value that each selected control can potentially produce.

With regards to the payoff values each recognised framework and best practice would generate the Utility metric. The utility is a numerical figure that comprises the difference of the gained value from mitigating risks and the cost of control and/or process implementation and ongoing maintenance.

**Utility (U) = Gained Value (from mitigating defined risks) – Implementation Cost and ongoing Maintenance of controls/processes**

Table 6.1 outlines the five payoff levels along with some guidance on how to estimate the payoff value of each strategy.

**Table 6.1: G-Model Payoffs Guidance**

| Payoff | Description of possible risk mitigation scenarios |
|---|---|
| -2 | Risk is not mitigated or slightly mitigated. |
| -1 | Risk is mitigated but at high cost, i.e. control is quite expensive to implement and maintain. Control overlaps with other controls/processes from another framework or best practice. |
| 0 | Breakeven - cost vs returned value. |
| 1 | Partially mitigating risks. Good returned value, shared with other controls from other implemented frameworks. |
| 2 | High returned value, implemented control/process from one framework, fully or largely mitigating the defined risks |

Various IT functions and activities have different risks; furthermore, depending on the environment and business context, identified risks assessment could differ from

one organisation to another. Risks are analysed and evaluated, based on the outlined Risk Assessment processes defined in Chapter 2, section 2.1. Risks that require mitigation, for example overall risks with medium and high overall risk rating, are to be classified as per the Risk Space Matrix defined in Table 6.2.

**Table 6.2: Risk Space Matrix**

| Risk Space | | |
|---|---|---|
| **Strategic** | **Project** | **Operational** |
| | | |

Classifying risks according to the Risk Space Matrix can help practitioners define relevant controls and to what extent selected controls can mitigate the identified risks. Once risks are positioned within the Risk Space Matrix, practitioners are able to outline selected relevant controls and processes from the recognised frameworks and best practices. Furthermore, the Risk Space Matrix helps calculate the controls' payoff values that practitioners need to determine as part of using the G-Model.

### 6.1.3 G-Model Development

Gambit 14.1.0 has been selected to build G-Model as shown in Figure 6.7. The figure illustrates the three players: COBIT 4.1, ITIL 3.0 and ISO 27001/2 - 2005. Each player has two strategies: Implement, and N(ot)-Implement. It can be seen that the 'Not' is truncated to 'N' only, for visibility purpose. The figure also shows that COBIT is marked in Red, while ITIL in Blue and ISO 27001/2 in Green, so that payoff values can be easily associated with each player. In case the colours are not shown, the first payoffs column is for COBIT, the middle is for ISO 27001/2 and the last is for ITIL values. The payoffs are initially set to zero, thence, payoffs can be edited, as shown in Figure 6.8.

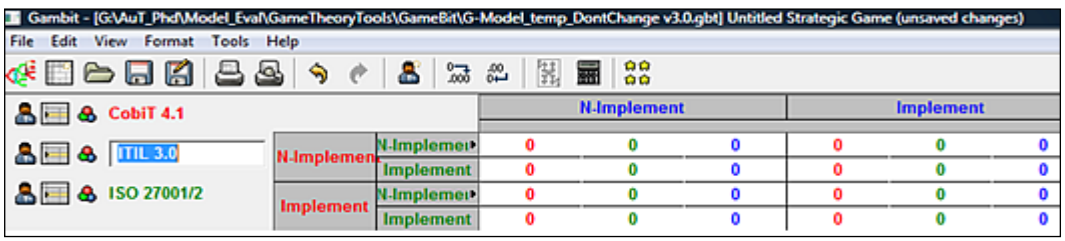


**Figure 6.7: G-Model using Gambit Strategic Game Display**

Payoff values can be entered at any order based on how the game is designed. In this example, the row (-2,-2,-2) denotes the payoff values for the three frameworks

in the order: COBIT, ISO 27001/2 and ITIL, when the 'Not Implement' strategy is selected. While the next row to the right (-1, 0, 2) denotes payoff values for the players, when only ITIL is implemented.

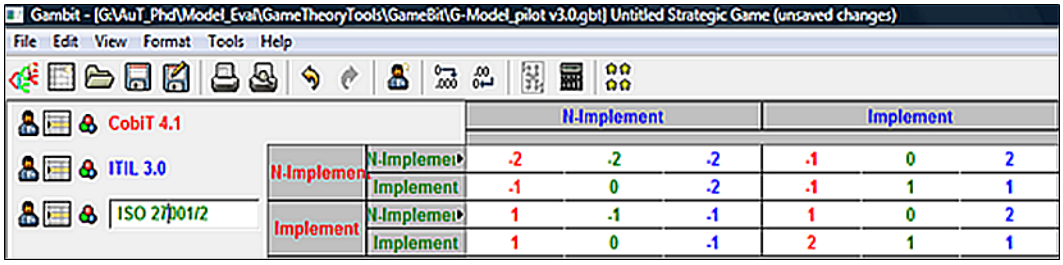


**Figure 6.8: G-Model Populated with Payoff Values**

As explored in Chapter 3, section 3.4, when game payoff values are determined for all the possible actions or strategies profiles, then the game is solved. The resulting strategy deontes the best strategy that would return the best payoff for all players. Some games could have one dominant strategy; other games have more than one. The Nash Equilibrium (NE) can be calculated, as shown in Figure 6.9. The NE, which is in this case 'Implement' for the three players, that is implementing all the included controls and processes, in the game setting.

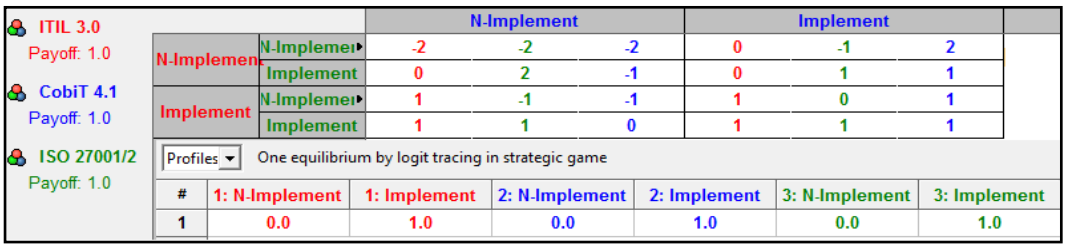


**Figure 6.9: G-Model with Nash Equilibrium Calculated**

Furthermore, Gambit provides other functionalities, for example: a game could have more than one dominant strategy as shown Figure 6.10. This can help conduct further analysis and determine other alternatives, if the resulting strategy doesn't provide the best solution. The figure is further explained in section 6.3.

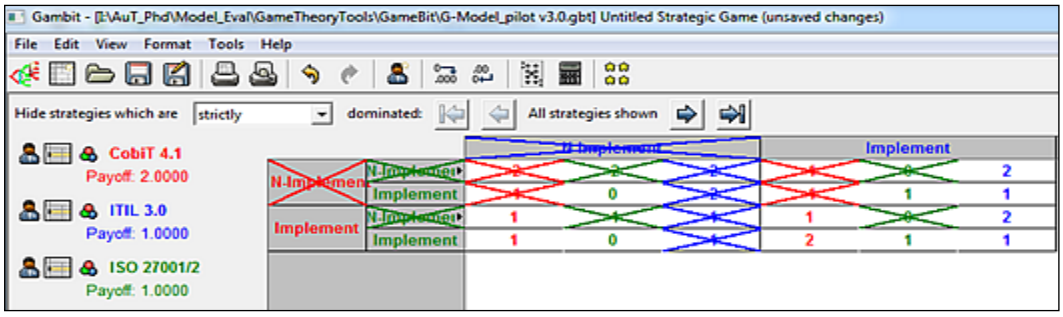


**Figure 6.10: G-Model Game Dominant Strategies**

## 6.2 ARETEFACTS EVALUATION

In Chapter 4, sub-section 4.3.4, a great emphasis has been made on the evaluation aspects of practical research, and the necessity of validating the theory design solution empirically. In similar fashion to what has been done in Chapter 5, section 5.2, artefacts will be subject to the two types of experts' evaluation: Artificial and Naturalistic evaluation. Gathering experts' evaluation and collecting resulting data must follow AUT Ethics Committee procedures and its requirements. For details please see Appendix A.

This section comprises the following sub-sections: 6.2.1 outlines the evaluation preparation activities, while sub-section 6.2.2 includes the artificial evaluation procedure and analysis. In sub-section 6.2.3 the critical reflection on the outcomes of the evaluation outcomes is conducted and experts' suggested changes are outlined. Sub-section 6.2.4 reports the naturalistic evaluation, activities, and gathered data and analyses, while sub-section 6.2.5 provides critical reflection on the outcomes of the naturalistic evaluation.

### 6.2.1 Evaluation Preparation Activities

In section 6.1 an interactive DSS has been referred to, which is essentially a spreadsheet that contains an IT risk register, with a common risk assessment of impact and likelihood rating criteria before and after applying the corresponding controls. In a similar fashion to what has been done in Chapter 5, 'Access Management' (AM) has been selected as it is a good representative of the full IT General Controls (ITGC). AM has strategic, project and operational risks. AM controls vary, from policy, to physical and logical access controls, to manage access to hardware and software including operating systems and applications. Another reason for selecting AM was that anticipated experts to participate in the evaluation are specialised in IT audit, risk and security management, and IT operations management. Those experts should have sufficient knowledge to assess the risk and advise adequate controls, or at least be able to form an opinion of the artefact. While some experts have experience across all IT risks, depending on their type of work, for example, IT auditors, IT risk and security managers, others have a limited scope. For example, IT operations managers, business continuity or project managers might have good experience in some IT risks areas, but not all of the IT risks. AM

is common to all roles, as it relates to every aspects in IT systems. Therefore, selected experts would have sufficient knowledge and experience in AM risks that enables them to evaluate the artefacts and provide quality feedback.

As indicated in the introductory paragraph of section 6.1, that AM risks will be defined utilising publicly available documents for common AM risks (ISACA, 2009a). Four risks were selected, as shown in Table 6.3. Note that the list is not exhaustive.

**Table 6.3: Identified Access Management Risks**

| Risk No. | High Level Scenarios | Description |
|---|---|---|
| R1 | Software Integrity | Intentional modification of software leading to wrong data or fraudulent actions. |
| | | Unintentional modification of software leading to unexpected results |
| | | Unintentional configuration and change management errors |
| R2 | Infrastructure (hardware) | Erroneous misconfiguration of hardware components |
| | | Intentional tampering with hardware (e.g. security devices) |
| R3 | Logical Attacks | Unauthorised users trying to break into systems |
| | | Industrial espionage |
| R4 | Logical Trespassing | Users obtaining access to unauthorised information |
| | | Users stealing sensitive data |

Utilising the researcher's experience in IT risk management and auditing, relevant controls to the identified risks were chosen from COBIT 4.1. In addition, referencing mapping documents between COBIT4.1, ITIL v3.0 and ISO 27001/2 (ISACA, 2008), corresponding controls and processes from those best practice and standards have been added to the potential controls list to mitigate the defined AM risks, as shown in Table 6.4

**Table 6.4: Selected Mitigating Measures for the Defined AM Risks**

| Risk No | Mitigating Measures | | | |
|---|---|---|---|---|
| | **Guidance** | **COBIT 4.1** | **ISO 27001** | **ITIL 3.0** |
| **R1** | Have data integrity ownership and responsibilities been communicated to appropriate data/business owners and have they accepted these responsibilities? | **PO4.9**<br>Provide the business with procedures and tools, enabling it to address its responsibilities for ownership of data and information systems. Owners should make decisions about classifying information and systems and protecting them in line with this classification.<br>**PO6.5**<br>Communicate awareness and understanding of business and IT objectives and direction to appropriate stakeholders and users throughout the enterprise. | **PO4.9:**<br>• 6.1.3 Allocation of information security responsibilities<br>• 6.1.4 Authorisation process for information processing facilities<br>• 7.1.2 Ownership of assets<br>• 9.2.5 Security of equipment off premises<br><br>**PO6.5:**<br>• 5.1.1 Information security policy document<br>• 6.1.1 Management commitment to information security<br>• 6.1.2 Information security co-ordination | **PO4.9:**<br>• SO 6.3 Technical management<br>**PO6.5:**<br>• ST 5.1 Managing communications and commitment<br>• SO 3.6 Communication |
| **R2** | Adequate physical security controls are in place | **DS12.2**<br>Define and implement physical security measures in line with business requirements to secure the location and the physical assets.<br>Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, | **DS12.2**:<br>• 9.1.1 Physical security perimeter<br>• 9.1.2 Physical entry controls<br>• 9.1.3 Securing offices, rooms and facilities<br>• 9.2.5 Security of equipment off premises<br>• 9.2.7 Removal of property<br>**DS12.3**: | **DS12.2:**<br>• SO App E Detailed description of facilities management<br>**DS12.3:**<br>• SO App E Detailed description of facilities management |

| Risk No | Mitigating Measures | | | |
|---|---|---|---|---|
| | **Guidance** | **COBIT 4.1** | **ISO 27001** | **ITIL 3.0** |
| | | fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.<br>**DS12.3**<br>Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs,<br>including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should<br>apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party. | • 6.2.1 Identification of risks related to external parties<br>• 9.1.2 Physical entry controls<br>• 9.1.5 Working in secure areas<br>• 9.1.6 Public access, delivery and loading areas<br>• 9.2.5 Security of equipment off premises | • SO App F Physical access control |
| **R3** | Appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorised access via public networks. | **DS5.10**<br>Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion<br>detection) to authorise access and control information flows from and to networks. | • 6.2.1 Identification of risks related to external parties<br>• 10.6.1 Network controls<br>• 10.6.2 Security of network services<br>• 11.4.1 Policy on use of network services<br>• 11.4.2 User authentication for external connections<br>• 11.4.3 Equipment identification in networks<br>• 11.4.4 Remote diagnostic and configuration port protection | • SO 5.5 Network management |

| Risk No | Mitigating Measures | | | |
|---|---|---|---|---|
| | **Guidance** | **COBIT 4.1** | **ISO 27001** | **ITIL 3.0** |
| | | | • 11.4.5 Segregation in networks<br>• 11.4.6 Network connection control<br>• 11.4.7 Network routing control<br>• 11.6.2 Sensitive system isolation | |
| | | **DS5.4**<br>Life cycle management of user accounts and access privileges. | • 6.1.5 Confidentiality agreements<br>• 6.2.1 Identification of risks related to external parties<br>• 6.2.2 Addressing security when dealing with customers<br>• 8.1.1 Roles and responsibilities<br>• 8.3.1 Termination responsibilities<br>• 8.3.3 Removal of access rights<br>• 10.1.3 Segregation of duties<br>• 11.1.1 Access control policy<br>• 11.2.1 User registration<br>• 11.2.2 Privilege management<br>• 11.2.4 Review of user access rights<br>• 11.3.1 Password use<br>• 11.5.1 Secure logon procedures<br>• 11.5.3 Password management system<br>• 11.6.1 Information access restriction | • SO 4.5 Access management<br>• SO 4.5.5.1 Requesting access<br>• SO 4.5.5.2 Verification<br>• SO 4.5.5.3 Providing rights<br>• SO 4.5.5.4 Monitoring identity status<br>• SO 4.5.5.5 Logging and tracking access<br>• SO 4.5.5.6 Removing or restricting rights |
| **R4** | Existing controls to assign and revoke user access on need to have basis.<br>Access should be | **DS5.3** - Identification of all users (internal, external and temporary) and their activity.<br><br>**DS5.4** - Life cycle management of user accounts and access privileges. | **DS5.3:**<br>• 11.2.3 User password management<br>• 11.3.1 Password use<br>• 11.4.1 Policy on use of network services<br>• 11.5.1 Secure logon procedures | **DS5.3:**<br>• SO 4.5 Access management<br>**DS5.4:**<br>• SO 4.5 Access management<br>• SO 4.5.5.1 Requesting access<br>• SO 4.5.5.2 Verification |

| Risk No | Mitigating Measures | | | |
|---|---|---|---|---|
| | **Guidance** | **COBIT 4.1** | **ISO 27001** | **ITIL 3.0** |
| | reviewed on regular basis. | | • 11.5.2 User identification and authentication<br>• 11.5.3 Password management system<br>• 11.5.5 Session time-out<br>• 11.5.6 Limitation of connection time<br>• 11.6.1 Information access restriction<br>**DS5.4:**<br>• 6.1.5 Confidentiality agreements<br>• 6.2.1 Identification of risks related to external parties<br>• 6.2.2 Addressing security when dealing with customers<br>• 8.1.1 Roles and responsibilities<br>• 8.3.1 Termination responsibilities<br>• 8.3.3 Removal of access rights<br>• 10.1.3 Segregation of duties<br>• 11.1.1 Access control policy<br>• 11.2.1 User registration<br>• 11.2.2 Privilege management<br>• 11.2.4 Review of user access rights<br>• 11.3.1 Password use<br>• 11.5.1 Secure logon procedures<br>• 11.5.3 Password management system<br>• 11.6.1 Information access restriction | • SO 4.5.5.3 Providing rights<br>• SO 4.5.5.4 Monitoring identity status<br>• SO 4.5.5.5 Logging and tracking access<br>• SO 4.5.5.6 Removing or restricting rights |
| | Have data integrity ownership and responsibilities been | **PO4.9**<br>Provide the business with procedures and tools, enabling it to address its | **PO4.9:**<br>• 6.1.3 Allocation of information security responsibilities | PO4.9:<br>• SO 6.3 Technical management |

| Risk No | Mitigating Measures | | | |
|---|---|---|---|---|
| | **Guidance** | **COBIT 4.1** | **ISO 27001** | **ITIL 3.0** |
| | communicated to appropriate data/business owners and have they accepted these responsibilities? | responsibilities for ownership of data and information systems. Owners should make decisions about classifying information and systems and protecting them in line with this classification.<br>**PO6.5**<br>Communicate awareness and understanding of business and IT objectives and direction to appropriate stakeholders and users throughout the enterprise. | • 6.1.4 Authorisation process for information processing facilities<br>• 7.1.2 Ownership of assets<br>• 9.2.5 Security of equipment off premises<br><br>**PO6.5:**<br>• 5.1.1 Information security policy document<br>• 6.1.1 Management commitment to information security<br>• 6.1.2 Information security co-ordination | PO6.5:<br>• ST 5.1 Managing communications and commitment<br>• SO 3.6 Communication |

Defined risks are assessed based on the defined risk impact and likelihood rating as illustrated in Table 6.5 and the overall risk rating shown in Table 6.6.

**Table 6.5: Risk Assessment Rating**

| Likelihood \ Impact > | Insignificant | Minor | Moderate | Major | Extreme |
|---|---|---|---|---|---|
| Almost Certain | Medium | Significant | High | High | High |
| Likely | Medium | Medium | Significant | High | High |
| Moderate | Low | Medium | Significant | High | High |
| Unlikely | Low | Low | Medium | Significant | High |
| Rare | Low | Low | Medium | Significant | High |

**Table 6.6: Overall Risk Rating**

| Overall Risk Rating |
|---|
| High |
| Significant |
| Medium |
| Low |

Using the risk rating shown in Table 6.5 and 6.6, the identified AM risks have been assessed as illustrated in Table 6.7.

**Table 6.7: AM Risks (R1-R4) Assessment**

| | Risk Space | | | Risk Rating | | |
|---|---|---|---|---|---|---|
| **Risk No.** | **Strategic** | **Project** | **Operational** | **Impact** | **Likelihood** | **Overall** |
| R1 | | | Yes | Major | Moderate | High |
| | | | Yes | Major | Moderate | High |
| | | | Yes | Major | Moderate | High |
| R2 | | | Yes | Extreme | Unlikely | High |
| | | | Yes | Extreme | Unlikely | High |
| R3 | | | Yes | Major | Likely | High |
| | Yes | | | Major | Moderate | High |
| R4 | | | Yes | Major | Likely | High |
| | Yes | | | Major | Likely | High |

Information contained in Tables 6.3, 6.4, 6.5, 6.6 and 6.7 were all provided in a single tab in an Excel file. As noted in Table 6.9, the spreadsheet is part of the risk register component of the interactive DSS, provided to the experts. Experts were informed that the risk assessments noted in Table 6.7 could change, should that

found necessary. Several other columns are provided for the experts, to enter the selected strategy after using the G-Model, risk rating post applying the controls included in the selected strategy.

In the same Excel file, a set of payoff matrices are provided in a separate tab for each risk, along with an example as shown in Table 6.8. The payoff guidance listed in Table 6.1 is also provided in the same tab, so that experts could fill up each risk payoff matrix before using G-Model game files.

**Table 6.8: G-Model Payoff Matrix Example**

| | | | **ITIL 3.0** | |
|---|---|---|---|---|
| | | **ISO 27001/2** | Not-Implement | Implement |
| **COBIT 4.1** | Not-Implement | Not-Implement | (-2,-2, -2) | (-1, 0, 2) |
| | | Implement | (-1, 0, -2) | (-1, 1, 1 ) |
| | Implement | Not-Implement | (1, -1, -1) | (1, 0, 2) |
| | | Implement | (1, 0, -1) | (2, 1, 1) |

Also provided, was an instructions document on how to use the provided files and what parts to complete and how to use the Gambit software and G-Model. Experts were asked to apply their knowledge and expertise to assess the effectiveness and efficiency of the G-Model resulting strategy. To aid experts in providing their feedback and evaluation of the DSS and G-Model, a number of questions have been prepared to solicit the experts' views. They answered those questions after using G-Model to devise the best strategy, and to give the best control configuration. The set of questions was categorised in the following groups: The DSS overall evaluation; Using (Gambit) G-Model (not the software but the application of Game Theory based Model); Cost-benefit aspect of the (DSS_G-Model); and the Provided Artefacts and how to use the Instructions document. Each set of questions contains a number of sub-questions, as listed in Table 6.11 along with the experts' answers. The experts' written feedback along with the oral remarks were analysed to populate the artefacts evaluation criteria and corresponding questions shown in Table 4.6 articulated by Prat et al. (2014).

The list of the files described in this sub-section, in addition to the game files using Gambit software, have been prepared as listed in Table 6.9,which provides more details on the prepared files. All files have been packaged into a CD.

**Table 6.9: Artefacts List Provided for Experts Evaluation**

| No. | Name of the File | Description |
|---|---|---|
| 1 | Gambit-14.1.0.msi | Installation file for Gambit 14.1.0 software for Windows, it has been tested for Win Vista, 7 and 8. Installation files for Mac and Linux are also available on the project web side. |
| 2 | Game files<br>G-Model_MitigateRiskX v2.0.gbt | 1- 4 game files in gambit format for Experts to use, where X is (1-4) for risks (R1, R2, R3 and R4). The files are identical as the payoff values are initially zeroed, as depicted in Figure 6.7. The files are provided separately for ease of use and also to conduct further analysis after the payoff values are populated and the Nash equilibrium is calculated.<br>2- 2 more game files are provided, one file as a backup and another for demonstration. |
| 3 | Spreadsheet<br>DSS_G-Model_Evaluation_Fieldwork v0.4 | An Excel file, which contains a number of tabs as follows:<br>1- Evaluation Instructions is the first tab and contains the simple instructions<br>2- Access Management Risks<br>3- Mitigating Strategies Payoffs<br>4- DSS-G_Model Evaluation |
| 4 | Instructions document<br>DSS_G-Model_Evaluation_Instructions v0.2 | A word document detailing the model background and instructions on how to use the spreadsheet and G-Model, and what sort of files to update and produce and send back to the researcher. |
| 5 | Aligning-COBITITILV3ISO27002-Bus-Benefit-12Nov08-Research.pdf (ISACA, 2008) | Supplement reading if needed |
| 6 | CobiT_4.1.pdf (ITGI, 2007). | Supplement reading if needed |
| 7 | CD | All the files are packaged in a CD |

### 6.2.2 Artificial Evaluation

For the artificial evaluation, two experts (Exp1 and Exp2) have been approached and agreed to evaluate the artefacts. While both experts have experience in IT audit, risk management, and both work in financial companies. However, Exp1 has more years (> 20 years) of mixed work experience in IT as well as business and has considerable knowledge of the recognised IT controls frameworks. While Exp2 has (=< 10 years) and also has some experience in software development and has worked previously in a Chartered Accounting (CA) firm. The aim is not only to get their feedback on the applicability of the DSS and G-Model, but also on the usability, functionality, effectiveness and efficiency of the developed artefacts.

This section comprises the following sub-sections: 6.2.2.1 outlines the evaluation fieldwork activities, and 6.2.2.2 includes the experts' evaluation outcomes.

#### 6.2.2.1 Fieldwork Activities

Initially some emails were exchanged with the two experts explaining the objectives of the research and the proposed model. Then, an initial meeting was arranged with each expert when the CD and hard copies of the files were provided. During the meetings the researcher demonstrated the model for the experts explaining briefly the background of game theory, and how to install and use Gambit software. Following that, the researcher went through the risk register and the defined access management risks to ensure the experts understanding of the evaluation procedure. Furthermore, the researcher explained the instructions on how to use the model and what the expert was expected to do, the game files, and the set of evaluation questions they need to answer at the end of the evaluation exercise.

The experts were given 1-2 weeks to try the model. During that time; Exp2 raised some questions about the payoff values and how to calculate them. Another question was raised when controls and processes from more than one framework are implemented. Also when selected controls and processes overlap, the question was: *which framework would take precedence?* That stirred some discussion and reflected the Exp2's interest in using the model. It also gave the researcher an opportunity to enhance the payoffs calculation guidance as noted in Table 6.1. It was emphasised to the experts that the payoff rules are not fixed, and could evolve and improve as more data is obtained and analysed from the evaluation exercises.

When the experts managed to use the model other meetings were arranged to meet up with them individually to collect the game files and the updated spreadsheet. The files were checked by the researcher to ensure the instructions were followed according to the provided document. On a few occasions some re-work needed to be carried out by Exp1 as some of the instructions were not clear.

#### 6.2.2.2 Experts' Evaluation

Experts' artefacts evaluation is an essential stage in a DS based research as theory and developed artefacts applicability are put to the test. More knowledge could be

obtained as the evaluation unravels new findings and/or clarifies any ambiguity that might have been presented.

Two experts used the DSS and G-Model and then provided updated game files, the updated risk register including the residual risks assessment, and written feedback. Oral feedback also has been obtained from interviewing the experts during the second meeting. The researcher made notes from the oral feedback for analysis and triangulation with the written notes to validate the captured feedback. This sub-section contains the collected data from the two experts that comprises of a screen shot of the four game files populated with the payoff values along with the calculated Nash Equilibrium (NE). For each expert, all files outputs are combined in one screenshot. Lastly, the expert's written feedback to the set of the questions was prepared by the researcher. With regards to the experts' feedback, data were extracted from the spreadsheet and tabulated in a table. The text is checked to ensure the experts' identities remain anonymous and, if it was found necessary, the feedback text was edited and any typos were rectified. In the experts' feedback tables, salient points are highlighted in gray to attract the readers' attention.

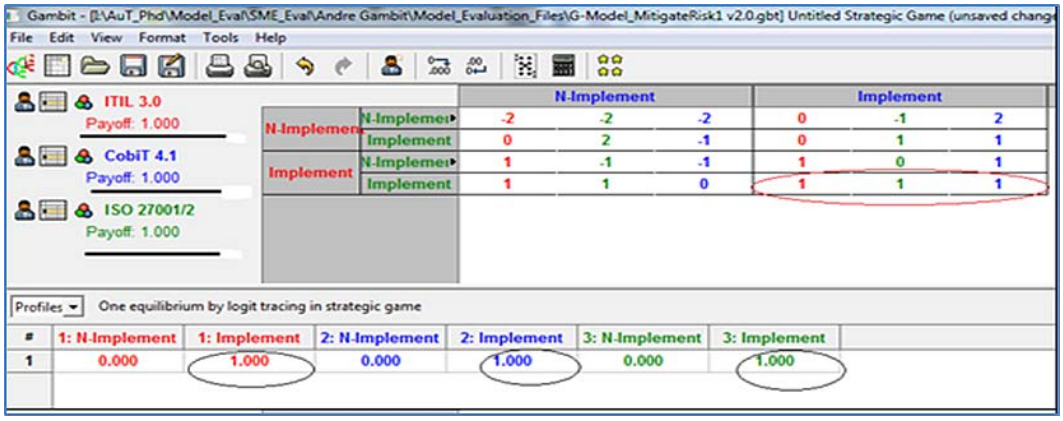


**Figure 6.11: Exp1 Risk1 Game File with Nash Equiliberium (NE)**

In Figure 6.11 the payoff values for Risk1 mitigating measures possible strategies, populated by Exp1, and the NE has been calculated as shown in the lower half of the display. In this figure, on the left hand side, underlined values reflect the payoff values vector that entails the resulting NE value. In this case, the selected strategy is implementing the controls and processes from the three players, i.e. from COBIT, ITIL and ISO 27001.

Exp1 provided assessment for the defined AM risks and the corresponding controls and processes selected by the researcher from the recognised frameworks.

In Figure 6.12, the four game files along with the best strategy displays are stacked up for better visibility and comparison of the four risks results. It can be seen that all the assigned payoff values for the four risks are the same; subsequently, the resulting strategy is the same.

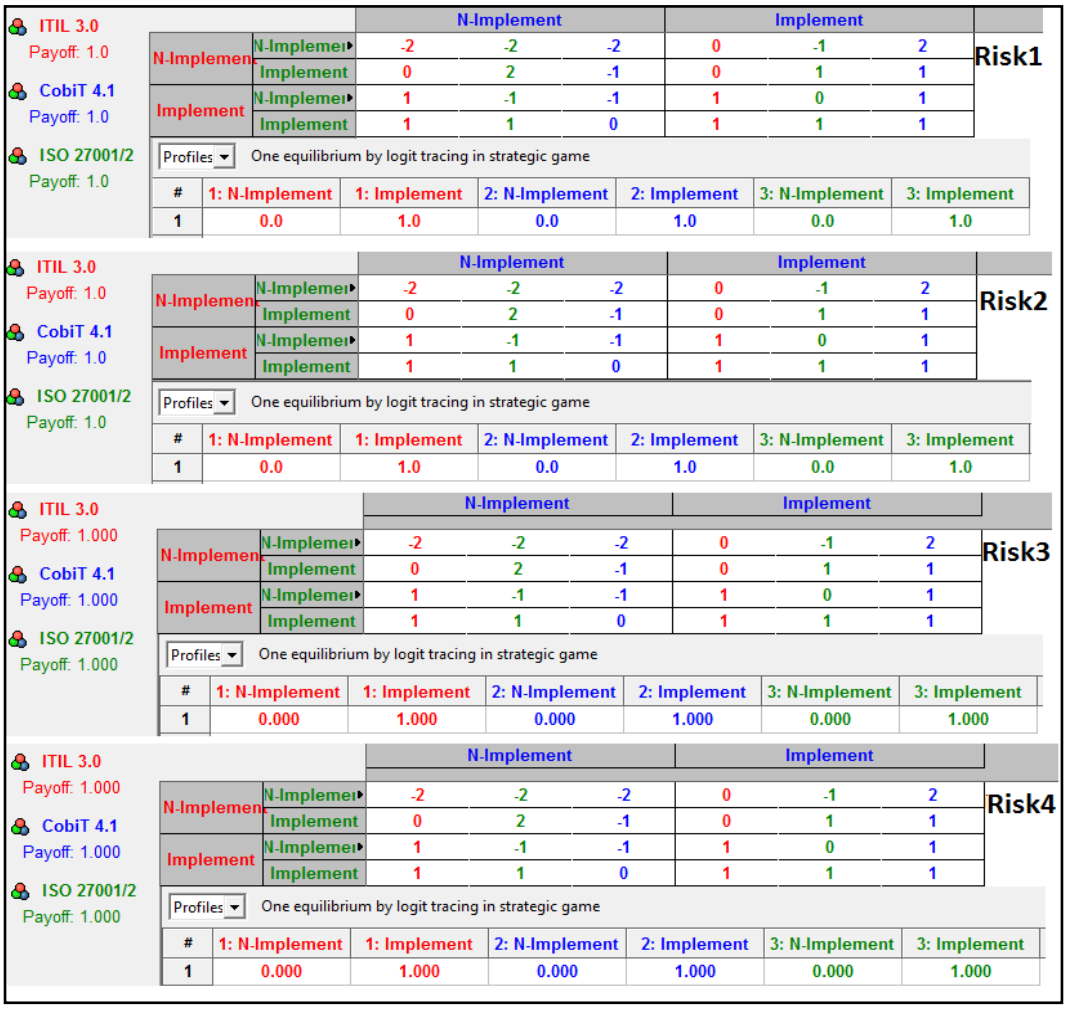


**Figure 6.12: Exp1 Risks Game Files Solutions**

However, it is also shown that the payoff value from implementing the relevant controls from the frameworks is set to 1. In another words, that strategy vector does not return the maximum payoff value. The upper row shows implementing COBIT would return the maximum value 2. Despite that, the lower row has been selected as the set of strategies that would return the best value vs the effort invested.

As for Exp2, similar output files have been gathered, and the respective payoff values and best strategy found are depicted in Figure 6.13. Prior to that, Exp2 reviewed the controls and processes and assessed the mitigation percentage of the provided mitigating measures to the defined risks as tabulated in Table 6.10.

**Table 6.10: Exp2 Assessment of the Frameworks Mitigation Percentage**

| Risk No. | Framework | % of mitigation | Comments |
|---|---|---|---|
| **Risk 1** | ITIL alone | 20% | Does not address governance （ownership), change process, access control |
| | ISO alone | 70%-100% | Mitigates most of Risk 1. It addresses ownership, change process, communications, physical and logical access. |
| | COBIT alone | 50-60% | Addresses ownership, communications, but not change process and access controls |
| **Risk 2** | ITIL alone | 50% | Has only broad facility management and physical access control, but not other controls |
| | ISO alone | 80%-100% | Most comprehensive including physical security (including offices, rooms and facilities and equipment off premises) as well as procedures for specific situations e.g. procedure/control around removal of property, and procedures while working in secure areas. |
| | COBIT alone | 70%-90% | Covers most aspects of controls for the risk, but not some specific procedures mentioned under ISO. |
| **Risk 3** | ITIL alone | 50% | Lacking vulnerability assessment control and broad in network controls. |
| | ISO alone | 80% | Most comprehensive in network, access and vulnerability assessment control, but lacking intrusion detection/monitoring control |
| | COBIT alone | 50% | Lacking vulnerability assessment control and broad in access controls. |
| **Risk 4** | ITIL alone | 70% | Sufficient controls for user access maintenance (granting & removal) and monitoring, but weak in ownership aspect |
| | ISO alone | 100% | Complete and specific controls in user access management, password, monitoring, ownership & policy, mitigating all risks. |
| | COBIT alone | 60% | Emphasize ownership and communication. Broad controls in user access management. |

Looking at the various payoff matrices in Figure 6.13 and the resulting best strategies, it shows Exp2 leaning towards selecting ISO 27001 as the favoured framework, as ISO 27001 focuses on IT security. It can also be seen that the best strategy is depending on the risk and corresponding mitigating measures, in comparision to the Exp1 assessment. For example, Risk1 – game 1, shows the strategy vector: the righ hand side, second row, denoting implementing COBIT with higher payoff, and ISO 27001, with less return value. The NE enforces that view, as implementing COBIT and ISO 27001 is the favourite strategy, while implementing ITIL process is not. Comparing this to Table 6.10, the resulting strategy is aligned with the Risk1 assessment. Similar anlysis and outcome can be

observed in the Risk 2 assessment and game file results. However, as for Risk3, implementing ITIL and ISO 27001 is the prefered stategy, while COBIT is not to be implemented; although, according to Table 6.10 it shows ITIL and COBIT have equally mitigating percentage.

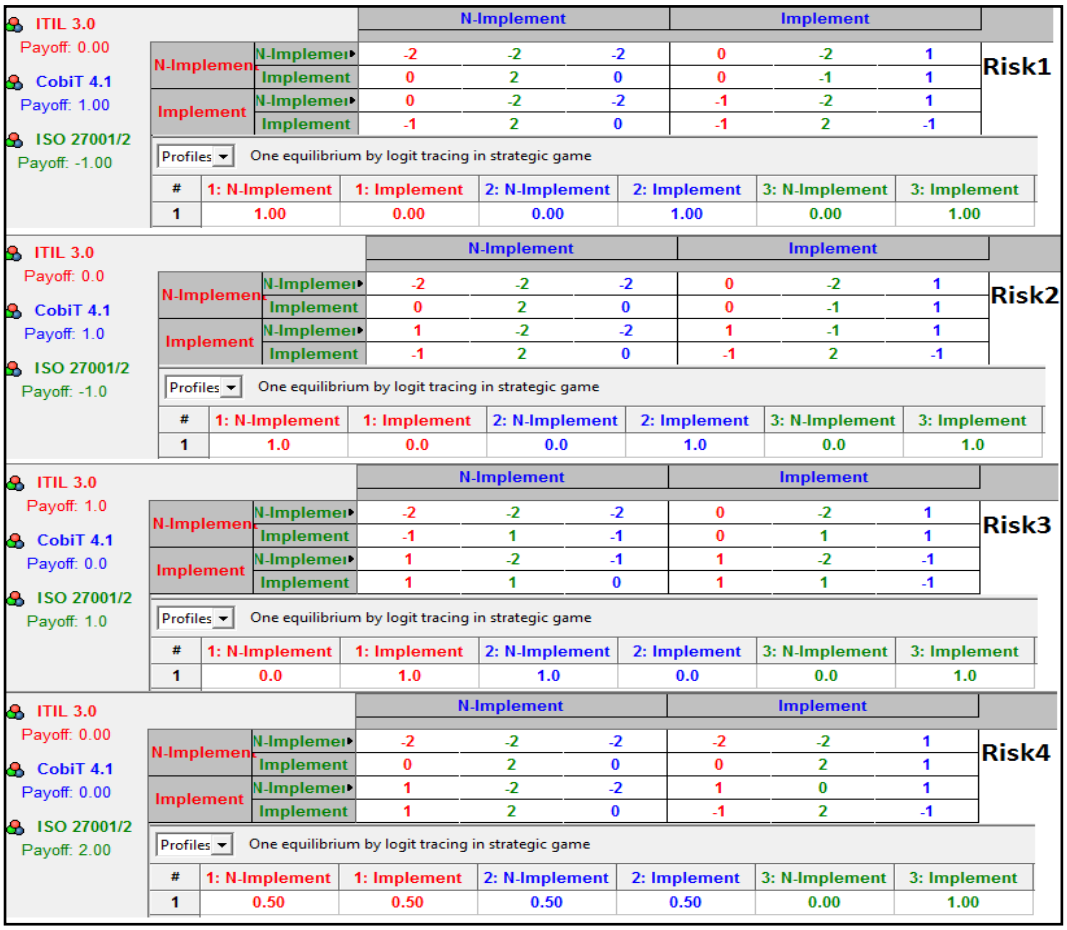


**Figure 6.13: Exp2 Risks Game Files Solution**

Lastly, Risk4 screen shot, which shows an interesting resulting strategy favoring ISO 27001 implementation. However, for ITIL and COBIT, it shows that the same payoff would be gained from implementing or not implementing their corresponding controls and processes.

A number of artefact evaluation criteria based on the system approach articulated by Prat et al. (2014) and corresponding questions were formed as listed in Table 4.6. Questions are prepared to obtain experts' feedback after using the G-Model along with the simplified risk register that was provided. Table 6.11 lists the set of questions and sub-questions and both experts' replies. Salient points of their answers have been shaded indicating the experts' key points.

**Table 6.11: Experts' Evaluation Feedback**

| No. | Questions | Exp1 Answers | Exp2 Answers | Researcher's Comment/Action |
|---|---|---|---|---|
| **1** | **The DSS overall evaluation:** | | | |
| 1.1 | Overall, how effective the proposed DSS is (the spreadsheet with risk space, payoffs matrix and G-Model) in managing the defined risks? | "It gives the participant a good reference point to see all the frameworks in one place." | "Yes, the DSS is largely effective. I made a few small cosmetic changes in the excel file including rearranging the order of the ITIL, ISO, COBIT columns (in 'Access Management Risks' tab); and merging some cells which belonged to the same Risk. The payoff value guidelines are a little difficult to apply. It is also subjective, even the same person applying the values, can sometimes get confused and not being consistent in how the values are applied." | Agreed to suggested changes by Exp2 regarding re-arranging COBIT, ITIL and ISO to match the G-Model layout.<br><br>As for the Exp2 second remark about working out payoff values, it is anticipated practitioners would need to go through a learning curve to get use to that. |
| 1.2 | Were the defined risks relevant to IT Access Management? | "Yes" | "Yes" | |
| 1.3 | Was the provided risk space categorisation adequate/useful? | "I did not reference this section when completing the matrix. However in saying that it will be helpful for a person just starting in risk." | "No, didn't have much bearing on the controls and payoff." | |

| No. | Questions | Exp1 Answers | Exp2 Answers | Researcher's Comment/Action |
|---|---|---|---|---|
| 1.4 | Were the provided strategies-payoffs guidelines matrix realistic and adequate? | "At first the guidelines are a bit confusing. One must remember that each framework has a different level of strategic and operational focus. Dependent on this focus it will mitigate the risk differently." | "Guidelines were a little difficult to apply, as mentioned above. Perhaps examples could be provided for different scenarios such as the ones we discussed in the emails exchanged." | Both Experts commented on the payoff guidance, which needs revising. Again working out the payoff values is the most challenging part in game theory. Also it represents the core of the game's rule, which would evolve with more evaluation and data analysis. |
| 1.5 | How easy it was to use the DSS, and switching between the spreadsheet and the G-Model? And working out the residual risks? | "Not too difficult. It is possible to use two screens." | "It was easy to use the DSS. Switching between excel and the G-Model isn't a problem. Working out residual risks is somewhat subjective, as controls given were high level ones, without further delving into the frameworks, I was making some broad assumptions about how much the high level controls were covering. Interpreting and applying the payoff value was the most difficult." | |
| 1.6 | How long it took you to go through each risk, from start | "Yes. However refer to my questions below: | "It didn't take me long to go through each risk and populate % of risk mitigated by each framework alone | |

| No. | Questions | Exp1 Answers | Exp2 Answers | Researcher's Comment/Action |
|---|---|---|---|---|
| | to finish? Was that reasonable? | 1) Why would the strategy for implementing the different frameworks change for the different risks?<br>a. Do you not think that the above would always be a question when only one person is engaged in completing the strategy matrix? Or b:<br>b. If you are using a person that has bias for one or more of the frameworks? Or c:<br>c. The person does not have knowledge of one or more of the frameworks?<br>2) Have you thought about the fact that implementing controls and processes, including deferent frameworks are very subjective and also depends on the buy in of management?<br>3) The understanding of the risk differs from person to person and depending the understanding by management | and what gaps / residual risks exist for each framework. I recorded this in the spreadsheet beside each risk. But it took me a while (many emails) to figure out what they meant in terms of payoff value when more than one framework is applied." | |

| No. | Questions | Exp1 Answers | Exp2 Answers | Researcher's Comment/Action |
|---|---|---|---|---|
| | | and their willingness to widen their lens on the risk, the implementation or not of controls/processes/frameworks is in balance. " | | |
| 1.7 | What area of improvement - you can think of? Please list as many as possible - DSS perspective. | "Look at my Excel file as I have made the changes." | "As mentioned above, I struggled the most in coming up with the payoff values. The payoff value guidelines maybe a little vague." | Payoff guidance wording will be re-worked out and provide some examples, during the demonstration. |
| 1.8 | Modifications needed | "See above" | "same as above" | |
| **2** | **Using (Gambit) G-Model (not the software, but the application of Game Theory based Model):** | | | |
| 2.1 | Do you think G-Model (game theory based) model is effective/efficient in determining the right combinations of controls/processes, in a 3-player-game setting? | "I think that it is something that could be used. However is can also make the decision process more cumbersome if the people using it does not have an understanding of the frameworks. See my questions." | "Probably. I say this because 2 out of 4 risks I reviewed had outcomes that I would have picked/expected. The other 2 had same outcomes as they had similar inputs (ISO being the best, and the other two frameworks mitigates risks partially), and the strategy picked by the game was to implement ISO PLUS another framework, which | |

| No. | Questions | Exp1 Answers | Exp2 Answers | Researcher's Comment/Action |
|---|---|---|---|---|
| | | | creates duplicate efforts. But overall, all 4 risks were mitigated after the strategies." | |
| 2.2 | Usability and ease of operation | "Not difficult." | "The DSS is quite easy to use and operate. A small note to make is to keep the order of the 3 frameworks consistent in every place (excel spreadsheet, payoff matrix and the games). The game application has the strategy output listed on the left hand side vertically in one order (ITIL, COBIT, ISO) and then on the right, in the matrix showing horizontally another order (ITIL, ISO, COBIT). " | Exp2 comments are noted and changes are made in the new set of files. |
| 2.3 | Strengths and weaknesses for the model | "See my questions" | "Nothing further apart from that mentioned above." | |
| 2.4 | Area of improvement | | "Nothing further apart from that mentioned above." | |
| **3** | **Cost-benefit aspect of the (DSS_G-Model)** | | | |

| No. | Questions | Exp1 Answers | Exp2 Answers | Researcher's Comment/Action |
|---|---|---|---|---|
| 3.1 | Effort spent on finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the effort)** | "Having the right controls/ processes in place will always depend on managements understanding of the risks/issues at hand and also their reluctance/willingness to spend the appropriate amount of money to implement the right controls/processes. Having the DSS_G-Model may just be a tool to assist in the decision process." | "I spent a little bit of time working on the coverage of risk for each individual framework. These are documented in the payoff matrix tab of the spreadsheet. Once that's done, the strategy became quite obvious. I didn't need to do the payoff value and the game to come up with a strategy. And the game returned different strategy than what I would have expected for Risk 1 & 2. One may ask whether there's any value in working on the payoff value and using the game engine." | |
| 3.2 | Time Taken for finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the time?)** | "This will always depend on the knowledge base of the participants." | "same as above" | |
| **4** | **Provided Artefacts and how to use Instructions** | | | |
| 4.1 | Were the provided instructions helpful/clear? | "Yes" | "Yes. I suggest some improvement on the payoff value definition" | |

| No. | Questions | Exp1 Answers | Exp2 Answers | Researcher's Comment/Action |
|---|---|---|---|---|
| 4.2 | How to improve that? (Clarity, Details, Demonstration) | "I am sure you have already thought of this. Ensure that you get a good proof reader that will assist you in getting clarity, detail, grammar and spelling correct. Out of my own experience this is always a tripping point and a hole that I have fallen into." | "Payoff value may need to be defined differently, i.e. individual framework's perspective as opposed to risk for the company as a whole; opportunity loss; residual risk etc. Use some examples to explain the impact on another framework's payoff when one framework is implemented. Like the scenarios we discussed in our emails." | |

### 6.2.3 Critical Reflection on Artificial Evaluation Results

Based on the artefacts evaluation criteria devised by Praft et al. (2014) and the corresponding question, and similar to what has been done in Chapter 5, the experts' evaluations are analysed and critiqued against the criteria as shown in Table 6.12. Furthermore, in this section the suggested changes resulting from the expert artificial evaluation are outlined in sub-section 6.2.3.1.

**Table 6.12: DSS and G-Model Experts' Artificial Evaluation**

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| **Goal** | **Efficacy** | | Q1. How effective is the proposed DSS in managing the defined IT risks. | Exp1 and Exp2 answers to Q 1.1, both confirmed that the DSS is effective and it gives participants a good reference point. |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | **Validity** | | Q1. How reliable the DSS outcomes are?<br>Q2. Is the risk assessment adequate? | 1. Generally speaking the DSS – knowledge base, defined controls, risk assessment and the use of G-Model is acceptable, as noted by both experts, in their answers to Q1.1, 1.2, 1.5, however, working out the residual risk is a bit subjective, according to the Exp2, in response to Q1.5. While both experts suggested some improvements and that was anticipated, but no major negative remarks were made, which indicates the DSS is reasonably reliable.<br>2. The risk assessment is adequate, as it is commonly utilised methodology; this has been noted in the answers to Qs 1.1 and 1.4. However, the provided risk space was not very useful as noted by the two experts. This however, didn't have much bearing on the risk assessment or on the resulting outcomes. |
| | **Generality** | | Q1. How easy is it to update the included frameworks in the DSS? E.g. replace ITIL 3.0 with ITIL 2011, ISO 27001-2005 with 27001/2013.<br><br>Q2. Is DSS capable of including all ITGC risks? | 1. Through the obtained oral feedback, both experts indicated, as noted in their answers to Q 1.6 in particular Exp1, and Q2.1 and throughout the discussion that took place when collecting the data of them, the feasibility of updating utilised frameworks depends on the changes made to those frameworks. If the change doesn't affect the framework architecture as is the case in ITIL 3.0 to |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | | Q3. Could the DSS include other frameworks, e.g. ValIT, COSO_ERM? | 2011 edition, and ISO27001-2005 to ISO27001-2013, it is reasonably easy, however, changing COBIT 4.1 to COBIT 5, requires considerably more effort, as COBIT 5 is architecturally different than COBIT 4.1. However, by utilising knowledge and expertise of some practitioners, would replace the relevant controls and processes, then the model can be used by less experienced users.<br><br>2. Both experts indicated the feasibility of adding more risks into the risk register, and add more corresponding controls and processes.<br>3. While including another framework to the DSS possible controls and processes, however, adding more controls to the G-Model, is viable, but it has been noticed that games with more than 3 players, increases the mathematical complexity of the model. However, given that Gambit framework is it is possible to build more than 3 player games. |
| **Environment** | **Consistency with people** | **Utility** | Q1. What is the total gained value, from practitioner's perspective? | Exp1 indicated that DSS could be a good reference and Exp2 stated the DSS with its G-Model is effective, along with risk assessment and provided controls, while there are some improvements to the proposed DSS and G-Model. However, by inference the DSS and G-Model |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | | | would help practitioners make an informed decision in mitigating IT risks. |
| | | **Understand-ability** | Q1. Is the DSS intuitive? | Exp1 and Exp2 noted in Q1.5 the DSS is easy to use, also in Q1.6 and 2.1 and Q2.2, their only concern was using the payoff guidance to generate the payoff values for the various strategies. Exp2 in particular made a number of remarks and exchanged some emails with the researcher concerning how to apply the payoff guidance. That was totally expected, as calculating the payoff values is about the game rules themselves, which is the most challenging part of the game design. Also, as experts did not use such a method of working out controls gain by such a holistic approach. It was anticipated to have a learning curve until the experts become familiar with the model and used it with confidence.<br>This view can be seen in experts' answers to Q3.1 and 3.2. |
| | | **Ease of use** | Q1. Is the DSS easy to use? | Yes, as noted by both experts in Q1.5 and 2.2. |
| | | **Ethicality** | Q1. Does using the DSS have or could cause any ethical issue? | No ethical issue noted. |
| | | **Side effects** | Q1. Does the DSS or model produce new risks and/or incur further cost? | Exp1 and Exp 2, did not have any concerns about new risks, however, as noted in Q1.6, and 3.1 and 3.2, both referred to a possible overlap among the proposed controls resulting from using the G-Model. This is a valid point, and is crucial to the effectiveness of the DSS |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | | | and G-Model in particular. However, it depends on first, how the risks are defined and the associated controls. While defined risks were adequate as noted by both experts, however, the proposed controls from (COBIT, ITIL and ISO 27001) are at high level, especially in ITIL, that was done by design, to simplify the model and required evaluation. Should controls and processes be analysed to a more granular level, then more games would be required for each risk, and with possibly a multi-level game. This would be a candidate for further improvement. |
| | **Consistency with organisation** | **Utility** | Q1. What is the total gained value, from organisation's perspective? | It was not possible to measure the value from a business point of view, however, given that both experts indicated the possible gain in using the model from practitioners' point view, then by inference, organisations would benefit from the model, by managing IT risk in a cost effective fashion. |
| | | **Fit with Organisation** | Q1. Is the DSS (Risk Register, selected frameworks, model) adequately fit the organisation's Internal/External environment? | Both experts indicated that defined risks are very relevant to IT-AM, as noted in Q1.2, 2.2 and 3.2, with exceptions to the provided Risk Space Matrix, as it was not found useful. |
| | | **Side effects** | Q1. Any issues caused by using this DSS? E.g. incurring further cost, complicating the environment. | No new risk, but the G-Model could potentially incur further cost of implementing overlapping controls and processes. Once again, this could be rectified, as the |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | | | model is further refined, payoff guidance and rules are articulated clearly, using the G-Model can produce efficient and cost effective strategies. |
| | **Consistency with technology** | **Harnessing of recent technologies** | Q1. How effective and easy it is to accommodate new technology by the DSS? | Potential new risk introduced by new technology could be added to the list of possible risks. No issues are noted by any of the experts in that regard. |
| | | **Side effects** | Q1. Any issues, this DSS could cause? E.g. introducing new risks, overusing/underutilising resources, etc. | No issues or new risks could be caused. |
| **Structure (Static, the artefact's construct)** | **Completeness** | | Q1. How complete the DSS is?<br>Q2. Any area of improvement? | 1. It was admitted by the researcher that the developed artefacts are in a rudimentary stage, and would require further improvement and the risk registers and the G-Model to be integrated. That was found acceptable by both experts however; they made valuable remarks and suggestions on how to improve the DSS components and the evaluation instructions.<br>2. A number of improvements have been proposed by both experts as noted in their answers to Q1.6, 1.7, 2.2, 3.1 and 4.1. |
| | **Simplicity** | | Q1. How simple the DSS is structured? | DSS comprises of risk register and G-Model, although not fully integrated, but sufficient for the purpose of evaluation at this stage. |
| | **Clarity** | | Q1. Are the DSS components clear | Yes they are clearly distinguished |
| | **Style** | | N/A- Not to be enquired about. | N/A |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | **Homomorphism** | **Correspondent with another model** | Q1. Does the DSS map well to other Enterprise settings if any, for example IT Governance, Enterprise Risk Management, Internal Audit, Business/IT Strategic plans? | While developing an interactive DSS is not new, however, utilising game theory based G-Model in managing IT risks, is an innovative method. The concepts used in defining risks, and devising mitigating measures from IT controls frameworks, are common to the practice of the mentioned enterprise settings. |
| | | **Fidelity to modelled phenomena** | Q1. Does the designed DSS align with the theorised solution design and meet fidelity criteria exhibiting least deficiency (redundancy, incompleteness, excess, and overload)? | 1. The DSS risk register including defined risks, controls and risk assessment matrix all are professionally developed and used over and over for many years.<br>2. The DSS components each provides its intended outcomes, no redundancy, overload or excess are noticed, however, some improvement is required to integrate the risk register with the G-Model |
| | **Level of detail** | | Q1. Does the DSS provide enough details and instructions on use? | Some remarks were made by the experts on the instructions and payoff guidance. |
| | **Consistency** | | Q1. Are the DSS components developed in (spreadsheets, MS-word documents, and other applications) consistent? | All DSS components are consistent. |
| **Activity (Dynamic, the operations and functionality** | **Completeness** | | Q1. Does the DSS have the right set of functions? | All DSS components are functioning properly, it needs to be integrated indicated earlier. |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| **of the artefact)** | | | | |
| | **Consistency** | | Q1. Does the DSS operate consistently? | The DSS, in particular, G-Model operates, consistently with the expected outcomes. |
| | **Accuracy** | | Q1. How accurate are the DSS functionalities? | While the input, data and knowledge base component of the DSS provide adequate risk assessment and suggest relevant controls and processes, however, to determine how accurate G-Model is in producing optimum mitigating measures is under investigation. |
| | **Performance** | | Q1. Any issues with performance? | No performance issues have been reported. |
| | **Efficiency** | | Q1. How efficient the DSS is in terms the utilised time/resource and the obtained outcomes? | Using the risk register is quite easily done by the experts as noted in Q1.2, 1.5 also in Q3.1 and 3.2 |
| **Evolution** | **Robustness** | | Q1. Does the DSS accommodate changes in internal/external environments? E.g. business dynamics, regulatory requirements, that requires assessing risks in timely fashion. | Although this was initially anticipated for naturalistic evaluation, however both experts indicated via oral feedback that this would not be an issue. As previously discussed, the model is capable of accommodating new risks introduced by new technologies or business dynamics. |
| | **Learning capability** | | Q1. Could the DSS – knowledge base – component enhanced with use?<br>Q2. Could practitioners add more knowledge as they use the DSS? | There was a learning curve in particular around working out the payoff values. Using the DSS and G-Model was fairly easy, as noted by both experts. |

### 6.2.3.1 Changes Motivated by Artificial Evaluation

As it can be seen in Table 6.11 a number of changes were suggested by the experts and incorporated as noted in the comments/actions for questions: 1.1, 1.7 and 2.2. These changes were around the risk register and game files layout, also improving the payoff guidance. The suggested payoff matrix layout by Exp1, as it is shown in Table 6.13, has been adapted and updated in the spreadsheet accordingly.

**Table 6.13: Suggested Payoff Matrix by Exp1**

| | | | ITIL 3.0 | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ISO 27001/2 | Not-Implement | | | Implement | | |
| COBIT 4.1 | Not-Implement | Not-Implement | -2 | -2 | -2 | 0 | -1 | 2 |
| | | Implement | 0 | 2 | -1 | 0 | 1 | 1 |
| | Implement | Not-Implement | 1 | -1 | -1 | 1 | 0 | 1 |
| | | Implement | 1 | 1 | 0 | 1 | 1 | 1 |

Also, Exp2 suggested the order of the framework and best practice to be aligned with the game files layout. The suggestion has been incorporated and a new set of game files has been generated for the second round of experts' evaluation. The new layout is shown in Figure 6.14, where COBIT strategies are aligned to the left, and payoff values in Red while ITIL strategies are aligned to the top, and payoff values in Blue. Figure 6.14 shows a game file with payoff values different from the ones shown in Table 6.13.

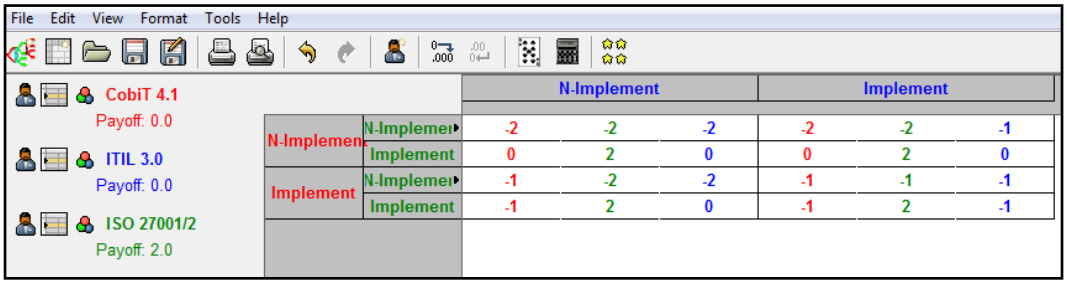


**Figure 6.14: New Game File Layout**

Furthermore, another set of questions has been added to the questionnaire around integrating controls and frameworks. In a similar fashion to the other questions, a number of sub-questions have been prepared. All outlined additions and changes made to the game files, spreadsheet and instructions document, have been produced. New versions of those files have been prepared and included in a new CD for the second evaluation cycle, the naturalistic evaluation.

### 6.2.4 Naturalistic Evaluation

Naturalistic evaluation is described often as the ‘real’ test where the designed solution or artefact is tested in an actual environment to check how effective and efficient the designed solution is. Naturalistic evaluation, evaluates the artefacts, solution in real setting, this approach is always empirical. Following the DSR roadmap outlined by Alturki et al. (2011b), naturalistic evaluation has been carried out, and a number of experts in various but related specialties have been approached. The types of experts that were sought come from IT audit, IT security and risk management, IT business continuity planning (BCP), and IT operations management groups, respectively.

This section comprises of a number of sub-sections structured as follows: sub-section 6.2.4.1 describes the fieldwork work preparations, while sub-section 6.2.4.2 outlines the experts’ evaluation outcomes and gathered data from the participated experts.

#### 6.2.4.1 Fieldwork Preparation

Changes outlined in sub-section 6.2.3.1 stemmed from the artificial evaluation have been implemented. A new set of files have been created and included in a CD. Concurrently, a number of experts have been approached to participate in conducting the artefacts evaluation. The researcher utilised his network of professional contacts accumulated throughout the years in the local community and contacted a number of professionals. The approached experts work for different organisations that vary in size and industry. However, while the selected experts share some attributes and common knowledge their expertise and depth of knowledge were diverse, which helps obtain different results and views on the use of the model. It is anticipated that different resulting outcomes would provide a valuable discussion through analysing the data and reflecting on the designed artefacts aspects outlining the fore and against arguments.

Table 6.14 lists the number of experts that have been approached and have responded. The researcher demonstrated the model and handed over a CD containing the set of files as shown in Table 6.9. Experts are coded in order to obscure their identity and work environment. The Experts will be referenced as Expert X, where X is the unique number.

**Table 6.14: List of Selected Experts for Naturalistic Evaluation**

| Expert's code | Expert's background and current role | Justification for selecting the expert | Fieldwork activities and gathered data |
|---|---|---|---|
| Expert1-Biz_IT_Aud | General and IT auditor. CISA, ITIL, Risk Management. Financial Industry | Has extensive knowledge in IT auditing, risk management. Have presented about 3-lines of defense. Not a big fan of recognised frameworks. Has very good Knowledge in COBIT 4.1, ITIL and ISO 27. | 1- Initial meeting, handed over the files, and demonstrated the model.<br>2- Gambit software did not install at the experts' computer, another meeting was arranged and sorted it out.<br>3- Exchanged a few emails clarifying a number of points regarding payoff values.<br>4- Third meeting was arranged to get the experts resulting game files, risk assessment and oral feedback. |
| Expert2-IT_BCP | BCP and IT Operation manager, CISA, BCI, | BCP and IT manager, has wealth of knowledge in BCP management. Has good experience in applying ITIL best practices. | 1- Initial meeting, handed over the files, and demonstrated the model.<br>2- A second meeting was arranged, did a quick review on the G-Model to make sure expert's understanding and has followed the right procedure, to get the experts resulting game files, risk assessment. Also oral feedback was obtained regarding the model and research objectives. |
| Expert3-IIT_Aud | IT Auditor /BCP Manager, CISA, CSK, IIA | Extensive knowledge and experience in IT auditing and risk management practices. Has a thorough knowledge in COBIT 4.1, ITIL and good exposure to | 1- Initial meeting, handed over the files, and demonstrated the model. The researcher lent his laptop for Expert3.<br>2- A second meeting was arranged, to get the experts resulting game files, risk assessment. Also oral |

| Expert's code | Expert's background and current role | Justification for selecting the expert | Fieldwork activities and gathered data |
|---|---|---|---|
| | | ISO 27001/2 standards. | feedback was obtained regarding the model and research objectives. |
| Expert4-CA_ITA | IS Advisory consulting - Senior Manager - CA firm, CISA | A senior manager in an IT advisory team works for a CA firm. | 1- Files were provided and sent over email, then a phone call was arranged to go through the instruction and demonstrated the model to Expert4.<br>2- Exchanged some emails; then a second meeting was arranged and a quick review was made on the resulting files, as Expert4 needed to clarify a few things. Files were collected as well as Expert4 oral feedback. |
| Expert5-InfoSec1 | Information Security Senior Consultant. CISM, CISSP. Professional Service provider | Extensive experience in Information Security management | 1- Initial meeting, handed over the files, and demonstrated the model.<br>2- A second meeting was arranged, did a quick review on the G-Model to make sure expert's understanding and has followed the right procedure.<br>3- Third meeting was arranged to get the experts resulting game files, risk assessment and oral feedback. |
| Expert6-IT_Ops | IT Ops manager. CISA, COBIT 5, ITIL | Expert in ITIL best practice and has good exposure to COBIT 5. | 1- Initial meeting, handed over the files, and demonstrated the model.<br>2- Exchanged a number of emails, but Expert6, was quite busy with an ongoing project.<br>3- No data obtained from Expert6. |

| Expert's code | Expert's background and current role | Justification for selecting the expert | Fieldwork activities and gathered data |
|---|---|---|---|
| Expert7-InfoSec2 | Information Security manager, CISA, CISM, CISSP. | Worked for many corporate businesses as Information Security manager, IT auditor. | 1- Initial meeting, handed over the files, and demonstrated the model.<br>2- A few emails were exchanged, and a second meeting was arranged to gather the files and feedback, which were obtained, however, it was incomplete evaluation, no risk assessment, game files not populated. Only answers provided to the evaluation questions. So can't take Expert7 evaluation into account. |
| Expert8-ExtIT_Aud | IS Auditor – External auditor, with internal IT auditing, CA, CISA. | Expert8 has extensive knowledge in ITGC based on COBIT 4.1. Would be great to see this expert's view on adding ITIL and ISO 27001 to the scene. | 1- Initial meeting, handed over the files, and demonstrated the model.<br>2- Expert8 got busy with work, arranged a couple of meetings, later were postponed as Expert8 went overseas. A Skype meeting was planned but did not eventuate.<br>3- No data obtained from Expert8. |

From the eight approached experts, only 5 experts have participated in the evaluation and returned the required files. Expert6, was quite keen to participate in the evaluation and exhibited a great enthusiasm and was impressed with the model and the research objectives, during the initial meeting. However, all attempts to get that expert to evaluate the model were to no avail. In an email, the researcher enquired from Expert6 about the reason for not evaluating the model. The researcher indicated if the model was too difficult or the instructions were not clear, the answers were negative. However, when the researcher implied in one of the emails, if the reason is because Expert6 was not very familiar with conducting risk assessment and devising mitigating measures from recognised frameworks. Expert6's answer was implicitly confirmative. Which demonstrates the challenging

task a novice practitioner could face with when attempt to conduct such an exercise. It also suggests the potential benefits a business and practitioners could gain when such a DSS is available.

#### 6.2.4.2 Experts' Evaluation

As noted in Table 6.14 that 5 out of 8 experts, have used the DSS and G-Model, who then provided updated game files, and the risk register with the residual risks assessment. In addition, written and oral feedback was obtained from the experts during those meetings. This sub-section reports the collected data from the 5 experts, in the respective five sub-sections. In each sub-section is a screen shot of the four game files populated with the payoff values and the calculated NE. Also included is a table that depicts the residual risk assessment post applying the mitigating measures resulted from using G-Model. Lastly, the expert's written feedback to the set of the questions. With regards to the experts' feedback, data were extracted from the spreadsheet and tabulated in respective tables, checked to ensure experts' identities remain anonymous and as it was found necessary, the feedback text was edited and typos were rectified. In the experts' feedback tables, salient points are highlighted in gray to attract readers' attention.

As indicated that 5 experts, have participated in the evaluation and returned the required files. A sub-section is designated to report each expert's gathered data.

##### 6.2.4.2.1 Expert1

For Expert1, who has considerable knowledge in business as well as IT audit, risk management, and works for a financial company. Experts1 is a Certified Information System Auditor (CISA), ITIL, and Risk Management. In addition, Expert1 has presented about three lines of defense. They are not a strong advocate of recognised IT controls frameworks, although, they have very good knowledge in COBIT 4.1, ITIL and ISO 27001/2 Standard. Expert1 used Gambit software on Windows 10, and produced the following game files, and updated excel spreadsheet containing the risk assessment.

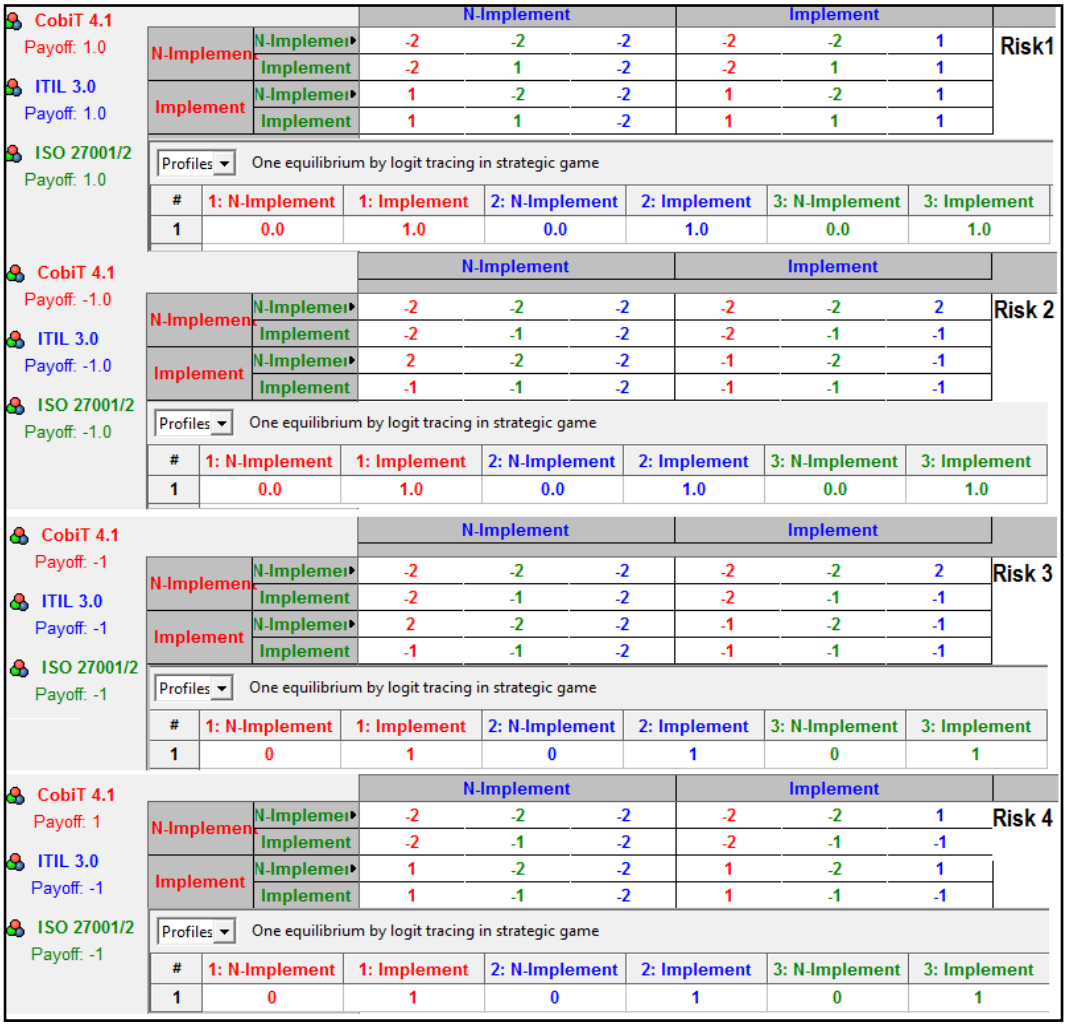


**Figure 6.15: Expert1 Game File Solutions**

As outlined in Figure 6.11 the game file upper half, shows the players, their strategies and payoff values, if populated. Once the NE is calculated, it will appear in the lower half of the display. The four risks-game files displays are shown in one screenshot. Looking at Figure 6.15, it can be seen that Expert1 has a consistent way of applying the payoff values to the various risks and corresponding mitigating measures resulting in similar NE. The implied strategies vector is implementing the corresponding controls and process from the three recognised methods, COBIT, ITIL and ISO 27001/2.

Once the resulting strategies were determined and mitigating measures identified, Expert1 assessed the residual risks post applying the controls and processes as shown in Table 6.15. However, it can be seen that for Risk 2 and 3, the strategy was misinterpreted, as it shows that no control is to be implemented; while looking at Figure 6.15 it denotes implementing them all.

**Table 6.15: Expert1 Residual Risk Assessment**

| | Risk Rating | | | Applied Controls | | | Residual Risk Rating | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Risk No.** | **Impact** | **Likelihood** | **Overall** | **COBIT** | **ISO 27001** | **ITIL** | **Impact** | **Likelihood** | **Overall** | **Comment** |
| R1 | Major | Moderate | High | Y | Y | Y | Major | Unlikely | Significant | "All 3 frameworks are partially adequate. " |
| | Major | Moderate | High | | | | | | | |
| | Major | Moderate | High | | | | | | | |
| R2 | Extreme | Unlikely | High | Y | Y | Y | GAMBIT suggests not implementing (all -1), so no change in ratings. I would recommend implementing the COBIT controls | | | "All 3 frameworks are okay on their own, but use of more than 1 is expensive" |
| | Extreme | Unlikely | High | | | | | | | |
| R3 | Major | Likely | High | Y | Y | Y | GAMBIT suggests not implementing (all -1), so no change in ratings. I would recommend implementing the COBIT controls | | | "All 3 frameworks are okay on their own, but use of more than 1 is expensive" |
| | Major | Moderate | High | | | | | | | |
| R4 | Major | Likely | High | Y | Y | Y | Minor | Moderate | Medium | "COBIT and ITIL give partial mitigation. ISO is good but expensive" |
| | Major | Likely | High | | | | | | | |

Expert1 responded to the questions in the fashion as outlined in Table 6.16.

**Table 6.16: Expert1 Feedback**

| No. | Description | Expert's Answer |
|---|---|---|
| **1** | **The DSS overall evaluation:** | |
| 1.1 | Overall, how effective the proposed DSS (the spreadsheet with risk space, pay-offs matrix and G-Model) in managing the defined risks? | "It is not really viable in its current form for the reasons listed below." |
| 1.2 | Are the defined risks relevant to IT Access Management? | "Yes" |
| 1.3 | Are the provided risk space categorisations (Strategic, Project, and Operational) adequate and helpful to determine relevant mitigating measures? | "Not really." |
| 1.4 | Is the provided strategies' payoff guidance realistic and adequate? | "The instructions need to be simplified before they can be considered for wider use. " |
| 1.5 | How easy it was to use the DSS, and switching between the spreadsheet and the G-Model? And working out the residual risks? | "Not very easy or intuitive" |
| 1.6 | How long it took you to go through each risk, from start to finish? Was that reasonable? Has that improved from R1 to R4? | "It took me about 2 hours in total once I understood the process." |
| 1.7 | What area of improvement - you can think of? Please list as many as possible - from overall DSS perspective. | "1. The whole end-to-end process should be automated<br>2. The input screens need to be simplified<br>3. The user instructions need to be simplified" |
| **2** | **Using (Gambit) G-Model (not the software, but the application of Game Theory based Model):** | |
| 2.1 | Do you think G-Model (game theory based) is effective and efficient in determining the right combinations of controls/processes, in a 3-player-game setting? | "No. I am more confident of my own selection of controls from multiple frameworks" |
| 2.2 | Usability and ease of operation | "As per section 1" |
| 2.3 | Strengths and weaknesses of the model | "As per section 1" |

| No. | Description | Expert's Answer |
|---|---|---|
| 2.4 | Area of improvement | "As per section 1" |
| **3** | **Cost-benefit aspect of the (DSS_G-Model)** | |
| 3.1 | Effort spent on finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the effort)** | "No, for the reason listed in 2.1" |
| 3.2 | Time Taken for finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the time?)** | "No, I had a good idea of the right combinations before I input anything into Gambit" |
| **4** | **Provided Artefacts and how to use Instructions** | |
| 4.1 | Were the provided instructions helpful/clear? | "Not really" |
| 4.2 | How to improve that? (Clarity, Details, Demonstration) | "They need to be structured in a way that avoids the user having to page back and forth between the different sections." |

#### 6.2.4.2.2 Expert2

Next in the list shown in Table 6.14 is Expert2, who is a BCP and IT Operations Manager, qualified with CISA, and Business Continuity Institution (BCI), and has extensive knowledge and work experience in BCP, IT auditing, and IT operations. Expert2 also has experience in applying ITIL best practices. Expert2 conducted the evaluation using Windows 8, followed the provided instructions and provided the files as shown in the following figure and tables, also oral feedback has been obtained from Expert2.

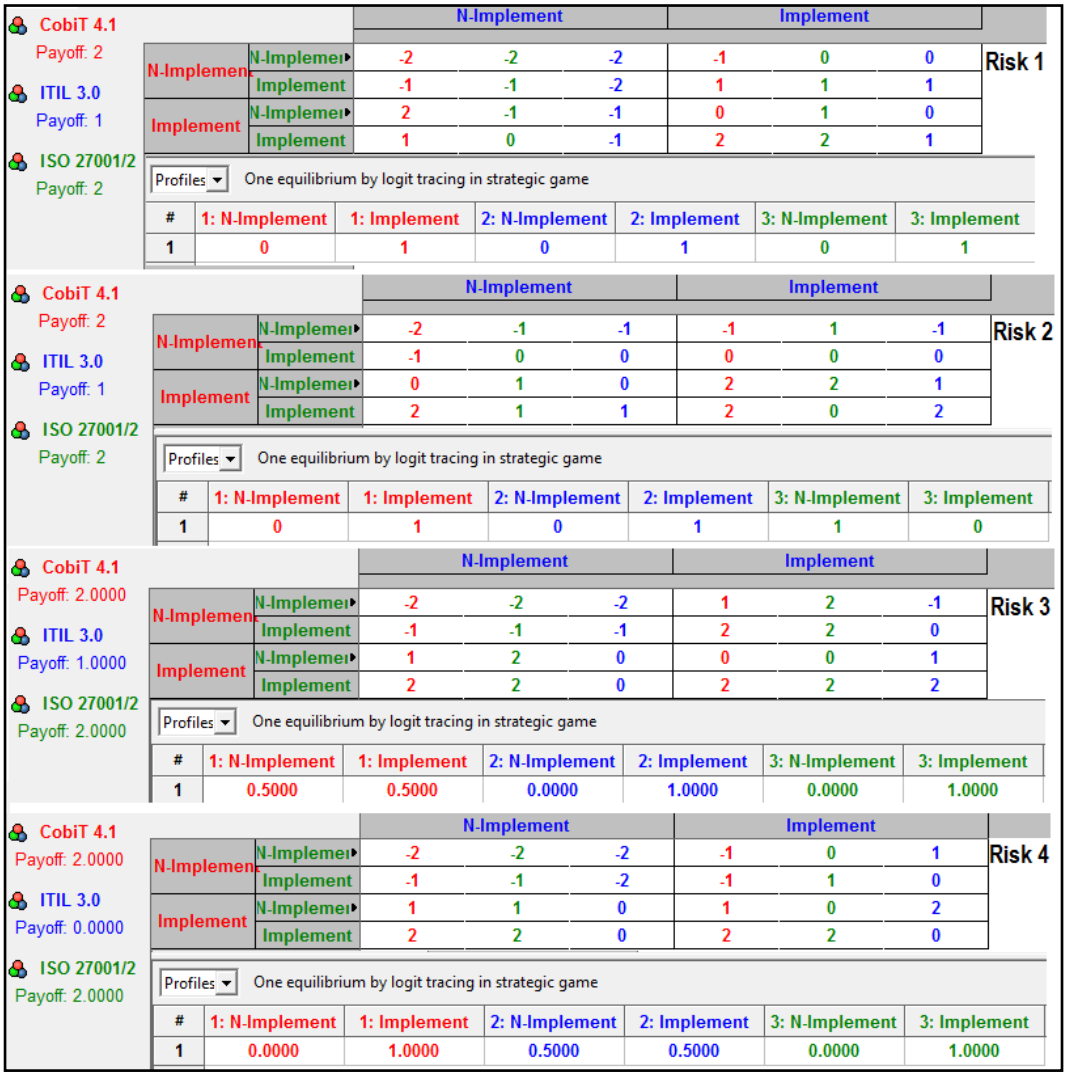


**Figure 6.16: Expert2 Game Files Solution**

Figure 6.16 shows the four game files populated with the payoff values and the calculated strategies. It is interesting to see that Exprt2 assignment of payoff values for the different risks have resulted, accordingly, in different mitigating measures. For example, Risk1 resulting strategy implies implementing all corresponding controls and processes from the three frameworks and that is aligned with the strategy vector with the payoff values of (2,1,2) shown on the left hand side. While for Risk2 the resulting best strategy is to implement COBIT and ITIL controls, but not ISO 27001. The resulting strategy reflects Expert2 view that ISO 27001 controls would overlap with other controls and could incur further cost. As for Risk3 the best strategy according to the payoff values (2, 1, 2) while the best NE strategy is to implement ITIL and ISO controls. As for COBIT it is equally likely for both strategies. This could give the decision maker another chance to rethink

the decision and apply their professional judgment that suits the situation. In similar fashion, the Risk4 game file shows that the NE indicates to implement COBIT and ITIL, but for ISO 27001, it is 50/50 for the two possible strategies. The results of Risk3 and Risk4 demonstrate the possible outcomes that G-Model could produce. It requires further investigation to determine the effectiveness of the strategy and subsequently the benefit that could be gained.

Expert2 applied the G-Model with resulting outcomes and assessed the residual risk as depicted in Table 6.17. In that table, Expert2 applied their view on the defined risks and associated controls and processes, besides the results driven from using G-Model. However, in Table 6.17 it shows Expert2 tendency to implement COBIT and ISO 27001 controls as they would provide the comprehensive mitigating effect on the defined risks. As for ITIL processes, as it can be seen it is confirmed for Risk3, but not for Risk4, while it is possible to implement ITIL process for Risk1 and Risk2, because the return payoff is not as high as the return payoff of COBIT and ISO 27001 as shown in Figure 6.16. With regards to the residual risk assessment for Risk1, Risk2 and Risk3 the overall risk rating was reduced to Medium, Low and Low respectively, which is a positive sign. However, with regards to Risk4 the residual risk is still Significant, but has no indication whether implementing ITIL process would help reduce the risk or not.

**Table 6.17: Expert2 Residual Risk Assessment**

| | Risk Rating | | | Applied Controls | | | Residual Risk Rating | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Risk No.** | **Impact** | **Likelihood** | **Overall** | **COBIT** | **ISO 27001** | **ITIL** | **Impact** | **Likelihood** | **Overall** | **Comment** |
| R1 | Major | Moderate | High | Yes | Yes | maybe | moderate | unlikely | medium | |
| | Major | Moderate | High | | | | | | | |
| | Major | Moderate | High | | | | | | | |
| R2 | Extreme | Unlikely | High | Yes | Yes | 50% | Minor | rare | low | |
| | Extreme | Unlikely | High | | | | | | | |
| R3 | Major | Likely | High | Yes | Yes | Yes | Minor | unlikely | low | |
| | Major | Moderate | High | | | | | | | |
| R4 | Major | Likely | High | Yes | Yes | No | moderate | moderate | significant | |
| | Major | Likely | High | | | | | | | |

Expert2 answers to the set of questions shown in Table 6.18:

**Table 6.18: Expert2 Feedback**

| No. | Description | Expert's Answer |
|---|---|---|
| **1** | **The DSS overall evaluation:** | |
| 1.1 | Overall, how effective the proposed DSS (the spreadsheet with risk space, pay-offs matrix and G-Model) in managing the defined risks? | "Overall very good and clear risk analysis from the spread sheet." |
| 1.2 | Are the defined risks relevant to IT Access Management? | "Yes they are" |
| 1.3 | Are the provided risk space categorisations (Strategic, Project, and Operational) adequate and helpful to determine relevant mitigating measures? | "Yes they are" |
| 1.4 | Is the provided strategies' payoff guidance realistic and adequate? | "Yes they are" |
| 1.5 | How easy it was to use the DSS, and switching between the spreadsheet and the G-Model? And working out the residual risks? | "Not very difficult. Easy actually." |
| 1.6 | How long it took you to go through each risk, from start to finish? Was that reasonable? Has that improved from R1 to R4? | "Around 3 minutes and it gradually went faster from risk 2 onwards." |
| 1.7 | What area of improvement - you can think of? Please list as many as possible - from overall DSS perspective. | "Maybe include some Cloud Risk questions. Better guidelines on the payoff results and considerations to work out the best strategy." |
| **2** | **Using (Gambit) G-Model (not the software, but the application of Game Theory based Model):** | |
| 2.1 | Do you think G-Model (game theory based) is effective and efficient in determining the right combinations of controls/processes, in a 3-player-game setting? | "In my initial exposure to Game theory, I have to say yes. It clarifies the best outcome for all." |
| 2.2 | Usability and ease of operation | "Good" |
| 2.3 | Strengths and weaknesses of the model | "Sorry not too much exposure to other DSS systems and have therefore only listed my |

| No. | Description | Expert's Answer |
|---|---|---|
| | | experience with Gambit. I found it fairly easy to understand and use after some face to face guidance of course." |
| 2.4 | Area of improvement | "None I can think of, maybe just a bit more clarification around the N-Implement and Implement columns next to the rating area." |
| **3** | **Cost-benefit aspect of the (DSS_G-Model)** | |
| 3.1 | Effort spent on finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the effort)** | "Oh, definitely. No need to go through months and months of trial and error with physical implementation attempts." |
| 3.2 | Time Taken for finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the time?)** | "Very quick and also provides for a cheaper alternative in some cases." |
| **4** | **Provided Artefacts and how to use Instructions** | |
| 4.1 | Were the provided instructions helpful/clear? | "Yes, very clear, especially after some face to face guidance." |
| 4.2 | How to improve that? (Clarity, Details, Demonstration) | "None, working well and clear as is." |

#### 6.2.4.2.3 Expert3

With regards to Expert3 an IT Auditor and BCP Manager at one of the largest financial companies in the locality, with CISA and Internal Audit qualifications as well as thorough knowledge and work experience in COBIT, ITIL and ISO 27001/2. Expert3 has over 20 years of work experience in well reputed organisations with extensive knowledge and experience in IT auditing, risk management and IT Governance practices. Expert3 has evaluated the DSS and G-Model in a Windows 7 environment, provided the updated game files, written reply and the oral feedback. In Figure 6.17, Expert3 payoff values for the four risks are depicted alongside with the calculated NE and the payoff vector that entails the dominant strategy.


**Figure 6.17: Expert3 Game Files Solutions**

Expert3 appreciates the necessity of having an overarching framework like COBIT that provides a strategic and governance capability. Hence a high payoff value was assigned to the COBIT controls. In the second order ISO 27001 controls are needed to accommodate the security aspects of AM risks. However, the NE resulted from the four game files; for the respective risks indicated implementing the three recognised frameworks as having the best payback. Expert3 assessed the residual risks after applying the mitigation measures informed from using G-Model, as illustrated in Table 6.19.

**Table 6.19: Expert3 Residual Risk Assessment**

| | Risk Rating | | | Applied Controls | | | Residual Risk Rating | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Risk No.** | **Impact** | **Likelihood** | **Overall** | **COBIT** | **ISO 27001** | **ITIL** | **Impact** | **Likelihood** | **Overall** | **Comment** |
| R1 | Major | Moderate | High | Yes | Yes | Yes | Major | Unlikely | Significant | "Controls should be sufficient. Residual Risk Rating (RRR) is assuming controls are operating effectively" |
| | Major | Moderate | High | | | | | | | |
| | Major | Moderate | High | | | | | | | |
| R2 | Extreme | Unlikely | High | Yes | Yes | Yes | Major | Unlikely | Significant | "Controls should be sufficient. RRR is assuming controls are operating effectively" |
| | Extreme | Unlikely | High | | | | | | | |
| R3 | Major | Likely | High | Yes | Yes | Yes | Major | Unlikely | Significant | "Controls should be sufficient. RRR is assuming controls are operating effectively" |
| | Major | Moderate | High | | | | | | | |
| R4 | Major | Likely | High | Yes | Yes | Yes | Major | Unlikely | Significant | "Controls should be sufficient. RRR is assuming controls are operating effectively" |
| | Major | Likely | High | | | | | | | |

According to the Expert3 risk assessment applying the mitigating measures would reduce the likelihood of the four risks resulting in reducing the overall risk rating into a tolerable level. An assumption note is made by Expert3 that controls are operating effectively, to ensure the assumed risk rating.

Expert3 written feedback is provided and reported accordingly in Table 6.20. Furthermore, oral feedback has been provided, in which Expert3 emphasised the importance of the research objective in mitigating IT risks in a holistic manner by providing an interactive DSS to practitioners.

**Table 6.20: Expert3 Feedback**

| No. | Description | Expert's Answer |
|---|---|---|
| **1** | **The DSS overall evaluation:** | |
| 1.1 | Overall, how effective the proposed DSS (the spreadsheet with risk space, pay-offs matrix and G-Model) in managing the defined risks? | "Useful to consider" |
| 1.2 | Are the defined risks relevant to IT Access Management? | "Yes (although it would be useful to distinguish R3 (external) vs R4 (internal)" |
| 1.3 | Are the provided risk space categorisations (Strategic, Project, and Operational) adequate and helpful to determine relevant mitigating measures? | "It doesn't add much value in this case (access control), as all four risks are Operational (rather than Strategic or Project). ITIL and ISO27k are mostly concerned with operational risk" |
| 1.4 | Is the provided strategies' payoff guidance realistic and adequate? | "Yes" |
| 1.5 | How easy it was to use the DSS, and switching between the spreadsheet and the G-Model? And working out the residual risks? | "Easy" |
| 1.6 | How long it took you to go through each risk, from start to finish? Was that reasonable? Has that improved from R1 to R4? | "On average, about 30 - 40 min each. The biggest time requirement is thinking through the pay-off allocations. Yes it improved from R1 - R4." |
| 1.7 | What area of improvement - you can think of? Please list as many as possible - from overall DSS perspective. | |
| **2** | **Using (Gambit) G-Model (not the software, but the application of Game Theory based Model):** | |

| No. | Description | Expert's Answer |
|---|---|---|
| 2.1 | Do you think G-Model (game theory based) is effective and efficient in determining the right combinations of controls/processes, in a 3-player-game setting? | "Yes it is useful to consider" |
| 2.2 | Usability and ease of operation | "Easy" |
| 2.3 | Strengths and weaknesses of the model | "Strength is systematic consideration of applicability of each framework's controls for the given risk" |
| 2.4 | Area of improvement | |
| **3** | **Cost-benefit aspect of the (DSS_G-Model)** | |
| 3.1 | Effort spent on finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the effort)** | |
| 3.2 | Time Taken for finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the time?)** | "30-40 min for each" |
| **4** | **Provided Artefacts and how to use Instructions** | |
| 4.1 | Were the provided instructions helpful/clear? | "Yes" |
| 4.2 | How to improve that? (Clarity, Details, Demonstration) | "Explanation of Yes/No process can be clearer" |

#### 6.2.4.2.4 Expert4

Expert4 works for one of the Chartered Accounting (CA) firms in an IS advisory consulting division providing clients of various sizes and industries with IT audit, risk management and assurance services. As a senior manager with the CISA qualification, Expert4 has a broad work experience in the relevant domains.

In a similar fashion to the other experts, Expert4 provided game files, the updated spreadsheet containing risks assessment and answers to the provided questions, as well as oral feedback in the second meeting. Figure 6.18 exhibits the game files solutions provided by Expert4.

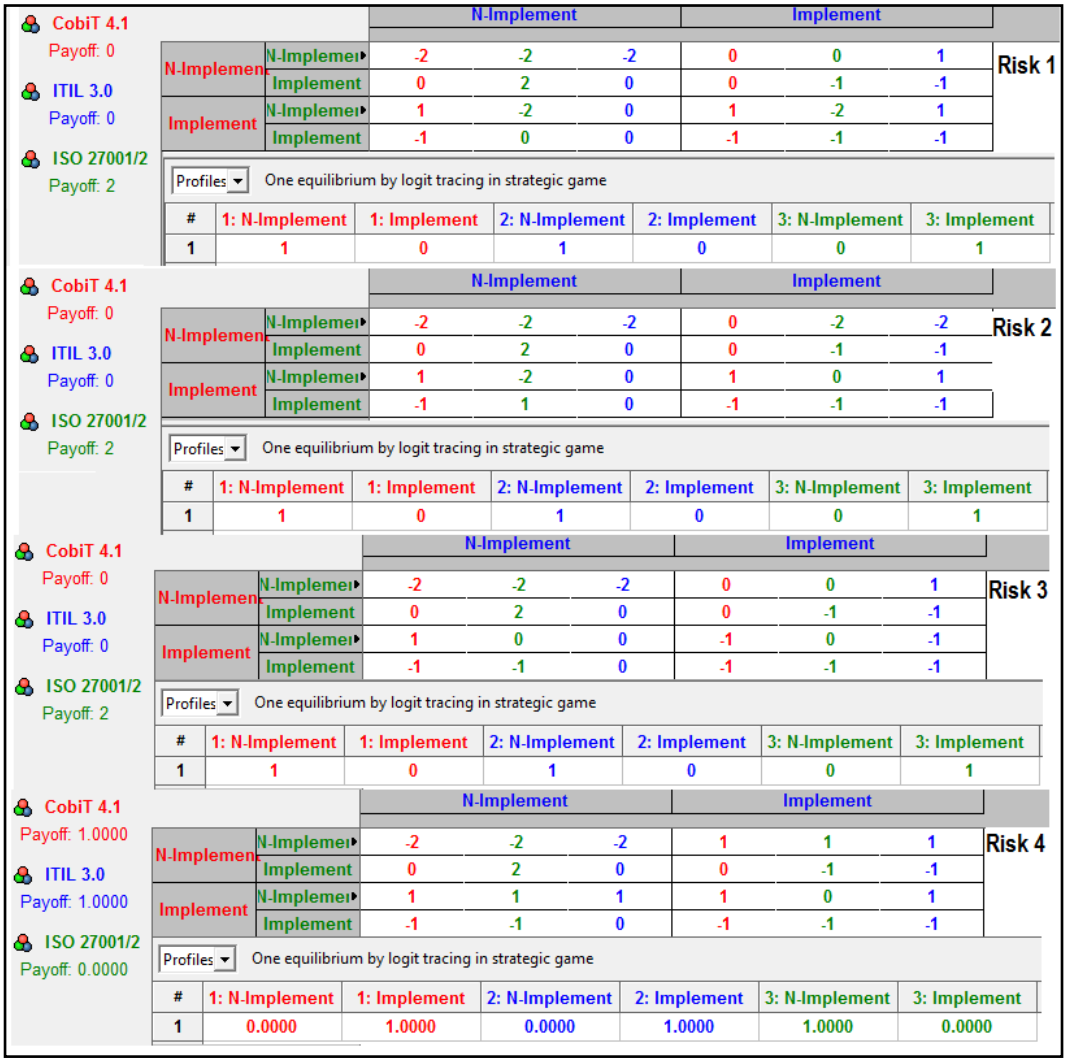


**Figure 6.18: Expert4 Game Files Solutions**

In Expert4 oral feedback it was pointed out that AM risk has high security emphasis, which would be best, mitigated by ISO 27001 controls. As it is evident in Risk1, Risk2 and Risk3 assigned payoff values. Only Risk4 shows that COBIT and ITIL controls would have more gain than ISO 27001 controls. In addition, Expert4 indicated a negative payoff when controls and processes from the entire recognised framework are to be implemented. However, not implementing any of them showed the maximum negative payoff values as well. Moreover, the calculated NE for the four risks indicates that implementing ISO 27001 controls for Risk1,2 and 3, respectively. While for Risk4, COBIT and ITIL mitigating measures are sufficient when it is aligned with the payoff vectors for the respective risks.

In Table 6.20 depicts residual risk assessment by Expert4, which shows that ISO 27001 controls to be implemented to mitigate the four identified risks, reducing the overall risk rating. However, the resulting best strategy for Risk4, as shown in

Figure 6.18, indicates that controls from COBIT and ITIL to be implemented but not ISO 27001 controls based on the payoff values that Expert4 has worked out. This indicates a possible misunderstanding of Expert4 of the provided instructions.

**Table 6.21: Expert4 Residual Risk Assessment**

| | Risk Rating | | | Applied Controls | | | Residual Risk Rating | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Risk No.** | **Impact** | **Likelihood** | **Overall** | **COBIT** | **ISO 27001** | **ITIL** | **Impact** | **Likelihood** | **Overall** | **Comment** |
| R1 | Major | Moderate | High | no | yes | no | moderate | unlikely | medium | |
| | Major | Moderate | High | | | | | | | |
| | Major | Moderate | High | | | | | | | |
| R2 | Extreme | Unlikely | High | no | yes | no | Minor | unlikely | low | |
| | Extreme | Unlikely | High | | | | | | | |
| R3 | Major | Likely | High | no | yes | no | Minor | unlikely | low | Preferred the ISO standard overall. However, I also felt that ITIL is a better standard when compared only to COBIT for this risk |
| | Major | Moderate | High | | | | | | | |
| R4 | Major | Likely | High | no | yes | no | Minor | unlikely | low | |
| | Major | Likely | High | | | | | | | |

Expert4 feedback listed in Table 6.22, shown below.

**Table 6.22: Expert4 Feedback**

| No. | Description | Expert's Answer |
|---|---|---|
| **1** | **The DSS overall evaluation:** | |
| 1.1 | Overall, how effective the proposed DSS (the spreadsheet with risk space, pay-offs matrix and G-Model) in managing the defined risks? | "- Effective but introduced a level of complexity when having to score the frameworks against each other. I found myself with a predisposition towards ISO but that is because I haven't seen the 'underlying detail' for COBIT and ITIL<br>- There was also some overlap between the -2 and 1" |
| 1.2 | Are the defined risks relevant to IT Access Management? | "Yes" |
| 1.3 | Are the provided risk space categorisations (Strategic, Project, and Operational) adequate and helpful to determine relevant mitigating measures? | "I would also suggest introducing a 'Financial' categorisation but this is also driven by my background in external audit" |
| 1.4 | Is the provided strategies' payoff guidance realistic and adequate? | "No - may require distinction between:<br>- The -2 and -1 (difference between partial mitigation and slight mitigation)<br>- How do you score a framework when this is not implemented (is this a 0 or a -2)<br>- Does a 2 mean that you "can't" have aspects of the other frameworks" |
| 1.5 | How easy it was to use the DSS, and switching between the spreadsheet and the G-Model? And working out the residual risks? | "The link between the G model and the residual risks wasn't clear to me but keen to explore that further with [the researcher] as I suspect I haven't understood this well enough" |
| 1.6 | How long it took you to go through each risk, from start to finish? Was that reasonable? Has that improved from R1 to R4? | "15-20 minutes for R1 and then 10 minutes subsequently" |
| 1.7 | What area of improvement - you can think of? Please list as many as possible - from overall DSS perspective. | "Interface of the Gambit application<br>Ability to automate the population of the matrix in Gambit<br>Clarification as to whether the user needs to 'know' ISO, COBIT and ITIL<br>Enhance the point of differentiation between A) risk being addressed vs. B) cost of implementation<br>visualization" |
| **2** | **Using (Gambit) G-Model (not the software, but the application of Game Theory based Model):** | |

| No. | Description | Expert's Answer |
|---|---|---|
| 2.1 | Do you think G-Model (game theory based) is effective and efficient in determining the right combinations of controls/processes, in a 3-player-game setting? | "Yes - The principles are terrific" |
| 2.2 | Usability and ease of operation | "Would be easy to use in a workshop setting" |
| 2.3 | Strengths and weaknesses of the model | "Will not cover areas like:<br>- users having a 'preference' for a certain framework as that is where their experience lies (perhaps a form of bias?)<br>- the level of update/enhancement to models which organisations may want to tap into<br>- the community supporting a framework (e.g. ISO practitioners vs. COBIT practitioners)" |
| 2.4 | Area of improvement | "See above" |
| **3** | **Cost-benefit aspect of the (DSS_G-Model)** | |
| 3.1 | Effort spent on finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the effort)** | "The value would be in "weighing" up the alternatives in a transparent manner." |
| 3.2 | Time Taken for finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the time?)** | "As above." |
| **4** | **Provided Artefacts and how to use Instructions** | |
| 4.1 | Were the provided instructions helpful/clear? | "Yes…but I would have struggled to navigate had [the researcher] not taken the time to walk me through the material" |
| 4.2 | How to improve that? (Clarity, Details, Demonstration) | "Use of alternative tools to focus on the presentation aspect? If the intent is to roll this out in business, the idea (although very credible) may not proliferate in an organisation as it may appear too informal" |

#### 6.2.4.2.5 Expert5

Lastly, in this sub-section a report of Expert5 evaluation of the designed artefacts, the DSS and G-Model. Expert5 is a senior information security consultant, with reputed qualifications of CISM, CISSP, who works for a professional service provider in the public sector. Expert5 has extensive knowledge and many years of work experience in Information security management.

Expert5 tested G-Model on Mac with OSx, and provided the updated game files as well as written and oral feedback.


**Figure 6.19: Expert5 Game Files Solution**

Figure 6.19 displays Expert5 output of the game files. The figure shows Expert5 favouring ISO 27001, which is quite expected as Expert5's is information security manager. As illustrated in Figure 6.19 for Risk1 the payoff vector is (0,0,2), which denotes the strategy of implementing ISO 27001 controls only. However, looking at the calculated NE it denotes implementing ISO 27001 but blocks COBIT controls but it gives equal weights to ITIL processes. The results are based on the payoff values that Expert5 has assigned to the possible strategies. The interesting results are in Risk3, which evidently denote implementing ISO 27001. However, it gives equal weights to COBIT controls possible strategies while it gives ITIL processes 70%, 30%, respectively. As for Risk2 and Risk4 the NE indicates clearly implementing ISO 27001 controls and blocks COBIT and ITIL mitigating measures, although the payoff vector in Risk4 denotes maximum payoff (2,2,2).

**Table 6.23: Expert5 Residual Risk Assessment**

| | Risk Rating | | | Applied Controls | | | Residual Risk Rating | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Risk No.** | **Impact** | **Likelihood** | **Overall** | **COBIT** | **ISO 27001** | **ITIL** | **Impact** | **Likelihood** | **Overall** | **Comment** |
| R1 | Major | Moderate | High | No | Yes | Yes | Minor | Low | Low | |
| | Major | Moderate | High | | | | | | | |
| | Major | Moderate | High | | | | | | | |
| R2 | Extreme | Unlikely | High | No | Yes | No | Minor | Low | Low | |
| | Extreme | Unlikely | High | | | | | | | |
| R3 | Major | Likely | High | Yes | Yes | Yes | Minor | Low | Low | |
| | Major | Moderate | High | | | | | | | |
| R4 | Major | Likely | High | Yes | Yes | Yes | Insignificant | Low | Low | Low |
| | Major | Likely | High | | | | | | | |

Expert5 answers to the provided set of questions and sub-questions are listed in Table 6.24.

**Table 6.24: Expert5 Feedback**

| No. | Description | Expert's Answer |
|---|---|---|
| **1** | **The DSS overall evaluation:** | |
| 1.1 | Overall, how effective the proposed DSS (the spreadsheet with risk space, pay-offs matrix and G-Model) in managing the defined risks? | "I am biased towards iso27 not the other frameworks" |
| 1.2 | Are the defined risks relevant to IT Access Management? | "Very much so, they are the major issues " |
| 1.3 | Are the provided risk space categorisations (Strategic, Project, and Operational) adequate and helpful to determine relevant mitigating measures? | "Yes" |
| 1.4 | Is the provided strategies' payoff guidance realistic and adequate? | "Based on the game yes" |
| 1.5 | How easy it was to use the DSS, and switching between the spreadsheet and the G-Model? And working out the residual risks? | "Difficult at first but finally got the hang of it" |
| 1.6 | How long it took you to go through each risk, from start to finish? Was that reasonable? Has that improved from R1 to R4? | "It was not that easy at first but after some further explanation it became easy" |
| 1.7 | What area of improvement - you can think of? Please list as many as possible - from overall DSS perspective. | "The instructions would do with the example explained step by step" |
| **2** | **Using (Gambit) G-Model (not the software, but the application of Game Theory based Model):** | |
| 2.1 | Do you think G-Model (game theory based) is effective and efficient in determining the right combinations of controls/processes, in a 3-player-game setting? | "Not sure but it gives the overall picture from the three players" |
| 2.2 | Usability and ease of operation | "Once you have the hang of it its easy" |

| No. | Description | Expert's Answer |
|---|---|---|
| 2.3 | Strengths and weaknesses of the model | "First time to use it so cannot comment" |
| 2.4 | Area of improvement | "again first time" |
| **3** | **Cost-benefit aspect of the (DSS_G-Model)** | |
| 3.1 | Effort spent on finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the effort)** | "Biased towards iso [27001/2]" |
| 3.2 | Time Taken for finding the right controls/processes configuration. **(if you use the (DSS_G-Model) does it help in reducing the time?)** | "biased towards iso [27001/2]" |
| **4** | **Provided Artefacts and how to use Instructions** | |
| 4.1 | Were the provided instructions helpful/clear? | "not for the example" |
| 4.2 | How to improve that? (Clarity, Details, Demonstration) | "step by step instructions on how the example was completed" |

### 6.2.5 Critical Reflection on Naturalistic Evaluation

Gathered experts' feedback resulting from the naturalistic evaluation is to be analysed in a similar fashion to what has been done in sub-section 6.2.3. Table 6.25 is populated with answers to questions based on the artefacts evaluation criteria devised by Praft et al. (2014).

**Table 6.25: DSS and G-Model Experts' Naturalistic Evaluation**

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| **Goal** | **Efficacy** | | Q1. How effective is the proposed DSS in managing the defined IT risks. | Experts' answers to Q 1.1 vary from being useful, overall good, to effective but increased complexity, and not viable in its current form. Those views suggest that the DSS is potentially good, but requires some improvement, which is anticipated, as it will be discussed more. |
| | **Validity** | | Q1. How reliable the DSS outcomes are?<br>Q2. Is the risk assessment adequate? | 1. Generally speaking the DSS – knowledge base, identified AM risks, defined controls, risk assessment all good and relevant according to the experts' answers to Q1.1, 1.2, 1.5. However, for the use of G-Model, all indicated that they needed a bit of time to understand and apply the payoff guidance, which is expected, and in fact it would be very surprising to hear that they didn't find it, at the beginning a bit confusing, as it is a new approach to manage IT risks. The researcher exchanged a number of emails with the experts clarifying points around working out the payoff values and how to apply the best strategy, yet, most of them had some misinterpretation and misapplied the results as the instructions specified. While experts suggested some area of improvement, which is anticipated, but no |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | | | major negative remarks were made, which indicates the DSS is reasonably reliable.<br>2. The risk assessment is adequate, as it is commonly utilised methodology this has been noted in the answers to Qs 1.1 and 1.4. However, the provided risk space was not very useful as noted by Expert1 and Expert3 in their answer to Q1.3. Expert2 and Expert5 answered positively, and Expert3, indicated that it did not help, possibly because of the type of defined risks. And possibly if other IT risks with Strategic and Project elements, then the Risk Space Matrix could be of more help. |
| | **Generality** | | Q1. How easy is it to update the included frameworks in the DSS? E.g. replace ITIL 3.0 with ITIL 2011, ISO 27001-2005 with 27001/2013.<br><br>Q2. Is DSS capable of including all ITGC risks?<br><br>Q3. Could the DSS include other frameworks, e.g. ValIT, COSO_ERM? | 1. Through the obtained oral feedback, all experts indicated, throughout the discussion that took place when collecting the data of them, the viability of updating utilised frameworks depends on the changes made to those frameworks. If the change doesn't affect the framework architecture as is the case in ITIL 3.0 to 2011 edition, and ISO27001-2005 to ISO27001-2013, it is reasonably easy, however, changing COBIT 4.1 to COBIT 5, requires considerable effort, as COBIT 5 is architecturally different than COBIT 4.1. However, by utilising knowledge and expertise of experienced |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | | | practitioners, the model could replace the relevant controls and processes. In this way the model can be used by less experienced users.<br><br>2. All experts' feedback showed it would be easy to add more risks into the risk register, and include more corresponding controls and processes.<br>3. While including another framework to the DSS possible controls and processes, however, adding more controls to the G-Model, is viable, but it has been noticed that games with more than 3 players, increases the mathematical complexity of the model. However, given that Gambit framework is being used, it is possible to build more than 3 player games. |
| **Environment** | **Consistency with people** | **Utility** | Q1. What is the total gained value, from practitioner's perspective? | While Exper2 and Exper3 indicated positive implications in their answer to Q1.1 and 3.1, on the other hand, Expert1 stated the need to improve the model; Expert4 pointed out it has good use with some reservation. In addition to the discussion that took place with the experts, that the model (DSS and G-Model) could be a good reference along with risk assessment and provided controls, while there are some improvements to the proposed DSS and G-Model. However, by inference the DSS and G-Model would help practitioners make an informed decision in mitigating IT risks. |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | **Understa nd-ability** | Q1. Is the DSS intuitive? | Expert1 answer to Q1.5 is that the DSS is not very easy or intuitive however, Expert2 said it is not very difficult. Expert3 and 4 indicated that once they managed to understand the procedure and got more clarification from the researcher, then it was easy to use. Similarly, Expert5 pointed out that it was a bit difficult, but once he got help from the researcher it was Ok.<br>Generally speaking answers to Q1.6 and 2.1 and Q2.2, indicate experts' concerns about using the payoff guidance to generate the payoff values for the various strategies. Also applying the best strategy into assessing residual risks.<br>Again that was expected, as calculating the payoff values is about the game rules themselves, which is the most challenging part of the game design. Also as experts did not use such a method before it was anticipated to include a learning curve until the experts became familiar with the model and used it with confidence.<br>This view can be seen in experts' answers to Q3.1 and 3.2.<br>Also it is worth mentioning what Expert4 had indicated in Q2.2, that the DSS and G-Model, would be of more use if it is used in a workshop environment, in other words more than one experts participating in working out |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | | | payoff values and use of G-Model, which describes the real life scenarios when a number of stakeholders collectively assess risks and devise mitigating measures. |
| | | **Ease of use** | Q1. Is the DSS easy to use? | Generally speaking Yes, as noted in the experts' answers to Q1.5 and 2.2. Apart from Expert1 who had a number of reservations on the use of the model in its current form. |
| | | **Ethicality** | Q1. Does using the DSS have or could cause any ethical issue? | No ethical issues have been mentioned by the experts. |
| | | **Side effects** | Q1. Does the DSS or model produce new risks and/or incur further cost? | Expert4 in their Q1.1 answer indicated that the DSS introduced a level of complexity when controls overlap so this could increase cost, but it doesn't introduce new risk.<br>Other experts did not have any concerns about new risks, however, as noted in Q1.6, and 3.1 and 3.2, indication about a possible overlap among the proposed controls resulting from using the G-Model. Which is a valid point, in fact, this point is crucial to the effectiveness of the DSS and G-Model in particular. However, it depends on first, how the risks are defined and the associated controls. While defined risks were adequate as noted by both experts, however, the proposed controls from (COBIT, ITIL and ISO 27001) are at high level, especially in ITIL, that was done by design, to simplify the model and required evaluation. |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | | | Should controls and processes are analysed to a more granular level, then more games would be required for each risks, possibly a multi-level game. This would be a candidate for further improvement. |
| | **Consistency with organisation** | **Utility** | Q1. What is the total gained value, from organisation's perspective? | It was not possible to gage the value from a business point of view, however, given that experts, apart from Expert1, indicated the possible gain in using the model from practitioners' point view, then by inference, organisations would benefit from the model, by managing IT risk in a cost effective fashion. |
| | | **Fit with Organisation** | Q1. Is the DSS (Risk Register, selected frameworks, model) adequately fit the organisation's Internal/External environment? | Experts indicated that defined risks are relevant to IT-AM, as noted in Q1.2, 2.2 and 3.2, with exceptions such as not to provide a Risk Space Matrix, as it was not found useful. |
| | | **Side effects** | Q1. Any issues caused by using this DSS? E.g. incurring further cost, complicating the environment. | No new risk, but the G-Model could potentially incur further cost of implementing overlapping controls and processes. Once again this could be rectified as the model is further refined and payoff guidance and rules are articulated clearly, using G-Model could produce efficient and cost effective strategies. |
| | **Consistency with technology** | **Harnessing of recent technologies** | Q1. How effective and easy it is to accommodate new technology by the DSS? | Potential new risk introduced by new technology could be added to the list of possible risks. No issues noted by any of the experts in that regards. |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | **Side effects** | Q1. Any issues, this DSS could cause? E.g. introducing new risks, overusing/underutilising resources, etc. | No issues or new risks could be caused. |
| **Structure (Static, the artefact's construct)** | **Completeness** | | Q1. How complete the DSS is?<br>Q2. Any area of improvement? | 1. It was admitted by the researcher that the developed artefacts are in a rudimentary stage, and would require further improvement and the risk registers and G-Model to be integrated. That was found acceptable by all experts however, they have made valuable remarks and suggestion on how to improve the DSS components and the evaluation instructions.<br>2. A number of improvements have been proposed by the experts as noted in their answers to Q1.6, 1.7, 2.2, 3.1 and 4.1. |
| | **Simplicity** | | Q1. How simple the DSS is structured? | DSS comprises of risk register and G-Model, although not fully integrated, but it is sufficient for the purpose of evaluation at this stage. |
| | **Clarity** | | Q1. Are the DSS components clear | Yes they are clearly distinguished |
| | **Style** | | N/A- Not to be enquired about. | N/A |
| | **Homomorphism** | **Correspondent with another model** | Q1. Does the DSS map well to other Enterprise settings if any, for example IT Governance, Enterprise Risk Management, Internal Audit, Business/IT Strategic plans? | While developing an interactive DSS is not new, however, utilising game theory based G-Model in managing IT risks, is an innovative method. The used concepts in defining risks, and devising mitigating measures from IT controls frameworks, are common to the practice of the mentioned enterprise settings. |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | | **Fidelity to modelled phenomena** | Q1. Does the designed DSS align with the theorised solution design and meet fidelity criteria exhibiting least deficiency (redundancy, incompleteness, excess, and overload)? | 1. The DSS risk register including defined risks, controls and risk assessment matrix are all professionally developed and used over many years.<br>2. The DSS components each provides its intended outcomes, no redundancy, overload or excess are notice, however, some improvement is required to integrate the risk register with the G-Model |
| | **Level of detail** | | Q1. Does the DSS provide enough details and instructions on use? | Some remarks were made by the experts on the provided instructions and payoff guidance. |
| | **Consistency** | | Q1. Are the DSS components developed in (spreadsheets, MS-word documents, and other applications) consistent? | All DSS components are consistent. |
| **Activity (Dynamic, the operations and functionality of the artefact)** | **Completeness** | | Q1. Does the DSS have the right set of functions? | All DSS components are functioning properly. It needs to be integrated as indicated earlier. |
| | **Consistency** | | Q1. Does the DSS operate consistently? | The DSS, in particular, G-Model operates, consistently with the expected outcomes. |
| | **Accuracy** | | Q1. How accurate the DSS functionalities are? | While the input, data and knowledge base component of the DSS provide adequate risk assessment and suggest relevant controls and processes however, to determine how accurate G-Model is in producing optimum mitigating measures is under investigation. |
| | **Performance** | | Q1. Any issues with performance? | No performance issues have been reported. |

| System dimensions | Evaluation criteria | Sub-criteria | Questions | Feedback/Reply |
|---|---|---|---|---|
| | **Efficiency** | | Q1. How efficient the DSS is in terms the utilised time/resource and the obtained outcomes? | Using the risk register is quite easily done by the experts as noted in Q1.2, 1.5 also in Q3.1 and 3.2 |
| **Evolution** | **Robustness** | | Q1. Does the DSS accommodate changes in internal/external environments? E.g. business dynamics, regulatory requirements, that requires assessing risks on timely fashion. | Experts indicated via oral feedback that this would not be an issue. As previously discussed, the model is capable of accommodating new risks that could be introduced by new technologies or business dynamics. |
| | **Learning capability** | | Q1. Could the DSS – knowledge base – component enhanced with use?<br>Q2. Could practitioners add more knowledge as they use the DSS? | There was a learning curve in particular around working out the payoff values. Using the DSS and G-Model was fairly easy, as noted by all experts. But once they go through the learning once it became quite easy to use. |

## 6.3 G-MODEL GAME FILES – FURTHER ANALYSES

Gambit software provides other functionalities to further analyse a game file, for example, finding out a dominant strategy in a strategic game table. This strict dominance is indicated by the solid "X" drawn across the corresponding strategy labels for both players. In addition, the corresponding payoffs to the dominated strategies are also drawn with a solid "X" across them, as shown in Figure 6.10, in sub-section 6.1.1.3. Strategies that are weakly dominated are similarly indicated, except where the "X" shape is drawn using a dashed line instead of the thick, solid line as shown in Figure 6.20. Clicking the next level icon removes the strictly dominated strategies from the display, and eliminates the dominated strategies until a conclusion is reached.

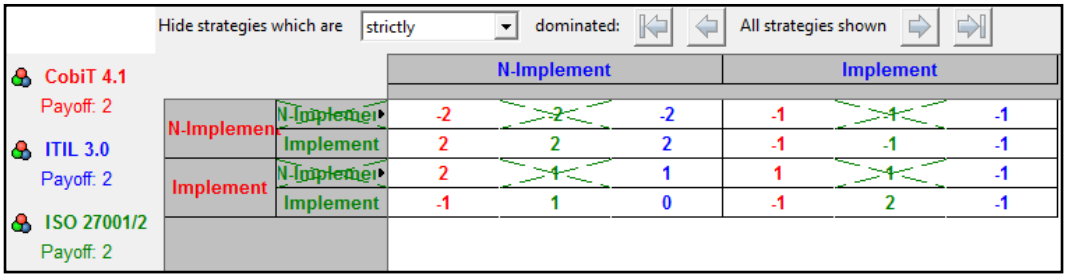


**Figure 6.20: Game File with Weakly Dominated Strategy**

Also in Gambit it is possible to calculate more than one Nash Equilibria a game file could possibly have, by selecting different option, as shown in Figure 6.21.

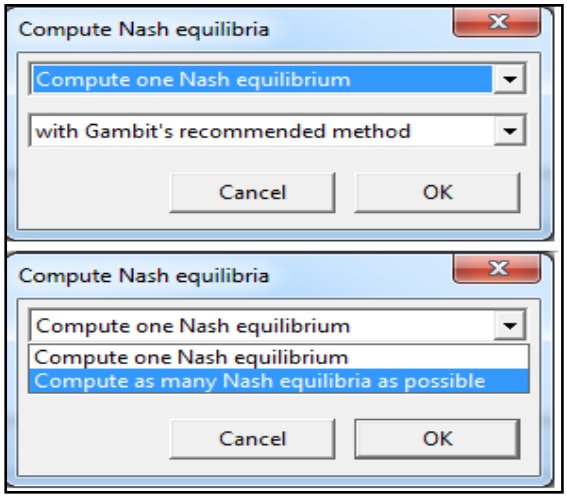


**Figure 6.21: Computing Game File Nash Equilibria**

In this section some of the game files produced by the experts who participated in the naturalistic evaluation are briefly examined to outline the possible scenarios and how the payoff values would cause the variations.

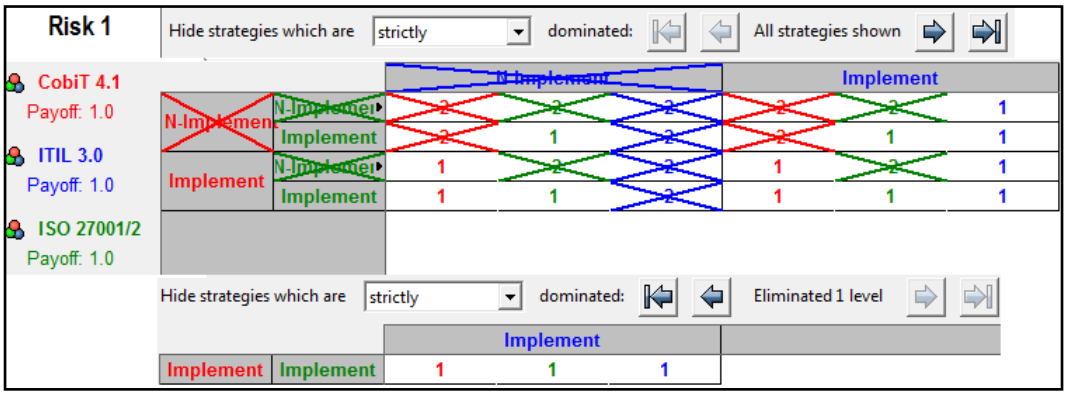


**Figure 6.22: Expert1 Dominating Strategy for Risk1**

In Figure 6.22 Risk1 game analysis by Expert1, it shows the strictly dominating strategy that is implementing controls and processes from COBIT, ITIL and ISO 27001. As illustrated the game file has two levels only, in the upper part of the display the strictly dominated strategies are highlighted. By clicking on the right arrow it displays the second and last level, which shows the dominating strategy after eliminating the dominated ones. As Expert1 game files contained similar payoff values exploring other game files would not demonstrate other scenarios.

Depending on the payoff values some games could have more than one levels of eliminated strategies, as shown in Figure 6.23, which illustrates a weakly dominated strategy that is 'Implementing' the ITIL process in the first level. The setting was set to hide strictly dominated strategies only. By clicking on the right arrow on the top right hand side corner the second part of the display shows the remaining strategies after eliminating the first level. The third part of the figure displays the remaining strategy after eliminating the second level, which shows that implementing ISO 27001 controls would have payoff of 2. It also shows not implementing COBIT and ITIL, would have 0 payoff value. Which is according to the G-Model payoff guidance in Table 6.1, it is a break even case of the cost verses gained value. However, it has been noticed that Expert5's payoff values are somehow not consistent across the four risks of the game; nonetheless, the discussion here is to demonstrate the possible scenarios that could take place.

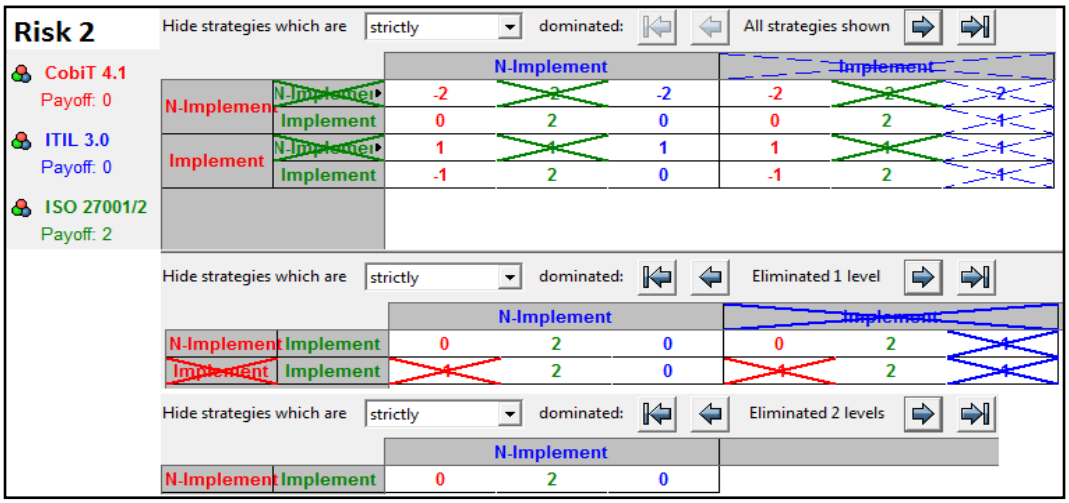


**Figure 6.23: Expert5 Game File for Risk2**

However, by selecting to hide strictly or weakly dominated strategies, as shown in Figure 6.24, it leaves the only strategies displayed in the figure. This could give the practitioner an understanding of the possible options a game could have for the various payoff values assigned to the game strategies.

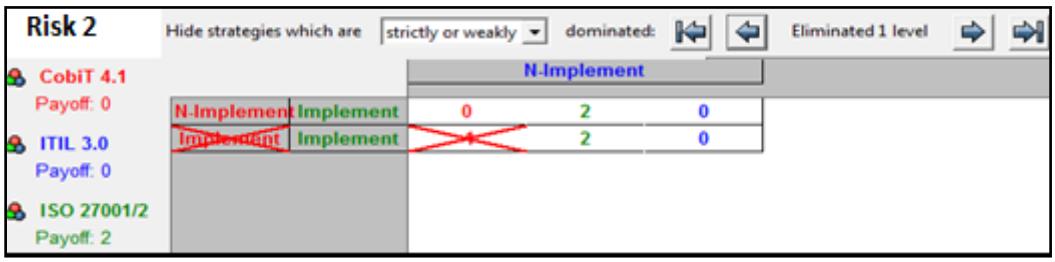


**Figure 6.24: Expert5 Game File for Risk2-2**

On the other hand, the Risk 3 game file resulted in no strictly or weakly dominated strategies as illustrated in Figure 6.25. Interestingly, it shows the best strategy payoff vector with of (-0.7, -1, 1.5).

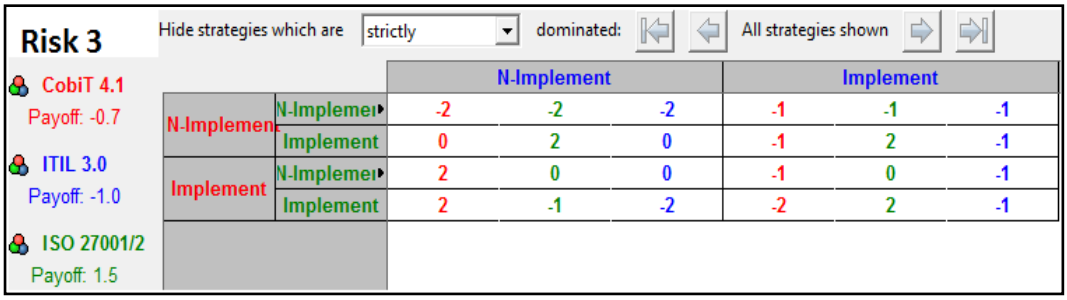


**Figure 6.25: Expert5 Game File Risk3**

In Risk4 of the Expert5 game file, depicted in Figure 6.26, by hiding strictly dominated strategies. It only shows the weakly dominated strategies and the game display is set to that.

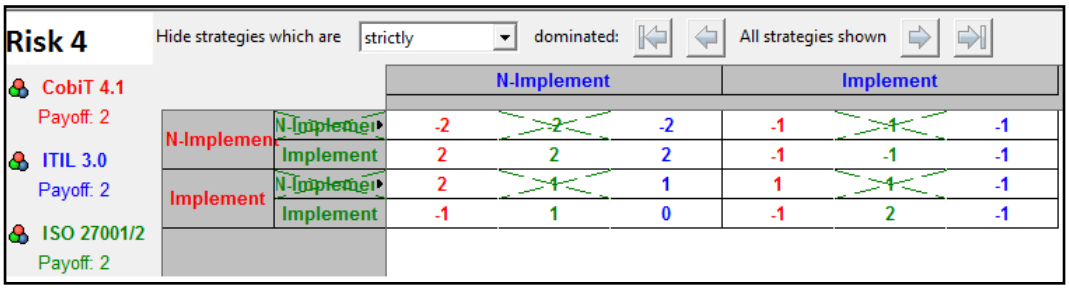


**Figure 6.26: Expert5 Risk4 Hide Strictly Dominated Strategy**

However, by selecting to hide strictly or weakly dominated strategies, it eliminates respective strategies and solves the game file as illustrated in Figure 6.27 in the second and third part of the display.

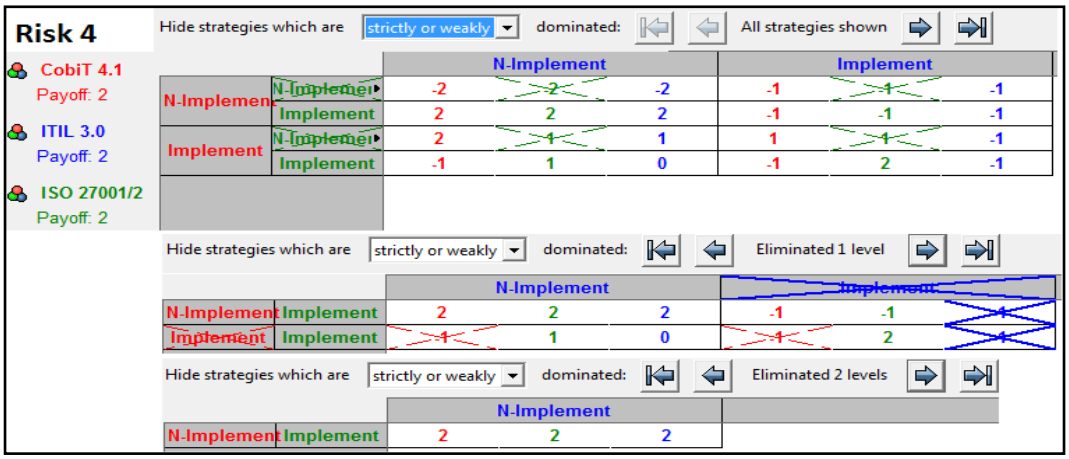


**Figure 6.27: Expert5 Risk4 Hide Strictly or Weakly Strategies**

There are far too many possible scenarios that can be examined, however, the objective of this section was to demonstrate viable analyses and how a practitioner could make use of, and arrive at, a conclusion if the game file was not solved.

## 6.4 DS RESEARCH PROGRESS

It has been discussed in section 6.1 that reviewing research activities as per the DSR roadmap, depicted in Figure 4.5, resulted in developing the G-Model as the core of the interactive DSS as the potential design solution. In sections 6.2 and 6.3, artificial and naturalistic artefacts evaluations outcomes are reported respectively.

In this section the activities according to the various DSR roadmap stages are reported. What has been developed, tested, any changes made, and what were the justifications for the amendments. The aim of this section is to evaluate the cause and effects that mainly relate to the DS Design cycle: Evaluation outcomes, Changes to Artefacts. In Chapter 4, it was indicated that the research progress is outlined in Table B-1, which is constructed in Appendix B. The table comprised of the DS three cycles based on the DS guidelines and DSR roadmap tasks and populated with taken action to that stage. The table was updated with changes that have been made in Chapter 5. Susequntly, updates and additions resulted from the conducted activites in Chapter 6 are prefixed with "Chapter 6 (G-Model) Amendments" and appended to the table.

## 6.5 CONCLUSION

In this chapter the interactive DSS components comprising of the risk register and game theory - G-Model were defined and detailed. The G-Model aspects: players, strategies, rules, and payoff guidance have been outlined. Two cycles of experts' evaluation were conducted and reported. Fieldwork preparations and a complete set of files along with documented procedures and steps were provided to guide practitioners on how to use the DSS model. As part of the required preparations to present the DSS model to experts in the field of IT audit, risk management, and security. The aim was to get the experts' evaluation of using the DSS and G-Model model and obtain their feedback. The fieldwork activities were documented and the data and experts' feedback have been analysed and critiqued against the defined DS artefacts evaluation criteria.

Data was coded around the set of question devised to evaluate developed artefacts to ensure that DSR artefacts are systematically evaluated. Furthermore, the research progress was evaluated again against the DSR roadmap noting changes, updates, additions, and challenges for discussion in the next chapter. Chapter 7 will conclude the discussion of the findings and outline the research contribution to the intended audience. It will find answers to the research sub-questions, test the proposed hypotheses and answer the research question.

# Chapter 7

# Research Contribution

## 7.0 INTRODUCTION

The evaluation of the artefacts comprising the C-Model was reported in Chapter 5, and the DSS and G-Model experts' evaluation was reported in Chapter 6. The reported evaluation and gathered feedback were structured around the artefacts evaluation criteria that were specified by Prat et al. (2014) in addition to the associated questions articulated by the researcher. In the literature review an examination was made of potential business value gains from managing IT risk in control-based structured environments. Furthermore, various IT controls frameworks have been examined and the necessity of finding the best set of controls from the myriad sets of IT controls frameworks, best practices and standards, has been established. This chapter presents the analysis of the findings to answer the research question as well as to validate the hypotheses that have been proposed in Chapter 4. Based on the analysis and evaluation of the outcomes, an answer will be formed to the research question that concerns how to select the best controls configurations to manage IT risk for the best value gain to the business.

Chapter 7 is structured in the following way: section 7.1 addresses the research sub-questions, validates the proposed hypotheses, and answers the research question. Section 7.2 discusses the research contribution to academia and business audiences. Section 7.3 includes an update of the research progress according to the DSR roadmap and section 7.4 concludes the chapter.

## 7.1 REVIEW OF RESEARCH QUESTION, SUB-QUESTIONS AND HYPOTHESES

This section examines the designed solution and the collected data from the various stages of the research and the resulting outcomes from the artefacts evaluation. This will lead towards finding answers to the articulated research question.

The answers are formed from analysing experts' feedback when they evaluated the developed artefacts, both instances of the interactive DSS and its model. However, it is imperative to indicate that as the C-Model was only subjected to artificial evaluation as it was deemed inefficient at that stage, and inappropriate to put it forward to experts. Subsequently, the G-Model was developed and evaluated by experts in two stages. Consequently, the answers are analysed and through critical reflection, foundation for the theory is developed. The evidence comes from the resulting outcomes of the G-Model evaluation.

The section is structured as follows: in sub-section 7.1.1 the research sub-questions answers are provided and in sub-section 7.1.2 the research hypotheses are evaluated. In sub-section 7.1.3 the answer to the research question is formed. Lastly, in sub-section 7.1.4 the research limitations are revisited.

### 7.1.1 Research Sub-Questions

In this sub-section the experts' evaluation feedback reported in Chapters 5 and 6, on the developed artefacts is critiqued in light of the sub-questions along with the researcher's observations made throughout the research duration. This section is structured in four sub-sections 7.1.1.1-7.1.1.4 that discuss the findings related to the research four sub-questions.

#### 7.1.1.1 Sub-Question 1

Sub-question 1 is: What is the minimal set of recognised IT controls/process Frameworks, Best Practices and Standards that could be integrated to provide a comprehensive structure of controls configurations?

In the two developed models, C-Model and G-Model, three recognised IT controls and processes methods have been utilised: COBIT 4.1, ITIL v3.0 and

ISO/IEC 27001/2 2005 edition. In Chapter 2, sub-section 2.4.3, a justification for using those frameworks was made. However, some controls and processes from the noted methods overlap, which would incur unnecessary cost should all controls and processes are implemented. Not all IT risks require all the controls and processes from those frameworks as one or two could be sufficient and cost-effective. On the contrary, some other IT risks would require controls and processes from the three selected methods and possibly a residual risk might still require mitigation. The residual risk might require controls from another framework, for example, Val IT, PMI, TOGAF or ISO 27031 for Business Continuity Planning (BCP). The gathered feedback provided by the experts who evaluated G-Model, when they calculated the payoff values as exhibited in Chapter 6, sub-sections 6.2.2.2, Figures: 6.12, 6.13 and sub-section 6.2.4.2 Figures 6.15-6.19; showed that more than one expert was inclined, initially, to favour controls from one framework, as noted in answers to Q1.1 and Q1.2 in Tables 6.11, 6.16, 6.18, 6.20, 6.22 and 6.24. Thence, the selected mitigating measure would be supplemented with controls and processes from the other frameworks, if found necessary. For example, experts initially selected controls from ISO 27001/2 and then supplemented that with controls from COBIT or ITIL. Also from the oral feedback, it was emphasised that it would be better to have one framework to act as an overarching framework, which would have high precedence when selecting controls. For example, COBIT could be supplemented with controls and processes from ISO 27001 or ITIL to add value by mitigating the residual risk.

As it was discussed in Chapter 2, section 2.1, IT risks could have strategic, operational elements or could be associated with projects. In addition, risks could impact various systems at different impact levels depending on the associated business assets or processes. In line with that, in section 2.4 it was shown that controls and processes are designed to mitigate risks at the corresponding levels, strategic, tactical and operational. Some controls and processes are, by design, IT system oriented, while others are more involved in the business processes, depending on the framework that comprises those controls and processes.

In Chapter 6, sub-section 6.1.1, which describes G-Model aspects, and in Table 6.2 that illustrates the Risk Space Matrix: strategic, project and operational; was probably extra information that not always used. Most of experts indicated in their tabulated feedback in Tables 6.11, question 1.3, that they did not make much use of the defined risk matrix. Furthermore, in the naturalistic evaluation cycle answers to the same question noted in sub-section 6.2.4.2, from Experts1, 3 in Tables 6.16 and 6.20 respectively, are aligned to the former answers. However, answers of Experts 2, 4 and 5, in Tables: 6.18, 6.22 and 6.24 respectively, were in favour of using the Risk Space Matrix. In fact, Expert4 indicated adding another category of Financial into the matrix.

In line with the Risk Space Matrix some categories could be defined to align recognised frameworks, best practices and standards; as shown Table 7.1. Table 7.1 shows a number of attributes that a framework could be associated with to a degree of primary or secondary cover, denoted by P and S letters, respectively.

**Table 7.1: Frameworks Categorisation**

| Recognised Frameworks | Frameworks Categories | | | | | |
|---|---|---|---|---|---|---|
| | **Strategic** | **Operational** | **Security** | **Business Oriented** | **IT Oriented** | **BCP** |
| COBIT 4.1 | P | S | S | P | S | S |
| ITIL v3.0 | S | P | S | S | P | S |
| ISO 27001/2 | S | P | P | S | P | S |
| Microsoft Operation Framework (MOF) | S | P | S | S | P | S |
| Val IT | P | S | - | P | S | - |
| COBIT 5 | P | S | S | P | S | S |
| ISO 27031 | S | S | S | S | P | P |
| ISO 31000 | P | S | - | P | - | S |
| COSO_ERM | P | S | - | P | - | S |
| TOGAF | P | S | S | P | P | S |

It has been established that no one framework covers every aspect of IT risk. However, it is not feasible to implement all frameworks, best practices or standards. It was indicated by a number of experts that implementing one overarching

framework supplemented by other frameworks when necessary, would be an effective way to solve this dilemma. This is noted in sub-section 6.2.2.2 and subsequently critiqued in sub-section 6.2.3, Table 6.12, and the other set of expert evaluations in sub-section 6.2.4, and discussed in sub-section 6.2.5, and Table 6.25.The opinion of experts suggests that COBIT 4.1 would typically be that overarching IT framework as it provides a means to convey business objectives in IT strategic planning. Furthermore, COBIT maps well to other frameworks and best practices. For example, given that IT security and operational aspects are vital to the overall IT assurance, then supplementing COBIT with controls and processes from ISO 27001/2 and ITIL would provide a comprehensive coverage to potential IT risks.

In Table 7.1 it is assumed that compliance is part of operational matters and hence 'compliance' is not listed separately. Some experts believed that compliance is part of operational, while some other practitioners think that 'compliance' should be a separate attribute in itself. The researcher is inclined to favour the former experts' view.

In conclusion, there is no fix number to how many frameworks, best practices and standards to integrate. Rather frameworks should be selected if they add value and depending on the organisation's internal and external environment assessment. It is necessary to follow a systemic approach in providing a holistic and comprehensive risk management and security assurance program. It is also imperative to indicate organisations that desire to have a factual assurance status of their IT systems must have adequate capabilities developed and implemented to the right capacity. This assures that an effective IT assurance program is established by facilitating adequate auditing process and undertaking effective and proficient audit reviews, whether they are conducted internally or externally.

#### 7.1.1.2 Sub-Question 2

Sub-question 2 is: What are the criteria for selecting a recognised IT controls Frameworks, Best Practices and Standards?

In line of the feedback that has been obtained from the experts who evaluated the DSS with the G-Model and their answers to the questions as noted in the answer of sub-question 1. The criteria can be summarised in Table 7.2.

**Table 7.2: IT Control Frameworks Selection Criteria**

| No. | Criterion | Description |
|---|---|---|
| 1 | Scope of context | From organisation internal and external enviroments perspectives, what aspects does the framework cover? For example, business rules, compliance and regulatory requirements. |
| 2 | Sepecifications of impact | With regards to the enterprise and IT risk profile, including vulnerabilities and threats landscape. How effective does the framework mitigat the risk impact. |
| 3 | Sepecifications of business value | At a higher level, what is the associated business value of the IT control framework. For example, strategic business-IT alignment, compliance. |

Selection of frameworks, best practices and standards will be measured against those criteria. In addition, a mechanism is required to ensure a systemic way of selecting the farmeworks and to ensure the objectivity of the selected frameworks. The mechanism can be identified as follows; to start with, the defined categories in Table 7.1 can be utilised to determine how the framework fits within that matrix, and in comparison to the other frameworks. Depending on the environment and the available frameworks, identify the potential frameworks that fit for purpose. Utilising Table 7.3, which lists the attributes of an overarching framework; identify which framework would provide the overarching framework capabilities.

**Table 7.3: Overarching Framework Attributes**

| No. | Attribute | Description |
|---|---|---|
| 1 | Business and IT alignment | Align business with IT objectives by providing strategic planning and facilitates governance activities, risk management, compliance, and BCP. |
| 2 | Organisation wide controls | Develop organisation wide controls e.g. policies, governance structure and high level processes ensuring, security and associated risks, process performance and asset management. |
| 3 | High level IT functions and processes | At a higher level, define IT system functions and processes. |

| No. | Attribute | Description |
|---|---|---|
| 4 | Alignment with other IT controls framework and best practices | The framework maps and aligns well with other frameworks that cover other aspects in more detail. For example operational, security, IT architecture, and BCP. |

Secondly determine if such a framework has been implemented, then identify if there are any gaps in managing potential IT risks. Considerations should be made to the association degree of (P or S) shown in Table 7.1, of the implemented frameworks. Then it should be clearer if other frameworks are required to supplement the implemented overarching framework. Thirdly, define one or more supplementary frameworks, best practices or standards that meet the attributes listed in Table 7.4.

**Table 7.4: Supplementary Framework Attributes**

| No. | Attribute | Description |
|---|---|---|
| 1 | Complement the overarching framework. | Complement the selected overarching framework, in specific areas, for example: Security, Operational, BCP, and Enterprise Architect. |
| 2 | Alignment with other IT controls framework and best practices | Aligns well with other frameworks, and uses, to some extent, common terminologies adopted by other frameworks. |
| 3 | Define IT functions and processes at a detailed level | Define IT system functions and processes at a detailed level. Indicate the 'how' of the 'what' is required to be done. Specify this in the overarching framework. |
| 4 | Risk based, ensuring business value | Framework is structured to ensure business value is achieved via managing associated risks. |

Frameworks should be assessed based on their merits in achieving defined objectives, ensuring business value and managing defined risks. In addition, consideration should be made if there are any regulatory requirements that warrant implementation, for example, the Privacy Act (1993) or other industrial standards like Payment Card Industry (PCI).

#### 7.1.1.3 Sub-Question 3

Sub-question 3, is about: How is the business value assessed in managing IT risk in a control-based structured environment that is established through implementing recognised frameworks?

In Chapter 2, sub-section 2.4.4 it was demonstrated that evaluating the business value of recognised frameworks is a challenging undertaking. However, the answer here is not to provide a mathematical formula for calculating the business value. Rather, the attempt is to indicate the possible tangible and intangible forms where business value could be obtained. Supporting evidence is in Chapter 6, sub-sections 6.2.2.2 and 6.2.4.2, as noted in the answers to questions Q1.1, 2.1, 2.3, 3.1 and 3.2 in Tables 6.11, 6.16, 6.18, 6.20, 6.22 and 6.24. However, Expert1 provided feedback after evaluating the DSS and the G-Model to the contrary of the previously stated answers by the other experts. In general, it was noted that implementing recognised frameworks, while it comes at a cost it provides assurance that IT risks are managed holistically. Business and IT objectives are aligned, and strategic planning is undertaken, ensuring adequate IT capabilities are developed with the right capacity and Capability Maturity Model Integration (CMMI) level. A crucial aspect of implementing a recognised framework is providing an authentic sense of assurance by managing security in a risk based approach. Structuring a control based environment based on recognised methods provides a means to facilitate internal and external auditing. Which provide businesses with the necessary assurance of their IT systems performance, readiness, resilience and reliability.

#### 7.1.1.4 Sub-Question 4

The last sub-question is: Once an IT controls configuration is selected, it is imperative to validate the controls configuration? What are the validation criteria?

Experts who evaluated the DSS, which included a risk register, used the G-Model to determine the best control configurations to mitigate the defined IT risks related to Access Management (AM). Part of the evaluation was to apply the selected mitigating measures, to assess the residual risks, and comment on the effectiveness of the applied mitigating measures. The measures comprised of the controls and processes combination. In Chapter 6, sub-sections 6.2.2.2 and 6.2.4.2, reported the experts' answers to questions Q1.1 and 2.1 around the effectiveness of using the DSS and the G-Model in mitigating the identified risks, which are tabulated in Tables 6.11, 6.16, 6.18, 6.20, 6.22 and 6.24. The experts who indicated

any issues with the applied mitigating measures focused, mainly on cost-effectiveness of the selected controls. Experts'(1-5) risk assessment of the identified IT risks relate to AM, pre and post applying the mitigated measures based on the resulting strategy from using G-Model, are reported in Tables 6.15, 6.17, 6.19, 6.21 and 6.23, respectively. Furthermore, it is imperative to assess if the controls and processes introduced any new risks, or conflicted with the existing controls. Selected and implemented controls and processes should not be business prohibitive, by either incurring further cost or impacting the performance of the associated business processes. Lastly, reviewing and maintaining those controls and processes should be achieved at a reasonable cost in time and effort.

### 7.1.2 Hypotheses Evaluation

In Chapter 4 a set of hypotheses were formulated to assert the researcher's proposed theory developed in the literature review in Chapters 2 and 3. In this section relevant evidence is evaluated from within the collected and analysed data from the obtained experts' written and oral feedback, and the researcher's observations as they were articulated in Chapter 6, Table 6.25. The relevant points will be referenced and cross-examined to determine a verdict for the hypotheses. The relevant points will be presented in text, as demonstrated in Table 7.5. The text will be analysed with a qualitative approach quasi-judicial method, where a rational argument is used to interpret the data in searching for 'for' and 'against' statements that prove or refute the hypothesis in question. The qualitative approach relies on a weighted judgment regarding the force of arguments for and arguments against the hypothesis.

**Table 7.5: Hypotheses Validation**

| **H1:** Establishing a risk-based effective IT-assurance program ensures business-IT value. | |
|---|---|
| **For** | **Against** |
| In the literature review, it was discussed and argued, that business dynamics; technology and regulatory requirement changes require continual risk assessment to ensure the risk profile is current and that it is executed consistently. To ensure quality outcomes and goals are achieved; Research Method | No reference found that refute the stated hypothesis. |

| | |
|---|---|
| process should be executed as part of an assurance program. IT risks are identified, assessed and managed holistically. IT risks are continually evaluated; ensuring adequate overall risks evaluation is done in timely fashion.<br>Experts' written and oral feedback, and the researcher's observations, were critiqued and articulated in Chapter 6, Table 6.25, in the list of artefact evaluations criteria and their corresponding questions:<br>- Environment> Consistency with People > Utility: Q1<br><br>- Environment> Consistency with People > Side effects: Q1<br><br>- Environment> Consistency with Organisation > Fit with Organisation > Utility: Q1<br><br>- Environment> Consistency with Organisation > Side Effect: Q1<br><br>- Environment> Consistency with Technology> Harnessing of recent technologies: Q1<br><br>Corresponding mitigating measures are reviewed accordingly and ensuring their effectiveness and efficiency. An IT assurance program entails, balancing invested effort in managing the adverse effect of IT risks and capitalising on the business opportunities that resemble the positive side of the IT risks.<br>However, implementing an effective assurance program comes at cost and has a number of implementation and maintenance challenges. | |
| **Verdict: Accepted**<br>From the evidence obtained to ensure effective IT risk management process, it should be executed in an assurance program rather than a one-off project. The verdict H1 is supported. | |
| | |
| **H2:** Assessing IT risks holistically results in obtaining factual risk assessment. | |
| **For** | **Against** |
| Experts' written and oral feedback, and the researcher's observations, were critiqued and articulated in Chapter 6, Table 6.25, in the list of | No clear and direct statement that contradicts the notion stipulated in this |

| | |
|---|---|
| artefacts evaluations criteria and their corresponding questions:<br>- Goal>Validity: Q2<br><br>- Environment> Consistency with Organisation > Fit with Orgnisation:Q1<br><br>- Environment> Consistency with Organisation > Side Effect: Q1<br><br>- Environment> Consistency with Technology> Harnessing of recent technologies:Q1<br><br>In the developed DSS – the provided risk register along with risk rating matrix and the construct of G-Model used a sub-set sample of AM risks for the evaluation. The experts with their years of relevant work experience indicated the importance of assessing IT risks holistically to ensure the overall risks assessment is adequate. Some risks effect various business processes and assets to a different degree. Furthermore, when some of the internal or external environment attributes change, it results in the changing of corresponding underpinning assets' value and other vital aspects. | hypothesis that a holistic approach would provide a fair assessment. |
| **Verdict: Accepted**<br>Given the noted positive evidence the H2 hypothesis is supported, and accepted. | |
| | |
| **H3:** Structuring IT controls and processes in a framework ensures business's overall objectives are achieved. | |
| **For** | **Against** |
| Experts' written and oral feedback, and the researcher's observations, were critiqued and articulated in Chapter 6, Table 6.25, in the list of artefacts evaluations criteria and their corresponding questions:<br>- Goal> Efficacy: Q1<br>- Goal> Validity: Q1<br>- Goal> Generality: Q2<br>- Environment> Consistency with Organisation > Utility: Q1<br><br>All experts, apart from Expert1, indicated that establishing, risk based, controls and processes structured environment through implementing a | Only Expert1 indicated that they would use their expertise in finding the best controls that would mitigate defined, risks. However, the Expert1 opinion was not strongly held against this hypothesis.<br><br>Refer to feedback to evaluation criteria:<br>- Goal> Efficacy: Q1<br>- Goal> Validity: Q1 |

| | |
|---|---|
| framework is beneficial. While it comes at cost, it manages IT risks, to ensure business and IT objectives alignment. A framework provides a systematic way of creating required functions and processes, assessing associated risks and placing necessary mitigating measures to ensure desirable outcomes. | - Goal> Generality: Q2<br>- Environment> Consistency with Organisation > Utility: Q1 |
| **Verdict: Accepted**<br>The presented evidence supporting this hypothesis carries more weight than the disapproving evidence, leading to the conclusion that H3 is supported and accepted. | |
| | |
| **H4:** Regularly evaluating IT Controls' effectiveness and efficiency ensures management of IT risks is cost-effective and current. | |
| **For** | **Against** |
| Experts' written and oral feedback, and the researcher's observations, were critiqued and articulated in Chapter 6, Table 6.25, in the list of artefacts evaluations criteria and their corresponding questions:<br>- Goal> Efficacy: Q1<br>- Goal> Validity: Q2<br>- Environment> Consistency with Organisation > Utility:Q1<br>- Environment><br>Consistency with People > Utility: Q1<br><br>Experts indicated that while this is quite desirable by business however, it is not easily done, for various reasons, apart from the cost in time and resources. It includes the complexity of utilised technologies and the increasing reliance of business on IT systems. This requires depth of knowledge in the deployment of technologies, business processes and regulatory requirements. | It was indicated that while it is important to do, it is quite a challenging undertaking by organisations and practitioners.<br><br>Refer to feedback to evaluation criteria:<br><br>- Goal> Efficacy: Q1<br>- Goal> Validity: Q2<br>- Environment> Consistency with Organisation > Utility:Q1<br>- Environment> Consistency with People > Utility: Q1 |
| **Verdict: Accepted**<br>Given the aforementioned evidence, this hypothesis is supported and accepted. | |
| | |
| **H5:** Integrating IT controls and processes from recognised IT controls frameworks in a complementary fashion is a key to establishing an effective IT assurance program | |
| **For** | **Against** |
| Experts' written and oral feedback, and the researcher's observations, were critiqued and | Only Expert1 indicated that they would use their |

| | |
|---|---|
| articulated in Chapter 6, Table 6.25, in the list of artefacts evaluations criteria and their corresponding questions:<br><br>- Goal> Efficacy: Q1<br>- Goal> Validity: Q2<br>- Environment> Consistency with Organisation > Utility:Q1<br>- Environment><br>Consistency with People > Utility: Q1<br><br>All experts, apart from Expert1, indicated that establishing the risk-based and structured environment through implementing recognised frameworks in a complementary fashion was a benefit. While it comes at a cost it manages IT risks and ensures business and IT objectives alignment; among many other benefits an organisation would gain. | expertise in finding the best controls that would mitigate defined, risks. However, Expert1 opinion was not strongly held against this hypothesis.<br><br>Refer to feedback to evaluation criteria:<br><br>- Goal> Efficacy: Q1<br>- Goal> Validity: Q2<br>- Environment> Consistency with Organisation > Utility:Q1<br>- Environment> Consistency with People > Utility: Q1 |
| **Verdict: Accepted**<br>While it is important to integrate the implemented frameworks and best practices it is difficult to achieve. Obtained evidence is not enough to refute, but rather to tentatively accept this hypothesis; hence H5 is supported and accepted. | |

### 7.1.3 The Research Question

In Chapter 4, sub-section 4.1.2, the research question was articulated as follows:

> **What are the criteria for selecting the most effective and efficient controls configurations for the best business value outcomes?**

From the answers of the research sub-questions and evaluating the proposed hypotheses in sections 7.1.1 and 7.1.2, respectively; it is evident that establishing IT control-based structured environments that have integrated frameworks, best practices and standards is resource intensive, costly and face a number of challenges. However, the return outweighs the cost, where the key outcome is an effective IT assurance program. The business would have the ability to holistically view the whole business context and analyse corresponding IT risks, leading in designing or selecting and applying adequate mitigating measures. That enables the organisation to make informed decisions and to avoid undesirable circumstances

with adverse effects or the negative type of risk. Moreover, should the positive side of the risk take place in forms of opportunities, organisations would have the adequate capacity and capability to capture these opportunities and gain the business value. In Chapter 2, Figure 2.6 illustrates the IT role as a value inhibitor verses a value enabler, where the former takes place when IT negative risk is not managed. While the latter, happens when IT resources are utilised and the anticipated business value is obtained. The satisfactory balance enables an organisation to make the best decision to reduce the negative effect and gain desirable business value. Business value comes in various forms, for example: the security of the organisation's assets; a genuine sense of compliance within regulatory requirements; business and IT objectives alignment; and, performance and transparency of information systems.

As some controls and processes overlap, hence frameworks controls and processes are not required to be implemented in their entirety; as this could cause overwork and incur unnecessary cost. Furthermore, overlapping controls could complicate the environment and introduce new risks if they conflict or compromise existing controls or processes. For that purpose it is imperative to define the criteria and the mechanisms of selecting controls from the myriad set of recognised IT controls frameworks, best practices and standards. The key aspect in finding adequate IT controls and processes is to assess the corresponding IT risk(s), which requires a holistic risk assessment that takes into consideration the business context and all the challenges that were explored at length in Chapter 2. Furthermore, selected controls configuration should yield a reasonable utility. The selection criteria are listed in Table 7.6.

**Table 7.6: IT Control Configurations Selection Criteria**

| No. | Criterion | Description |
|---|---|---|
| 1 | Scope of context | From the business-IT risk context, IT risk appitite and tolarence, risk factors and KPI if any. IT environment: outsources, deployed cloud services. |
| 2 | Sepecifications of impact | How effective the controls configuration, collectively, mitigate the defined IT risks. |
| 3 | Specification of utility | What is the gained net utility from implementing the controls configuration, taking into consideration |

| No. | Criterion | Description |
|---|---|---|
| | | the cost of the implementation and ongoing maintenance detucted from the anticipated gained value. |

Selection of controls and processes set will be measured against those criteria. In addition, a defined mechanism help ensure a systemic way of selecting the controls configuration. As noted in the answer of sub-question 1, that no specific minimum number of frameworks is defined. Rather, the frameworks are selected based on their merits to mitigate defined risk, as per the defined categories noted in Table 7.1. Furthermore, the answer to sub-question 2 included frameworks selection criteria defined in Table 7.2. Also, the overarching framework attributes that were defined in Table 7.3. Those frameworks could be supplemented, if found necessary by other frameworks that possess the attributes defined in Table 7.4. Also the use of detailed documents from specialised organisations that map controls and processes from various IT controls frameworks and best practices, for example, the documentation and processes used in testing the DSS and G-Model. Relevant controls and processes to the defined risks could be initially identified as potential mitigating measures. Utilising the Risk Space Matrix (strategic, project, operational), as noted in Chapter 6, Table 6.2; factros of the defined risk can be identified. By using Table 7.1, first select controls from the framework that addresses the risk's primary element. Should the residual risk require further mitigation, then controls from other relevant frameworks could be selected to treat the unmitigated risk to an acceptable level. The remaining risk should be checked against the 'Risk Tolerance' of the organisation.

It is worth indicating that based on the obtained feedback from the DSS and G-Model evaluation regarding the use of Risk Space Matrix. The Risk Space Matrix which is defined in Table 6.2, it is possible to add other categories to this matrix for example, finance, security and compliance.

### 7.1.4 Mitigating Research Limitations

In Chapter 4, section 4.6, a number of limitations have been identified that a DS research application could potentially subjected to, such as reliability, validity and

generalisation. This sub-section explores efforts made throughout the research to mitigate the risks implied by those limitations.

Reliability is the accuracy of the selected research method in measuring or developing a proposed model. It is regarding, if another party attempts to conduct the same research, and weather similar results will be gained or not?

Reliability related concerns were mitigated by, firstly, utilising experts' evaluations in two stages, as noted in Chapters 5 and 6. Secondly, the selected experts, especially in testing the G-Model, were made as noted in specific detail in Chapter 6, Table 6.9, were chosen by who and why they were qualified to evaluate the developed artefacts. The education level, work experience and relevant industry certification each expert had, were critical to their selection. Furthermore, the set of questions that have been designed to collect experts' feedback after using the model, along with the oral feedback that has been obtained from each expert can be benchmarked against the DSR requirements. All played an important role in ensuring the evaluation quality, and the ability to generate similar outcomes should any other researchers attempt to do so by following the documented activities.

With regards to the validity limitation, which is the relationship between what a researcher intends to measure or develop and what it is actually measured or developed. In Chapters 2 and 3, a design solution was proposed that comprises of an interactive DSS with a model in its core. In Chapter 5, C-Model based on cumulative impact probability analysis was detailed, and the experiment was reported. The model was evaluated and artefacts accordingly assessed based on a set of defined criteria and associated questions shown in Table 5.11. As the C-Model was found inefficient to use to resolve the research problem another avenue was explored, where a game theory based G-Model was developed. In Chapter 6 the G-Model was detailed and an artefacts evaluation was conducted in two stages. The G-Model experts' evaluations, Artificial and Naturalistic, outcomes were analysed, critiqued and benchmarked as shown in Tables 6.11 and 6.25, respectively. In addition, the research progress has been documented, and benchmarked in Chapters, 4, 5 and 6, against the Design Science Research (DSR) roadmap that has been developed by Alturki et al. (2011b) which is based on DS

three cycles from Hevner et al. (2004) and a DS set of questions devised by Hevner and Chatterjee (2010), as shown in Appendix B, Table B-1.

Another common limitation in qualitative types of research is the high level of 'subjectivity' in running experiments, testing the design, preparing questionnaires, and in collecting and analysing the collected data. Another source of subjectivity is stemmed from the involvement of the experts who provide their feedback after evaluating the artefacts. However, as it was argued in Chapter 4, that in qualitative research, subjectivity is not a negative aspect, entirely, and it cannot be totally eliminated. Bearing that in mind, the research activities were conducted, embedding some objectivity, aiming at reducing the subjectivity in the research results. In Chapter 3, the research problems were argued and selected based on designed criteria. Furthermore, the research question and sub-questions were argued and justified based on the research focus problem. In Chapter 4, a set of artefacts evaluation criteria and corresponding questions were developed to assess the experts' feedback and assess the artefacts evaluation. In Chapters 5 and 6, experts' feedback was collected as well as oral feedback gathered from each expert and data files were obtained from the experts after using the developed DSS with its model.

The last identified limitation was generalisation that is defined as the external validity, which is the ability to apply the research findings into a wider setting. In a DS research study generalisation is considered an issue as it can be difficult to generalise the findings from the use of an artefact in a single situation and applying them into a wider context. As argued in Chapter 4, section 4.3.4, DS research and artefacts evaluation is paramount in DS based research. Part of the obtained experts' feedback, written and oral questions were formed around the possibility of expanding the model across the wider IT risks, in comparison to the defined IT access management (AM) related risks. Experts' feedback, in particular relating to the use of the G-Model, shown in Tables 6.11 and 6.25, indicated that it is possible to include other IT risks. Likewise, it is possible to add corresponding controls and processes from the selected IT controls frameworks: COBIT 4.1, ITIL v3.0 and ISO/IEC 27001/2 – 2005. Additionally, through the verbal discussion,

experts confirmed the viability of including the updated versions of the noted frameworks, for example ITIL v3.0 to the newer edition known as 2011 edition. Moreover, a new release of ISO/IEC 27001/2-2013, and corresponding controls and processes from the respective best practice and standard could be determined utilising publicly available documents. Figure 7.1 depicts the game files produced using the new releases of each control framework, with the same three players having the new definitions.

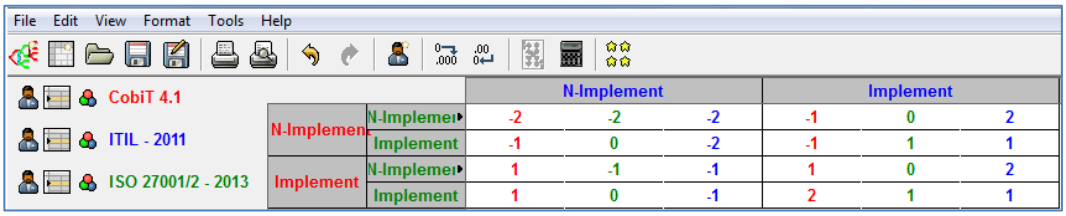


**Figure 7.1: Game File with Updated Frameworks Editions**

Furthermore, experts were asked about the possibility of replacing one framework with another, for example ITIL with Microsoft Operational Framework (MOF). It was agreed that since MOF operates in the same space as ITIL, and as there are documents that map COBIT 4.1, to MOF, then it is possible to re-construct G-Model around COBIT 4.1, MOF v4.0 and ISO 27001/2, as depicted in Figure 7.2.

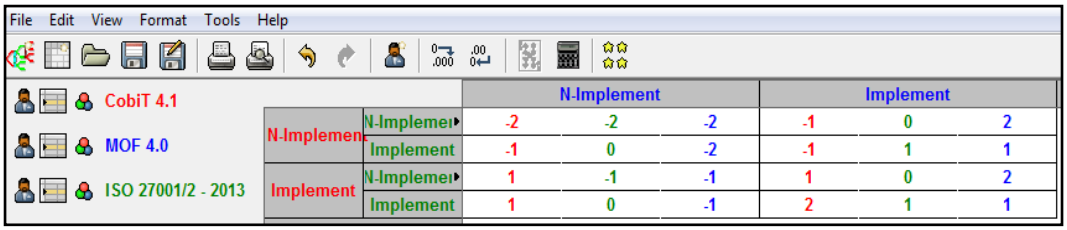


**Figure 7.2: Game File with a Replaced Framework**

The results of DS research conducted in a specific context can be generalised once the DS research is evaluated and its applicability is approved. Then another project could take place to generalise the research outcomes into a wider context. Similar to the examples demonstrated in Figures 7.1 and 7.2, G-Model could be constructed with COBIT 5 framework, as depicted in Figure 7.3.

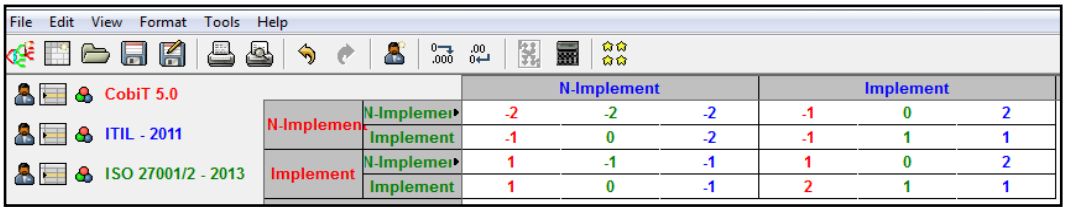


**Figure 7.3: Game File with COBIT 5.0 Framework**

However, it is vital to indicate that replacing COBIT 4.1 with COBIT 5 requires considerable preparation work. Because COBIT 5 is architecturally different from the older release COBIT 4.1. Despite the anticipated required effort to prepare G-Model with COBIT 5, it is still expected to be a workable model, and will still generate business value outcomes. The releasing of new framework editions can be accommodated with these attentions.

The other possible setting is adding another framework to the game file, for example TOGAF, Val IT, ISO 27031 or any other applicable frameworks. In theory, adding another framework or another player to the game model, while it entails a complex mathematical analysis, as it was discussed in Chapter 3, section 3.4.1. However, using Gambit software a 4-player game setting could be developed. Figure 7.4 shows the suggested G-Model with 4 players, however, the figure shows a misalignment of the possible strategies. This could be investigated or explored in another software framework that can build such a game setting.

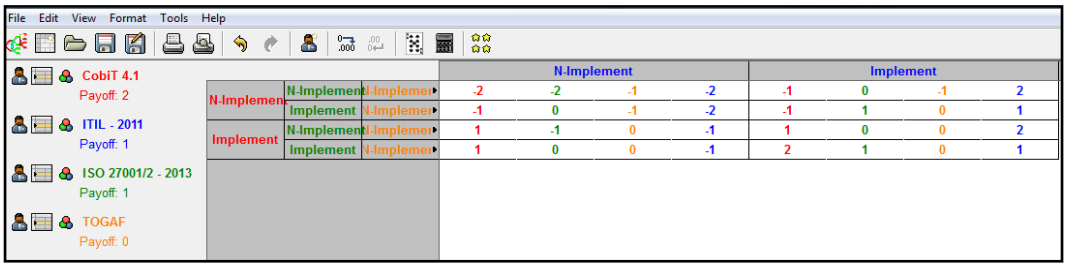


**Figure 7.4: Game File with 4 Frameworks**

In the last two cases, adding a framework that is structuerly different like COBIT 5.0, or adding another framework to the game setting like Val IT, or TOGAF. Experienced practitioners in those frameworks could utilise their expertise and update the knowledge base component of the interactive DSS, so that practitioners who do not possess that knowledge, could use the updated DSS, with ease. Hence

the G-Model based interactive DSS, will be agile pragmatically to the described scenarios.

## 7.2 CONTRIBUTION OF THE RESEARCH

In Chapter 4, sub-section 4.3.3, it was argued that in DSR the produced artefacts are meant to serve an objective and must produce value for the specified problem. The value will be verified when the artefacts are evaluated. Artefacts must be novel and a new knowledge must be added to the domain. The research outcomes must be communicated to an adequate audience of technical as well as business management people. The DS guidelines listed in Table 4.3, guideline no. 7 regarding communicating the research outcomes to technology and management oriented audiences. Also according to the DSR cycles illustrated in Figure 4.2, the third cycle 'Rigor', where the foundations for theory leading to either new or enhanced existing knowledge, is added to the knowledge base. Figure 4.3 shows the DSR process stages, in which 'Communication' is noted as the last stage of the process, where the outcome of the research is communicated through scholarly and professional publications. Furthermore, the DSR roadmap depicted in Figure 4.5, Task 14, is about communicating the research findings, which requires preparation and the outcomes to be articulated before communicating them through the possible means.

In this section, the DSR findings will be articulated to targeted audiences in academia and business. Sub-section 7.2.1 outlines the research contribution to academia, while sub-section 7.2.2 discusses the research contribution to business from practitioners and organisations' perspectives.

### 7.2.1 Contribution to Academia

In this research the DS methodology was adopted following the DS guidelines developed by Hevner et al. (2004), as shown in Table 4.3, and DS process framework model developed by Peffers et al. (2007) as depicted in Figure 4.3. Furthermore, Hevner (2007) has developed the DS cycles, as shown in Figure 4.2, to ensure quality DS research outcomes. The research progress has been

benchmarked against the tasks adopted from the DSR roadmap developed by Alturki et al. (2011b) as illustrated in Figure 4.5. Developed artefacts of the design solution were evaluated against criteria articulated by Prat et al. (2014).

In the literature review, the concept of control capital has been explored, which is about prioritising controls to determine which controls to implement from the COBIT 4.1 framework. The prioritisation is done utilising social network analysis (SNA) based on the controls connectedness degree. The concept has been examined and while it is an ineresting concept, however, it does not consider associated risks or business-IT value of the corresponding assets. Associated risks and business-IT value are crucial to consider when implementing IT controls frameworks. A cube model has been theorised, shown in Figures 2.23 and 2.24, where controls, corresponding risks and cost verses gained value dimensions are formed to aid prioritisng controls and processes to select the most cost-effective controls configuration.

The design solution of this research is an interactive DSS with a model to calculate, or aid in, selecting the best controls configuration. Initially, a cumulative impact analysis based model (C-Model) was designed and evaluated, but it was found inefficient. Following DS methodology, another approach, game theory was explored and the G-Model came to existence, which is a 3-player game theory based setting. The G-Model design, along with the developed payoff values matrix and rules on how to determine a payoff value were developed, tested and subsequently evaluated by a set of experts in the field. While the G-Model and its use in the interactive DSS could be improved in many aspects, it has shown the applicability of a game theory based model to holistically select a best set of IT controls.

As described in the answers of the research's sub-questions and the main question, a set of criteria have been articulated to select an IT controls framework, a main or overarching framework and supplementary frameworks and best practices. Furthermore, a mechanism has been articulated, for selecting controls and processes from various frameworks that would best mitigate identified IT risks and return the best business value outcomes. The defined criteria and selection

mechanism could be used as guidelines to integrate IT controls frameworks, best practices and standards. Table 7.7 lists by description the research contribution to the academia.

**Table 7.7: The Research Contribution to Academia**

| No. | Contribution | Description |
|---|---|---|
| 1. | G-Model | A game theory based 3-player model developed using Gambit software, where COBIT 4.1, ITIL v3.0 and ISO/IEC 27001/2 compete to mitigate identified IT risks. Risk Space Matrix, strategies and payoff values matrix are designed. |
| 2. | Adoption of DSR methodology | Adopted DS guidelines, process framework, 3 cycles, DSR roadmap tasks and DS artefacts evaluation criteria. Checked the research progress on a number of milestones. Tested and evaluated the developed artefacts utilising the DS artefacts evaluation criteria, adequate questions have been devised to ensure gathered data relevance to the DSS and its models. |
| 3. | Recognised IT controls frameworks and best control configuration mechanism and selection criteria | Based on the outcomes of the artefacts evaluation, the criteria for selecting frameworks and a mechanism to form best controls configurations from the recognised frameworks, best practices and standards, are articulated. |
| 4. | Control capital in cube model | Expanded control capital concept and theorised cube model where controls capital is calculated based on the controls attributes and associated IT risks. |

### 7.2.2 Contribution to Business

As noted in the introductory paragraph that DS research outcomes are to be communicated to management through professional publication. For that purpose, this sub-section summarises this research's contributions to the business from organisations' and practitioner's perspectives when using the developed DSS and the game theory based G-Model. Furthermore, the defined criteria for selecting IT control frameworks and controls configurations are disclosed.

From a practitioners' point of view, the G-Model enables practitioners to holistically assess IT risks and their corresponding controls and processes. Subsequently, this facilitates the design and the implementation of the most

effective mitigating measures, in a timely fashion. Implementing, current and best cost-effective mitigating measures, based on a realistic risk assessment, would significantly reduce the audit risk described in Chapter 2, Figure 2.17, and consequently improve the audit performance.

In sub-section 7.1.4, it has been demonstrated that by using G-Model, the utilised frameworks could be replaced by other frameworks, or upgraded when new editions are released, for example ITIL v3.0 to 2011 edition, and ISO 27001/2-2005 edition to 2013 edition. If a framework's new release is structured differently, as is the case in COBIT 4.1 to COBIT 5, a considerable effort is still required to update the DSS knowledge base component. However, by utilising expertise of some knowledgeable practitioners the DSS knowledge base could be updated and G-Model is prepared to be used by other practitioners. The model is still viable and the gained benefits would outweigh the invested resources in updating the DSS. Subsequently, other practitioners, inexperienced or are not trained yet on the newly released IT controls frameworks, can benefit from the updated DSS and G-Model. The indicated benefits which practitioners could gain from using the proposed interactive DSS and G-Model, would lead to structuring an effective, efficient and concrete IT governance structure and assurance program.

With regards to the organisatons' perspective, they would also benefit from the valuable gains that practitioners get from the interactive DSS and the G-Model that have been discussed so far. Ultimately, the return on investment (ROI) of implementing and maintaining an effective IT assurance program will be enhanced considerably. The driving factors are summarised in Figure 7.5, and further detailed overleaf.

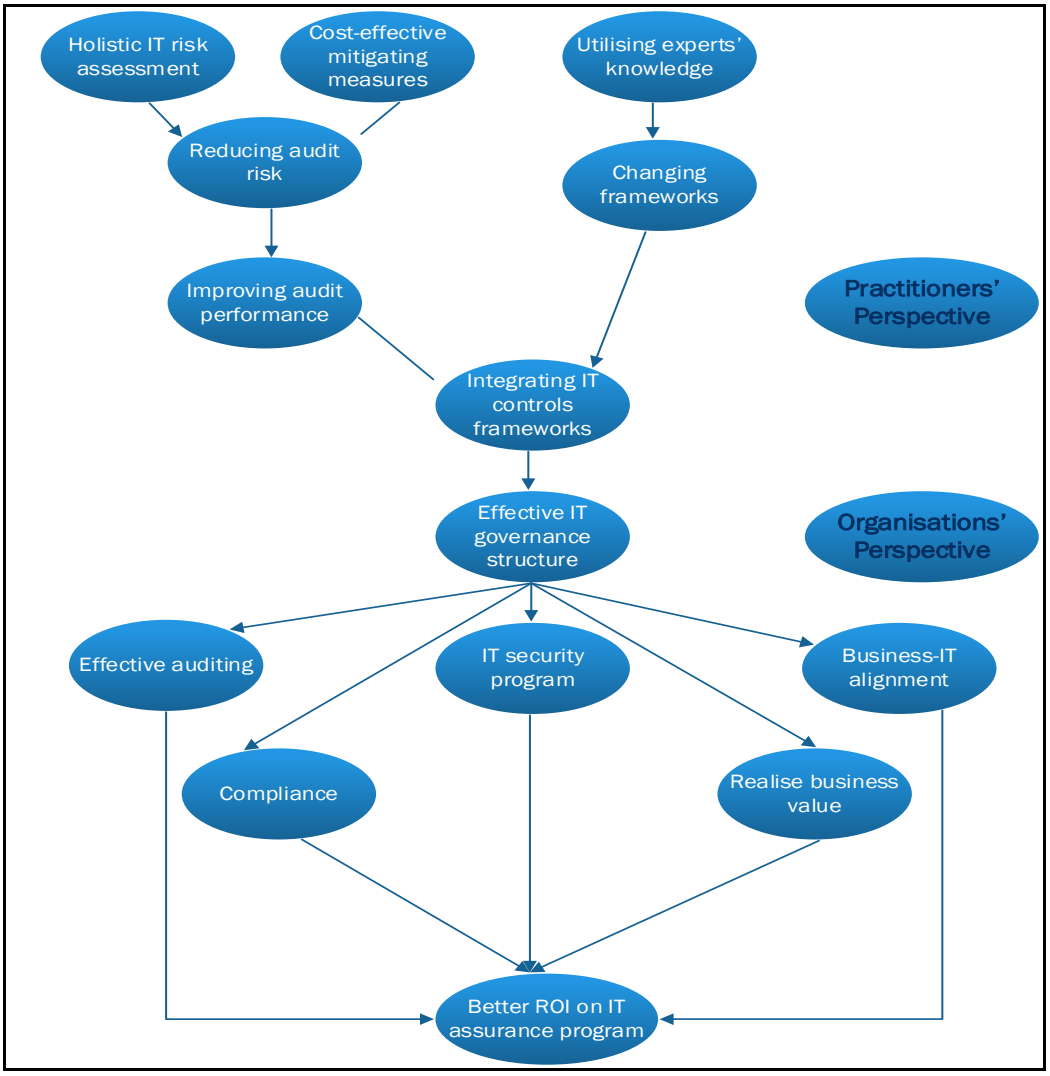


**Figure 7.5: The Research Contribution to Business**

Organisations can have the ability to realise the value of integrating IT control frameworks and ultimately establish an effective IT governance structure. Such a structure entails managing IT risks effectively, business and IT objectives alignment, business value realisation, and an effective and efficient security assurance program. Furthermore, businesses will be able to conduct thorough auditing reviews and ensure compliance with regulatory requirements, proficiently. This ensures IT risks are managed as changes in the internal and the external environments take place, as shown in Chapter 2, Figure 2.20. When necessary, organisations could develop proactively, adequate capabilities to accommodate anticipated changes and assess associated risks and embed mitigating measures in the design solution.

## 7.3 DS RESEARCH PROGRESS

In this section the research progress is checked in a similar fashion. The undertaken activities according to the various DSR roadmap stages thus far are highlighted. In addition, what updates have been further added to the proposed design. Any changes made and what are the justifications for that are reported. The aim of this section is to evaluate the cause and effects that are related to the DS Relevance cycle – verifying if the research question has been answered. Also verifying the DS Rigor cycle and related tasks; and any additions made to the DS Repository, are articualted. In Chapter 4, it was indicated that the research progress is outlined in Table B-1, which is constructed in Appendix B. The table comprised of the DS three cycles based on the DS guidelines and DSR roadmap, illustrated in Figure 4.5, tasks and populated with taken action to that stage. The table is amended with updates and additions resulted from the conducted activites in Chapters 5 and 6. Updates resulted from Chapter 7, are added in similar fashion and are prefixed with "Chapter 7 Amendments".

## 7.4 CONCLUSION

In this chapter the reported findings from Chapters 5 and 6 were examined in relation to the research sub-questions presented in Chapter 4. The outcomes provided ground for evaluating the hypotheses proposed in Chapter 4 as well as answering the research question. Qualitative testing of the hypotheses resulted in validating the proposed hypotheses as enough supporting evidence was obtained. Subsequently, the answer to the research question was formed. Further discussion was conducted to examine the research contribution to both academia and business audiences. When necessary, references were made to the relevant reviewed literature and to the research methodology sections. In addition, a section was set to discuss the research progress according to the DSR roadmap.

The following chapter will conclude the thesis and present recommendations for further research.

# Chapter 8

# Summary and Conclusion

## 8.0 INTRODUCTION

This Chapter is structured as follows: section 8.1 summarises the research activities. Section 8.2 includes the recommendations for further research and section 8.3 concludes the chapter and the thesis.



## 8.1 RESEARCH SUMMARY

This section summarises the research from inception by recapping the relevant literature, identified problems and the selected research problem. Thence, it continues through the chosen research methodology, proposed design solution, and evaluation of the developed artefacts. Then the discussion and reflection on the evaluation's outcomes are presented and lastly the research contributions are outlined. This section is structured as follows: sub-section 8.1.1 reviews the research motivation, literature and identified problems. Sub-section 8.1.2 outlines Design Science (DS) as the selected research methodology and sub-section 8.1.3 contains the developed solutions and the experts' evaluation. Lastly, sub-section 8.1.4 recaps the research contribution.

### 8.1.1 Reviewed Literature

In Chapters 2 and 3 a literature review was carried out using online databases of journals and conferences papers in addition to published books. The search was conducted following a thematic approach where a set of key words (IT audit, IT assurance, IT control frameworks, IT controls, IT risk, risk management, business value, IT value, and IT governance) was used to select the relevant papers. Later

Decision Support Systems (DSS) and Game Theory publications were added to the key word list.

#### 8.1.1.1 IT Risk Management, IT Assurance

The ever increasing reliance of businesses on IT systems and the challenge of the increasing complexity of utilised technologies have made it paramount for organisations to ensure confidence in their IT systems. Risk is inherent in business as well as in IT. For businesses, risk implies value gains as well as liabilities and hence risks require adequate management. Risk drives growth and opportunity, which is the positive side of risk. Risk, however, needs to be analysed, identified and managed to reduce its negative side. To achieve that, a risk based IT assurance program implemented through integrated IT control frameworks, best practices and standards is required. The integration of control frameworks produces an IT controls configuration that leads to establishing effective and efficient risk based IT governance and to obtain the best business value outcome.

To ensure IT risks are managed adequately organisations are required to establish an infrastructure of controls and processes to meet desirable objectives. Controls are subject to change as their corresponding risks and business contexts change. Controls must be tested and evaluated continuously through auditing to ensure their effectiveness, reliability and efficiency. Various audit reviews are performed by staff and third parties on the organisation's IT systems and processes. Controls designed and implemented in an integrated rather than disjointed setting can be more efficient and effective. This is particularly so if the focus is on generating value rather than merely managing the risk. Figure 2.22 depicts a suggested system of intelligently constructed controls, where not all controls are active simultaneously. The IT assurance function provides the business with a reasonable assurance through IT audit reviews conducted by auditors.

Establishing a controls-based structured environment via recognised frameworks, best practices and standards, albeit it comes at cost, but it provides a risk management solution. Implementing recognised IT controls frameworks enables organisational management to fulfill legal and business obligations. When a recognised framework is implemented an element of customisation is required to

ensure the implemented controls are fit for purpose. Given the complexity of IT systems and its interwoven relationship with business, no one framework suffices to establish a comprehensive risk based controls infrastructure. Controls of those frameworks overlap, therefore, it is not viable to implement all the frameworks in their entirety. Hence practitioners need to select relevant controls for their business' context. This necessitates establishing a systemic way of selecting controls and processes from various recognised frameworks, standards and best practices.

#### 8.1.1.2 Research Problems and Motivation

In Chapter 3, seven problems have been identified and assessed. Reflecting on the evaluation of the identified problems, the research focus problem is:

**Selecting the best set of IT controls configurations in any situation for the highest business value outcomes.**

Researching this problem and attempting to find a solution by identifying associated risks and corresponding controls will provide practitioners a means to evaluate controls based on their associated risks and cost-benefit analysis. Organisations and practitioners in IT auditing, risk, security and operation management, will benefit from solving such a problem.

Research publications regarding integrating recognised IT control frameworks and best practices along with and business-IT value are scarce. In addition, such publications are described by researchers as either limited or lacking empirical data. The researcher investigated this problem and this thesis presents findings that contribute to the academic research literature and to address the practical applications of the conceptualised solution. The outcomes of the research can benefit organisations and practitioners in applying guidelines to enable businesses realise the best business value outcome.

#### 8.1.1.3 Theorised Proposed Solution

The concept of control capital has been discussed and expanded to include other factors that would ultimately form a weight for each control to aid practitioners in making a reliable decision when selecting risk mitigating measures. The research

subject domain of managing IT risks for ensuring business value is complex. Practitioners need to monitor, process, and understand and process an enormous amount of data, in order to make an informed decision. That requires having Decision Support Systems (DSS), which is classified as a class of information systems that support organisations and professionals in decision-making. DSS aspects have been explored indicating that an interactive model based DSS would suit the environment of the research. Game Theory aspects and applications have been explored, and a number of definitions have been discussed. Game Theory is the study of strategic behavior, also described as the study of how individuals interact in situations involving moves and countermoves.

### 8.1.2 Research Methodology

Research in an academic context is an activity of a systematic inquiry in an area, with the objective of discovering new or revising existing knowledge. In Chapter 4, the research methodology chosen for the research was examined, and argued that it could potentially provide a solution to the identified problem.

#### 8.1.2.1 Research Question

Based on the selected research problem, a number of corresponding sub-questions were formed. The following main question has been stated:

**What are the criteria for selecting the most effective and efficient controls configurations for the best business value outcomes?**

As some controls and processes could overlap and not all controls are required to mitigate the same risks, this could cause overwork and incur unnecessary cost and complexity. It is imperative to define selection criteria of controls from the myriad of recognised frameworks. Finding a solution or solutions to the stated problem would contribute to solving the other identified problems. Furthermore, a number of hypotheses have been proposed to guide the research and data gathering.

#### 8.1.2.2 Design Science Research Methodology

The selected research methodology is Design Science DS, which is gaining prominence in IS research. DS as a research strategy utilised in developing IT

products, or ‘artefacts’. The key aspect of DS methodology is ‘learning via making’, which is practiced throughout the methodology phases. DS phases are not to be followed in a rigid fashion, but rather in fluid and iterative cycles. The aim is to enhance the artefacts by practicing the DS strategy of learning through making. An advantage of this approach is producing a tentative solution, without having full understanding of the whole system. The case is true for IS researchers who have to study complex and extensive systems.

The DS paradigm is considered in IS research as it is a pragmatic research paradigm. It sponsors the making of innovative artefacts to solve an identified problem. DS has been progressively accepted by IS researchers since 1990s, to improve effectiveness and utility of the developed IT artefacts. Produced artefacts must yield utility (value) for the specified problem, which will be verified through the evaluation stage. The artefacts evaluation criteria based on a system approach are noted in Table 4.6. A set of guidelines depicted in Table 4.3, has been developed to help researchers and reviewers follow a systematic method in conducting a DS based research. The guidelines also help researchers plan, develop and evaluate the resulting artefacts. In sub-section 4.3.3 tables and figures have been formed outlining the DS guidelines and roadmap. Contents of these tables and figures evaluate the DS research as a whole, as well as the artefacts, for which the researcher has adopted and prepared a set of checklist questions.

#### 8.1.2.3 Design Science Methodology Limitations

The selected method for this research has been designed to provide reliably, and a means to collect and analyse data. This leads to answering the outlined questions and finding a solution to the research focus problem. However, the selected DS methodology has its limitations, such as the challenge to prove it is innovative research and it can be difficult to generalise the research outcomes. Furthermore, the research outcomes could be invalidated by rapidly evolving technologies that may render the artefacts inapplicable and/or obsolete. Subsequently, the worth of the conducted research and resulting outcomes could be questionable.

### 8.1.3 Research Design Solution Evaluation

In Chapter 3, section 3.3, it has been emphasised that attempting to resolve problems in complex systems can require a DSS to facilitate finding potential solutions. An interactive DSS equipped with an interface that provides the input-output component, a knowledge base and data components, were detailed in Chapter 4.Table 4.5, also listed, a risk register in a spreadsheet where the defined IT risks could be captured, and assessed. Furthermore, in Table 4.5, corresponding controls and processes from recognised IT controls frameworks can be selected, utilising publicly available documents.

#### 8.1.3.1 C-Model Evaluation

Initially, the DSS was designed with its core C-Model, which is based on cumulative impact probability analysis. The C-Model was developed in Excel to simulate the cumulative impact probability distribution of the defined risks along with the associated controls configurations. An experiment was conducted and documented and results presented to experts to evaluate the model. Oral feedback has been provided by the selected experts about the design solution, which was evaluated against the criteria listed in Table 4.6. Feedback and answers were tabulated and used to populate Table 5.11. Reflecting on the evaluation outcomes and experts' feedback and discussion that was tabulated in Table 5.11; C-Model was deemed inefficient to fit the purpose of this research and then other alternatives were explored.

#### 8.1.3.2 G-Model Evaluation

Evaluating the C-Model and establishing its limitations resulted in exploring game theory applications, and subsequently a game theory based model was developed. The G-Model, is a competitive 3-player game where each player represents one of the recognised IT control frameworks: COBIT, ITIL, ISO 27001. Using Gambit 14.1.0 software application the 3-player model has been constructed. In the G-Model, each player has two strategies: Implement and Not-Implement as depicted in Figure 6.6, which shows examples of payoff values for each player's strategy in the parentheses. To evaluate the developed model, a set of files, a risk register

including a number IT risks relate to Access Management (AM). Risk rating, and a number of relevant controls and processes from COBIT, 4.1, ITIL v3.0 and ISO 27001/2 2005 edition; were all included in a CD for experts' use and evaluation.

The DSS with the G-Model was subject to the two types of evaluation: Artificial and Naturalistic evaluation. For the artificial evaluation, two experts (Exp1 and Exp2) evaluated the artefacts. The aim is not only to get their feedback on the applicability of the DSS and the G-Model, but also on the usability, functionality, effectiveness and efficiency of the developed model. Experts' answers were tabulated, then evaluated and benchmarked against the artefacts evaluation criteria and the corresponding questions. Some changes were made to the model files and a new set of files were produced and packaged in a new set of CDs. For the Naturalistic Evaluation of G-Model another group of experienced experts were approached. The experts were selected based on a number of factors to ensure the quality assessment of the model. Experts' updated game files, risk assessment post implementing the mitigating measures, were gathered. In addition, the experts' replied to the set of questions and oral feedback was obtained. The various data forms were analysed, evaluated and critiqued.

### 8.1.4 Research Contribution

A crucial stage of a DS based research is communicating the findings to the target audience. To articulate that firstly answers to the raised sub-questions were formed and the proposed hypotheses were tested to find support or repudiation evidence. That laid the ground to answer the research main question. Furthermore, the outcomes of the research were critiqued and presented in this thesis for two audiences: academia and business.

#### 8.1.4.1 Answers to the Research Questions

The answers are drawn from analysing experts' feedback when they evaluated the developed artefacts, the interactive DSS and its model. However, it is imperative to point out that as the C-Model was only subjected to the artificial evaluation, because it did not come up to a standard that was good enough for expert exposure. Subsequently, the G-Model was evaluated by experts in two stages; both artificial

and naturalistic. Consequently, the answers are analysed and the theory growth is mainly driven from the resulting outcomes of the G-Model evaluation.

With regards to sub-question 1, there is no fixed number to how many frameworks, best practices and standards to integrate. Rather, frameworks should be selected if they add value depending on the organisation's internal and external environment assessment. For sub-question 2, it was concluded that frameworks should be assessed based on their merit in achieving defined objectives, ensuring business value and managing defined risks. Selection criteria for controls formework are defined as noted in Table 7.2. Also, attributes of overarching and supplementing frameworks were devised, as listed in Tables 7.3 and 7.4, respectively.

For sub-question 3 the answer provided some examples of business value outcomes. For example, implementing recognised frameworks provides assurance that IT risks are managed holistically, Business and IT objectives are aligned, and strategic planning is undertaken, ensuring adequate IT capabilities are developed with the right capacity and capability maturity level. Frameworks also provide a justified sense of assurance by managing security in a risk based approach and facilitating quality internal and external audit reviews. Lastly, sub-question 4, which was about how to validate the controls configurations resulted from using the DSS and its core model. The cost-effectiveness of the applied mitigating measures was the main concern. Also whether applying suggested controls and processes would incur further cost, complexity and introduce new risks. Furthermore, selected and implemented controls should be auditable at a reasonable cost in time and effort.

Hypotheses were evaluated and sufficient evidence was found to support the five hypotheses. The evidence has been used to decide the weight of opinion for or against any given assertion. The obtained evidence and facts led to theory formation that enabled the researcher to answer the research question. In Chapter 4, sub-section 4.1.2, the research question was stated as follows:

**What are the criteria for selecting the most effective and efficient controls configurations for the best business value outcomes?**

From the answers of the research sub-questions and evaluating the proposed hypotheses in sections 7.1.1 and 7.1.2, respectively: It is evident that establishing IT control-based structured environments that has integrated frameworks, best practices and standards is a resource intensive task, costly and faces a number of challenges. However, the return outweighs the cost where the key outcome is an effective IT assurance program. The business would have the ability to holistically view the whole business context and analyse corresponding IT risks, leading in designing or selecting and applying adequate mitigating measures. In Table 7.6 controls configuration criteria have been defined. To ensure the objective controls selection a mechanism has been also outlined.

#### 8.1.4.2 Mitigating Research Limitations

As the findings were presented and critiqued, the research identified limitations were revisited. In Chapter 7, section 7.1.4, states how the limitations were mitigated to ensure their impact is minimal and the resulting outcomes can be reliably utilised by researchers as well as practitioners and ogranisations. The aim is to allow interested researchers to undertake a similar path and to be able to introduce similar findings or further the research and prove or improve the theory.

To ensure the research validity, the research progress has been reviewed and benchmarked against the adopted DS roadmap. Starting in Chapter 4 and through to Chapters 5, 6 and 7, the research progress examination was carried out to ensure desirable objectives have been achieved and any deviations were detected and addressed accordingly. With regards to the‘subjectivity’ limitation, highly experienced experts were sought after. While they shared a common background in IT auditing, security and risk management, however, they worked in different companies from industry and size perspectives. Oral and written feedback was obtained and notes were taken by the researcher, to ensure that the collected evidence was valid and objective as much as practical.

#### 8.1.4.3 Research Contribution

A key aspect in DS based research is the research findings must be communicated to the target audience of academic as well as business management people. In

Chapter 7, section 7.2, the research contribution was articulated into two categories: academia and business. With regards to the academia, the research theorised a solution about control capital. The findings from the use of a cumulative impact distribution utilised in C-Model and the G-Model changes resulting from the experts' evaluation were all articulated and tabulated. The research contribution to business was discussed from organisations and practitioners' perspectives. While there is a profound common ground for the two perspectives, however, it was found necessary to draw the demarcation line as noted in the Figure 7.5. High business value outcomes can be obtained when practitioners are able to execute an adequate IT risk assessment process. An effective IT risk mananemnt process takes into account all impacting factors enabling practitioners design and apply cost effective mitigating measures.

## 8.2 RECOMMENDATIONS FOR FURTHER RESEARCH

The evaluation of the developed artefacts and the reflection on the obtained data resulted in a number of thoughts and suggestions that were formed to further research the subject and to explore other aspects of the developed artefacts.

### 8.2.1 Sub-Games and Game Structure

One of the noted comments made by the experts is that the referenced controls, especially from ITIL, were quite high level controls. For that reason experts were not able to calculate the payoff value easily and to determine whether controls and processes, when selected, were sufficient or required more controls from the other frameworks to be included. In this research high level controls were selected purposefully so that a manageable number of gaming files were created for the experts' evaluation. In order to define controls at a granular level it would have required far more game files than what had been created and this would have complicated the model testing. In game theory it is possible to build games comprised of sub-games. Gambit software has another form of gaming structure called 'Extensive' form that could possibly be used for that purpose as was exhibited in Chapter 6, Figure 6.3.

### 8.2.2 Nash Equilibrium (NE) and CMMI Level

Chapter 6, section 6.3 demonstrated the possible further analysis which can be done using Gambit application. For example, solving the game file by hiding dominated strategies, be they a strictly or weakly dominated strategy, as shown in Figures 6.22-6.27. Also in Figure 6.21, it shows that game files could have more than one NE value. In Figure 8.1 it shows a game file with the resulting strategy and NE value surrounded by RED rectangles. The dominating strategy and NE values are driven from the payoff values allocated to the game's possible strategies.

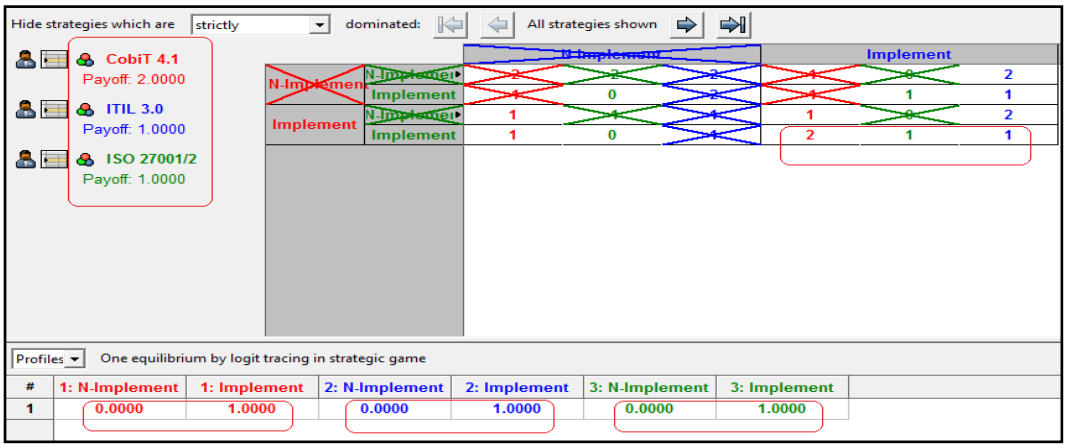


**Figure 8.1: Game File Analysis**

In Figure 8.1 it shows that NE is to implement controls and processes from the three players, COBIT, ITIL and ISO 27001. Also it shows that the payoff values vector (2, 1, 1) that entail the dominating strategy, which means implementing COBIT controls would return the highest payoff value: 2. If the correlation between the NE and the dominating strategy alongside with the payoff values is investigated. Then a possible form of fuzzy setting could be structured to denote the CMMI level of the selected controls and processes. This would add a crucial feature to the proposed G-Model by devising the best set of controls and advise the CMMI level to implement the mitigating measures. That would further enhance the outcomes quality of the G-Model.

### 8.2.3 Utilise Control Capital to Calculate Payoff Values

Experts who evaluated the DSS and its G-Model indicated that the most challenging part was calculating the payoff values. While guidance was provided and further

clarifications were made when experts enquired about possible scenarios. However, the problem was expected, as calculating the payoff values is a complicated exercise. It requires anticipating the cost of implementing the controls and processes from the three frameworks and whether the identified risk is mitigated by one or more controls. In Chapter 2, sub-section 2.4.1, the concept of control capital was introduced. The concept was expanded by the researcher to include other factors, for example, is the control strategic or operational? across an organisation? or for specific applications or systems? detective? preventive? or corrective? Furthermore, in sub-section 2.4.1, Figures 2.23 and 2.24, where controls and associated risks are identified to determine the controls and risks in a many-to-many relationship. Organisations develop a risk register to capture possible risks, along with their assessment with other information and existing corresponding existing controls and processes. The cube model concept could be developed alongside or incorporated in the existing risk register to provide more information that would enable practitioners calculate the payoff values. This would not only ease the use of the G-Model, but also provide actual payoff values that would improve the output quality.

### 8.2.4 G-Model Cooperative Game

G-Model was based on a competitive type game setting. In Chapter 3, section 3.4.1 regarding game theory, the term cooperative game was examined. Cooperative game refers to a type of game setting when the involved players collaborate rather than compete. In IT controls frameworks and best practice, it is often mentioned that COBIT and ITIL do not antagonise but rather complement each other as COBIT indicates 'what' to implement, while ITIL states 'how'. It has been discussed in depth that while both COBIT and ITIL address IT security, but not at the extent to which the ISO 27001 standard does. Reflecting on that perspective and onto the designed G-Model, controls and processes from COBIT, ITIL and ISO 27001 could be formed in a cooperative game setting. It was not possible to attempt that in Gambit software as it is implemented for competitive games only. This would be a

very interesting aspect to investigate for further research and compare the outcomes with the G-Model evaluation results.

## 8.3 CONCLUSION

This Chapter 8 has concluded the thesis by summarising the thesis from inception to conclusion. A number of researchable problems have been identified, focusing on selecting best IT controls that return best business value, as the focus problem. The research area is a complex domain hence the DS research methodology was adopted. Two DS development cycles were conducted where an interactive DSS tool with its core: C-Model and G-Model were developed, tested and evaluated. Answers to the research sub-questions and proposed hypotheses were validated. Subsequently, the research main question's answer was formed. Evaluation outcomes are analysed and critiqued, and findings are further reflected upon and the research contribution to academia and business were articulated.

A number of recommendations have been made for further research that would provide an opportunity to enhance the DSS tool and its core G-Model. For example, structuring sub-games or multi-layer games; investigating the correlation between the Nash Equilibrium and the corresponding payoff values and the possibility of forming a fuzzy logic system to calculate the CMMI level of the selected controls. Furthermore, in the reviewed literature the concept of control capital and the cube model were introduced. Investigating integrating such models into the DSS tool to aid practitioners calculate the payoff values was also recommended. The proposed further research recommendations would improve the quality of the designed game theory based model and overall DSS performance.

This research has investigated managing IT risks and devising corresponding controls that return the best business value. This is a challenging undertaking but so crucial to every aspects of business in current and future time. The reliance on IT systems will continue to grow in importance and magnitude. IT risk comes along with the enablement the technology brings. When the IT risk is managed adequately, the business value, in its various forms, is gained, which is the core contribution of this research.

# References


Abram, T. (2009). The Hidden Values of IT Risk Management. *ISACA Journal*. 2, 52-56

Abu-Musa, A.A. (2008). Information Technology and its Implications for Internal Auditing: An Empirical Study of Saudi Organisations. *Managerial Auditing Journal*. 23(5), 438-466

Afzali, P., Azmayandeh, E., Nassiri, R., & Shabgahi, G.L. (2010). *Effective Governance through Simultaneous Use of CobiT and ValIT*. Paper presented at International Conference on Education and Management Technology. 46-50.

Aliahmadi, A., Sajadi, S. J., & Jafari-Eskandari, M. (2011). Design a New Intelligence Expert Decision Making Using Game Theory and Fuzzy AHP to Risk Management in Design, Construction, and Operation of Tunnel Projects (Case Studies: Resalat Tunnel). *International Journal Advanced Manuf Technol*. 53. 789-798.

Al-Khazrajy, M. (2012). Business value in Managing IT Risk: a Case Study. An MPhil Thesis. Auckland University of Technology, Auckland, New-Zealand.

Alturki, A., Gable, G. G, & Bandara, W. (2011a). *A Design Science Research Roadmap*. Paper presented at the DESRIST, Milwaukee, USA.

Alturki, A., Gable, G. G, & Bandara, W. (2011b). Developing an IS-Impact decision tool: a literature based design science roadmap. In V. K., Tuunainen (Ed.). *Proceedings of the 19th European Conference on Information Systems – ICT and Sustainable Service Development*. (pp. 1-9). Helsinki, Finland: Alto University School of Economics.

Alturki, A., Gable, G. G, & Bandara, W. (2013). *BWW Ontology as a Lens on IS Design Theory: Extending the Design Science Research Roadmap.* Paper presented in 8th International Conference on Design Science at the Intersection of Physical and Virtual Design (DESRIST), Helsinki, Finland

Ames, M. (2007a). *Implementation an Information Security Management System in a Large Organisation.* Paper presented at the Oceania CACS Conference, 9-12 September, Auckland, New Zealand.

Ames, M. (2007b). *Risk Management in Context.* Paper presented at the Oceania CACS Conference, 9-12 September, Auckland, New Zealand.

Bagranoff, N., & Henry, L. (2005). Choosing and Using Sarbanes-Oxley Software. *ISACA Journal*. 2, 49-51.

Bailey, C., (2007). *A Guide to Qualitative Field Research.* Thousand Oaks, Calif.: Pine Forge Press.

Barneir, B. (2009). Driving Value From Nonrevenue-generating Activities: Myths and Misunderstandings of Governance and Risk Management. *ISACA Journal*. 2, 37-43.

Barnier, B., & Fischer, U. (2010). Manufacturers Can Get More Return, Less Risk from IT.

Retrieved 5th September, 2010, from Industry-week web site:

http://www.industryweek.com/articles/manufacturers_can_get_more_return_less_risk_from_it_21038.aspx?Page=2&SectionID=2

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). *Thesis Projects.* (2nd Edition). London: Springer-Verlag London Limited.

Bierman, H. S., & Fernandez, L. (1998). *Game Theory with Economic Applications.* USA: Addison-Wesley Publishing Company, Inc.

Bowles, S., & Gintis, H. (2010). Cooperation. In S.N. Durlauf, L.E. Blume. (Eds.), *Game theory* (pp. 66-77). New York: Palgrave Macmillan

Brand, K., & Boonen, H. (2005). *IT Governance based on COBIT 4.0 - A Management Guide*: Van Haren Publishing.

Bryan, E. L. (1966). Philosophy of Research. Paper presented at the *Proceedings of the 18th Western Dry Kiln Association*, Eureka, California. http://hdl.handle.net/1957/5806

Buckby, S., Best, P., & Stewart, J. (2009). The Current State of Information Technology Governance Literature. In A. Cater-Steel (Eds.), *Information*

*Technology Governance and Service Management: Frameworks and Adaptations* (pp. 1-43). New York, NY: IGI Global

Bunge, M. (1984). Philosophical inputs and outputs of technology. In *History and philosophy of technology*. G., Bugliarello & D., Donner (Eds.) Urbana, IL: University of Illinois Press, (pp 263-281).

Cash, J. I., Bailey, A. D., & Whinston, A. B. (1977). A Survey of Techniques for Auditing EDP-Based Accounting Information Systems. *The Accounting Review*, *52*(4), 813–832. Retrieved from http://www.jstor.org/stable/245581

Champlain, J.J. (2003). *Auditing Information Systems.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Chan, Y. E., Huff, S.L., Barclay, D.W., & Copeland, D.G. (1997). Business Strategic Orientation, Information Systems Strategic Orientation, and Strategic Alignment, *Information Systems Research,* 8:2, 125-150

CICA. (1998). *Information Technology Control Guidelines.* Toronto, Ontario: The Canadian Institute of Chartered Accountants.

Collis, J., & Hussey, R. (2009). *Business Research* (3nd ed.): Palgrave Macmillan.

Cox, L.A. (2009). Game Theory and Risk Analysis. *Risk Analysis.* 29(8), 1062-1068

Creswell, J. (2011). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research*. Upper Saddle river, NJ: Pearson.

Curry, A., Flett, P., & Hollingsworth, I. (2006). *Managing Information and Systems: The Business Perspective.* London: Routledge.

Cusack, B. (2010). *ISO/IEC Standardisation Developments for Digital Forensics*. Paper presented at the Digital Forensics International Conference, 6-7 September, Auckland, New Zealand.

Damore, K. (2009). *Getting Serious with HIPAA.* HIPPA Guideline – TechTarget Application Security, Inc.

Datardina, M. (2005). Comparative Analysis of IT Control Frameworks in the Context of SOX. Publication of University of Waterloo Centre for Information Systems Assurance.

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management Information Systems*. 19(4), pp. 9-30.

DeLone, W. H., & McLean, E. R. (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research.* 3(1), pp. 60-95.

Denzin, K., Lincoln, Y. (1998). *Collecting and Interpreting Qualitative Materials.* SAGE Publication Ltd

Doughty, K., O`Driscoll, J. (2002). Information Technology Auditing and Facilitated Control Self-assurance. *ISACA Journal*. 4. 33-38.

Doughty, K. (2003). Implementing Enterprise Security: A Case Study – Part1. *ISACA Journal.* 2. 34-39.

Eilifsen, A., & Willekens, M. (2008). In the Name of Trust. In R. Quick, S. Turley, M. Willekens (Eds.), *Auditing, Trust and Governance* (pp. 1-18). New Yourk, NY: Routledge.

Ellis, T.J., & Levy, Y. (2008). Framework of Problem-Based Research: A Guide for Novice Researchers on the Development of a Research-Worthy Problem. The International Journal of an Emerging Transdiscipline. 11, 17-33.

El-Najdawi, M. K., & Stylianou, A.C. (1993). Expert Support Systems: Integrating AI Technologies. *Communication of ACM.* 36(12), 55-66.

Eriksson, P., Kovalainen, A. (2008). *Qualitative Methods in Business Research.* SAGE Publication Ltd.

Fischer, U. (2008). New Framework for Enterprise Risk Management in IT. *ISACA Journal.* 4. 22-23

Flynn, L. R., & Goldsmith, R. E. (1999). A Short, Reliable Measure of Subjective Knowledge. *Journal of Business Research,* 46(1), 57-66.

Fuhrer, C., Cucchi, A. (2012). Relations between Social Capital and Use of ICT: A Social Network Analysis Approach. *International Journal of Technology and Human Interaction.* 8(2), 15-42.

Gibbons, R. (1992). *A Primer in Game Theory.* London: Harvester Wheatsheaf

Gibbs, G., R. (2002*). Qualitative Data Analysis Exploration with NVivo.* Wiltshire, UK: The Cronwell Press.

Gregor, S. (2006). The Nature of Theory in Information Systems, *MIS Quarterly*, 30:3, 611-642.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.). *Handbook of qualitative research* (pp. 105-117). Thousand Oaks: Sage Publications.

Hadden, L. B., DeZoort, F. T., & Hermanson, D. R. (2003). IT Risk Oversight: The Roles of Audit Committees, Internal Auditors, and External Auditors. *Internal Auditing*. 18(6). 28-30.

Haber, J. (2006). Research questions, hypotheses, and clinical questions. In G. LoBiondo-Wood, J. Haber. (Eds.), *Nursing research: methods and critical appraisal for evidence-based practice* (pp. 27-55). St. Louis, Mo.: Mosby Elsevier.

Haes, S. D., & Van Grembergen, W. V. (2005). *IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group.* Paper presented at the Proceedings of the 38th Hawaii International Conference on System Sciences.

Hall, J. A., & Singleton, H. (2005). *Information Technology Auditing and Assurance.* US: South-Western, Thomson Corporation.

Hardy, C.A., (2011). *Exploring Continuous Assurance In Practice: Preliminary Insights.* Paper presented at Proceedings Pacific Asia Conference on Information Systems (PACIS). AIS Electronic Library (AISeL). Paper 74, 1-15.

Halpern, J. Y. (2008). Computer science and game theory. In S.N. Durlauf, L.E. Blume. (Eds.), *Game theory* (pp. 48-65). New York: Palgrave Macmillan

Havelka, D., Merhout, J. (2007). *Development of an Information Technology Audit Process Quality Framework.* Paper presented at Proceedings Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL).

Heier, H., Borgman, H.P., Maistry, M.G. (2007). *Examining the Relationship between IT Governance and Business Value of IT: Evidence from Four Case*

*Studies.* Paper presented at the proceedings of 40th Annual Hawaii International Conference-System Science, HICSS. pp. 234c

Henczel, S. (2001). *The Information Audit: a Practical Guide.* Munchen: K.G.Saur.

Hevner, A., & Chatterjee, S. (2010). Design Research in Information Systems Theory and Practice. US: Springer.

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 75-105.

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. Scandinavian Journal of Information Systems. 19(2), Article 4

Holsapple, C.W. (2008). DSS architecture and types. In F. Burstein, & C.W. Holsapple, (Eds.), *Handbook on decision support systems 1: Basic themes* (pp. 163-189). Berlin Heidelberg, Germany: Springer.

Hult, M. and Lennung, S. (1978). Towards a definition of action research: a note and bibliography, *Journal of Management Studies*, *17*(2), 241-50.

Hunton, J. E., Bryant, S. M., & Bagranoff, N. A. (2004). *Core Concept of Information Technology Auditing.* US: John Wiley & Sons, Inc.

IT Governance Institute (ITGI). (2007). COBIT 4.1: IT Governance Institute.

IT Governance Institute (ITGI). (2008). *IT Governance Global Status Report,* Report published by ITGI and PriceWaterhouseCoopers, from itgi.org.

ISACA. (2007). *Certified Information Security Manager (CISM) review manual*, ISACA.

ISACA. (2008). Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit. Retrieved 10th October, 2010, from: http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf

ISACA. (2009a). *The Risk IT Framework Practitioner Guide*. ISACA.

ISACA. (2009b). *The Risk IT Framework*. ISACA.

ISACA. (2009c). *Val IT Overview* [power point]. ISACA.

ISACA. (2011). *Certified Information Systems Auditor (CISA) review manual*, ISACA

Jensen, B., Cline, M., & Guynes, C. (2007). HIPPA, Privacy and Organisational Change: a Challenge for management. *ACM SIGACAS Computer and Society.* 37(1), 12-17.

Jiang, H., & Carroll, J.M. (2009). Social Capital, Social Network and Identity Bonds: A Reconceptualisation. ACM, C&T, University Park, Pennsylvania. 51-60.

Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Veen, A., & Verheijen, T. (2009). *ITIL V3 Foundation Exam – The Study Guide*: Van Haren Publishing

King, D. (1993). Intelligent support systems: Art, augmentations, and agents. In R. H. Sprague, Jr., & H. J. Watson. (Eds.), *Decision support systems: Putting theory into practice* (3rd ed., pp. 137-159). Englewood Cliffs, NJ: Prentice-Hall.

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. MIS Quarterly. 23(1), 67-94.

Kouns, J., & Minoli, D. (2007). *Information Technology Risk Management in Enterprise Environment.* Wiley-Interscience

Kvale, S. (1996). *Interviews – An Introduction to Qualitative Research Interviewing.* SAGE Publications Ltd.

Lau, F. (1997). A Review on the use of action research in information systems studies. In A.S. Lee, J. Liebenau, J. I. DeGross, (Eds.), *Information systems and qualitative research* (1st ed., pp. 31-68). London, UK: International Federation for Information Processing (IFIP) - Chapman & Hall.

Lovaas, P., & Streff, K. (2009). *A Comprehensive Information Technology Risk Assessment Audit Framework for Small- and Medium-Sized Financial Institutions.* Paper presented at Proceedings of Midwest Association for Information Systems (MWAIS), AIS Electronic Library (AISeL).

Lee, A. (1999). Inaugural Editor's Comments. *MIS Quarterly.* 23(1), v-xi.

Leitch, M. (2008). *Intelligent Internal Control and Risk Management.* Hampshire, England: Gower Publishing Limited.

Luconi, F. L., Malone, T. W., & Scott Morton, M.S. (1993). Expert systems: The next challenge for managers. In R. H. Sprague, Jr., & H. J. Watson, (Eds.), *Decision support systems: Putting theory into practice* (3rd ed., pp. 365-379). Englewood Cliffs, NJ: Prentice-Hall.

Lutui, P. R. (2015). Digital Forensics Procedures for Mobile Business Devices: Smart Technologies. A PhD Thesis: Auckland University of Technology, Auckland, New-Zealand.

Mantelaers, P., (1997). Acquiring expert knowledge on IS function design. In A.S. Lee, J. Liebenau, J. I. DeGross, (Eds.), *Information systems and qualitative research* (1st ed., pp. 31-68). London, UK: International Federation for Information Processing (IFIP) - Chapman & Hall.

Markus, M.L., (1997). The Qualitative difference in information systems research and practice. In A.S. Lee, J. Liebenau, J. I. DeGross, (Eds.), *Information systems and qualitative research* (1st ed., pp. 11-27). London, UK: International Federation for Information Processing (IFIP) - Chapman & Hall.

Markus, M. L., Majchrzak, A., & Gasser, L. (2002). A Design Theory for Systems that Support Knowledge Processes. *MIS Quarterly.* 26(3), 179-212.

March, S. & Smith, G. (1995). Design and Natural Science Research on Information Technology. *Decision Support Systems*, 15, 251-266.

Marinos, L., Kirchner, L., & Junginger, S. (2009). *Integration of an IT-Risk Management/Risk Assessment Framework with Operational Processes*. Paper presented at Proceedings of Wirtschaftinformationk AIS Electronic Library (AISeL).

Mandarano, L.A. (2009). Social Network Analysis of Social Capital in Collaborative Planning. *Society and Natural Resources. Taylor & Francis Group.* 22, 245-260

Mckay, J., & Marshall, P. (2004). *Deriving Business Value from IT: Converging IT Expenditures into Assets with Desired Impact.* Paper presented at Proceedings European Conference on Information Systems (ECIS) at AIS Electronic Library (AISeL).

Merhout, J.W., Flittner, M. A., & Havelka, D. (2008). *Misalignment of Expectations for Entry-Level IT Auditors.* Paper presented at Proceedings Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). 1-9.

Merhout, J.W., Havelka, D. (2008). Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit. *Communication of the Association for Information Systems (CAIS).* 23(26), 463-482.

Miccolis, J., Brehm, P., Dickson, K., Franklin, B., Kirschner, G., Kollar, J., Mango, D., Morin, F., Nelson, C., & Zubulake, T. (2003). *Overview of Enterprise Risk Management*. ERM Committee -Casualty Actuarial Society Retrieved 18th May, 2016, from: https://www.casact.org/area/erm/overview.pdf

Mishra, S. (2007). *Information Security Governance and Internal Audits: A Processual Model.* Paper presented at Southern AIS (SAIS) Proceedings at AIS Electronic Library (AISeL). 98-103.

Mishra, S., & Dhillon, G. (2008). Defining Internal Control Objectives for Information Systems Security: a Value Focused Assessment. Paper presented at the Proceedings of ECIS at AIS Electronic Library (AISeL).

Moeller, R.R. (2011). *COSO Enterprise Risk Management.* N.J: John Willey & Sons, Inc.

Moeller, R.R. (2008). *Sarbanes-Oxley internal Controls, Effective Auditing with AS5, CobiT, and ITIL*. N.J: John Willey & Sons, Inc.

Monahan, G. (2008). *Enterprise Risk Management*. N.J: John Willey & Sons, Inc.

Murphy, T. (2002). *Achieving Business Value from Technology: A practical guide for Today's Executive.* N.J: John Willey & Sons, Inc.

Myers, M. (1997). Qualitative Research in Information of Software Reliability. *MIS Quarterly*, 21(2), 241-242.

Neely, A., & Bourne, M. (2000). Why Measurement Initiatives Fail. *Measuring Business Excellence.* 4(4), 3-6.

Nicho, M. (2006). *COBIT as an Effective Measurement Framework for Measuring Information Systems.* Paper presented at the IT Governance International

Conference, 13-15 November, Auckland University of Technology, Auckland, New-Zealand.

Nicho, M. (2008). Information Technology Audit: Systems Alignment and Effectiveness Measures. A PhD Thesis: Auckland University of Technology, Auckland, New-Zealand.

NIST. (2002). Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30
Retrieved 19th September, from: http://csrc.nist.gov/publications/nistpubs/800-30/NIST-SP800-30.pdf

NIST. (2006). Guide for Developing Performance Metrics for Information Security. NIST Special Publication 800-80. Retrieved 1st November 2012, from: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

NIST. (2008). Performance Measurement Guide for Information Security. NIST Special Publication 800-55 Revision 1. Retrieved 1st November 2012 from http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

North, M., North, M., & North, S. (2009). Security from the Bottom-UP: Compliance Regulations and the Trend Toward design-oriented Web Applications. *Journal of Computing Sciences.* 24(4), 54-60.

Nunamaker, J., Chen, M., & Purdin, T. D. M. (1991). Systems Development in Information Systems Research. *Journal of Management Information Systems*. 7(3), 89-106

Nuijten, A., Zwiers, B., & van der Pijel, G. (2008). *The Effect of IS-Auditors' Risk Information IS Managers' Perceived Risk.* Paper presented at Proceedings BLED at AIS Electronic Library (AISeL). 182-197

Oates, B.J. (2006). *Researching Information Systems and Computing*. London: SAGE Publications Ltd.

Offermann, P., Levina, O., Schonherr, M., & Bub, U. (2009). *Outline of Design Science Research Process*. Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology 1-11. US: ACM

Ogren, E. (2009). *HIPAA changes force healthcare to improve data flow*. Retrieved 21st September 2103, from: http://searchsecurity.techtarget.com/news/column/0,294698,sid14_gci1349580,00.html?track=NL-102&ad=691251&asrc=EM_NLN_6005064&uid=5500366

Orlikowski, W. J., & Baroudi, J. J. (2002). Studying information technology in organisations: research approaches and assumptions. In M. D. Myers & D. E. Avison (Eds.), *Qualitative research in information systems – A reader*. London: Sage Publicatoins

Ostrowski, L., & Helfert, M. (2012). Design Science Evaluation – Example of Experimental Design. *Journal of Emerging Trends in Computing and Information Sciences.* 3(9), 253-262.

Pang, Y., & Li, Q. (2013). Game Analysis of Internal Control and Risk Management. *International Journal of Business and Management.* 8(17), 103-111

Pathak, J. (2005). *Information Technology Auditing an Evolving Agenda.* Berlin: Springer-Verlag.

Peffers, K., Tuunanen, T., Rothenberger, M. & Chatterjee, S. (2007). Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*. 24(3), 45-77.

Peffers, K., Rothenberger, M., Tuunanen, T. & Vaezi, R. (2012). Design science research evaluation. In *Design science research in information systems. Advances in theory and practice* (pp. 398-410). Springer Berlin Heidelberg.

Power, D.J. (2008). Decision support system: A historical overview. In F. Burstein, & C.W. Holsapple, (Eds.), *Handbook on decision support systems 1: Basic themes* (pp. 121-140). Berlin Heidelberg, Germany: Springer.

Prat, N., Comyn-Wattiau, I., & Akoka, J. (2014). Artifact Evaluating in Information Systems Design-Science Research – a Holistic View. In PACIS (p. 23).

PricewaterhouseCoopers (PWC). (2016). pwc-global-state-of-information-security-survey-20.

Retrieved 4th June, 2016, from PWC web site:

http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html

Proctor, S. (1998). Linking philosophy and method in the research process: the case for realism. Nurse Researcher, 5(4), 73-90.

Rajbhandari, L., & Snekkenes, E. A. (2011). Mapping between classical risk management and game theoretical approaches. In B. de Decker, J. Lapon, V. Naessens, & A. Uhl, (Eds.), *Communication and multimedia security* (pp. 147-154). Berlin Heidelberg, Germany: Springer.

Ramakrishnan, M. (2009). IT Portfolio Management: A Pragmatic Approach to Implement IT Governance. In A. Cater-Steel (Ed.), *Information Technology Governance and Service Management: Frameworks and Adaptations* (pp. 297-312). New York, NY: IGI Global

Ramirez, D. (2008). Risk Management Standards: The bigger picture. *ISACA Journal.* 4, 38-40.

Rissi, J., & Sherman, S. (2011). Global Regulation and Cloud Computing. In B. Halpert (Ed.), *Auditing Cloud Computing a Security and Privacy Guide* (pp. 143-160). New Jersey: John Wiley &Sons, Inc.

Robinson, J. P., Shaver, P. R., & Wrightsman, L. S. (1991). Criteria for scale selection and evaluation. In L.P. Robinson, P. R. Shaver, L. S. Wrightsman (Eds.), *Measures of Personality and social psychological* attitudes (pp. 1-16). California: Elsevier Inc.

Sademies, A., Savola, R. (2005). *A Survey of Security Metrics Use in Some Finnish Organisations.* Paper presented at the IT Governance International Conference, 14-16 November, Auckland, New Zealand.

Schlarman, S. (2007). Selecting an IT Control Framework. *Publication of Information System Security*. 16(3), 147-151.

Scoring Guidance. (2016, February 13). Retrieved from https://grants.nih.gov/grants/policy/review/rev_prep/scoring.htm

Self, J. (2004). Metrics and Management: Applying the Results of the Balanced Scorecard. *Performance Measurement and Metrics.* 5(3), 101-105. doi: 10.1108/14678040410570111

Senft, S., Gallegos, F. (2009). *Information Technology Control and Audit.* Boca Raton, FL: Auerbach Publication.

Seddon, P. B. (1997). A Respecification and Extension of the DeLone and McLean Model of IS Success. *Information Systems Research.* 8(3), 240-253.

Shanks, G. (2002). Guidelines for Conducting Positivist Case Study Research in Information Systems. *Communications of AJIS*. Special Issue, 76-85

Shin, N. (2003). Creating Business Value with Information Technology: Challenges and Solutions.

Shortreed, J. (2008). *Risk Management best practice is ISO 31000*. Retrieved 18th May 2016, from: http://irr.uwaterloo.ca/pdf_files/ISO%2031000.pdf

Silvius, A. J. G. (2008). The Business Value of IT: A Conceptual Model for Selecting Valuation Methods. *Communications of the IIMA.* 8(3), 57-65.

Simon, H. (1996). *The Science of the Artificial,* third edition. Cambridge, MA: MIT Press.

Simones, H. (2009). *Case Study Research in Practice.* SAGE Publications Ltd.

Singh, H. (2010). *Selecting IT Control Objectives and Measuring IT Control Capital.* Paper presented at Proceedings of ACIS at AIS Electronic Library (AISeL). Paper 89.

Singleton, T. (2007). IT Audit Basics: Emerging Technical Standards on Financial Audits: How IT Auditors Gather Evidence to Evaluate Internal Controls. *ISACA Journal*. 4, 9-11.

Smith, H.A., & McKeen, J. D. (2009). Developments in Practice XXXIII: A Holistic Approach to Managing IT-based Risk. *Communications of the Association of the Association for Information Systems:* 25, Article 41, 519-530

Sprague, Jr. R. H. (1993). A framework for the development of decision support systems. In R. H. Sprague, Jr., & H. J. Watson. (Eds.), *Decision support systems: Putting theory into practice* (3rd ed., pp. 3-28). Englewood Cliffs, NJ: Prentice-Hall.

Sprague, Jr. R. H., & McNurlin, B. (1993). The mead Corporation. In R. H. Sprague, Jr., & H. J. Watson. (Eds.), *Decision support systems: Putting theory into practice* (3rd ed., pp. 226-232). Englewood Cliffs, NJ: Prentice-Hall.

Sprague, Jr. R. H., & Watson, H.J. (Eds). (1993). *Decision Support Systems Putting Theory into Practice.* Englewood Cliffs, New Jersey: Prentice Hall

Stockman, A. (1996). *Introduction to Microeconomics.* USA:The Dryden Press.

Tabor, S.W. (2009). *Exploring the Role of Frameworks and Methodologies in Information Security Management and Governance – Research in Progress.* Paper presented at the Proceedings of AMCIS at AIS Electronic Library (AISeL). Paper 522.

Tarantino, A. (2006). *Manager's Guide to Compliance.* New Jersey: John Wiley & Sons, Inc.

Tavalea, I. (2008). *The factors Influencing Information Communication and Technology (ICT) Governance implementation: A Case Study (master's dissertation).* Auckland University of Technology, Auckland, New-Zealand.

Taylor, S., J., Bogdan, R. (1998). *Introduction to Qualitative Research Methods*. : NYE, US: John Wiley & Sons, Inc.

Thakar, S., & Ramos, T. (2009). *PCI Compliance for Dummies.* West Sussex, England: John Wiley & Sons, Inc.

Trauth, E. M. (1997). Achieving the research goal with qualitative methods: lessons learned along the way. In A.S. Lee, J. Liebenau, J. I. DeGross, (Eds.), *Information systems and qualitative research* (1st ed., pp. 31-68). London, UK: International

Turban, E., & Aronson, J.E. (2001). *Decision Support Systems and Intelligent Systems.* Upper Saddle River, New Jersey: Prentice Hall.

Turban, E., & Watkins, P. R. (1986). Integrating Expert Systems and Decision Support Systems. *MIS Quarterly,* 10(2), 121-136.

Vaishnavi, V.K., & Kuechler Jr, W. (2008). *Design Science Research Methods and Patterns. Innovating Information and Communication Technology.* New Yourk: Auerbach Publications

Vanstraelen, A., & Willekens, M. (2008). Audit Regulation in Belgium. In R. Quick, S. Turley & M. Willekens (Eds.), *Auditing, Trust and Governance* (pp. 19-41). New Yourk, NY: Routledge.

Venable, J. (2006). A framework for design science research activities. In *Proceeding of the 2006 Information Resource Management Association Conference* (pp. 21-24). Washington, DC.

Voon, P., & Salido, J. (2009). *Trustworthy Computing Group*, Microsoft Corporation

Von Solms, B. (2005). Information Security Governance: CobiT or ISO 17799 or Both?. *Computers & Security*. 24, 99-104

Von Neumann, J., & Morgenstern, O. (1944). *Theory of Games and Economic Behavior*. Princeton: Princeton University Press.

Vose, D. (2008). *Risk Analysis a Quantitative Guide*. West Sussex, England: John Wiley & Sons, Inc.

Wallhoff, J. (2004). *Combining ITIL with CobiT and 17799.* Silicon Information AB. Retrieved 25th December 2012 from:

http://www.scillani.se/assets/pdf/Scillani%20Article%20Combining%20ITIL%20with%20Cobit%20and%2017799.pdf

Walser, K., Kuhn, A., & Riedl, R. (2009). *Risk Management in E-Government From The Perspective of IT Governance.* The Proceedings of the 10th International Digital Government Research Conference. Digital Government Society of North America. pp. 315-316.

Walls, J. G., Widmeyer, G. R, & El Sawy, O. A. (1992). On the Deep Structure of Information Systems. *Information Systems Research*. 3(1), pp. 36-59.

Watson, H.J., & Sprague, Jr., R.H. (1993). The components of an architecture for DSS. In R. H. Sprague, Jr., & H. J. Watson. (Eds.), *Decision support systems: Putting theory into practice* (3rd ed., pp. 99-124). Englewood Cliffs, NJ: Prentice-Hall.

Watson, J. (2002). *Strategy an Introduction to Game Theory*. New York: W.W. Norton& Company, Inc.

Webster, T.J. (2009). *Introduction to Game Theory in Business and Economics.* New York: M.E. Sharp, Inc.

Westerman, G., & Hunter, R. (2007). *IT Risk: Turning Business Threats into Competitive Advantage.* US: George Westerman and Gartner, Inc.

Whitman, M., & Mattord, H. (2004). *Management of Information Security*: Thomson Course Technology.

Woda, A. (2007). Achieving Compliance with the PCI Data Security Standard. *ISACA Journal*. 4. 46-50.

Wright, C., Freedman, B., & Liu, D. (2008). *The IT Regulatory and Standards Compliance Handbook.* Burlington, MA: Syngress Publishing Inc.

Yin, R. K. (1984). *Case Study Research: Design and Methods* (1st ed.). Beverly Hills, CA: Sage Publications.

# Appendix A

**ETHICS EXCEPTIOIN**

**EXCEPTIONS TO ACTIVITIES REQUIRING AUTEC APPROVAL**

The following activities do not require AUTEC approval:

6.7. Where a professional or expert opinion is sought, except where this is part of a study of the profession or area of expertise.

-

See more detail at:
http://www.aut.ac.nz/researchethics/guidelines-and-procedures/exceptions-to-activities-requiring-autec-approval-6

# Appendix B

## RESEARCH PROGRESS

Appendix B outlines the research progress against DS cycles, questions formed by Hevner and Chatterjee (2010) that mapped to DS roadmap activities from Alturki et al. (2011b). Table B-1 includes updates and amendments made resulted from conducting activites in Chapter 5, 6 and 7, which are prefixed with "Chapter 5 (C-Model) Amendments", "Chapter 6 (G-Model) Amendments" and "Chapter 7 Amendments", respectively.

**Table B.1: Research Progress**

| DS Cycle | Questions from (Hevner & Chatterjee, 2010) | Tasks and Activities from (Alturki et al., 2011b) | How the Question/Task is answered/implemented - Taken Actions |
|---|---|---|---|
| **Relevance** | Q1. What is the research question (design requirements)? | T1. Document the 'Spark' of an idea/problem | 1- A number of issues/challenges have been highlighted, in Chapter 2, section 2.4. In Chapter 3, section 3.2 a number of problems have been identified as listed in Table 3.2.<br>2- The research question: What are the criteria for selecting the most effective and efficient controls configurations for the best business value outcomes? This has been discussed as part of the thesis progress report and it has been accepted. |
| | | T2. Investigate and evaluate the importance of the idea/problem | In Chapter 3, section 3.2 the identified problems have been discussed and evaluated to be researchable problems and checked against defined criteria and a research focus problem has been selected. |

| DS Cycle | Questions from (Hevner & Chatterjee, 2010) | Tasks and Activities from (Alturki et al., 2011b) | How the Question/Task is answered/implemented - Taken Actions |
|---|---|---|---|
| | | T3. Evaluate the new solution feasibility | In Chapter 3, sections 3.3 , developing a model based DSS would enable practitioners assess IT risks and devise mitigating measures holistically, taken into account the business value from implementing various IT controls/processes. |
| | | T4. Define research scope | The research focus problem has been argued and the relevant question has been driven. |
| | Q6. How is the artefact introduced into the application environment and how is it field tested? What metrics are used to demonstrate artefact utility and improvement over previous artefacts? | | 1- The model based DSS, with its components as listed in Table 4.5, comprising of risk register spreadsheet, so users can assess defined risks.<br>2- A Model, initially will be evaluated internally according to the defined criteria listed in Table 3.6, when the DSS/Model is deemed ready for external evaluation or 'naturalistic' evaluation a number of Experts will be contacted for that purpose<br>3- Make required changes to the Model Evaluation files.<br>4- Contact a number of Experts and arrange time to meet up and demonstrate the model. |
| | Q8. Has the research question been satisfactorily addressed? | | TBA - this will be done in the discussion chapter after analysing the feedback from the second Experts' evaluation.<br>" Chapter 7 Amendments":<br>**Research sub-questions have been answered based on the collected feedback from the experts who evaluated mainly the DSS and G-Model. Also the proposed hypotheses were validated and the research question has been answered.** |

| DS Cycle | Questions from (Hevner & Chatterjee, 2010) | Tasks and Activities from (Alturki et al., 2011b) | How the Question/Task is answered/implemented - Taken Actions |
|---|---|---|---|
| **Design** | | T5. Resolve whether within the Design Science paradigm | In Chapter 4, section 4.3 a thorough discussion has been conducted arguing the suitability of DS to the research. |
| | | T6. Establish type (IS Design Science vs IS Design Research) | In Chapter 4, sub-section 4.3.2 specifically, DS methodology in IS research has been established. |
| | Q2. What is the artefacts? How is the artefact represented? | T7. Resolve theme (Construction, Evaluation or both) | 1- A literature review has been conducted, a number of problems have been identified, and a problem statement, the focus of the research, has been produced.<br>2- To attempt resolve the stated problem, a model based DSS has been proposed. An interactive DSS comprised of a spreadsheet to capture the identified IT risks. A subset of 'Access Management' risks have been identified.<br>3- A Risk Space Matrix<br>4- Suggested controls and processes from COBIT 4.1, ITIL 3.0, and ISO 27001.<br>5- A model based on cumulative impact probability analysis, to aid practitioners determine the best controls configurations.<br><br>"Chapter 5 (C-Model) Amendments"<br>6- **The C-Model described in 5 has been developed and evaluated. However, as it has been reported in 5.2.1 and further discussed in 5.2.2, C-Model has many limitations, identified by the Experts (internal)** |

| DS Cycle | Questions from (Hevner & Chatterjee, 2010) | Tasks and Activities from (Alturki et al., 2011b) | How the Question/Task is answered/implemented - Taken Actions |
|---|---|---|---|
| | | | **evaluation only. Subsequently it was deemed inefficient and not adequate to pass it on to the second evaluation cycle, the external or naturalistic evaluation.**<br>"Chapter 6 (G-Model) Amendments":<br>7- **Further research in game theory and its application arrived at developing game theory based to be utilised in the interactive DSS instead of C-Model**<br>8- **The DSS with risk register, Risk Space Matrix, game theory model named G-Model, gaming files, and payoff values matrix all have been articulated and prepared.** |
| | Q3. What design processes (search heuristics) will be used to build the artefacts? | T8. Define requirements | IT risk management to provide assurance of the IT systems, ensuring alignment of business-IT objectives. |
| | | T9. Define Alternative solutions | 1- Risk simulation model based on Monte Carlo simulating method.<br>2- Game theory based model |
| | | T10. Explore knowledge base support of alternatives. | 1- Monte Carlo simulating method used in Finance, Insurance.<br>"Chapter 5 (C-Model) Amendments"<br>2- **Game theory has been reviewed, and its applications have been explored.**<br>"Chapter 6 (G-Model) Amendments" |

| DS Cycle | Questions from (Hevner & Chatterjee, 2010) | Tasks and Activities from (Alturki et al., 2011b) | How the Question/Task is answered/implemented - Taken Actions |
|---|---|---|---|
| | | | 3- **Game theory software applications to build various game settings have been explored.** |
| | Q5. What evaluations are performed during the internal design cycles? What design improvements are identified during each design cycle? | T11. Prepare for design and/or evaluation | 1- The research stated problem, research questions and proposed approach to find an answer to the question and solutions to the stated problem, have been reviewed and approved as part of the research program reviewing process.<br>2- The artefacts evaluation is to be reported in Chapter 5 and 6.<br><br>"Chapter 5 (C-Model) Amendments"<br>3- **Developed artefacts: DSS comprised of risk register, a number of AM risks have identified and corresponding controls and processes have been selected utilising some publicly available documents. C-Model has been developed in Excel, an experiment has been conducted results are prepared to be presented along with the model to three experts for initial/internal evaluation, called artificial evaluation, against a set of criteria and corresponding questions.**<br>"Chapter 6 (G-Model) Amendments"<br>4- **A 3-Player game setting using Gambit 14.01 framework, where COBIT, ITIL and ISO 27001 compete to devise the best combination of controls and processes that would return the best payoff value among all the possible options.** |

| DS Cycle | Questions from (Hevner & Chatterjee, 2010) | Tasks and Activities from (Alturki et al., 2011b) | How the Question/Task is answered/implemented - Taken Actions |
|---|---|---|---|
| | | T12. Develop (construction) | 1- As noted in Table 3.5 a DSS components have been created in spreadsheet, utilising some publicly available documents and the researcher's knowledge in IT risk management.<br>"Chapter 5 (C-Model) Amendments"<br>2- **C-Model developed in Excel.**<br>"Chapter 6 (G-Model) Amendments"<br>3- **The game theory based model G-Model is developed in Gambit and payoff guidance is devised, AM risk further defined and assessed in a risk register, and Risk Space Matrix is developed.** |
| | | T13a. Evaluate: Artificial evaluation | This will be reported in Chapter 5 and 6.<br>"Chapter 5 (C-Model) Amendments"<br>**1- Artefacts have been presented along with the experiment results and discussed with a mathematician, and supervisor 1 and 2. Oral feedback has been obtained from the three experts, around the defined criteria and corresponding questions listed in Table 4.6.**<br>**2- Critical reflection has been conducted assessing the C-Model readiness for the next evaluation cycle.**<br>**3- Discussion of Action 2, fed into activity T12 which in turn it feeds into activity T9, stimulating reviewing the proposed solution design and further theory research seeking other alternatives.**<br>4- **Findings of the artefacts evaluation, discussion and the other reviewed alternatives are documented and fed into the research repository, to be** |

| DS Cycle | Questions from (Hevner & Chatterjee, 2010) | Tasks and Activities from (Alturki et al., 2011b) | How the Question/Task is answered/implemented - Taken Actions |
|---|---|---|---|
| | | | **included in the T14, when communicating the outcomes of the research to the target audience.**<br><br>"Chapter 6 (G-Model) Amendments":<br>**5- Developed artefacts resulting from 4, DSS components and G-Model were prepared as noted in section 6.1**<br>**6- Artefacts were prepared as noted in Table 6.9, and 2 experts conducted artificial evaluation as reported in sub-section 6.2.2, and critical reflection were made and reported in sub-section 6.2.3, tabulated in Table 6.12**<br>7- **DSS components, in particular G-Model, deemed ready, with minor suggested changes, for next evaluation cycle, the Naturalistic evaluation.**<br>"Chapter 7 Amendments":<br>**8- Research sub-questions, and question have been answered.**<br>9- **Research hypotheses have been validated.** |
| | | T13b. Evaluate: Naturalistic evaluation | This will be reported in Chapter 5 and 6.<br>"Chapter 5 (C-Model) Amendments"<br>**1- As the C-Model, which is the core of the DSS, is deemed in adequate to proceed with further evaluation, this activity was not executed at this stage.**<br><br>"Chapter 6 (G-Model) Amendments" |

| DS Cycle | Questions from (Hevner & Chatterjee, 2010) | Tasks and Activities from (Alturki et al., 2011b) | How the Question/Task is answered/implemented - Taken Actions |
|---|---|---|---|
| | | | **2- In Chapter 6, Sub-section 6.2.4, a number of experts have been approached, as shown in Table 6.14, to conduct this evaluation, after adapting a few changes as noted in T13a.**<br>**3- Game files, residual risk assessment and written and oral feedback were obtained from 5 experts who participated in the evaluation, as reported in Sub-section 6.2.4.2.**<br>4- **Collected data and feedback were analysed and critiqued in sub-section 6.2.5 and tabulated in Table 6.25 benchmarked against the artefacts evaluation criteria and corresponding question.** |
| **Rigor** | Q4. How are the artefacts and the design processes grounded by the knowledge base? What, if any, theories support the artefacts design and the design process? | | Risk management principles from ISO 31000, CoSo-ERM. General and IT auditing SAS70, ISAE3402, IIA and ISACA publications. Decision Support Systems DSS principles, types of systems, models and their applications. Probability and cumulative impact distribution to build C-Model. Game theory principals, types of games settings and their applications. |
| | Q7. What new knowledge is added to the knowledge base and in what form (e.g. peer-reviewed literature, meta-artefacts, new theory, and new method)? | T14. Communicate findings | TBA – this will be done in the discussion chapter after analysing feedback and experts' evaluations (Internal/Artificial and External/Naturalistic) evaluation.<br><br>"Chapter 7 Amendments":<br>**Research contribution to academia and business have been identified, in a separate section. With regards to academia, the adoption of DS** |

| DS Cycle | Questions from (Hevner & Chatterjee, 2010) | Tasks and Activities from (Alturki et al., 2011b) | How the Question/Task is answered/implemented - Taken Actions |
|---|---|---|---|
| | | | **methodology, guidelines and roadmap; the application of game theory based model in selecting best controls configurations. As for business, the contribution was examined from practitioners' and organisations' perspectives, all summarised in Figure 7.5**<br>**Findings could be published in academic as well as professional conferences and journals.** |