Risk Based Assessment of IT Control Frameworks: A Case Study

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

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

2012
School of Computing 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.

....

Signature

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, without, which it would not have been possible to complete the research.

First and foremost the researcher wishes to thank the supervisor Dr. Brian Cusack for his constant mentoring and endless support, encouragement and advice during the two semesters, 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. Secondly, the researcher would like to thank the people from the two case studies who helped in arranging the field work interviews, and also the subject matter experts who spared their valuable time and participated in the interviews, provided their answers and shared their thoughts and experience, which enriched the research immensely. 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, including the AUT Ethics Committee 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.

Abstract

Businesses are constantly advised to implement Information Technology Governance (ITG) frameworks or adapt best practices to gain efficiency, accountability, and/or to meet regulatory compliance. However, organisations require a clear statement of the business value to be gained from implementing resource intensive IT control-based structured environments. Business value has many facets, depending on the industry, size of the organisation, and how business value is perceived. Business risk provides both positive and negative metrics for an assessment of potential business gain and loss. It has often been contested that the implementation of control frameworks is a liability that is not supported by measurable business benefits.

This study proposes to investigate the relationship between IT control frameworks, best practices and standards, and business risk treatment. The expectation is that the value generated by the relationship will become apparent and that by implication the costs and benefits of ITG can be identified. At present there are many tools available to assist business managers with risk management. An assessment of a representative set of control frameworks, best practices and standards is made to identify which risks may be treated, the scope of a framework, and what benefits may be expected from implementing those frameworks and best practices. Part of the literature review investigates the challenges that organisations face when implementing IT control frameworks and best practices. Also, the set of related problems is explored and the research focuses on one researchable problem, how to identify business value from managing IT risks in control-based structured environments. The research question is: **How could a business realise the value of managing IT risk in control-based structured environments?**

Identifying business value in risk based IT control-based structured environments is a complex and subjective domain that suits qualitative research methods. Research reports in the subject area suggest that case study research methods are most commonly used to obtain factual data and to construct theory. Consequently in this study face-to-face semi-structured interviews, document collection, analysis and observation are the main source of data gathered for analysis. The researcher has interviewed staff with relevant roles in two organisations to understand what liabilities, challenges and benefits are observed in practice. Collected data is analysed qualitatively utilising qualitative analysis software tools and the results are reviewed and further analysed by the author. The conclusion of the thesis summarises the challenges, problems and solutions derived from the data collected in the case study companies and shows the answer to the research question is conditional on a complex set of conditions. Among the identified business value outcomes are the improved business-IT communication and alignment. Improved communication leads to a better alignment between business and IT objectives. Subsequently, organisations are able to direct their efforts to secure their most valuable assets to ensure resilient business. In addition, these organisations continuously build required IT capabilities that allow them to capture business opportunities when they arise.

Lastly, recommendations for further research are also provided. To establish adequate ITG and risk management process, organisations have no choice but to adopt a mix of frameworks, best practices and standards. The justification is either to meet compliance requirements or to complement the applied frameworks, where one framework doesn’t cover certain aspects of ITG, security, risk and compliance. The author has learned from the research that an investigation into integrating frameworks, best practices and standards would be the next step in better understanding the issue of identifying business value in risk based IT control-based structured environments. Practitioners as well businesses would benefit from the outcomes of this type of research.

Table of Contents

DECLARATION I

ACKNOWLEDGEMENTS II

ABSTRACT III

TABLE OF CONTENTS V

LIST OF FIGURES XV

LIST OF TABLES XVI

LIST OF ABBREVIATIONS XVII

CHAPTER 1 INTRODUCTION 1

1.0 INTRODUCTION 1
1.1 THE PROBLEM DEFINED 2
1.2 MOTIVATION 4
1.3 METHODOLOGY AND EXPECTED FINDINGS 4
1.4 STRUCTURE OF THESIS 7

CHAPTER 2 LITERATURE REVIEW 8

2.0 INTRODUCTION 8
2.1 IT RISK MANAGEMENT OVERVIEW 9
2.1.1 Risk Governance 9
2.1.1.1 Risk Appetite and Risk Tolerance 10
2.1.1.2 Roles and Responsibilities 11
2.1.1.3 Documentation 11
2.1.2 IT Risk 12
2.1.3 IT Risk Management Process 12
2.1.3.1 Establish the Context 13
2.1.3.2 Identify Risks 14
2.1.3.3 Analyse Risks 14
2.1.3.4 Evaluate Risks 14
2.1.3.5 Treat Risks 15
4.1.3.6 Monitor and Review Risks 16

2.1.3.7 Communicate and Consult....17
2.2 REVIEW OF RISK FRAMEWORKS....19
2.2.1 International Organisation for Standardisation (ISO)....19
2.2.1.1 AS/NZS ISO 31000:2009....19
2.2.1.2 ISO 31010:2009....20
2.2.1.3 ISO 27001:2005....20
2.2.1.4 ISO 27002:2005....20
2.2.2 Risk IT....21
2.2.3 Others....21
2.2.3.1 Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)....21
2.2.3.2 National Institute of Standard and Technology (NIST) Special Publication (SP) 800-30....22
2.3 REVIEW OF IT CONTROL FRAMEWORKS AND BEST PRACTICES 22
2.3.1 Val IT....23
2.3.2 Control Objectives for Information and Related Technology (COBIT) 23
2.3.3 IT Infrastructure Library (ITIL)....24
2.4 REVIEW OF COMPLIANCE....25
2.4.1 Payment Card Industry (PCI)....25
2.4.2 Sarbanes- Oxley (SOX)....25
2.4.3 Health Insurance Portability and Accountability Act (HIPAA)....26
2.5 BUSINESS CHALLENGES....26
2.5.1 Business Changes....27
2.5.1.1 Outsourcing....27
2.5.1.2 Expansion....28
2.5.1.3 Globalisation....28
2.5.2 Technology Changes....28
2.5.2.1 Internet and Web Technologies....29
2.5.2.2 Wireless and Mobile Computing....29
2.5.2.3 Virtual Machines....30
2.5.2.4 Cloud Computing....30

2.5.3 Regulatory Demands 31
2.5.3.1 Political Drive 31
2.5.3.2 Market Drive 31
2.5.3.3 Industry Drive 32
2.6 IDENTIFYING BUSINESS VALUE 32
2.6.1 IT Systems Role and Business Value 33
2.6.2 IT Risk/Value within Business Context 35
2.6.3 Business Value of IT Risk Management Standards and Methods.....37
2.6.4 Value in Managing IT Risk Holistically 37
2.7 SUMMARY OF ISSUES AND PROBLEMS 39
2.7.1 List of Issues and Problems 40
2.7.2 Selecting the Focus Problem 43
2.8 CONCLUSION 44
CHAPTER 3 METHODOLOGY 46
3.0 INTRODUCTION 46
3.1 RESEARCH IN ESTABLISHING IT CONTROL-BASED STRUCTURED ENVIRONEMNTS 47
3.1.1 Enterprise Governance of IT in Practice 47
3.1.2 The Value, Effectiveness, Efficiency and Security of IT Controls ...49
3.1.3 Whatever Happened to Alignment? 50
3.1.4 Implementation of Information Security Management System 52
3.1.5 A Comparative Case Study Analysis of IT Governance Framework 54
3.2 DESIGNING A RESEARCH METHODOLOGY 55
3.2.1 Review of Case Study Research Methods.......................................56
3.2.2 Review of IT Risk Issues from the Literature Review......................57
3.2.3 The Research Question..60
3.2.4 The Research Sub-Questions and Hypotheses 61
3.2.5 Selected Research Methodology...61
3.2.5.1 Qualitative and Quantitative Research Methods in IT..................62
3.2.5.2 Case Study Method 64
3.2.5.3 Case Selection..66
3.2.5.4 Case Study Method Issues..67
3.2.6 Data Map 69

3.3 DATA REQUIREMENTS 71
3.3.1 Data Collection Methods..71
3.3.1.1 Interview..72
3.3.1.2 Interview Recording and Transcription..74
3.3.1.3 Documents Collection 75
3.3.1.4 Diary Recording..75
3.3.2 Data Analysis..76
3.3.2.1 Thematic Analysis..77
3.3.2.2 Coding - Indexing 77
3.3.2.3 Grounded Theory Analysis...78
3.3.2.4 Cross-Case Analysis...78
3.3.2.5 Computer-Assisted Qualitative Data Analysis (CAQDAS)..........79
3.3.3 Data Visualisation...79
3.4 RESEARCH METHODOLOGY LIMITATIONS 81
3.4.1 Reliability 82
3.4.2 Validity...83
3.4.3 Generalisation...84
3.5 FORECAST RESEARCH OUTCOMES 85
3.6 CONCLUSION 85

CHAPTER 4 RESEARCH REPORT...87

4.0 INTRODUCTION 87
4.1 FIELD WORK – PREPARATION..88
4.1.1 Variation...89
4.2 CASE STUDY SELECTION 91
4.2.1 Company A...92
4.2.2 Company B 94
4.3 FIELD FINDINGS REPORT..95
4.3.1 IT Risk Context...97
4.3.1.1 Business Requirements...97
4.3.1.1.1 Company A 97
4.3.1.1.2 Company B 99
4.3.1.2 Regulatory Requirements 101
4.3.1.2.1 Company A 101

4.3.1.2.2 Company B 102
4.3.2 IT Risk Management 103
4.3.2.1 Committee 103
4.3.2.1.1 Company A 103
4.3.2.1.2 Company B 103
4.3.2.2 Roles and Responsibilities 103
4.3.2.2.1 Company A 103
4.3.2.2.2 Company B 104
4.3.2.3 Ad hoc 105
4.3.2.3.1 Company A 105
4.3.2.3.2 Company B 108
4.3.2.4 Process 108
4.3.2.4.1 Company A 108
4.3.2.4.2 Company B 110
4.3.2.5 Risk Management Tool 112
4.3.2.5.1 Company A 112
4.3.2.5.2 Company B 112
4.3.2.6 Risk Register 112
4.3.2.6.1 Company A 112
4.3.2.6.2 Company B 113
4.3.2.7 BCP – DRP 113
4.3.2.7.1 Company A 113
4.3.2.7.2 Company B 114
4.3.3 Existing Control-Structures Framework and Best Practices 115
4.3.3.1 COBIT 115
4.3.3.1.1 Company A 115
4.3.3.1.2 Company B 116
4.3.3.2 ITIL 117
4.3.3.2.1 Company A 117
4.3.3.2.2 Company B 118
4.3.3.3 TOGAF 119
4.3.3.3.1 Company A 119
4.3.3.3.2 Company B 119

4.3.3.4 Prince2 –PMI 119
4.3.3.4.1 Company A 119
4.3.3.4.2 Company B 120
4.3.3.5 ISO 27001.. 120
4.3.3.5.1 Company A 120
4.3.3.5.2 Company B 120
4.3.3.6 Policies 121
4.3.3.6.1 Company A 121
4.3.3.6.2 Company B 121
4.3.3.7 Others 121
4.3.3.7.1 Company A 121
4.3.3.7.2 Company B 122
4.3.4 Benefits from Control-Structure Frameworks and Best Practices... 123
4.3.4.1 Business - IT Alignment.. 123
4.3.4.1.1 Company A 124
4.3.4.1.2 Company B 124
4.3.4.2 Effectiveness.. 129
4.3.4.2.1 Company A 129
4.3.4.2.2 Company B 129
4.3.4.3 Efficiency.. 131
4.3.4.3.1 Company A 131
4.3.4.3.2 Company B 132
4.3.4.4 Security.. 133
4.3.4.4.1 Company A 133
4.3.4.4.2 Company B 134
4.3.4.5 Defined Roles and Responsibilities 135
4.3.4.5.1 Company A 135
4.3.4.5.2 Company B 135
4.3.4.6 Communication.. 136
4.3.4.6.1 Company A 136
4.3.4.6.2 Company B 137
4.3.4.7 Holistic View – Planning.. 137
4.3.4.7.1 Company A 137

4.3.4.7.2 Company B 138
4.3.4.8 Increase IT Credibility 140
4.3.4.8.1 Company A 140
4.3.4.8.2 Company B 141
4.3.5 Challenges 141
4.3.5.1 Immature IT Risk Standard 142
4.3.5.1.1 Company A 142
4.3.5.1.2 Company B 142
4.3.5.2 Lack of Awareness 142
4.3.5.2.1 Company A 142
4.3.5.2.2 Company B 145
4.3.5.3 Lack of Local Expertise 145
4.3.5.3.1 Company A 145
4.3.5.3.2 Company B 146
4.3.5.4 High Resource Consumption 147
4.3.5.4.1 Company A 147
4.3.5.4.2 Company B 148
4.3.5.5 Lack of Executive Management Support 149
4.3.5.5.1 Company A 149
4.3.5.5.2 Company B 149
4.3.5.6 Business and Technology Demands 150
4.3.5.6.1 Company A 150
4.3.5.6.2 Company B 151
4.3.5.7 Resistance 151
4.3.5.7.1 Company A 151
4.3.5.7.2 Company B 153
4.3.5.8 Complexity 153
4.3.5.8.1 Company A 153
4.3.5.8.2 Company B 154
4.3.5.9 Many Frameworks 154
4.3.5.9.1 Company A 155
4.3.5.9.2 Company B 155
4.3.5.10 Ambiguous Regulatory Directions 155

4.3.5.10.1 Company A 155

4.3.5.10.2 Company B 156

4.3.6 Problems 157

4.3.6.1 Business - IT Silos 157

4.3.6.1.1 Company A 157

4.3.6.1.2 Company B 158

4.3.6.2 Business - IT Misalignment 158

4.3.6.2.1 Company A 158

4.3.6.2.2 Company B 159

4.3.6.3 Business - IT Structures 160

4.3.6.3.1 Company A 160

4.3.6.3.2 Company B 160

4.3.6.4 Risk Management Function 161

4.3.6.4.1 Company A 161

4.3.6.4.2 Company B 162

4.3.6.5 BCP-DRP 163

4.3.6.5.1 Company A 163

4.3.6.5.2 Company B 164

4.3.6.6 Reactive not Proactive 164

4.3.6.6.1 Company A 164

4.3.6.6.2 Company B 165

4.3.6.7 User’s Behaviour 165

4.3.6.7.1 Company A 165

4.3.6.7.2 Company B 165

4.3.7 Solutions 165

4.3.7.1 Define Objectives 166

4.3.7.1.1 Company A 166

4.3.7.1.2 Company B 166

4.3.7.2 Consult Third Party Experts 167

4.3.7.2.1 Company A 167

4.3.7.2.2 Company B 168

4.3.7.3 Make Use of Major Incidents 168

4.3.7.3.1 Company A 168

4.3.7.3.2 Company B 169

4.3.7.4 Educate and Train 169

4.3.7.4.1 Company A 170

4.3.7.4.2 Company B 171

4.3.7.5 Improve Business-IT Communication 172

4.3.7.5.1 Company A 172

4.3.7.5.2 Company B 174

4.3.7.6 Customise Frameworks to Business Environment 175

4.3.7.6.1 Company A 175

4.3.7.6.1 Company B 176

4.3.7.7 Demonstrate Value to Business 177

4.3.7.7.1 Company A 177

4.3.7.7.2 Company B 179

4.3.7.8 Integrate Frameworks and Best Practices.................................. 180

4.3.7.8.1 Company A 180

4.3.7.8.2 Company B 181

4.3.7.9 Co-operate with Internal Audit 181

4.3.7.9.1 Company A 181

4.3.7.9.1 Company B 183

4.4 CONCLUSION 184

CHAPTER 5 DISCUSSION OF FINDINGS 185

5.0 INTRODUCTION 185

5.1 REVIEW OF RESEARCH QUESTION, SUB-QUESTIONS AND HYPOTHESES 185

5.2 CROSS-CASE ANALYSIS 186

5.2.1 Research Sub-Questions 186

5.2.1.1 Establishing IT Risk Context 186

5.2.1.2 IT Risk Management Process 189

5.2.1.3 Business Value in Implementing IT Control Frameworks.......... 191

5.2.1.4 Business Value in Managing IT Risk in Control-Based Structured Environments.. 200

5.2.2 Hypotheses Evaluation 203

5.2.3 Research Question 205

5.3 CHALLENGES AND PROBLEMS REPORTED IN FIELDWORK FINDINGS 206

5.3.1 Challenges 206

5.3.2. Problems 210

5.4 RECOMMENDED SOLUTIONS 213

5.5 CONCLUSION 218

CHAPTER 6 CONCLUSION 219

6.0 INTRODUCTION 219

6.1 SUMMARY OF FINDINGS 219

6.2 ANSWERS TO RESEARCH QUESTIONS 222

6.3 RECOMMENDATIONS FOR FURTHER RESEARCH 225

6.4 CONCLUSION 227

REFERENCES 228

APPENDIX A – THEMATIC CODING METHODOLOGY 234

APPENDIX B – ETHIC APPROVAL 236

List of Figures

FIGURE 2.1: RISK MANAGEMENT PROCESS. 13
FIGURE 2.2: RELATING THE STRATEGIC ALIGNMENT TO BUSINESS AND IS STRATEGY...34
FIGURE 2.3: THE FIVE PILLARS OF BENEFITS REALISATION. 35
FIGURE 2.4: RISK AND OPPORTUNITY..36
FIGURE 2.5: IT RISK IN THE RISK HIERARCHY..36
FIGURE 2.6: THE ORGANISATIONAL ENVIRONMENT. 38
FIGURE 2.7: PRESENTATION OF A SYSTEM. 39
FIGURE 3.1: DDREERESENTATION OF A SYSTEM...39
FIGURE 3.2: AN EXAMPLE OF DATA VISUAL REPRESENTATION............................80
FIGURE 3.3: A SAMPLE CHART PRODUCED IN THE NVIVO MODEL EXPLORER.......81
FIGURE 6.1: BUSINESS VALUE AND THE ORGANISATIONAL ENVIRONMENT 225

List of Tables

TABLE 2.1:RISK COMMUNICATION FLOW. 18

TABLE 2.2: SUMMARY OF ISSUES IN MANAGING IT RISK IN CONTROL-BASED STRUCTURED ENVIRONMENTS. 43

TABLE 4.1: COMPANY A DATA SOURCES SUMMARY. 93

TABLE 4.2: COMPANY B DATA SOURCES SUMMARY. 95

TABLE 4.3: FIELDWORK FINDINGS SUMMARY. 96

TABLE 5.1: IT RISK CONTEXT IN CASE STUDY COMPANIES................................189

TABLE 5.2:IT RISK MANAGEMENT PROCESS. 191

TABLE 5.3: IMPLEMENTED IT CONTROL FRAMEWORKS, STANDARDS AND BEST PRACTICES. 192

TABLE 5.4: BUSINESS VALUE IN IMPLEMENTING IT CONTROL FRAMEWORKS, STANDARDS AND BEST PRACTICES..198

TABLE 5.5: BUSINESS VALUE IN MANAGING IT RISK IN CONTROL-BASED STRUCTURED ENVIRONMENTS. 202

TABLE 5.6: HYPOTHESES EVALUATION. 203

TABLE 5.7: REPORTED CHALLENGES IN IMPLEMENTING IT CONTROL FRAMEWORKS. 209

TABLE 5.8: REPORTED PROBLEMS IN THE CASE STUDY ORGANISATIONS. 212

TABLE 5.9: RECOMMENDED SOLUTIONS IN THE CASE STUDY ORGANISATIONS. ..217

TABLE 6.1: A SUMMARY OF CHALLENGES, PROBLEMS AND SOLUTIONS REPORTED IN TABLES 5.7, 5.8 AND 5.9. 222

List of Abbreviations

BCP	Business Continuity Planning
BIA	Business Impact Analysis
CAB	Change Advisory Board
CAQDAS	Computer-assisted Qualitative Data Analysis Software
CIO	Chief Information Officer
COBIT	Control OBjectives for Information and related Technology
CMMI	Capability Maturity Model Integration
COSO	Committee of Sponsoring Organisation
DRP	Disaster Recovery Planning
HIPAA	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
IGMP	Internet Group Management Protocol
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
ITGI	Information Technology Governance Institute
ITIL	Information Technology Infrastructure Library
MoH	Ministry of Health
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OGC	Office of Government Commerce
RACI	Responsible, Accountable, Consulted and Informed
RISK IT	Risk IT, IT Risk Framework
RM	Risk Management

RMF	Risk Management Framework
RoI	Return on Investment
SaaS	Software as Service
SDLC	System Development Life Cycle
SLA	Serviced Level Agreement
SOX	Sarbanes-Oxley
TOGAF	The Open Group Architecture Framework
PCI-DSS	Payment Card Industry Data Security Standard
PMI	Project Management Institute
Prince2	PRojects IN Controlled Environments
VAL IT	Value IT, IT Governance Framework

Chapter 1

Introduction

1.0 INTRODUCTION

The topic of this research is investigating how to realise business value from managing IT risk in control-based structured environments. Every aspect of business has elements of uncertainty, hence there is risk. Risk is defined as “the effect of uncertainty on objectives” (Shortreed, 2008, p. 5). Managing risk comes at cost to an organisation; however, managing the risk effectively adds value to the organisation. Risk exists in negative or positive forms. In the negative form it resembles the adverse impact of an unplanned event, while in the positive form risk presents new opportunities that a business might encounter or explore. However, organisations must have the capability to seize opportunities when they arise. The focus of this research is on IT risk, and in particular the various IT control frameworks (including best practice and standards) that are advocated to manage risk. IT risk must be managed to help organisations make informed and sound decision and to ensure business value. As IT systems underpin various business functions and processes at all levels, managing IT risk has become paramount to business existence. Managing IT risk, however, should not be performed in isolation from managing the business risk. The optimum IT risk management is achieved when IT risk is defined from business perspectives.

The research proposes to investigate the business value in managing IT risk in control-based structured environments established through implementing IT control frameworks, best practices and standards. The research question that best addresses the research focus is:

How could a business realise the value of managing IT risk in control-based structured environments?

The intention of the research question is to identify the benefits an organisation would get from managing IT risk at the various stages where IT risk resides within the business-IT structure. The investigation will be carried out in the forms of a comparative case study based research and will be conducted at two corporate organisations.

Chapter 1 introduces the research aspects in the following sections: Section 1.1 explores the problem focus of the research; Section 1.2 identifies the research motivation and drive; Section 1.3 introduces the research methodology the author intends to apply. The Chapter is concluded in Section 1.4 with the thesis structure.

1.1 THE PROBLEM DEFINED

Implementing control frameworks and applying standards and best practices could become a challenging task if it is not considered, planned and executed professionally, as the new structure might complicate the environment (Chatterji, 2007). To establish IT control-based structured environments and to manage IT risk among other business processes, functions and procedures could cause a number of challenges and problems for an organisation to handle. Among these challenges are business dynamics for continuity and profitability. For example, changes can result from expansion, globalisation and outsourcing. However, there is always an element of uncertainty that implies risk. Similarly, changing technologies are always a source of uncertainty and risk. For example, internet and web applications, Cloud computing, Mobility, and Virtual machines. New technologies are not commodities and they could resolve many issues and introduce endless business opportunities. However, that comes at a cost as each technology comes with vulnerabilities that could be exploited by threats. The other challenging aspect is the regulatory requirements that come in a form of standards or compliance systems. The drive for regulatory demands could come from different sources: Political, Industry, and Market.

Implementing a current, effective, and efficient IT risk management framework comes at a cost. In addition, implementing an IT risk management framework faces many hurdles, for example, lack of top management sponsorship. On the other hand, when structuring a framework and adapting a set of standards and best practices, an important factor to consider is the availability of local expertise in those standards, frameworks and the business itself (Chatterji, 2007). Should an organisation opt to utilise a third party that would increase the cost and the risk of lacking the knowledge of the local environment and business rules (Benvenuto & Brand, 2005). Organisations should be able to realise the gained value from implementing resource-intensive frameworks. The author is inclined to believe that identifying different perceptions of business values gained from managing IT risk in control-based structured environments is a key issue to the research. The ability to articulate the gained business value from implementing recognised frameworks would play a vital role in earning top management support (Murphy, 2002). When business values are identified, then some measuring means can be modelled that could help organisations realise the benefits and thence make informed decisions to seize opportunities as they arise. 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 in effectiveness of IT risk management framework (Ames, 2007).

Various business values for IT systems roles and management exist. However, with different perceptions of business values, tangible (financial) and intangible (reputational), demonstrating the business value remains a challenging goal to achieve. How could an organisation realise the value of implementing a risk management framework, that's integrated within the organisation's IT governance structure? This seems to be one of the most challenging tasks that organisations and professionals face because of the dynamic and complicated nature of the domain.

The researcher speculates that managing IT risk in a holistic approach optimises the best chances of valid solutions. To ensure the holistic approach is followed, recognised control frameworks, best practices and standards could be implemented and adapted, rather than relying solely on individuals' accumulative experience. Although this approach has some challenges in itself, it leverages activities performed through other processes and ensures managing IT risk is done in a timely manner and not in isolation from managing the rest of the business risk. As a result, IT would be able to demonstrate and communicate business value to the executive management. Such a research outcome would provide the guidance organisations require to realise the business value from managing IT risk.

1.2 MOTIVATION

Section 1 introduced the importance showing business value in managing IT risk in control-based structured environments. The potential challenges facing implementation was also noted. Researches about IT control environment and business-IT value are scarce and described by researchers as limited (Haes and Van Grembergen, 200; Behr, Castner, Kim, 2005). In addition, the nature of the domains (ITG, IT controls, security and risk management, business alignment and identifying business values) requires practitioners' perspective to obtain empirical data (Lee, et al., 2006). Haes and Van Grembergen (2005) claimed that there are not many research reports that analyse and draw inferences that could be utilised in testing devised hypotheses and forming proposed theories. Behr, Castner, Kim (2005) in the case study research claimed that the effect of the information system on business value has been the subject of many research studies. However, there are not many published research reports on the effect of IT-controls on business-IT value.

The author is persuaded to research this problem and present the findings to contribute to the literature and to provide suggestions for further research. In addition, the outcome of the research would benefit organisations and practitioners when applying guidelines to enable businesses to realise the value in managing IT risk in control-based structured environments.

1.3 METHODOLOGY AND EXPECTED FINDINGS

Qualitative and quantitative research methods have been utilised in the research of various topics in IT. Each method has exclusive advantages and disadvantages depending on the researched domain and available resources. Qualitative method is defined by Myers (1997, cited in Nicho, 2004, p 60) as that "which involves the use of qualitative data, such as interview, document, and participant observation data, to understand and explain social phenomena". On the other hand, quantitative method, as described by the author Myers (1997, cited in Nicho, 2004, p. 65), "assumes that reality is objectively given and can be described by measurable properties which are independent of the observer". Quantitative method is underlined by positivist paradigm where asserted hypotheses and propositions are tested (Taylor & Bogdan, 1998). Data collection methods utilised in Quantitative approach are mainly conducting a survey, which is very time consuming, to obtain facts or causes and filtering out the subjective statistics of individuals (Taylor & Bogdan, 1998, p. 3). However, depending on the researched domain-complexity quantifying research elements might not be at all feasible as argued by Yin (1984).

A positivist paradigm utilises quantitative data to test hypotheses (Taylor & Bogdan, 1998) and a positivist approach could utilise qualitative data. Qualitative method would suit a complex domain that involves high percentage of subjectivity where contributing factors are dynamic in nature. In addition the researcher would have to holistically examine the environment and gather factual insights with context (Taylor & Bogdan, 1998). Haes and Van Grembergen (2005) conducted IT governance and best practice controls case study. The researchers stated that relevant academic research is minimal, as the subject is relatively new. In addition, the existing research is either limited to the framework they examine or lacks empirical data that is necessary to identify different perceptions of business value.

It has been indicated that the topic researched in this paper namely IT risk management and business value, is complex, dynamic and interrelates with the business in many aspects and on various levels. The fact that the subject of this research is subjective to its context makes it imperative to obtain factual data besides the literature-review in an attempt to answer the research question. The business insight is paramount to test the theoretical assertions in order to gain a wider view of the problem indicated in the research.

The researcher believes that the best approach to achieve the research objectives is a combination of qualitative and quantitative approaches where proposed hypotheses are tested. The indicated test will be performed using the analysed qualitative data applying quasi-judicial method, where a rational argument is used to interpret the data (Collis & Hussey, 2009).

One method of qualitative method is case study, that has been utilised in researching many fields, indicated by (Yin, 1984), who further justified the use of case study by “where the structure of given industry may be investigated” (p. 14). Furthermore, case study is more a qualitative approach as stated by Collis and Hussey (2003, cited in Tavalea, 2008) that suits the subjective domains that have been researched. Case studies were conducted using various approaches in collecting and analysing data. Yin (1984, p. 14) indicated that a case study approach facilitates investigating holistically the characteristics of a real-life event. In addition, case study approach gives researchers the chance to make observations that might prove to be valuable to the research.

The proposed research method is a comparative case study research and will be conducted in two organisations from the public sector. The author has obtained ethics committee approval to interview a number of participants in each organisation, see appendix B. A comparative case study could be conducted on a single case indicated (Yin, 1984). However, the author argues that the rationale for that is when “the single case represents the critical case in testing a well formulated theory” (p. 47). (Flick, von Kardorff, Steinke, 2004, p. 147) stated that “the dimension of single case-comparative study represent one axis according to which the basic design of qualitative research may be classified”, the other axis follows the dimension of time to form a longitudinal study. In this research none of the selected companies meets Yin’s rationale. On the other hand, conducting a longitudinal case study is not feasible because of the limited time.

Data will be collected through the following methods: semi-structured interviews, document or archival records collection and diary recording. According to Collis & Hussey (2003) interviews and archival records are common data collection methods for case studies. Face-to-face interviews will be carried out with elected participants from the internal audit, IT audit, IT security and risk management, IT division manager, and business unit management. Relevant documents such as letters, agendas and administrative documents will be collected, when necessary and permissible. In addition, documents like organisation structure chart, policies and procedures, sample of audit report, incident report, and risk register will also be collected, when possible, to validate data gathered via the interviews.

The collected data will be filed into NVivo 8 software to conduct thematic analysis to find common themes. Further analysis will be conducted to identify any relations with the found themes-nodes. Coded data will be presented when possible with tables and diagrams.

1.4 STRUCTURE OF THESIS

The research thesis is planned to be structured in the following way: Chapter 2 is set to establish the literature review, where IT risk terms and definitions will be reviewed and established. IT risk management process will be examined and discussed, followed by a review of relevant frameworks, best practices, standards and IT risk models. Implementing IT control-based structured environments faces challenges that will be discussed as well as the set of related problems. The reported problems will be assessed to elect one of them to be the focus of the research.

Chapter 3 outlines the research methodology that the author derives from reviewing other similar research studies. Similar research will be explored and examined to identify any analogies with the research topic. Furthermore, aspects like the selected research method, industry selection and data reporting and presentation methods, will be examined to identify the justification for the selected method. Then, the research focus problem will be examined again to select a workable research question. In addition, research sub-question and set of hypotheses are to be devised to guide the author in finding answers to the research question. That leads to justifying the grounds for selecting the research method, which will be derived and reasoned. Part of the research method is to define the data collection methods and to propose analysis and reporting methods.

Chapter 4 is where the field work is reported, how the data was collected, any challenges the author might have faced and if any variations from the original plan occurred. Data will be coded and reported according to the proposed method described in Chapter 3. The analysis of findings will occur in Chapter 5.

In Chapter 5 a cross-case analysis will be conducted and reported. Data will be analysed to identify answers to the research sub-questions and to test the hypotheses devised in Chapter 3. At that stage an attempt will be made to answer the research question.

In Chapter 6 the research will be concluded with recommendations and suggestions for further research and related topics.

Chapter 2

Literature Review

2.0 INTRODUCTION

Risk has two aspects that can contribute either positively or negatively to an organisation: cost and benefit. 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 & Fischer (2010, para. 9) stated that “To grow, an enterprise must take risks”. In that view, risk represents value for business. Risk and value are two sides of the same coin”. Risk, however, needs to be analysed, identified, and managed to reduce its impact, which is the negative side of risk. On the other hand, Miccolis, et al. (2003, p. 9) stressed: “Risk is an essential part of any business. Properly managed, it drives growth and opportunity” and that is the positive side of risk. The focus of this research is on IT risk, and in particular the various IT control frameworks (including best practice and standards) that are advocated for treating risk. The positive and negative aspects of risk are evaluated throughout this chapter in order to develop management perspective on the best use of risk to generate optimal business value.

In this chapter, a literature review is performed using online databases or journals and conferences papers in addition to industry publication. The searches were conducted following a thematic approach, where a set key word (IT risk, risk management, business value, IT value, control framework) was used to select the readings. The search results were rated and filtered out based on recognised authors and reputed organisations in the field. This chapter is structured as follows: section 2.1 reviews IT risk management. Section 2.2 reviews risk frameworks, including IT Risk Management frameworks from Information Systems Audit and Control Association (ISACA) and standards from International Standards Organisation ISO and other organisations. Section 2.3 includes review of IT control frameworks and best practices, which examines IT

Control frameworks for example Control OBjectives for Information and related Technology (COBIT), Value IT (ValIT) and Information Technology Infrastructure Library (ITIL). Section 2.4 reviews compliance regulation Sarbanes-Oxley (SOX) and industry standards Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPPA). To manage risk optimally, business and technology challenges must be assessed. These points are reviewed in section 2.5. Section 2.6 identifies business value, and examines the business perspectives of managing risk in a structured environment and how compliant structures would add business value to the organisation. Section 2.7 explores the problems that were identified in the preceding sections and summarises the issues, challenges, and the associated risk. A final section concludes Chapter 2 and provides the link to Chapter 3.

2.1 IT RISK MANAGEMENT OVERVIEW

IT systems have become business enablers. Like any business activity, IT systems are susceptible to risk, which materialises when a threat exploits vulnerability. IT risk exists, as business risk does, within the asset and/or the processes that utilise and impact a number of assets. Once the risk is identified and evaluated it has to be treated. Risk Management is “the process of discovering and assessing the risks to an organisation’s operations and determining how those risks can be controlled or mitigated” (Whitman & Mattord, 2004, p. 287). 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.

This section is structured as follows: sub-section 2.1.1 examines risk governance, sub-section 2.1.2 discusses IT risk, and sub-section 2.1.3 details IT risk management process.

2.1.1 Risk Governance

In many organisations, IT risk management has become the core function of the IT security management (Whitman & Mattord, 2004, p. 320). While managing IT risk addresses the technical aspects of IT systems from IT security point of view, risks of other natures have to be identified by the respective activity manager:

project management, change management, research and development (R&D) and quality assurance (QA). To ensure effective outcomes of the risk management process, objectives of the risk management process need to be aligned with business objectives (Ames, 2007). Risk management governance structure is required to be established. The structure is to be an integral part of ITG, which in turn is an integral part of enterprise governance according to the definition of ITG stated by Brand & Boonen (2005). Risk governance defines policies and procedures, determines the organisation’s risk appetite and risk tolerance, and identifies roles and responsibilities. In addition, risk governance determines the periodic review and reporting at the frequency to ensure effective and efficient risk management process.

2.1.1.1 Risk Appetite and Risk Tolerance

According to Whitman & Mattord (2004, p. 340) risk appetite is the quantity and nature of risk that an organisation is willing to accept. 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 (Risk IT Practitioner guide, ISACA, 2009). Risk appetite is translated into standards and policies used to manage the risk level within the limits set by the risk appetite.

Risk Tolerance, on the other hand, is the permissible deviation from the level set by the risk appetite. 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 so long the overall risk has not exceeded the risk appetite.

Setting Risk Appetite at the enterprise level helps organisations to manage risk in a defined and methodical way. On the other hand, defining Risk Tolerance adds the agility attribute to the organisation’s capability and gives a needed and controlled flexibility should a business opportunity arise (RiskIT Practitioner guide, ISACA, 2009).

2.1.1.2 Roles and Responsibilities

In the Certified Information Security Manager (CISM) manual, ISACA (2007) it was indicated that information risk management is an integral part of security governance, which would be part of the enterprise IT governance structure. Roles and responsibilities for managing IT risk should be clearly identified at the enterprise level to ensure required activities are conducted according to the devised plans (CISM manual, ISACA, 2007, p. 79). RiskIT framework from ISACA, (2009) outlines comprehensively the overall IT risk management roles and responsibilities. Accountability as well as risk ownership should be assigned and communicated to the respective stakeholders (Shortreed, 2008, p. 13). On other hand, Whitman & Mattord (2004, p. 320) argued that IT risk management is part of the information security manager responsibilities. However, their statement refers to IT security risk rather than overall IT risk. While managing information security risk is vital due to its complexity and impact, other IT risk components that reside across the enterprise activities require senior management involvement to provide adequate resources.

2.1.1.3 Documentation

It is indicated in the CISM manual (ISACA, 2007, p.96) that at the enterprise level, it is important to establish a documentation process to record and update all risk relevant documents, such as: policies and procedures, roles and responsibilities, compliance and regulatory requirements. As for the risk management process, traceable records are required to be created to record outcomes of different stages (Shortreed, 2008, p. 7). Risk register, vulnerabilities and threats list, assets and their corresponding business values are among the documents that are required to be current and to represent correct values in relation to what they denote. Treatment plans with different controls types and a corresponding feasibility analysis are another set of documents an effective risk management would have (CISM manual, ISACA, 2007, p.96). Some commercial software applications might be used to ensure consistency and easy access to the risk related documents. All documents should be classified according to their contents, with appropriate documentation control put in place to ensure authorised level of access as well as ownership are applied adequately.

2.1.2 IT Risk

The focus of this research is on IT risk. Whitman & Mattord (2004, p. 321) stated 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. Furthermore, they define the four perspectives as Availability – for keeping business processes and information flowing, Access – for ensuring systems and information are accessible, Accuracy – for providing timely and complete information, and Agility – to have the ability to adapt to changes within budgeted time and cost. Ames (2007) argued that it is vital to coordinate IT risk management activities with the whole enterprise risk management. Managing risk in such a fashion ensures optimum results by avoiding activity silos and overlapping resources.

The way IT systems enable business and influence its activities leads to a few categories for IT risk as follows: IT benefit/value enablement risk, IT program and project delivery risk and IT operation and service delivery risk (Risk IT Framework, ISACA, 2009, p. 11). The operational risk seems to be the most challenging, as it frequently takes place, as shown in survey outcomes cited in (Miccolis, et al, 2003).

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, as the latter might not be cost-effective. On the other hand, because no organisation can build all hardware and software it needs, a great deal of attention is required to understand the dependency of all those systems, where most of IT risk issues reside (RiskIT Framework, ISACA, 2009, p. 11).

2.1.3 IT Risk Management Process

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). The Risk management task is depicted as a process in Figure 2.1; 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 2.1, with all the risk management process stages mentioned, as it will be re-visited once risk management frameworks are examined. In addition, the 'Monitor and Review' activity inter-relates with all process stages in a similar fashion as 'Document and Consult' stage does, and feeds back into the beginning of the process, which is the 'Establish the Context' activity. Conducting 'Monitor and Review' in such a fashion is crucial for ensuring the risk management process is continuous and dynamic and responds to changing threats and vulnerabilities in a timely fashion (CISM manual, ISACA, 2007, p. 81).

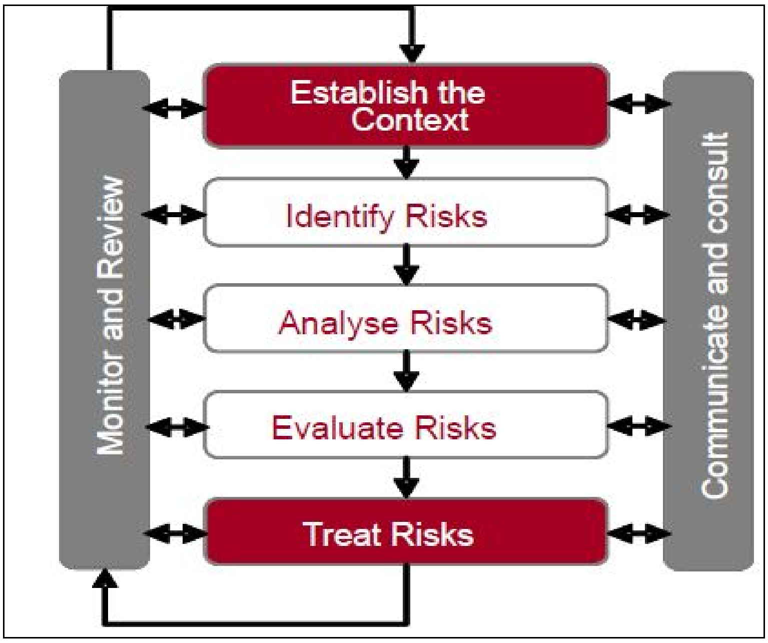


Figure 2.1: Risk Management Process. (Shortreed, 2008, p. 5)

An organisation must have the capability and ability to detect and respond in a timely fashion to risk when it occurs. An effective risk management program, however, is complex and encompasses the entire organisation (CISM manual, ISACA, 2007, p. 77).

2.1.3.1 Establish the Context

To assess IT risk, it is required to establish the context, be it internal or external, in relation to the business objectives. Establishing the context would have to be achieved by working through the business' objectives via means that would be established as part of the overall corporate governance. Once the context is defined, Risk Criteria need to be identified. Risk criteria identification is another task for the senior management to conduct, utilising the risk context attributes (Shortreed, 2008, p. 20). Risk criteria are used at the risk evaluation stage.

2.1.3.2 Identify Risks

Risk has to be identified by listing IT assets, including people, procedure, data and information, software, hardware, and networking elements (Whitman & Mattord, 2004, p. 290). It is vital to establish the asset business value. For that purpose, it is imperative to classify data sources: Customer, Corporate, Operational, and Third Party. Each category can be sub-classified into Confidential, Sensitive, and Public (TechTarget-ebook GRC, n.d.). Along with the IT assets inventory, Threat Identification and Vulnerability Assessment have to be conducted to identify the associated vulnerabilities and possible threats for each asset as stated by Whitman & Mattord (2004). The authors added that it is imperative to state that a vulnerability that is not associated with a threat poses no risk. As an outcome of this stage a document that lists assets and their corresponding vulnerabilities and threats, could be produced to be used in the following stage namely analyse risks.

2.1.3.3 Analyse Risks

Once assets, vulnerabilities and possible threats are identified along with the likelihood of exploiting the vulnerability and the expected impact, then risks could be estimated. To determine the likelihood and impact factors, data could be collated from respective stakeholders, relevant records from an incident management system and experienced staff in risk management (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 (CISM manual, ISACA, 2007, p. 77). Once risks are identified as well as the impacting factors, risks can be evaluated and prioritised.

2.1.3.4 Evaluate Risks

The outcomes of the Risk Analysis stage are compared to the risk criteria that have been set previously, to conclude whether the risk and its magnitude is acceptable or requires further treatment. Risks are evaluated in either qualitative or quantitative terms (Ames, 2007). Qualitative estimate is subjective and based on judgment, intuition and experience. On the other hand, quantitative analysis provides monetary value for risks. However, that's proved to be more difficult to calculate, because risk analysis is largely subjective (CISM manual, ISACA, 2007, p. 77). Risks that need treatment will be prioritised according to their impacts on the business that have been determined in the risk analysis stage.

2.1.3.5 Treat Risks

A risk treatment plan should be devised based on cost effective analysis that has been performed in the previous stages. The management, taking into account business objectives, decides how to proceed with the risk treatment plan. Whitman & Mattord (2004, p. 321) indicated that there are four categories of risk treatments. The first category is Acceptance - when the risk impact is considered within the risk tolerance and/or the mitigating measures are not cost-effective or feasible to implement. Then the business would accept the risk, if it materialises. The other risk treatment category is Mitigation – when the risk impact is intolerable, and there are feasible and cost-effective controls to implement. Mitigating controls are devised and applied to contain the risk impact and reduce it to an acceptable level. Avoidance or Eliminating is another category, where the risk is treated by disposing the asset or terminating the process altogether, thus eliminating the noted risk. The last category of risk treatment is Transference – where risk responsibility is shifted to a third party, for example purchasing an insurance policy to cover the cost should a risk materialise.

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 the type of controls to select and implement.

When risk control is devised a further analysis is instigated to assess the residual risk (CISM manual, ISACA, 2007, p. 88). The residual risk or the retained risk could be traced to many sources. It can be defined as the control-risk that has been devised in the treatment plan (Shortreed, 2008, p. 20). In addition, factors like undetected risk and uncertainty in risk evaluation could contribute to the residual risk (RiskIT Framework, ISACA, 2009). Further analysis is required to determine whether the residual risk exceeds the business risk tolerance threshold.

Further risk analysis might be warranted and more stringing measures could be applied until the remaining risk becomes tolerable. 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, p. 341).

4.1.3.6 Monitor and Review Risks

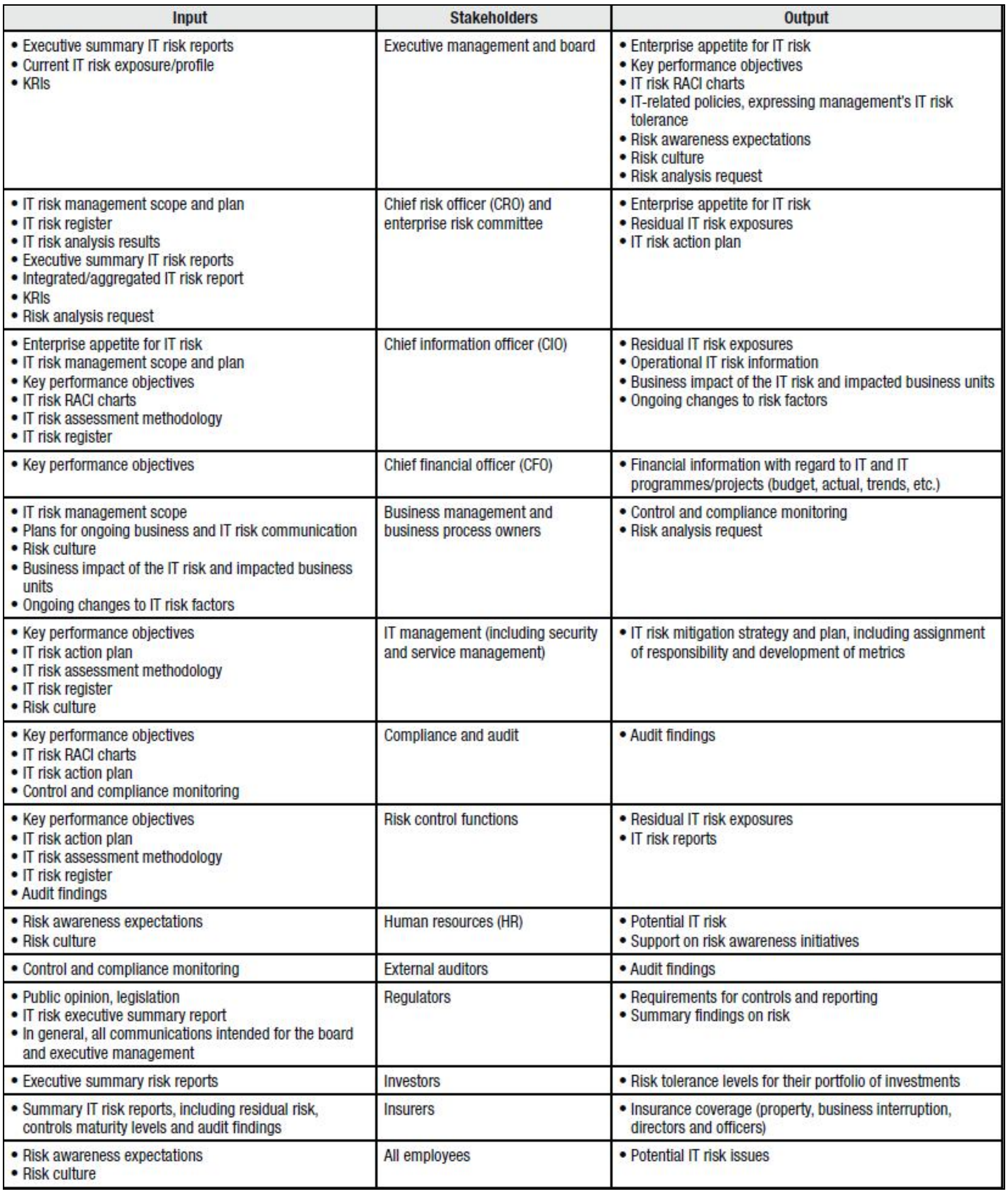
Business contexts, both internal and external, are subject to change and accordingly the risk profile also changes. New assets could be introduced, and their business value and impact need to be evaluated and included in the risk assessment. In addition, vulnerabilities and associated threats evolve 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 their effectiveness and efficiency. An essential attribute of risk management process is continuous improvement (Shortreed, 2008). To achieve that, periodic and ad-hoc reviews are required to be conducted by respective personnel as per the policy devised at the enterprise level (CISM manual, ISACA, 2007, p. 96). The ongoing revision is required to avoid common risk management pitfalls such as either overlook or overspend. (CISM manual, ISACA, 2007) indicated that Monitor and Review process ensures that management action plans remain relevant and updated.

It is paramount to coordinate IT risk management with other functions in the organisation, for example internal and external audit to ensure regular checks on the devised controls and advice on mitigating measures. While the audit cycles are not conducted more often due to its cost and purpose and the fact that they are done for the whole organisation. Event-driven revisions for corresponding risk of smaller scale changes (for example replacing or adding a new server, application, or process) could be conducted and the risk profile should be updated accordingly. The corresponding risk of those changes could be evaluated through other functions, for example change and configuration management, project management, and asset management. In similar fashion, indications or triggers from help desk and incident management could be fed and analysed by the risk management team to ensure timely responses are issued as required.

2.1.3.7 Communicate and Consult

As noted in Figure 2.1 the ‘Communicate and Consult’ process exists within all the stages of the Risk Management process. Kouns & Minoli (2007, p. 133) argued 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 & O`Driscoll (2002) indicated that consulting stakeholders helps increase participants understanding of their processes and potential risk exposure. Different messages are sent interactively at different stages to ensure mutual understanding and agreed upon devised actions.

Table 2.1:Risk Communication Flow. (Risk IT Framework, ISACA, 2009, p. 21)



Input	Stakeholders	Output
• Executive summary IT risk reports • Current IT risk exposure/profile • KRIs	Executive management and board	• Enterprise appetite for IT risk • Key performance objectives • IT risk RACI charts • IT-related policies, expressing management's IT risk tolerance • Risk awareness expectations • Risk culture • Risk analysis request
• IT risk management scope and plan • IT risk register • IT risk analysis results • Executive summary IT risk reports • Integrated/aggregated IT risk report • KRIs • Risk analysis request	Chief risk officer (CRO) and enterprise risk committee	• Enterprise appetite for IT risk • Residual IT risk exposures • IT risk action plan
• Enterprise appetite for IT risk • IT risk management scope and plan • Key performance objectives • IT risk RACI charts • IT risk assessment methodology • IT risk register	Chief information officer (CIO)	• Residual IT risk exposures • Operational IT risk information • Business impact of the IT risk and impacted business units • Ongoing changes to risk factors
• Key performance objectives	Chief financial officer (CFO)	• Financial information with regard to IT and IT programmes/projects (budget, actual, trends, etc.)
• IT risk management scope • Plans for ongoing business and IT risk communication • Risk culture • Business impact of the IT risk and impacted business units • Ongoing changes to IT risk factors	Business management and business process owners	• Control and compliance monitoring • Risk analysis request
• Key performance objectives • IT risk action plan • IT risk assessment methodology • IT risk register • Risk culture	IT management (including security and service management)	• IT risk mitigation strategy and plan, including assignment of responsibility and development of metrics
• Key performance objectives • IT risk RACI charts • IT risk action plan • Control and compliance monitoring	Compliance and audit	• Audit findings
• Key performance objectives • IT risk action plan • IT risk assessment methodology • IT risk register • Audit findings	Risk control functions	• Residual IT risk exposures • IT risk reports
• Risk awareness expectations • Risk culture	Human resources (HR)	• Potential IT risk • Support on risk awareness initiatives
• Control and compliance monitoring	External auditors	• Audit findings
• Public opinion, legislation • IT risk executive summary report • In general, all communications intended for the board and executive management	Regulators	• Requirements for controls and reporting • Summary findings on risk
• Executive summary risk reports	Investors	• Risk tolerance levels for their portfolio of investments
• Summary IT risk reports, including residual risk, controls maturity levels and audit findings	Insurers	• Insurance coverage (property, business interruption, directors and officers)
• Risk awareness expectations • Risk culture	All employees	• Potential IT risk issues

CISM manual, ISACA (2007, p. 96) stated that when risk treatment plans are devised, it is vital to communicate the outcomes to all concerned parties. Depending on the designed controls an awareness program could be designed and conducted to ensure target audience understanding. In RiskIT framework from ISACA (2009) a comprehensive risk communication flows have been provided as outlined in Table 2.1.

2.2 REVIEW OF RISK FRAMEWORKS

Risk management frameworks based on ISO-31000 and ISO-27001/2/5 standards or organisations like ISACA and National Institute of Standard and Technology (NIST) help organisations build a systematic risk management process.

> "risk management framework is 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" (Shortreed, 2008, p.5) .

This section is structured as follows: sub-section 2.2.1 describes the standards and guidelines from the International Organisation for Standardisation (ISO), while sub-section 2.2.2 explores Risk IT framework from ISACA, and sub-section 2.2.3 outlines some methods devised by other organisations.

2.2.1 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 section is on a selection of the ISO published standards and guidelines for managing risk. Implementation of risk management framework is based on ISO-31000 and ISO-27001/2 standards.

2.2.1.1 AS/NZS ISO 31000:2009

AS/NZS ISO 3100:2009 - Risk management – Principles and guidelines, that have superseded AS/NZS 4360:2004, risk management standard. According to Shortreed (2008) the guidelines consist of 11 principles and 5 attributes of excellence, and they are objectives driven within context by risk criteria. Cusack (2010, p. 43) cited saying "This standard is the parent of all risk based standards". Cusack further indicated 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 to IT systems and align that to business objectives, context, and risk in other business areas (Kouns & Minoli, 2007, p. 92). According to Cusack (2010) within the guidelines there is an Annex that details the attributes of enhanced risk management along with the relation of risk and Governance structure.

2.2.1.2 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.

2.2.1.3 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, p. 78; Cusack, 2010, p. 42). The standard consists of a set of mandatory sections and every organisation seeking accreditation to ISO-27001 standard, must comply with them. In addition, there are optional sections that could be tailored to the organisation's context to ensure optimum security management is in place. Risk management elements are included in the mandatory sections to ensure risk is identified, analysed and treated and continuously monitored (Audit course, BSI, 2009). ISO 27001 incorporates Deming's Plan-Do-Check-Act cycle (Kouns, Minoli, 2007, p. 79) to ensure continuous improvement of the effectiveness of the risk based devised controls.

2.2.1.4 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, p. 78; Cusack, 2010, p. 42). 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 (2007) indicated that devised controls in ISO 27002 need to be tailored to the organisation's specific context and structure and in particular around identifying accountabilities.

2.2.2 Risk IT

RiskIT is the most recent framework released by ISACA (2009), which addresses IT risk management in a holistic manner. RiskIT framework leverage the activities, controls and processes related to risk 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, and each domain contains three processes. RiskIT framework is part of ISACA product on IT governance (RiskIT Framework, ISACA, 2009).

2.2.3 Others

Institutions such as the National Institute of Standard and Technology (NIST) and Software Engineering Institute (SEI) at Carnegie Mellon University, as indicated by Albert and Dorofee (as cited in Whitman & Mattord, 2004, p. 345), have developed risk management methodologies that have been adapted by many organisations.

2.2.3.1 Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

OCTAVE is IT security risk evaluation methodology that aids organisations to define and treat IT security risk based on cost effective analysis. The methodology was developed by SEI. Albert and Dorofee (as cited in Whitman & Mattord, 2004, p. 345) stated that "OCTAVE method defines the essential components of a comprehensive, systematic, context-driven, self-directed information security risk evaluation". The method is described as self-directed, where a business unit and IT work together in small teams to identify and address security requirements. Flexibility is another attribute of OCTAVE that allows the method to be aligned with the business unique risk environment. Evolved is the last attribute that transfers the organisation operation into a risk-based view of security within business and technology context. (Carnegie Mellon University, Software Engineering Institute, n.d.)

2.2.3.2 National Institute of Standard and Technology (NIST) Special Publication (SP) 800-30

NIST SP 800-30 is a risk management guide for information technology published in July 2002 that specifically addresses the integration of risk management into the System Development Life Cycle (SDLC) (Futcher & von Solms, 2008). The publication-guide is to help organisations build effective risk management program. The guide is structured to provide an overview of roles and responsibilities of risk management process activities within the organisation. The conventional risk management process stages are outlined in the guide: risk analysis, evaluation and treatment. In addition to that the guide discusses the good practice and stresses on the need to establish ongoing risk evaluation to ensure the effectiveness of the risk management program (NIST, 2002).

2.3 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 not an unusual scenario where risk profile is not up-to-date that could lead to organisations have a false sense of assurance about their IT systems readiness. With invalid risk profile, the probability for the management to make ill-fated decisions would become 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 COBIT, Val IT, Microsoft Operations Framework (MOF) (Voon & Salido, 2009). In addition, known best practices like ITIL have been adapted to complement the COBIT-Val IT based structure. In the 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 2.3.1, 2.3.2 and 2.3.3 examine Val IT, Control Objectives for Information and related Technology (COBIT) and IT Infrastructure Library (ITIL), respectively.

2.3.1 Val IT

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 (Val IT Brochure, ISACA, 2009). According to Haes and Van Grembergen (2005, p. 183) Val IT framework "starts from the premise that value creation out of IT investment is a business responsibility in the first place". IT investments are about enabling business change and if managed properly, can bring enormous returns. Thorp (as cited in Val IT Overview, ISACA, 2009) indicated, 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) described Val IT as a complementary to COBIT and it follows the same structure and templates.

2.3.2 Control Objectives for Information and Related Technology (COBIT)

COBIT 4.1 is a framework for IT Governance developed by ITGI, 1996. COBIT, was initially developed as an IT audit framework, and has evolved to become IT Governance framework at version 4.1. A new version 5.0 is anticipated to be released in 2011 that combines COBIT, Val IT, and Risk IT. COBIT 4.1 comprises 34 processes structured in 4 domains: Plan and Organisation, Acquisition and Implementation, Delivery and Support, and Monitoring. Some of COBIT activities provide the "means" to facilitate risk management process (Risk IT Framework, ISACA, 2009), 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. 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 strategic, project, and, to some extent, operational levels.

Processes within the Monitor and Evaluate (ME) domain play big role in ensuring risk management effectiveness and relevancy as noted by Brand & Boonen (2005). COBIT helps in conducting Audit review at low cost with better value. COBIT helps in collaborating with other frameworks and/or best practices like Val IT, ITIL and ISO 27001/2 to achieve optimum risk management process objectives, as part of the whole IT governance objectives (Kouns & Minoli, 2007, p. 182).

2.3.3 IT Infrastructure Library (ITIL)

ITIL offers a systematic approach to the delivery of quality IT services (Jong, et al., 2009). ITIL helps in identifying risk implied in the service portfolio that consists of the list of services and underline 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 can help in identifying threats and analysing their impact and frequency of occurrences (Kouns, Minoli, 2007, p. 348). In addition, change and release management help in identifying vulnerabilities and corresponding threats and thence rectifying them at the design and implementation level. 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 or operational.

2.4 REVIEW OF COMPLIANCE

The increasing cases of financial fraud (Singleton, 2007), identity theft, and data leak resulted from intentional actions or out of negligence targeted IT systems and the hosted data. In addition, the vital role IT systems play in enabling businesses to be sustainable and resilient, as well as the increasing complexity of those systems have pressured governments and industrial agencies to enact or regulate acts and standards for organisations to comply with.

The section is structured as follows: sub-section 2.4.1 explores Payment Card Industry (PCI), while sub-section 2.4.2 examines Sarbanes-Oxley (SOX), and sub-section 2.4.3 discusses Health Insurance Portability and Accountability Act (HIPAA).

2.4.1 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. 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. PCI set of standards continue to evolve to accommodate changing and evolving technologies and their associated risks. For example PCI DSS wireless guideline is information supplement from PCI security standards council. While PCI covers IT systems hardware and software that process, store or transmit payment card data (Woda, 2007). However, North, et al. (2009) argue that the PCI standard perhaps is the best example of why meeting the compliance requirements at the design-level of the development cycle is becoming increasingly important, as that would reduce the overall compliance program cost.

2.4.2 Sarbanes- Oxley (SOX)

US-Congress passed the SOX Act in July of 2002 as part of an attempt to give the Securities and Exchange Commission more tools for the regulation of financial companies. 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). In addition, the reporting must also include an attestation by an external auditor or management's internal control assessment. SOX Act is mandatory for all organisations listed on NY Stock Exchange in the United States, and is overseen by the Public Company Accounting Oversight Board (PCAOB). Singleton (2007) indicated that many organisations started to adapt SOX even though they are not required to comply.

2.4.3 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 and environment 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, et al., 2007). HIPAA 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) indicated that the Healthcare industry is unique in storing and distributing health records among primary care and to specialised clinics and other health care and possibly insurance providers. That requires efficient data sharing systems to ensure patient privacy and legitimate claims processing. To comply with HIPAA, organisations must monitor their IT systems and the data they host and also must perform regular assessment to comply with the act requirements (Damore, 2009, n.p.).

2.5 BUSINESS CHALLENGES

Part of the Business Impact Analysis (BIA) asset business value is evaluated, which has a vital effect on quantifying and prioritising risks. An adequate BIA requires business inputs to be channelled via established means to ensure validity. On the other hand, factors like business dynamics and continually changing technology make it imperative to respond to these changes. The response has to be done in a timely fashion to ensure the devised risk treatment plan is effective and efficient. Responding in that manner comes certainly at a cost as noted in the CISM manual: “Experience shows that it [risk management program] can become a time-consuming task with cost implications” (ISACA, 2007, p. 77).

This section is structured as follows: sub-section 2.5.1 explores business changes, while sub-section 2.5.2 discusses technology changes, and sub-section 2.5.3 examines regulatory demands.

2.5.1 Business Changes

Business dynamics imply changes caused by different events, internal and external, and at all levels. High performing organisations strive to anticipate possible changes to some degree. Subsequently, the anticipated changes are incorporated in their strategic plans. However, there is always an element of uncertainty that entails risk, be it in the forecasting or at the planning stages. The sub-section consists of sub-sections 2.5.1.1, 2.5.1.2, and 2.5.1.3 that respectively examine: outsourcing, expansion, and globalisation.

2.5.1.1 Outsourcing

Outsourcing is an option to which businesses resort for different reasons. Common reasons are to reduce the cost and also that when needed expertise is not available locally. Although organisations could outsource a task or a service to a third-party, they are concerned about the gained value and risk involved in signing in their IT systems to a third-party (Weerakkody & Irani, 2010). Contracts and service level agreements (SLA) help in regulating and managing outsourcing. However, Huang & Goo (2009) indicated that SLAs without proper design could become either too limited or too cumbersome to manage. Organisations remain accountable for the quality of the products, services and the security of the IT systems as indicated in (CISM manual, ISACA, 2007, p. 144). Benvenuto & Brand (2005, p. 31) stated that “organisations must establish ways to manage and control their outsourced functions and processes”. The challenge remains that businesses have to incorporate vendor associated risk into the overall risk, argued Benvenuto and Brand (2004). It can be inferred that without a structured environment the risk within outsourcing could quite possibly become unmanageable.

2.5.1.2 Expansion

Business expansion is an example where positive risk resides. Organisations strive to expand their business and capture an opportunity that would add value to the organisation. Since the IT systems role has evolved to be a business enabler, it’s imperative to have the adequate capabilities and capacities that would facilitate the business enablement (Curry, et al., 2006, p. 7). Successful organisations tend to anticipate that in their strategic planning, and accordingly build the required capabilities. Strategic planning relies upon forecasting as noted by Dilworth (1992, p. 87). Organisations need to forecast future needs in order to avoid overspend or overlook when building their capacities, added Dilworth (1992, p. 87). While forecasting is vital to any organisation, it also has its own element of inaccuracy which carries uncertainty (Dilworth, 1992). Uncertainty implies risk as stated by (Shortreed, 2008, p. 5) that needs to be defined and managed.

2.5.1.3 Globalisation

Many organisations go beyond local borders, whether to expand or to outsource as noted in the previous two sections. Issues described in those sections would have greater visibility in cross-border business relations because there is a greater risk (both positive and negative) involved. In addition, understanding and complying with the regulatory requirements in different jurisdictions is quite a challenging task to achieve (Trivedi, 2007, p. 49). Countries have different legislations regarding all aspects of IT systems, for example information security and privacy. When an organisation expands beyond local borders, the risk management process-stages would have to be re-performed and adjusted to accommodate the changes and/or requirements the expansion might introduce.

2.5.2 Technology Changes

Emerging technologies are divers, for example Internet and web applications, Cloud computing, Mobility, and Virtual machines. New technologies are not commodities and they could resolve many issues and introduce endless business opportunities. However, that comes at a cost as each technology comes with vulnerabilities and threats, if materialised they could put the business into jeopardy. The following sub-sections review the positive and negative risks of technology changes. Sub-sections 2.5.2.1, 2.5.2.2, 2.5.2.3 and 2.5.2.4 examine Internet, Cloud computing, Wireless and Virtual machine, respectively.

2.5.2.1 Internet and Web Technologies

Internet is a series of interconnected networks that allows data to flow across it. This large mesh allows users a nearly infinite ability to communicate between systems (White, et al., 2003, p. 185). The term World Wide Web (WWW) or the Web is used synonymously with the Internet, although the former is a set of services available via the Internet. The advancement in Web technologies has introduced immense business opportunities including the e-commerce which revolutionised the traditional commerce (Hu, 2009). The complexity and obscurity of how data travels across the Internet and how information is exchanged between many and different technologies has made the Internet and web applications a challenging area for professionals and businesses alike. Internet based attacks are constantly increasing in volume and complexity (Kouns, Minoli, 2007, p. 359). The role of e-commerce for many businesses grows to a strategic level, for example Internet banking in the finance industry (Ramakrishnan, 2001). With the size and types of risks related to the use of the Internet and Web technologies organisations are required to invest proportionally in managing those risks.

2.5.2.2 Wireless and Mobile Computing

Wireless networks are changing the computing world and creating substantial business opportunities (Kennedy, 2004). Wireless technologies empower users with easier and greater access to data at reduced cost; however, their convenient usage comes at a cost, as stated by Kennedy (2004). Wireless technologies bring additional security concerns (White, et al., 2003, p. 164). Some examples of those concerns are insufficient policies, rogue WAPs, traffic eavesdropping, insufficient network performance, and MAC spoofing. That implies risks that need to be identified and treated (Kennedy, 2004).

On the other hand, devices like PDAs, cellular phones and BlackBerrys are other forms of wireless technology with increasing computing power that can perform significant business functions (Stanley, 2004). When these devices are connected to the network for Internet and Email access and/or data synchronisation, their implied risk has to be added to the risk profile (White, et al., 2003, p. 171). (Stanley, 2004) indicated that wireless high technical complexity is considered a big challenge that needs to be addressed at all levels, (e.g. defining usage policy, encrypting data) to continually monitor their access and traffic.

2.5.2.3 Virtual Machines

The advent of virtual machine has made a big impact on the computing power and cost. At the desktop level, it helps to reduce the cost of hardware at the development and testing phases, while at the server level, virtualisation utilises the hardware efficiently. That has immensely reduced the cost of data centres that enabled many organisations to change their way of managing system and data backups (Raval, 2010). However, those low-cost data centres have another source of cost as stated in Virtual Data-Centre e-Book from Tech-Target (2009). While the security of traditional physical data-centres is mature, the security of virtual data-centres is not. Virtualisation increases the technical complexity of IT systems and how data is stored and/or replicated. Virtualisation has hidden security issues both at desktop and at server level. Vulnerabilities and types of threats for both should be identified and the risks need to be profiled accordingly as pointed out in Virtual-Data-Centre e-Book from Tech-Target (2009).

2.5.2.4 Cloud Computing

The advent of virtualisation and advancement of Web applications increased the use of the Web in various ways and the data size that has been transferred and processed (Raval, 2010). As virtualisation matured, the drive to virtualised applications, services, platforms and infrastructure emerged. Cloud computing, is a concept that denotes a network of hardware, software and knowledge (Raval, 2010). On the other hand, demand for Software as Service (SaaS) has grown exponentially, added Raval (2010). That has been the drive for public cloud computing. Cloud computing brings opportunities as well as risks some are known and existing, others are new. New risks in cloud computing could be related to data security and privacy, authentication, interfacing with internal systems, system availability, ownership of content and other legal requirements.

All types of risks are required to be incorporated within the overall risk profile and managed accordingly and that surely adds to the level of complexity when it comes to analyse, evaluate and treat risk.

2.5.3 Regulatory Demands

The first stage in Risk Management process is establishing risk context (see sub-section 2.1.3.1). Part of the risk context are the regulatory requirements (Whitman & Mattord, 2004), that come in a form of standards or compliance systems. The drive for regulatory demands could come from different sources: Political, Industry, and Market, as explained in the following sub-sections 2.5.3.1, 2.5.3.2 and 2.5.3.3.

2.5.3.1 Political Drive

Changes in governments could lead to drastic changes in the economy. For example, governments that tend to privatise public sector companies would force organisations to change their strategic plans and goals (Curry, et al., 2006). Subsequently, policies concerning data retention and data disposal could be mandated and organisations would have to comply with them. On the other hand, some events like the Enron and WorldCom scandals in 2001, led the US-Government to introduce and mandate Sarbanes-Oxley (SOX), see section 2.4.2. In addition to Enron and WorldCom cases that led to SOX the recent economic recession has put immense pressure on governments to impose more regulations in order to ensure healthy finance systems (Grover, 2009, n.p.). Singleton (2007, pp. 9-11) stressed that “The impact of the new standards could potentially change financial audit plans and processes significantly”. In similar fashion, risk context would need to be re-assessed to accommodate the new compliance requirements (Shortreed, 2008, p. 20).

2.5.3.2 Market Drive

Organisations opt to comply with some standards systems for marketing purposes. For example, in the finance industry BASEL II Accord is a standard system to ensure adequate capital for credit risk (Scott, 2005, p. 3). One of the biggest challenges to comply with BASEL II requirements is to ensure that the IT systems, where data are stored and processed, are adequately controlled. Another example is ISO-9001 Quality Management System. Organisations implement ISO-9001 standards in order to be accredited with those standards, to improve their reputation and marketability (Clifford, 2005, n.p.). As IT systems became business enablers, being compliant with ISO-9001 would require changes in the business processes and the related IT systems processes. This would eventually add to the complexity when identifying risk and business context.

2.5.3.3 Industry Drive

The increase of the technology complexity and attacks led Credit Card companies to introduce PCI-DDS compliance (see section 2.4.1.). Companies that process a certain number of credit card transactions are obliged to comply with PCI standards or face heavy fines should customer credit card details are compromised. Another example is HIPAA (see section 2.4.3), where health providers require protecting patients' information when it is stored or in transition from one system to another. There are more industry standards, for example: GAMP 5, which is designed for automated systems in the pharmaceutical industry (ISPE, 2008). Organisations might need to comply with a number of compliance systems to meet regulatory and industry standards, for example: PCI, SOX, ISO-27001, and GAMP 5. That would expand and possibly complicate the risk context, which in turn requires more resources and effort to manage the defined risk.

2.6 IDENTIFYING BUSINESS 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, 2007). Changes do happen, risks materialise for different reasons and at different levels as outlined in section 2.5. When the business management have confidence in their reliable, well considered and wisely budgeted for capacities and capabilities, 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, 2007). It was stated by Barnier & Fischer (2010, para. 9) that “To grow, an enterprise must take risks”. To realise the value of responding to the various demands, organisations should make a sound and informed decision (Whitman & Mattord, 2004). Stockman (1996, p. 535) argued that ”Under certain conditions, a rational guess is the expected value”. 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”.

This section explores the various perceptions of business value gained through managing IT risk in control-based structured environments. As discussed earlier, information systems role has evolved throughout the years to become a strategic and business enabler. Organisations have expanded and technologies have become too complicated and need to be managed to ensure the information systems are effective, efficient and secure. Information systems and associated risk can be managed through accumulated experience or by implementing well known frameworks and best practices, for example COBIT, Val IT, ITIL, and Risk IT. In this section it will be argued that by following the latter approach, managing information systems will bring far more benefits then if the accumulated experience approach was chosen in large organisations. On the other hand, implementing those frameworks and best practices might become cumbersome, costly and could become business inhibitor. However, if the implementation was based on risk assessment basis, then the devised controls should meet business objectives cost-effectively and on a timely fashion.

The section is structured as follows: sub-section 2.6.1 reviews IT systems roles and business value, while sub-section 2.6.2 examines IT risk/value within business context. Sub-section 2.6.3 discusses Business value of IT risk management standards and methods, and sub-section 2.6.4 discusses value in managing IT risk holistically.

2.6.1 IT Systems Role and Business Value

According to (Curry, et al., 2006, p. 7) the IT systems role has evolved from helping organisations to improve operational efficiency and increase management effectiveness, to improving competitiveness through strategic information systems. (Shin, 2003) argued that high business value is gained from the interwoven relationship and strategic alignment between IT systems and the various business divisions needs, as shown in Figure 2.2.

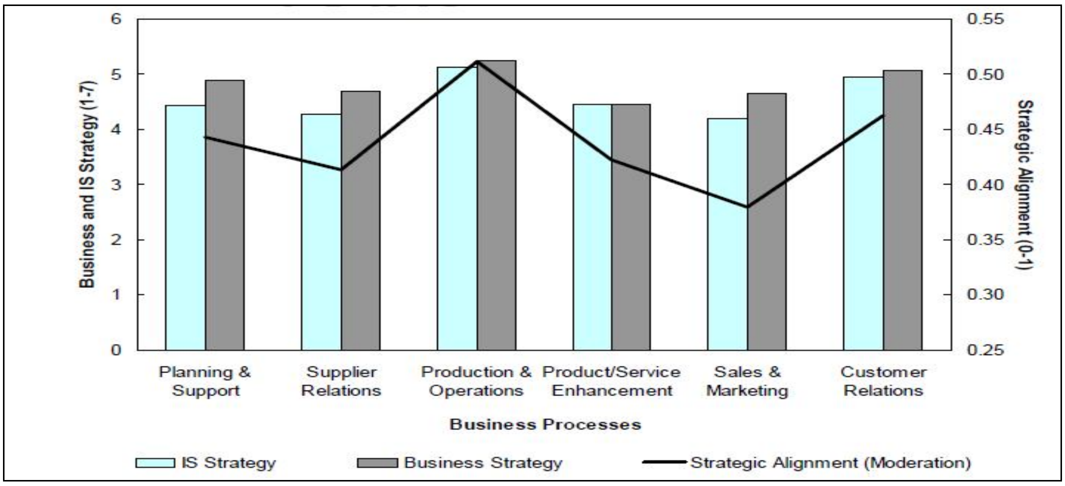


Figure 2.2: Relating the Strategic Alignment to Business and IS Strategy. (Shin, 2003, p. 13)

On the other hand Murphy (2002, p. 13) argued that IT value is gained from various business functions and divisions, as illustrated in figure 2.3. The figure indicates the “Ever changing Business context” and shows “Risk” as one of the “Pillars” a business is based on that ensures its existence. However, that doesn’t mean that 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.

As IT systems underpin all divisions’ activities, IT risk exists wherever IT systems are planned, implemented, operated and managed. Murphy (2002) encapsulates risk in Figure 2.3 in the dynamic of business action.

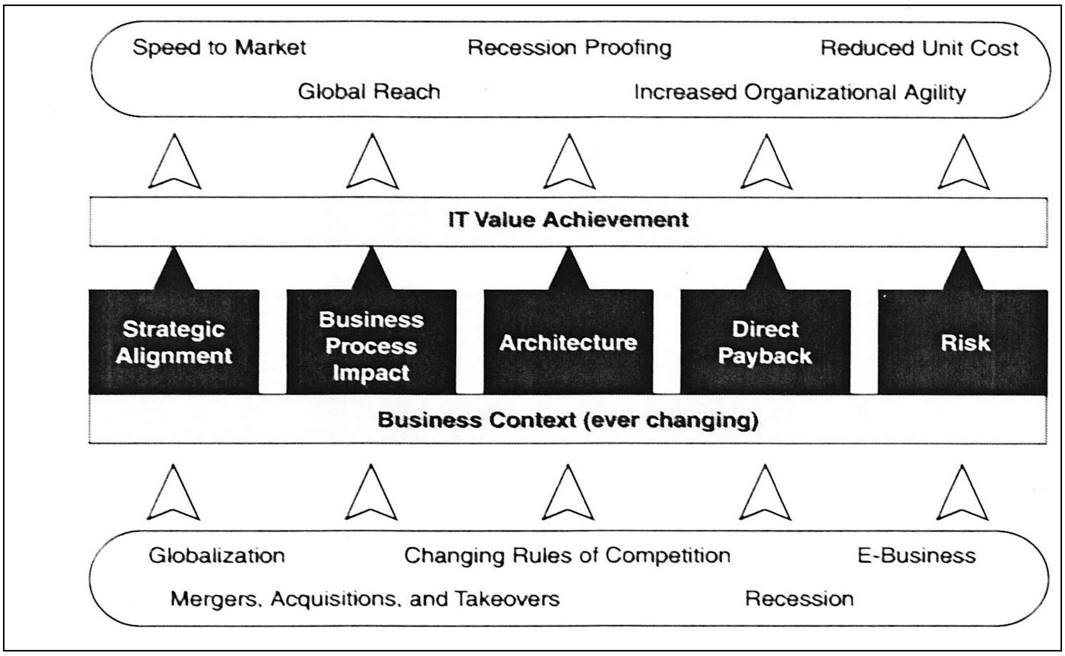


Figure 2.3: The Five Pillars of Benefits Realisation. (Murphy, 2002, p. 41)

2.6.2 IT Risk/Value within Business Context

Whitman & Mattord (2004) indicated that because IT is now readily available to everyone, all organisations have access to all technologies should they opt to use them. In other words, 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, p. 320) explained:

> “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”.

To retain their business, organisations must design, develop and maintain secure and reliable IT systems, added Whitman & Mattord (2004). 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, as noted in Figure 2.4 that shows the role of IT as value enabler.

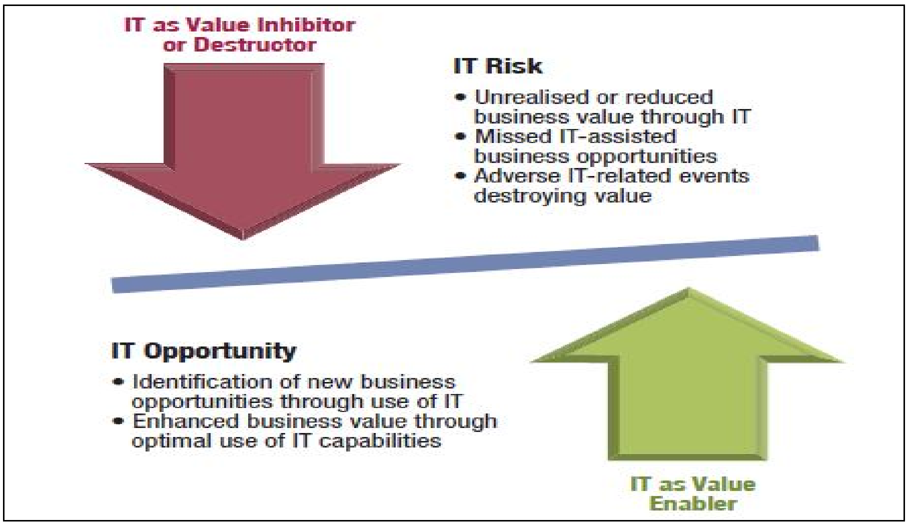

IT as Value Inhibitor or Destructor
IT Risk
• Unrealised or reduced business value through IT
• Missed IT-assisted business opportunities
• Adverse IT-related events destroying value
IT Opportunity
• Identification of new business opportunities through use of IT
• Enhanced business value through optimal use of IT capabilities
IT as Value Enabler

Figure 2.4: Risk and Opportunity. (Risk IT Framework, ISACA, 2009, p. 32)

At the enterprise level, as shown in figure 2.5, risk is categorised into the following: strategic risk, environmental risk, market risk, credit risk, operational risk and compliance risk. As IT has become business enabler, IT risk exists in all risk categories to various degrees, as depicted in figure 2.5 (Risk IT Framework, ISACA, 2009, p. 11).

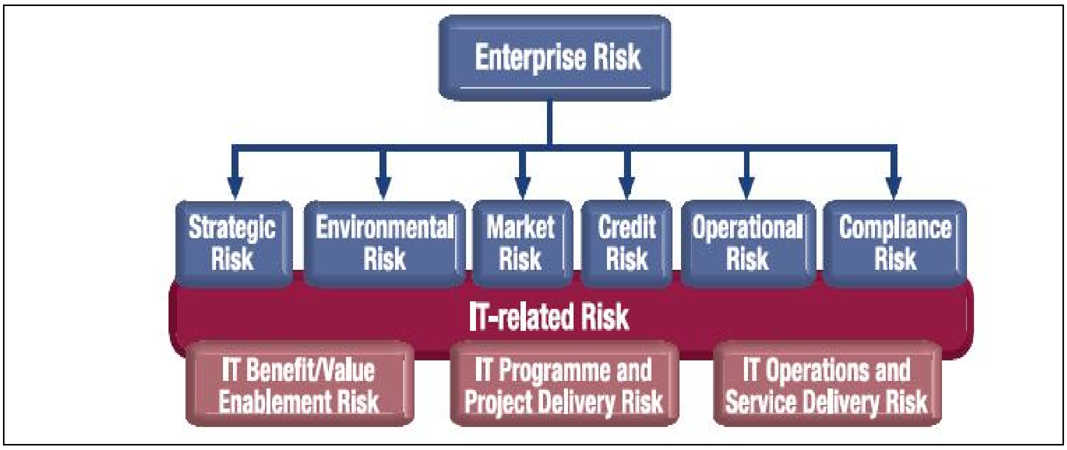


Figure 2.5: IT Risk in the Risk Hierarchy. (Risk IT Framework, ISACA, 2009, p. 11)

The way IT systems enable business and influence its activities lead 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 (RiskIT Framework, ISACA, 2009, p. 11). The operational risk seems to be the most challenging to address, as it frequently changes, as indicated in a survey outcomes cited by Miccolis, et al. (2003).

2.6.3 Business Value of IT Risk Management Standards and Methods

IT Risk management aspects were examined in section 2.1. Managing IT risk within business context requires considerable effort to accommodate many changing factors (Murphy, 2002, p. 41). Some organisations, for example ISO, NIST, SEI at Carnegie Mellon University, have developed and published standards and guidelines to manage risk in general or specifically to manage IT risk. Examples of those standards, as explored in sections 2.2.1 and 2.2.3, are ISO 31000, ISO 31010, ISO 27001, ISO 27002, OCTAVE and NIST SP 800-30. Those standards and methodologies provide efficient guidelines to ensure that IT risk is managed as part of the overall business risk management (Shortreed, 2008). In addition, Ramirez (2008) indicates that having a standardised methodology for risk management would allow practitioners to simplify their approach and provide mechanisms for continual improvement. However, to achieve that, immense time and effort would be required that could increase the cost of managing the risk to a level it becomes prohibitive (CISM manual, ISACA, 2007, p. 77).

One major obstacle for keeping the risk profile current is updating the risk profile when the corresponding elements change (Murphy, 2002). Examples for such changes are changes in assets inventory (software, hardware) changes in infrastructure and changes in business processes and the associated IT processes. Changes should be adopted in a timely fashion, and risk profile should be updated accordingly (Whitman & Mattord, 2004). However, to re-run the whole risk management process could be cost-prohibitive (Shortreed, 2008). At present, many organisations have implemented some forms of governance structures and/or program management to ensure strategic planning and compliance to various regulatory and business requirements (Pironti, 2006). Processes and activities of those structures and compliance programs could be leveraged to achieve objectives of compliance, IT risk and security management (Ames, 2007).

2.6.4 Value in Managing IT Risk Holistically

Organisations have to 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 2.6. The level of complexity caused by the number of interrelating factors creates a fundamental problem when attempting to analyse them for planning and managing purposes (Curry, et al., 2006, p. 97).

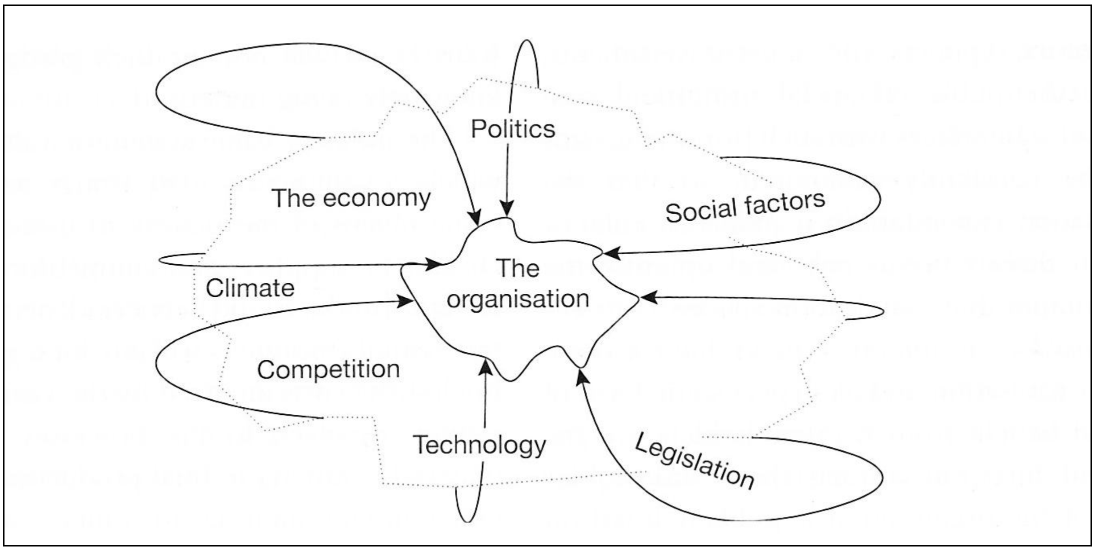


Figure 2.6: The Organisational Environment. (Curry, et al., 2006, p. 35)

System thinking as illustrated in figure 2.7 provides a powerful tool for modelling large complex problems in a logical and practical way (Curry, et al., 2006). While system approach doesn't guarantee the solution quality, it makes it possible to find such a solution as pointed out by Curry, et al. (2006). Richmond (1994) (cited in Curry, et al. (2006, p. 101)) stated that "Systems thinking is the art and science of making reliable inferences about behaviour by developing an increasingly deep understanding of the underlying structure". Applying Systems theory in analysing IT systems 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 effective IT risk management (Whitman & Mattord, 2004, p. 291).

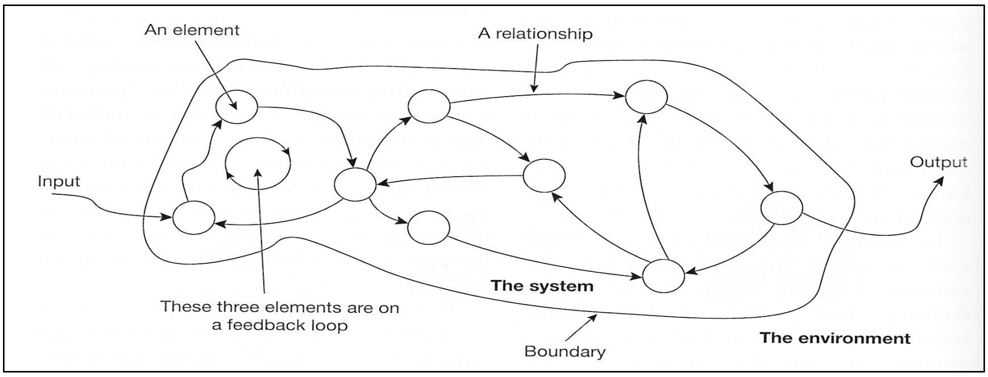


Figure 2.7: Presentation of a System. Cited in (Curry, et al., 2006, p. 100)

University of Southern California (USC), Marshal School of Business (MSB) formed the institute for Critical Information Infrastructure Protection (ICIIP) that researched and developed Systemic Security Management framework (Anderson, 2008). ISACA developed Business Model for Information Security (BMIS) (Anderson, 2008) and RiskIT framework based on the devised system (ISACA, RiskIT framework, 2009). One direct benefit of that 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 could be embedded within the enterprise culture (Doughty & O`Driscoll, 2002). Managing IT risk holistically would help in leveraging 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 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, awareness program. A framework that is implemented as an integral part of the enterprise IT governance structure (COBIT, Val IT, ITIL, RISK IT) would provide the holistic approach in managing IT risk (Fischer, 2008).

2.7 SUMMARY OF ISSUES AND PROBLEMS

Devising standards and best practices guidelines helps organisations and professionals in meeting business objectives. However, there are challenges and numbers of issues and problems when adopting these standards and guidelines.

In the first sub-section of this section a selection of issues and problems related to IT risk management and arising from the preceding sections, are summarised. In the second sub-section 2.7.2 specific and researchable issues and problems are examined.

2.7.1 List of Issues and Problems

For an organisation, implementing effective IT risk management framework is rewarding and costly at the same time. It was indicated in the (CISM manual, ISACA, 2007, p. 77) that establishing an effective IT risk management process could encompass the whole organisation, and could become extensive time-consuming that comes at a significant cost (see section 2.5). In embarking on implementing a risk management framework, executive management support is crucial (CISM manual, ISACA, 2007, p. 77). Huff, et al. (2004) pointed out the issue of IT attention deficit at the board level, attributing that to the lack of IT savvy board members. That could hinder the effort to gain support for strategic initiative of that kind. However, Huff, et al. (2004) suggested that within 5-10 years period a noticeable change in the board membership would eventuate. The same authors predicted that executives with more understanding of IT role would eventually tip the balance towards that.

Sections 2.1.3.2-4 explore 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 (Whitman & Mattord, 2004, p. 291). However, this is not a straightforward exercise, as certain errors are expected when applying best-judgment and experience. Furthermore, when analysing risk starting with vulnerability and threat assessment, an element of subjectivity is present that would affect the residual risk, which is retained within the asset indicated by Whitman & Mattord (2004). Followed that is the risk evaluation stage. There are two approaches to accomplish that: Qualitative, and Quantitative (CISM manual, ISACA, 2007, p. 77). The Qualitative approach is common, as it is easy to calculate (Whitman & Mattord, 2004). However, it is subjective as there will be different views in evaluating the risk. Since in business value is reflected in monetary figures (Ames, 2007), how could qualitative risk be presented in monetary terms? While risk practitioners have advised a more granular qualitative approach based on some estimation of likelihood and impact, the outcome remains subjective (Ames, 2007).

Implementing a current, effective, efficient and mature IT risk management faces a number of challenges, as outlined in section 2.5. Risk context changes over time for a number of reasons. Business and regulatory requirements change; new technologies are introduced and all this requires re-assessing the risk profile. As it was noted in sections 2.1.3.6-7, the adoption should be done in a timely fashion to ensure a true level of assurance. Establishing IT risk management process in control-based structured environments would generate new controls and processes. Newly created controls and processes would need to be communicated through an effective training program and ensure they are adhered to (CISM manual, ISACA, 2007, p. 77). Inadequately implemented or poorly communicated controls and processes, could be rejected by staff, which could cause delays and affect the outcomes quality (Curry, et al., 2006).

According to Ames (2007) a key measure for the effectiveness of an IT risk management framework is when risk awareness is embedded within the business culture. That would require educating staff and management through a well designed program undertaken by highly trained practitioners. Involving stakeholders through series of workshops would help in that regard, although that initially would consume resource and time (Doughty & O`Driscoll, 2002).

Frameworks, standards and best practices are subject to change, for example ITIL v.2 and v.3, Val IT v.1 and v.2, and COBIT, which has evolved from being an audit framework to a governance framework. Furthermore, COBIT v. 5.0, to be released in 2011, is expected to include COBIT 4.1, Val IT v.2, and Risk IT (ISACA, press release). In similar fashion, ISO 31000, 27000 series were preceded by another set of guidelines and are constantly updated to reflect relevant changes in their domain (Kouns & Minoli, 2007). Established framework or compliance structure would certainly need to be updated to adopt new changes. For example, when ISO 27001 was released it didn’t contain controls for wireless or RFID. Organisations would have to find relevant controls from other faculty to ensure their systems and processes are soundly controlled (Kouns & Minoli, 2007). Similarly, PCI Security Standards Council released an information supplement for wireless networks, besides the new amendments added to the first edition. Organisations would have to adopt new supplement and amendments in order to retain their PCI compliance status.

Implementing frameworks and applying standards and best practices is a challenging task. If it is not planned and executed professionally, the new structure might complicate the environment (Zarrella, et al., 2004). That could discourage stakeholders from adhering to the devised controls and processes, which would render the framework to be business prohibitive, added Zarrella, et al. (2004). On the other hand, in structuring a framework and adopting a set of standards and best practices, an important factor is the availability of local expertise in those standards, frameworks and the business itself (Chatterji, 2007). Should an organisation opt to utilise a third party that would increase the cost and the risk of lacking the knowledge of the local environment and business rules (Benvenuto & Brand, 2005).

As indicated in the previously explored issues, implementing a current, effective, efficient and mature IT risk management framework, comes at a cost.
In section 2.6, various business value perceptions for IT systems roles and IT risk management were explored. How could business realise the value of implementing risk management framework, that is integrated within the organisation's IT governance structure? When business values are identified, measuring means could be modelled help organisations realise the benefits and thence make informed decisions to seize opportunities as they arise. However, this seems to be one of the most challenging task organisations and professionals face because of the dynamic and complicated nature of the domain. To summarise, the indicated issues are listed in table 2.2, devised by the author.

Table 2.2: Summary of Issues in Managing IT Risk in Control-Based Structured Environments. (Author, 2010)

Issue No.	Description
1.	Lack of executive management support
2.	Subjectivity in evaluating assets values and associated risk
3.	Complexity of implementing current , effective and efficient risk management process in a changing IT risk context (business, regulatory, technological)
4.	Changes and incompleteness of standards, framework, best practices in control based structured environment
5.	Lack of local expertise in implementing control-based structured environments
6.	Demonstrate business value of managing IT risk in control-based structured environments.

2.7.2 Selecting the Focus Problem

The focus of potential research and key issues sit around the problem of identifying business values while structuring risk based control frameworks for information systems. As it was indicated in section 2.7.1-first paragraph; for an organisation, implementing effective IT risk management framework is rewarding and costly at the same time. How could organisations benefit from implementing risk management framework that meets the business objectives and comply with its requirements? When business value perceptions are identified, measuring means could be modelled that could help organisations realise the benefits and thence make informed decisions. In addition, the necessity to articulate the gained business value from implementing the framework remains high and it would play a vital role in earning top management support (Murphy, 2002).

Various business value perceptions for IT systems roles and management were explored in section 2.6. However, with different perceptions for business values such as tangible (financial) and intangible (reputational), demonstrating the business value remains a challenging task.

It was argued that managing IT risk with a holistic approach would provide a solution to this issue (see section 2.6.4). To ensure the holistic approach is taken, some recognised control frameworks, best practices and standards could be implemented and adapted. While this approach has challenges, it also leverages activities performed for other processes and ensures managing IT risk is done in a timely manner and not in isolation from the rest of the business risk. Demonstrating business value not only helps in gaining executive management support, but it 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 according to (Ames, 2007) a key measure of the effectiveness of IT risk management framework.

2.8 CONCLUSION

The reviewed literature in Chapter 2 established the duality of risk and value. To progress, organisations must take risk when responding to strategic and operational demands. The risk must be managed to help organisations make informed and sound decisions and to ensure business value. These are the positive and negative aspects of risk. As IT systems underpin business various functions and processes at all levels, managing IT risk has become paramount to business existence. Managing IT risk, however, should not be performed in isolation from managing the business risk. The optimum IT risk management is achieved when IT risk is defined from business perspectives. The IT risk management process is illustrated in figure 2.1, and shows the elements of effective IT risk management.

To manage IT risk, a number of standards and methods have been devised by reputed institutions, for example: ISO, NIST, and ISACA. Those standards and best practices give guidance on effective implementation. However, the accumulated experience remains vital for practitioners to tailor those standards and best practices to the business’s requirements to ensure desirable values are obtained. Because of the level of complexity of the business and technical environment, it was argued that managing IT risk in a holistic approach would ensure a quality solution. The author explored number of perceptions for business value andwhat could an organisation gain or perceive as a value from managing IT risk in control-based structured environments.

Managing IT risk faces many challenges, for example business dynamics, emerging technologies, and regulatory demands. On the other hand, implementing an IT risk management framework faces many hurdles such as lack of top management sponsorship and lack of local expertise in implementing these frameworks. Organisations require realising the gained value from implementing resource-intensive and demanding frameworks. The author is inclined to believe that identifying different perceptions of business values gained from managing IT risk in control-based structured environments is a key problem to the research. Furthermore, the author would be satisfied that the research outcomes would lead to enabling organisations to realise the business value from managing IT risk in that manner. In the following Chapter 3 a research methodology will be defined to systematically select a researchable problem, the relevant question and to address some of the key issues outlined in Chapter 2.

Chapter 3

Methodology

3.0 INTRODUCTION

Chapter 2 reviewed literature that is relevant to the proposed area of research of IT risk management, business value and IT control frameworks. Furthermore, a number of devised standards and best practices published by different organisations were reviewed. Some of the challenges organisations could face while managing IT risk were listed in section 2.5. Section 2.6 discussed the business values of IT systems and the gain that organisations would get from managing their IT systems in control-based structured environments. Existing and emerging challenges, underline problems and unanswered questions were explored in section 2.7.

The key problem outlined in Chapter 2, section 2.7 is how to identify the business value from managing IT risk in control-based structured environments. In Chapter 3 a research methodology is to be developed to provide answers to the proposed research question and sub-questions. Many research projects have been completed on IT controls frameworks and have predominantly used case studies. They involved interviews and document collection to collect data for further analysis. According to Collis and Hussey (2009) case study is considered a qualitative approach.

Chapter 3 is structured as follows: section 3.1 explores the research methodologies that were applied in similar research conducted by academics and practitioners in the field. In section 3.2, the reviewed studies are used to derive a suitable research methodology to fit the proposed research. Section 2.7 is also referred to in order to specify the focus problem of the research and to select a researchable question. The developed research methodology is designed to suit the topic context. In section 3.3, based on the proposed research methodology, data requirements are specified. In section 3.4 the research limitations are discussed, while section 3.5 explores the research forecast outcomes. Lastly, section 3.6 summarises the Chapter and provides a link to the next Chapter.

3.1 RESEARCH IN ESTABLISHING IT CONTROL-BASED STRUCTURED ENVIRONEMNTS

Many research projects on establishing IT control frameworks, security and risk management, business and IT alignment have predominantly used case studies (for example Haes and Van Grembergen (2005)). The research projects that utilise case studies involve interviews, surveys and documents collection to gather data,to test hypotheses and/or to validate a proposed framework. The following five sub-sections review a selection of five published papers that with the aim to identify the research methods used by other researchers addressing a similar research topic. The purpose is to learn from others how to conduct this type of proposed research.

3.1.1 Enterprise Governance of IT in Practice

Haes and Van Grembergen (2005, pp. 21-75) conducted a series of case studies researching IT Governance (ITG) best practices and effective implementation in a number of organisations. The researchers indicated (p. 21) that developing a high-level model for ITG does not imply governance is actually working in the organisation. Furthermore, the researchers stressed that deploying the ITG model across the organisation is the next challenging step. In order to identify the best practices in implementing effective ITG the authors selected a number of companies of various sizes in different sectors and researched their case studies. Some of those case studies were shallow because of the size of the organisations; however, an in-depth case study was conducted at KBC, a major Belgian financial group.

KBC is a major Belgian financial company that was formed in 1998 as the result of the merger of Kredietbank, Cera Bank and ABB Insurance. The use of a case study method showed that there was a history of more than 100 years in business. KBC is the third largest banking and insurance company in Belgium. It operates across many countries in the European continent, and employs around 49,725 professionals, among them 2,403 (internal and external) IT staff. Total IT budget for 2003 was €430 million. As KBC continued to grow and expand, the company required a flexible IT department that could respond to business requirements and meet its obligations. In addition, their IT systems grew proportionally to the business size that required to be managed and leveraged efficiently. KBC had a backlog of IT projects that needed to be prioritised based on their business values. Although an ITG structure was devised and communicated a number of challenges were encountered. The challenges were identified and countered through a number of iterations. ITG structure and the relational mechanisms were revised and issues were rectified to meet IT systems objectives as well as the business objectives they were supporting. The implementation and subsequent revisions involved internal and external expertise as well as other resources to achieve a desirable IT governance state. All stated reasons made KBC an ideal choice for the authors to conduct their in-depth case study.

The authors argued that research in ITG and its effect on the business/IT alignment is in its early stage and theoretical models are scarcely available. Furthermore, their argument continues that (p. 23) “the nature of this type of research is exploratory rather than hypothesis testing”. While the authors selected a number of organisations in different sectors and conducted some limited case studies, they selected a large financial company for an in-depth case study. The researchers selected the financial industry based on the assumption ”That this industry [Financial] is leading in the adoption of governance practices and that other sectors and industries can learn from it” (p. 24). The case studies were conducted to gather and analyse data about ITG implementation aspects and were concluded with practitioners’ perceptions of “effectiveness”, “ease of implementation” and “importance” of those aspects.

The case study was performed by utilising an ITG practice model that consisted of 33 practices for ITG, 12 structures, 11 processes and 10 relational mechanisms. To find out how ITG was being practiced face-to-face interviews were conducted utilising Delphi model to gather information/answers/perceptions from business and IT professionals in KBC in addition to collecting relevant documents. The authors utilised their business knowledge and background in the ITG domain to analyse the collected data and derive their conclusions. They presented their findings in tables, figures, and/or appendices where applicable.

3.1.2 The Value, Effectiveness, Efficiency and Security of IT Controls

A research conducted by Behr, Castner, and Kim (2004, pp. 23-33) investigated the gained business value, effectiveness, efficiency and security of IT in control-based structured environments and was based on ITIL and COBIT. The researchers stated that "IT managers are confronted with a myriad of best-practices frameworks for IT service management" (p. 23). Organisations require realising the benefits from implementing and/or adopting best-practice IT controls. The study collected data through a survey, then analysed the data using quantitative structural-equation-modeling technique to determine empirically whether IT controls effects the value, effectiveness, efficiency and IT security. Based on the research results organisations would be able to adopt recommended best-practice IT controls and undertake changes in their IT department to achieve their desirable objectives.

The motive for the research as indicated by the authors is that there are many research projects that examined the effect of IT on business value. However, while there is some research on IT controls effect on business value, there are few studies that investigate the effect of the whole framework. The authors focused their research on IT service management best-practice IT controls effects on business value. Furthermore, the research results will help organisations to better assess the efficiency and effectiveness of their IT process and IT security in comparison to high-performing organisations. The authors indicated that the research would also provide guidance on which controls would most likely affect the business value. In addition, the authors believed that the research outcomes would answer a number of questions in the IT operation domain, in particular around quantifying the value of repeatable and verifiable processes.

To achieve the research objectives, the researchers devised a research model and a set of hypotheses around the research focused points: effectiveness, efficiency, IT security and business value. Following a positivist paradigm they developed a set of questions that linked to their hypotheses. Initially a survey was formed that included general questions about the organisation in terms of the type of industry, IT department size, IT security, IT operating costs and how the IT department would measure the value of IT to the organisation.

Initially the survey was conducted in 50 interviews in large organisations in different sectors. The aim was to refine the survey questions as well as to get richer data from the respondents to form a good basis for a case study, as the researchers indicated. The survey was then distributed to 50 randomly selected samples of 1000 organisations. A mixture of email/mail was used in the latter stage. Furthermore, the researchers indicated that three pilot interviews would be conducted to further test the objectivity and effectiveness of the survey questions. The pilot interviews were conducted either via the phone or in person. The researchers preferred the in-person interviews due to the complexity of the survey and because that would bring a better opportunity to gather factual data.

The researchers utilised Positive case study techniques to anaylse the interviews. These techniques include using independent coders to verify the interpretation of the textual information and assessing responses for bias. In addition, Structural Equation Modeling (SEM) was used to analyse the quantitative survey data. Depending on the sample size of that data, either covariance-based or partial-least-squares procedures were employed. Furthermore, various techniques were utilised to verify the reliability of the items. On the other hand, the researchers indicated that the industry data would be used for benchmarking purposes and to perform sensitivity analysis.

3.1.3 Whatever Happened to Alignment?

Dowse & Lewis (2006) conducted a number of case studies (12) selected from Australian public sector orgnisations investigating business and IT alignment. The researchers stated that many organisations have adopted best practice ITIL controls to various degree and resources have been consumed. However, there was no clear evidence of proportional ROI nor business and IT alignment. The researchers performed the case studies on research the impact of infrastructure approach on business value and its alignment with IT. The research comprises one primary case study for a large organisation in the public sector and a few additional case studies that were conducted for external validity.

The primary case study involved a large Australian federal public sector organisation that has over 90,000 employees. The research method applied was a mix of qualitative and quantitative methods that investigated IT service outcomes.

Initially, interviews were held with business and IT managers. Other employees were also surveyed to gather data about their IT services. Applying qualitative analysis, the collected data provided supporting answers to the propositions that were devised by the researchers. The findings resulted in research actions that were communicated to the organisation and acted upon, over an 18 month-period. The research actions were around ITG processes, implementation of performance, reporting mechanisms and the introduction of service level management.

The researchers reported that the second stage was not so productive, because the orgnaisation had to undertake a number of changes that the applied research method could not account for. Some of those changes were around outsourcing of central IT operations, and introducing a major upgrade to their operating environment of regional IT support. On the other hand, the extent of the planned interventions was limited, as the researchers stated. The organisation IT services' performance, accordingly, reported the researchers, didn't improve over the 18 month-period. In addition, the organisation had some issues with the ITG structure, where committees did not have adequate presence of business and IT personnel. That had a large impact on the business and its IT alignment. Further observations were made by the researchers throughout the 18 month-period around other related IT services and infrastructure and around adding business value.

The researchers stated that to investigate whether the alignment issues were widespread in the public sector, they further extended the case study and selected 11 more organisations. For the newly selected organisations, structured interviews were conducted with their respective IT executives to collect and collate data. The interviews provided information about the organisations and their approach to ITG and service provision. The collected data were tabulated and cross-analysed to identify any common trends among orgnisations that were similar in terms of size or type of the business. The authors indicated that the studied cases showed that most researched organisations' IT service management processes were in early stages of CMMI level.

The research was conducted to answer a number of questions related to business and IT alignment as well as business value in applying best practice of

IT controls. The researchers selected a large organisation in the public sector and performed the first detailed case study that lasted for 18 months and reported their findings. Another 11 case studies on companies were conducted to further validate the findings of the primary case that supported their initial propositions. The outcomes of the research would help other organisations be they in public or private sectors that intend applying the same approach for managing their IT services

3.1.4 Implementation of Information Security Management System

Holappa & Wiander (2006) carried out a research that examined the experience of implementing information security management system utilising an agile approach (pp. 79-85). The researchers utilised the results of a survey conducted among the Information Security Forum members (ISF 2006) about the standard of Good Practice for Information Security (ISFSTD 2006). The survey gathered the participants rating of the expected outcomes of applying a security management standard. That justified the need to implement security standards. The research is based on a case study that examines the process of implementing a proposed framework. The case study was conducted at a middle-size enterprise to examine the challenges that small and medium-size organisations face.

The researchers were motivated by the fact that the relevance of information security is widely recognised in organisations as an important part of the business continuity. However applying technical measures is not enough for ensuring a true security status. The researchers argued, that “there must be an approach that takes the whole organisation, including human-related and financial assets” (p.79). The increasing complexity of the business and IT environment forced organisations to utilise third parties, which needed to be incorporated in the overall security profile. On the other hand, regulatory demands (for example HIPAA, SOX standards) have also added to the level of complexity, since the management has to comply with those standards. According to the researchers, those premises drive the need to apply standards like ISO/IEC 17799 (2005) as a way to achieve the desirable information security and compliance status.

The researchers argued that for small and medium-size enterprises (SME) implementing security management standards system is impractical, as it is a resource intensive (Holappa & Wiander, 2006, p. 81). However, SME still have to have some established means to manage security in a holistic manner. Wiander & Holappa (2006) in another publication developed a framework called Agile Security Development (ASD) that enables the iterative development of an information security management system that SME could utilise. The framework was piloted in the ITEA SHOPS (2005) project by the Finnish project partners, and was in use in various bilateral projects within Finnish industries. The researchers selected an SME company that had implemented ASD and conducted a single company case study that reviewed the process of implementing the proposed framework. The aim was to establish the fact that for SME organisations when implementing standards like ISO/IEC 17799 is cost prohibitive it is necessary for those organisations to find other means to establish information security management systems. The outcomes of the research would help other SMEs in adopting similar feasible approach and reach desirable information security status.

The case study was conducted on an SME company that has utilised the ASD framework. The selected company had an ISO 9001 quality management system and the security issues were addressed to some extent, although mostly technical measures were implemented. The company undertook a number of changes to their IT systems that required reassessing the IT risk profile. The new IT risk assessment revealed the necessity to implementing a form of information security management system, which led to implementing ASD as part of the existing quality management system. Adopting risk based approach helped the company to prioritise tasks that would assist in optimising their IT resources.

Although it was not specified by the researchers, a Positivist paradigm was adopted in the published paper for testing the implied hypotheses. The researchers however did not specify how they approached the company or how they gathered the data. It appears that the challenges and recommendations they made must have been made based on observations, and/or on some data collected in various ways, for example face-to-face interviews.

3.1.5 A Comparative Case Study Analysis of IT Governance Framework

A comparative case study analysis was conducted by Lee, et al. (2006, pp. 131-139) that investigated ITG implementation in two large companies in Korea. The increasing role of ITG in value creating and aligning business and IT at the strategic level has been the motive for this research. The researchers indicated that there are insufficient case studies that can be utilised as a guideline for implementing ITG. The researchers added that although there were some empirical case studies about the level of perception and execution of ITG in Korea, those case studies were limited to the proposed frameworks. The authors proposed an ITG framework with full details in the published paper and conducted a comparative case study involving two companies.

The selected organisations denoted as company A and company B were among the high-performing companies in Korea. At the time of publishing the paper, Company A was an IT-based service provider, the largest in Korea with annual sales of hundreds of millions Korean Won (₩ local currency). The company had 60 IT staff distributed in 9 teams within an independent IT department. Company B was at the third position in the same market, with 50 IT staff grouped in 5 teams. Both companies outsourced their system development and maintenance to leading IT service companies.

The research method applied in the research was a comparative case study to validate the proposed ITG framework. The selected companies as indicated earlier had similar size and IT capacity and both were known as high performing companies. The researchers cited Yin (1984) and Benbasat (1987) that conducting a comparative analysis with more than two organisations is known to assist in increasing the reliability and validity of qualitative studies. Furthermore, the source cited by the researchers (Benbasat, 1987) argued that it is also used to form a theory, to verify it academically, or to prove certain conditions in many different studies.

Data were collected utilising a trusted institutions in conducting surveys in addition to various relevant documents were collected and in-depth interviews that were held with CIO, IT team leaders and staff at the operational level. The authors didn’t specify what set of questions they used in the surveys or interviews. However, they have coded the collected data around five domains they have identified in their proposed frameworks and the corresponding phases. Finally, they conducted a cross-case analysis, prepared an ITG activity matrix using the proposed framework presented in a table. The table shows the five core domains of ITG activities, and IT coordination and control: decision-making, coordination mechanism, and control mechanism. Through this analysis the authors were able to draw some inferences and made a number of suggestions to ensure better alignment with the proposed framework.

This comparative case study presented by the researchers showed the benefits of validating a proposed solution. The researchers proposed an ITG framework in five domains and corresponding phases. However, no details were provided about the sub-elements of the proposed domains. In addition, no information was made available about the survey's content and who the audience was or what the sample size was, and how long it took to collect the responses. Furthermore, although the interviews were described as being in-depth, there was no information about whether they were structured or non-structured interviews. While these are negative remarks, as they seem, the case study demonstrates remarkable efforts made by the researchers and their findings would benefit future researchers in the ITG domain.

3.2 DESIGNING A RESEARCH METHODOLOGY

The research methodology design section explores various research methods that have been utilised by other researchers. The five similar studies reviewed above suggest that Case Study has been the most used approach. In the study discussed in section 3.1.2 only surveys were used, but these described in sections 3.1.1 and 3.1.5 a survey was embedded in the case studies. The subject of this research is in a number of fields, namely, ITG, best practice IT controls, Information security, Information risk management, business and IT alignment, IT business value, and Compliance. Guidance from other researchers (as above) suggests that case study is an appropriate methodology and that a selection of data collection methods can provide different data types

This section is organised as follows: 3.2.1 sub-section reviews methods of case study research that have been explored in the section 3.1. Sub-section 3.2.2 re-examines the issues and problems that have been identified in Chapter 2. Sub-section 3.2.3 includes a discussion to derive the research question. Sub-section 3.2.4 is where the research sub-questions and hypotheses are defined. Sub-section 3.2.5 presents the argument for the preferred research methodology. Lastly, sub-section 3.2.6 shows the data map.

3.2.1 Review of Case Study Research Methods

The explored research in section 3.1 mostly applied case study as the research method. Case study approach is applied for this kind of research because the subject of ITG is a relatively new matter (Haes & Van Grembergen, 2005). For that reason, there are not many examples to analyse and draw inferences that could be utilised doe testing hypotheses and forming proposed theories, as indicated by Haes and Van Grembergen (2005). In addition, the nature of the researched domains: (ITG, IT controls, security and risk management, business alignment and identifying business values) require practitioners' perspective to obtain empirical data (Lee, et al., 2006). Furthermore, case study approach is more a qualitative approach as stated by Collis and Hussey (2009) that suits the subjective domains that have been researched. Case studies were conducted using various approaches for collecting and analysing data.

As noted in section 3.1, some case studies (3.1.1, 3.1.4, and 3.1.5) included face-to-face interviews as a data collection method, other cases (3.1.2. and 3.1.3) utilised surveys as the main method for data collection. Cases (3.1.2, 3.1.3) used a mix of interviews and surveys, at various stages and for different purposes. For example, although, the survey described in case (3.1.2) was the prime method for collecting data, interviews were conducted initially to test the survey and to make some needed adjustment. Interviews provide subjective data that conveys the contributor's perception that will be analysed using qualitative methods whereas surveys gather direct answers and are analysed with quantitative methods. While each method has their strengths and weaknesses when they are adopted, for this research the available time and resources as well as the researched domain are factors that affect selecting the research method. Surveys could take long time and require resources to administer them, which is one of the reasons for being selected for the noted case studies.

When selecting an organisation to conduct a case study, it is imperative to choose the one where sufficient data could be collected or hypotheses can be tested. For example, for the case study explored in 3.1.1, the researchers selected a major financial company to conduct an in-depth case study investigating ITG best practice. That company was selected because the researchers argued that the financial sector is leading in implementing ITG best practice. On the other hand, the case study described in 3.1.3, where a public sector organisation was selected to conduct a prime case study. Then, the researchers selected 11 more companies to investigate whether their findings from the prime case were applicable across the public sector.

A selection of case studies was explored in section 3.1. While all studies adopted the case study research method, various data collection techniques were utilised, depending on what technique the respective researcher/s have deemed most adequate. When setting the research method design and data collection methods, it is important to consider both the external and internal factors.

3.2.2 Review of IT Risk Issues from the Literature Review

In Chapter 2, section 2.7 summarises the problems in managing IT risk that the author has identified from the literature review. The following are potentially researchable problems: (1) Lack of executive management support; (2) Complexity of implementing current, effective and efficient risk management process in a changing IT risk context (business, regulatory, technological); (3) How to demonstrate the business value of managing IT risk in control-based structured environments.

With regards to problem (1), it was established in Chapter 2, that it is crucial to gain executive management support before embarking on implementing a resource intensive risk management framework. Implementing a framework of that kind could take place over extended period of time and most probably would require re-engineering some of the business processes, let alone the IT processes. Making changes of that nature would require executive buy-in to succeed.

In relation to problem (2) Chapter 2, section 2.5 outlined a number of challenges an organisation would face if it desires a current, effective, efficient and mature IT risk management. Risk context changes over time for a number of reasons. Business and regulatory requirements change and technologies evolve and change, all that requires re-assessing the risk profile. As it was noted in Chapter 2, sections 2.1.3.6-7, responding to those kinds of changes should be done in a timely fashion to ensure a true level of assurance. Being able to retain the current status of risk profile require establishing adequate capabilities, that again would be resource intensive. This issue seems to be relating to the first problem, the importance of executive management support. While both problems are inter-related, executive management support is crucial. However, providing executive management support doesn't guarantee current and effective IT risk framework in control-based structured environments. An addition issue is on what basis would executive management offer their support? Similarly, what drives practitioners to execute such a costly initiative?

Problem (3) appears to be more independent. In Chapter 2, section 2.6 various business-value perceptions for IT systems roles and IT risk management were explored. When business values are identified, measuring means could be modelled that could help organisations realise the benefits and thence make informed decisions to seize opportunities as they arise. Resolving this problem, if feasible, seems to answer the question that was formulated in the previous paragraph. Being able to identify business values helps to articulate the business case to gain top management support. When executive management realise the value of any activity, they would have the right justifications to direct their resources adequately. As for the practitioners, it would help them prioritise the list of tasks that would require their attention, and they would be able to use their resources wisely. Furthermore, identifying and realising business values would help to gain the support of the rest of the stakeholders and would contribute to staff adoption of the devised controls and risk treatment measures. The latter factor plays a vital role in raising the risk management process level in the CMMI, where the risk management practices would be part of the organisations' culture.

As demonstrated in the previous paragraph, identifying the business value of managing IT risk in control-based structured environments would benefit the organisation in many ways. However, because of the dynamic nature of the researched domain, this seems to be one of the most challenging tasks organisations and professionals face. In Chapter 2, section 2.6, various business-IT value perceptions were explored at different stages where IT systems enable organisations to achieve their business objectives. With different perceptions for business values, both tangible (financial) and intangible (reputational), estimating the business value remains a challenge.

In Chapter 2, sections 2.1.3.2-4 explore various stages of the IT risk management process. It was argued that when identifying asset value, it is imperative to identify the asset business value rather than the asset intrinsic value. Furthermore, when analysing risk, starting with vulnerability and threat assessment, an element of subjectivity is introduced that would affect the residual risk retained within the asset. To evaluate risk, there are two approaches to accomplish that: Qualitative and Quantitative. The Qualitative approach is common, as it is easier to calculate, although it is subjective. It was further discussed that since in business value is reflected in monetary figures, it could be hard to present qualitative risk in monetary terms. While risk practitioners have advised a more granular qualitative approach based on some estimation of likelihood and impact, the outcome remains subjective.

In addition, the number of elements the IT risk management process comprises and the factors that affect its status (Business, Technical, and Compliance) increase the level of complexity of the domain. Similarly, subjectivity of the perceived value is another contributing factor to the complexity. For example IT auditor's perception of a devised control is that ensuring the activity output meets desirable outcomes, while the IT manager who performs the control would probably view the control as a bureaucratic request and as business inhibitor. While IT controls adoption is growing among organisations' IT systems. Those IT controls should be designed and applied to ensure business requirements are met. Identifying the value they add is equally important to ensure they meet their objectives, in efficient and effective manner.

Behr, Castner, Kim (2004) in a case study that was explored in section 3.1.2, claimed that the effect of an information system on business value has been the subject of many researchers. However, there are not many publications on the effect of IT-controls on business-IT value. Section 3.1.1, pointed out that the researchers that conducted ITG and best practice controls case study stated that relevant academic research is minimal, as the subject is relatively new. In addition, the existing research is either limited to the framework they examined or lacked the empirical data that was necessary to identify different perceptions of business value.

Chapter 2 discussed the importance of identifying business value in managing IT risk in control-based structured environments and also noted the difficulties in accomplishing that. Researches about IT control environment and business-IT value are scarce and 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 that would bridge the gaps in this domain. The author is persuaded to research this problem and present the findings to contribute to this part of the academic research and to further research. In addition, the outcome of the research would benefit organisations and practitioners in applying guidelines to enable businesses realise the value.

3.2.3 The Research Question

The derived focus of this research is, as noted in the previous section, identifying business value from managing IT risk in control-based structured environments. Therefore the objective of the research is to investigate various practitioners' perceptions and draw some conclusions from collected and analysed data. The research question that best addresses the research focus is:

> **How could a business realise the value of managing IT risk in control-based structured environments?**

The intention of the research question is to identify the benefits an organisation would get from managing IT risk at the various stages where IT risk resides within the business-IT structure as outlined in Chapter 2, section 2.5, and depicted in figure 2.5. Furthermore, the identified benefits will be presented in a meaningful form to the target audience. In the course of the research, attention will be paid to devising feasible means and mechanisms that would allow organisations to realise the gained value (for example communication and monitoring).

3.2.4 The Research Sub-Questions and Hypotheses

To supplement the research question, a set of sub-questions are devised below that can be utilised to gather data needed to answer the research question.
The sub-questions are:

(1) What is the IT risk context?

(2) How is the IT risk managed?

(3) What are the perceptions of business value derived from implementing IT control frameworks?

(4) What is the business value in managing IT risk in control-based structured environments?

In control-based structured IT environments the following hypotheses are to be assumed when attempting to answer the research question:
H1: Risk management is an ongoing process rather than a one-off project;
H2: Following a holistic approach in managing risk ensures valid outcomes;
H3: Reducing subjectivity in managing risk produces near factual results;
H4: Activities of other frameworks and best practices can be leveraged by meeting objectives at reduced cost.

3.2.5 Selected Research Methodology

The reviewed literature in Chapter 2 for business value in managing IT risk revealed a high percentage of subjectivity. Qualitative methods utilise best-judgment and experience to asses and evaluate risk. While risk practitioners have advised a more granular qualitative approach based on some estimation of likelihood and impact, the outcome remains subjective (Ames, 2007). As for business value associated with identified and managed risk, value is reflected in monetary figures. Quantifying the value is desirable; however, it is proved to be difficult to calculate.

This section examines research methods applied in similar domains, and will conclude with the logical research method for the context and the research question. The section is structured as follows: 3.2.5.1 reviews research methods in

IT. Sub-section 3.2.5.2 explores the case study method and its relevance to the research. Sub-section 3.2.5.3 discusses the selected case studies. Sub-section 3.2.5.4 includes issues with case study method.

3.2.5.1 Qualitative and Quantitative Research Methods in IT

Research in IT systems in general has been conducted by both qualitative and quantitative methods as indicated by Nicho (2004). Qualitative method is defined by Myers (1997, cited in Nicho, 2004, p. 60) as “which involves the use of qualitative data, such as interview, document, and participant observation data, to understand and explain social phenomena”. On the other hand, quantitative method as described by the same author Myers (1997, cited in Nicho, 2004, p. 65) “assumes that reality is objectively given and can be described by measurable properties which are independent of the observer”. Quantitative method is underlined by positivist paradigm where asserted hypotheses and propositions are tested (Taylor & Bogdan, 1998). Data collection method utilised in Quantitative approach is mainly by conducting surveys, which is very time consuming. It is used to obtain facts or causes and to filter out the subjective statistics of individuals (Taylor & Bogdan, 1998, p. 3). However, depending on the researched domain-complexity, quantifying research elements might not be at all feasible, argued Yin (1984).

Although the positivist paradigm utilises quantitative data to test hypotheses, Taylor & Bogdan (1998) asserted that it could also utilise qualitative data. The same authors indicated that “Durkheim (1915) used rich descriptive data collected by anthropologists as the basis for his treaties” (p. 4). 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 with context (Taylor & Bogdan, 1998). It has been established, (see Chapter 2 sections 2.5-7) that the domain of IT risk management and business value researched in this paper is complex, dynamic and interrelates with the business in many aspects and on various levels. The fact that the subject of this research depends on its context makes it imperative to obtain factual data besides the attempt made in the literature-review to answer the research question. The research question in itself is about how to identify business value perceptions of risk management. The business insight is paramount to test the theoretical assertions that have been made and to gain a wider view of the problem indicated in the research. The justifications discussed in section 3.2.5.1 led the researcher to believe that the best approach to achieve the research objectives is a combination of a positivist paradigm where proposed hypotheses are tested with qualitative data collection method. The indicated test will be performed using the analysed qualitative data applying quasi-judicial method, where a rational argument is used to interpret the data (Collis & Hussey, 2009).

One method of qualitative method is case study, that has been utilised by research in many fields, as indicated by Yin (1984), who further justified the use of case study by "where the structure of given industry may be investigated" (p. 14). Case study is the research method that fits most to research the described domain of this research and to investigate the problem that has been selected as a focus of this research. Yin (1984, p. 14) indicated that case study facilitates the holistic investigation of the characteristics of a real-life event. For example, individual life cycles, organisational and managerial processes and maturation of industries. That particular attribute of the case study method is largely the reason for being selected as a research method for the research reviewed in 3.1. Respective authors of each case study justified their selection of the case study method as it would allow them to investigate the subject and collect sufficient data from practitioners. In addition, case study approach gives researchers the chance to make observations that might prove to be valuable to the research.

Qualitative and quantitative research methods have been utilised for researching various topics in IT. 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 researches are scarce and that led many authoritative researchers to conduct case studies for the investigation of subjects within the domain of this research topic. Some of those papers were examined to determine what methods they have utilised and what were their selection criteria. Section 3.1 provides some reflection on the reviewed case studies in section 3.1 and some considerations about the attributes of qualitative research method. In addition, given the time and other available resources for this research it can be concluded that case study with interviewing as main data collection method is the most suitable approach to tackle research question of this study.

3.2.5.2 Case Study Method

As indicated in the previous section, case study is a qualitative research method. According to David (2006, cited in Eriksson & Kovalainen, 2008) case study research has a long history across academic disciplines. In addition Dyer and Wilkins (1991, cited in Eriksson & Kovalainen, 2008, p. 116) indicated that "many organisation and management studies can also be classified as case study studies". Eriksson and Kovalainen (2008) further indicated that the key point of the case study method is that the research questions relate to the understanding and solving of the case. In other words, the method helps to understand what the case is about and what can be learned from studying it. The authors added that the "main purpose is to investigate the case in relation to its historical, economic, technological, social and cultural context" (p. 116). Another definition from Yin (1984, p. 23) states that:

> "a case study is an empirical enquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between object of study and context are not clearly evident in which multiple sources of evidence are used".

This definition states what the case study is, what it does and why it has been chosen as a research method.

Collis and Hussey (2009) also refer to case study as exploratory research. Dul and Hak (2008) simplified the definition of case study to be a study of a single case or multiple cases in its real life situations and to analyse data that are obtained from these cases qualitatively. Yin (1984, p. 17) takes another consideration when deciding which research strategy suits the researched problem. Yin argued that the case study approach is the most adequate method to apply for research questions that contain "how" and "why". That seems to fit the question of this research that has been formulated in section 3.2.2. The researched domain in this research fits neatly with the case study definition. As managing IT risk in control-based structured environments is subjective and its context is constantly changing, as well as, identifying business values in managing IT risk in that context is subjective. In order to be able to understand the context and to form an answer to the research question, a holistic approach is required to consider various aspects of the researched domain.

The case studies that have been reviewed in section 3.1 showed that a few different methods have been applied to collect data: survey, interviews, or mix of both. All scenarios are plausible depending on the scope of the case, nature of environment and available resources (Yin, 1984). For example, surveys are known for consuming considerable amount of time for collecting and processing the data. Since there is a time constraint for this research that doesn't allow conducting a survey, this approach has been ruled out. In contrary, interviews are a suitable method when there is a limited time. In addition, with regards to the data quality interviews provide rich source of practitioner's perspective (Haes & Van Grembergen, 2005). Furthermore, interviews allow more flexibility to the author of this research to gain factual insight about the researched environment.

The reviewed case studies in section 3.1 revealed a few other important aspects to the case study design namely type, size and number of the subject organisations. Depending on the objectives and available resources, one or more companies were selected in the reviewed studies. For example, the case study described in 3.1.1 selected a number of companies and conducted limited case studies. Then they selected a large enterprise in the finance sector and performed an in-depth case study. The industry and company were selected as the finance sector and the company were deemed to be in a leading position in applying ITG best practice, which is the focus of the case study. On the other hand, the case study discussed in 3.1.3 conducted a research on a large firm in the public sector, and then the researchers performed another 11 case studies to further-validate the findings of the first case study. Section 3.1.5 a comparative case study conducted on two companies to assist in increasing the reliability and validity of the research. The researchers Yin (1984) and Benbasat (1987) cited in Lee, et al., (2006) stated that conducting a comparative analysis with more than two organisations is known to assist in increasing the reliability and validity of qualitative studies.

A comparative case study could be conducted on a single case as indicated by Yin (1984). However, the author argues that the rationale for that is “the single case represents the critical case in testing a well formulated theory” (p. 47).

(Flick, von Kardorff, Steinke, 2004, p. 147) stated that “the dimension of single case-comparative study represents one axis according to which the basic design of qualitative research may be classified”. The other axis follows the dimension of time to form a longitudinal study. In case study design for this research, none of the selected companies meets the Yin’s rationale. On the other hand, conducting a longitudinal case study is not feasible for this research.

Eriksson and Kovalainen (2008) stated that the case study research method should offer the possibility to combine qualitative and quantitative approcaches. In line with that Stoecker (1991) cited in Eriksson & Kovalainen (2008, p. 127) stated that “The common divide between qualitative and quantitative should not be an issue in case study”. Eriksson & Kovalainen (2008) based their argument on the latter statement and asserted that researchers should apply what is appropriate considering the research question. Hammersley (1996, cited in Eriksson & Kovalainen, 2008, p. 127) presented three forms of combining Qualitative and Quantitative research: triangulation, facilitation and ‘complementarity’. Triangulation is the most common form that has been discussed (see section 3.2.5.4). Facilitation is when one research method facilitates the other. Complementarity is defined by the same source as “both types of materials and methods can be used side by side to enrich the case description” (p. 127). Since the collected data for the research is qualitative data, the focus of this discussion is on qualitative method types.

3.2.5.3 Case Selection

Learning from previous studies’ approaches for conducting research in similar domains, it is therefore proposed that a case study should be performed at two companies in New Zealand. The selection was made considering factors like available time and resources. In addition, the size of the organisations, industry, and level of contact the researcher has with some of the staff members at those organisations are also taken into account. The two companies are considered large enterprises in the public sector with large IT teams and internal audit divisions.

The aim is to find evidence that tests the theorised assertions made in the literature review section and the hypotheses outlined in section 3.2.4.

Multiple-case studies research with a single case study design should "consider multiple cases as one would consider multiple experiments, that is, to follow a [sic] (replica) logic" (Yin, 1984, p. 53). In line with this view Eisenhardt (1989, cited in Eriksson & Kovalainen, 2008) stated that multiple-case study should follow replication rather than sampling logic, which relates to survey research. This assertion is demonstrated in section 3.1 in which discusses researches with multiple-case studies that have been conducted to serve different purposes. The selected companies for the comparative case study will be subjected to the same research design. The research question and sub-questions will be identical, as well as data collection methods.

The case study will be carried out by conducting semi-structured interviews with staff members in IT, audit division, security and risk management, project and program office, and business that could be from finance or HR. A set of questions and sub-questions driven from section 3.2 will be prepared and used to drive the interviews. These questions are meant to be as a guideline only. An element of flexibility is required, so that further observations can be made and allow participants to contribute beyond the initial set of questions. Other means will be used to collect relevant data, such as email and any documents that could be collected from the organisations under study.

The author has obtained the approval from both companies to conduct the interviews with staff members of the designated roles outlined in the previous paragraph. The set of sub-questions as well as research synopsis along with the author's brief biography were sent to the contact person who was coordinating the interviews. The aim is to build a rapport with the interviewees at an earlier stage, that should help in conducting the interviews in due course. In addition, information was provided to the perspective participants about the interview procedure, duration, and that the interviews will be audio-recorded with their permission.

3.2.5.4 Case Study Method Issues

Case study is not different to any other research methods in having downside or limitation that attract rejections from some researchers (Yin, 1984). Yin indicated that the issue with case study method is that it could be perceived as biased and limited and could take a long time. The first issue has been raised because of concerns about searchers who would focus only on the area that might imply the data they could solicit. In addition, some researchers might direct the research intentionally to get the answers they need. This is quite possible to happen and for that reason, research would have to overcome that by adopting different data collecting techniques to avoid an undesirable trend.

With regards to the second issue Yin (1984, p. 21) stated that “case studies provide little basis for scientific generalisation”, which seems logical. However, Yin argues that case study, like any scientific experiment, can be generalised to the theoretical propositions and to the populations or universe. Another view on resolving the generalisation issue is presented by Bonoma (1985, cited in Nicho, 2004, p. 64) who states that “a researcher can simultaneously pursue high levels of data validity and generalisability by adopting triangulation strategies to provide replication and/or corroborations of findings across methods within a single research project”. Triangulation can be achieved when data is collected by a number of investigators or various data collection methods are utilised and then the data are cross checked (Taylor & Bogdan, 1998). The third common concern about case study method is that it could take a long time and would result in a large amount of data. While this is a legitimate concern, these are observations of case studies that have been performed in the past. This issue with case study could be rectified by controlling the duration and utilising some adequate data collection methods to avoid collecting unreadable documents.

Despite the noted issues with the case study research method, the author believes that case study is the method that suits the researched domain. As for the stated deficiencies, a number of measures could be taken to reduce their impact. For example, this research is limited by the academic calendar, and the field work is limited to the set of interviews that will be conducted in two organisations. As for data collection, the semi-structured interviews will be the main source of data where 5-6 people are to be interviewed for about 30-45 minutes. The other means for data collection, are collected documents and diary recording and are not expected to produce large amount of data.

The other issue is generalisation. The author believes that the justification provided by Yin (1984) is valid, and the findings will be generalised for alike organisations that have similar IT environments. The only remaining issue is bias, which the author acknowledges will be one of the research limitations. However, it is the nature of the research to focus on IT risk management and business value. While other business aspects will be examined as part of the holistic view to the problem, Yin (1984) indicated that a research unit has to be decided at the research design stage, so that the case study would not spiral out in many different directions.

3.2.6 Data Map

The research question along with the sub-questions, data collection methods and analysis as well as the expected research outcomes and further research recommendations, are all summarised in the diagram shown in figure 3.1.

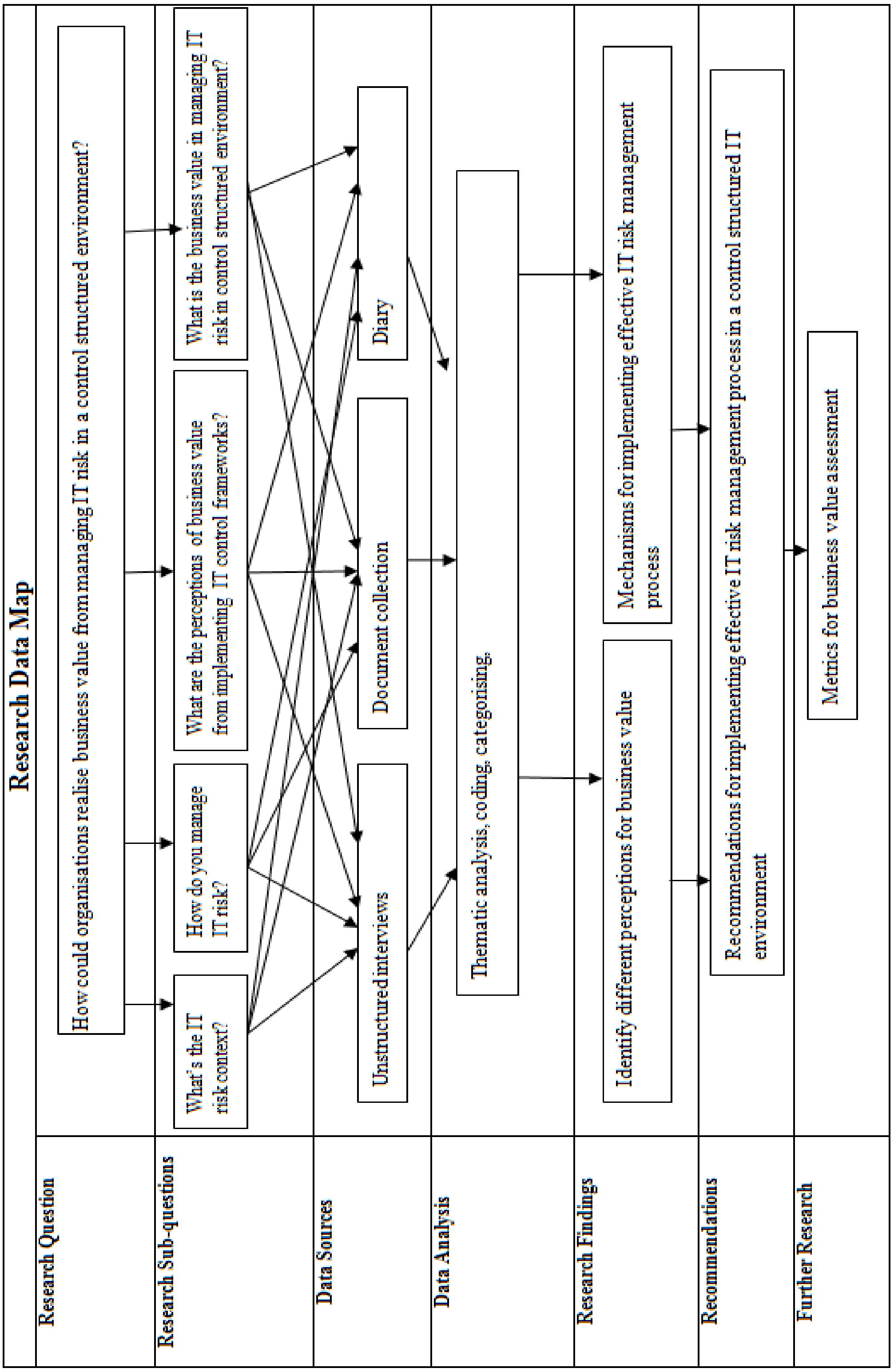

Research Data Map
Research Question
How could organisations realise business value from managing IT risk in a control structured environment?
Research Sub-questions
What's the IT risk context?
How do you manage IT risk?
What are the perceptions of business value from implementing IT control frameworks?
What is the business value in managing IT risk in control structured environment?
Data Sources
Unstructured interviews
Document collection
Diary
Data Analysis
Thematic analysis, coding, categorising.
Research Findings
Identify different perceptions for business value
Mechanisms for implementing effective IT risk management process
Recommendations
Recommendations for implementing effective IT risk management process in a control structured IT environment
Further Research
Metrics for business value assessment

Figure 3.1: The Research Data Map. (Author, 2010)

3.3 DATA REQUIREMENTS

Collis and Hussey (2009, p. 143) describe qualitative data as “normally transient, understood within context and are associated with an interpretative methodology”. They argued that since qualitative data need to be understood within context, it is imperative to gather data about the subject background, which is defined as “contextualisation”. Collecting data in a case study method is one of the hardest parts, claimed Yin (1984, p. 62). He added that to gather data the investigator needs to have a set of skills, for example: able to ask good questions, be a good listener, flexible and adaptive, know the subject very well and unbiased. However, data collection should be controlled to some extent to avoid having unreadable documents, 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 and analysed so that asserted hypotheses will be tested to draw inferences as indicated by Yin (1984). Analysed data will be presented in various forms using NVivo software for analysing qualitative data (Gibbs, 2002).

The section is structured as follows: sub-section 3.3.1 explores data collection methods used in the research. Sub-section 3.3.2 discusses data analysis, while sub-section 3.3.3 explores data visualisation.

3.3.1 Data Collection Methods

Data will be collected from four sources: semi-structured interviews, document collection or archival records and diary recording (Yin, 1984). According to Collis & Hussey (2009) interviews and archival records are common data collection methods for case studies. While other forms of data collection are also possible, for example survey, this has been ruled out because of the time constrain. Interviews will be carried out with some participants from internal audit, IT audit, IT security and risk management, IT division manager, and business unit management. Interviews will be carried on in the North Island of New Zealand. Relevant documents such as letters, agendas, and administrative documents will be gathered, when necessary. Other documents like organisation structure chart, policies, procedure, sample of audit reports, incident reports, and risk register will also be collected, when possible, to validate data gathered via the interviews. If supporting data can be found in classified documents for internal use, then participant's approval will be obtained to use such data. Data will be carefully censored to ensure participant's privacy and confidentiality protection terms are not violated.

This section is structured as follows: sub-section 3.3.1.1 discusses interviews. Sub-section 3.3.1.2 explores conducting interview and transcribing them while sub-section 3.3.1.3 reviews document collection methods. Sub-section 3.3.1.4 discusses diary recording.

3.3.1.1 Interview

It is planned to conduct semi-structured interviews with selected people from the proposed organisations. Easterby-Smith, Thorpe and Lowe (1991, cited in Collis & Hussey, 2009) suggest that unstructured or semi-structured interviews are appropriate when the aim is to gather respondents' perceptions, or when researching a confidential subject. (Collis & Hussey, 2009; Gillham, 2000) have recommended unstructured interview with open-ended questions that would give a chance to explore answers at deeper levels. However, there should be some guidance from the researcher, to keep the focus on the topic and avoid digression. Interviews will be done in face-to-face form, which provides better chances to the researcher to gather rich data (Haes & Van Grembergen, 2005; Lee, et al., 2006). In addition face-to-face interviews allow probing beyond the questions and giving the interviewee the liberty to talk about matters that might have not been identified by the researchers. There are three main stages in interviewing process: selection of interviewees, preparing interviews, and conducting the interviews.

It is anticipated to select one or two key interview participants from Internal Audit team, IT division, and business management. For example, the internal audit manager, IT auditor, IT security and risk manager, IT project and program office managers, senior business analyst, and business unit manager, can participate in the proposed interviews. It is anticipated to interview about 5- 6 people from each organisation, each for person 30-45 minutes.

When selecting interviewees researchers should consider their availability and ability to contribute to the research. This will mainly involve considering interviewee’s position within the organisation, the researcher’s knowledge and the participant’s ability to respond to the questions during the interview. One can argue that this selection method might appear biased. However, from the researcher’s perspective these are the interviewees that can provide rich information required for this research.

As for interviews preparation, the author obtained the approval from the Ethics Committee (See Appendix B) to conduct interviews with a number of designated staff at two organisations. A set of questions and sub-questions have been derived from the research question and the sub-questions. The set of questions, conversation starters, along with the research synopsis and brief biography of the author have been prepared and will be sent to the participants in due course. This is to be done as part of building a rapport with the participants, as Simones (2009) emphasised its importance for generating in-depth data.

As part of the preparation, the author has gathered as much information as possible about the organisation, mainly through their web site. Many organisations place on their web site quite valuable information about their structure, number and kind of boards within the organisation. In addition, information about the size of the organisation, history, new and in-progress projects can be found on companies’ web sites as well. This information could be used to gain good insight about the organisation before conducting the interviews. It would be useful to rehearse the questions and interviews a number of times, as well as to prepare a copy of the set of questions for each interviewee, preferably with their names and positions. This is for note taking during the interviews. Audio digital recorder has been purchased and tested to record the interviews. Finally, when interviews are scheduled and everything is set, it is important to get in touch with the contact person the day before the interviews, to make sure the interviews are on schedule.

As for conducting the interviews, the more preparations the better, however meeting people for the first time and trying to get as much information within a limited period of time is a challenging task. The author has worked as an IT auditor for a short while and gained some experience in conducting structured interviews. On the day of interviews, a certain routine should be followed, for example allowing enough time to arrive early, as suggested by Collis and Hussey

(2009). When meeting people, briefly go through the research synopsis and ask for interviewee’s permission to record the interview and to take notes, as indicated by Collis and Hussey (2009). The interview duration should not exceed the agreed time, since interviewees are usually busy people. In general it’s important to respect people’s time and other commitments. At the end of the interview it would be good to thank and inform the participant that there might be further communication via email if a need arises for some clarification.

3.3.1.2 Interview Recording and Transcription

Kvale (1996, p. 144) stated that “the interview is the raw material for the later process of meaning analysis”. Furthermore, Kvale added that the quality of the interview plays a vital role for the quality of the later analysis and reporting of the interviews. Interview recording would be also crucial so that researcher can focus on conducting the interview and interact as the interview progresses, stated Kvale (1996). Collis and Hussey (2009) indicated that interviewee’s permission to record the interview must be obtained before doing so. The common type of recording is audio recording, Kvale argued that “the audiotape gives a ‘decontextualised’ version of the interview” (p. 160). However, audio recording, as expected, doesn’t capture the setting and facial gestures or body-language. With current technology, digital audio recording devices are available to acquire and easy to use. Large amount of data could be saved on the device and could be saved to a computer for back up purposes as well as further processing (Arksey & Knight, 1999).

The other form of interview recording is by video (Gillham, 2000, Kvale, 1996; Arksey & Knight, 1999). Video recording captures body language and gestures, as expected, which would be lost if audio recording was used, indicated Arksey and Knight. Video recording provides richer contexts for interpretations that audio recording does, argued Kvale (1996, p. 161). However, the large amount of information produced makes videotape data analysis very time consuming, Kvale continues his argument. For this research audio recording will be used as indicated earlier.

The logical step that follows the interviewing is interview transcription. Arksey and Knight stated that “transcription is a part of the organisation and management of the data” (p. 141). Furthermore they indicated that transcription is one interpretation of the interview and no more than one interpretation. (Collis & Hussey, 2009; Gillham, 2000) indicated that it is very important to transcribe the interview straight after the actual interview while the researcher still remembers the information from the interviews. Interview note-taking would be helpful as well when transcribing the interviews. Kvale (1996) claims that researcher's subjectivity and memory maybe reflected on the recorded interview, which can be defined as one of the limitation of the data collection method. Kvale added that there is no one way of transcribing interviews, i.e. whether to transcribe everything said or not. (Gillham, 2000; Arksey & Knight, 1999) recommend focusing on the statement relevant to the key subjects and omitting the irrelevant parts that would not add value to the transcript. Recorded interviews can be replayed to capture all information that could be gained from the interviews. With an aid of computer and software (Collis & Hussey, 2009) interviews can be backed up, transcribed and analysed as well.

3.3.1.3 Documents Collection

Interview alone is not sufficient for data collection. However, documents relevant to this research from the case companies will be copied and collected for analysis and will be used to verify or clarify some of the points in the interviews. Documents can also be collected as supportive evidence for this research, emphasised Collis and Hussey (2009). Documents such as letters, memos, IT policy, and IT strategic plan, will be sorted by category or similar aspect. In addition, some other documents can be also useful, such as: organisation chart, sample of incident report, sample of audit report, risk register, risk profile if any (Yin, 1984). It is expected that most of these documents will be available in digital form; documents placed in public domain could be obtained from the organisation's web site.

3.3.1.4 Diary Recording

It is widely known that diary recording method is used by people to record daily events or issues for different purpose. The researcher will be using this method to record any issues that may arise during the research in relation to what people do, think and say regarding the research topic. Collis and Hussey (2009) stated that diary recording is a good method for collecting qualitative data. Diary recording may also be used to record informal conversations with some of the interviewees, as indicated by Tavalea (2008).

3.3.2 Data Analysis

After collecting data from interviews, documents, and diary data will be processed by transcribing all collected data and then analyzing it. Yin (1984, p. 124) stated that “case analysis is the most difficult stage of doing case studies”. As noted in section 3.2.1.2, interviews should be transcribed right after conducting the interviews. Kvale (1996) indicated that transcription could be the first step in data analysis. Transcribed interviews will be coded, using thematic analysis (Taylor & Bogdan, 1998) so that data from diary recording, collected documents and archival records could be associated to the corresponding categories. To analyse qualitative data there is a number of methods that could be utilised depending on the case study design (Eriksson & Kovalainen, 2008). In the past, manual handling for the collected documents and transcribed data were utilised, with coloured pens and cards to code and map variables with the corresponding data (Kvale, 1996). However, (Tesch, 1990; Weitzman & Miles, 1995; Miles & Huberman, 1994) (cited in Kvale, 1996, p. 172) indicated that if computer based transcription and analysis are utilised, that would save time and would allow for a multitude of analytic operations. NVivo 8 qualitative analysis software will be used to code and process the collected data (Gibbs, 2002). The researcher’s role remains unchanged in conducting the analysis and testing the research propositions.

Data analysis methods are either qualitative or quantitative. However, it is necessary to reiterate what has been mentioned in section 3.2.5.1 that the case study research method offers the possibility to combine qualitative and quantitative materials (Eriksson & Kovalainen, 2008). As the collected data for the research is qualitative, the focus of this discussion is on qualitative method types.

This section is structured to discuss thematic analysis in sub-section 3.3.2.1. The next sub-section 3.3.2.2 discusses coding, while sub-section 3.3.2.3 explores grounded theory approach. Sub-section 3.3.2.4 reviews cross case analysis for multiple-case study. Lastly, sub-section 3.3.2.5 explores some of computer-assisted qualitative data analysis.

3.3.2.1 Thematic Analysis

The first step in analysing data as described by (Eriksson & Kovalainen, 2008, p. 128) is by organising all collected empirical data into a primary resource package that is called a case record. The case records can be assembled either thematically or chronologically. However, the most important feature of that record is manageability. This implies that there will be some data reduction, where ‘background noise’ and any other irrelevant data are left out. Stake (1995, cited in Eriksson and Kovalainen, 2008) stated that a thematic order emphasises themes, issues, actors, and conceptual categories. The objective of this assertion is to form a holistic configuration by associating empirical patterns (theme, events, and processes) to each other. Similarly, Braun and Clarke (2006, cited in Tavalea, 2008, p. 54) define thematic analysis as “a method for indentifying and analysing themes in the data”. Braun and Clarke indicated that thematic analysis has no rules and it is not widely used. However, they claimed that some methods of analysis like content analysis and grounded theory are mostly thematic, although they are not called thematic analysis. In this research the thematic analysis will be used to categorise and build a relational structure from the collected empirical data.

3.3.2.2 Coding - Indexing

Coding means that the feature, instances, issues, and themes in empirical data are classified and given a specific label (Eriksson and Kovalainen, 2008, p. 128). According to Taylor and Bogdan (1998, p. 150) “coding is a way of developing and refining interpretation of the data”. The process involves associating and analysing data that share the same themes, ideas, concepts, and propositions. While the initial data were vague and appeared incoherent, when processed, these are refined, expanded and discarded added Taylor and Bogdan (1998). Arksey and Knight (1999) renamed ‘coding’ with ‘indexing’ with a similar definition, although they claimed the terms are not identical as they cited (Bryman & Burgess (1994)). Arksey and Knight (1999) argued that ‘indexing’ needs to be consistent and its categories need to be considered carefully. Eriksson and

Kovalainen (2008) indicated that in case study research predefined propositions are established and systematic coding is preplanned and used to test the asserted propositions. The predefined propositions would give a basis for a pre-developed thematic coding scheme to be used when collecting and analysing the empirical data. The codes would be derived from the theory not from the empirical data as such, in contrary to grounded theory where the coding system is developed from the gathered empirical data.

3.3.2.3 Grounded Theory Analysis

According to Sauders, Lewis and Thorhill (2000, cited in Tavalea, 2008) the purpose of the grounded theory approach is to obtain meanings from the studied subject. As noted in section 3.3.2.1 Braun and Clarke (2006, cited in Tavalea, 2008) indicated that some methods of analysis like grounded theory are mostly thematic, although they are not called thematic analysis. Arksey and Knight (1999) described grounded theory where empirical data are collected in many rounds, compared and interrogated in a number of iterations to attempt answering the research question. As noted in the previous section, in grounded theory a coding system is developed from the empirical data. This type of analysis requires plenty of resources to conduct more interviews as needed, as well as analysing and devising the data in many cycles. That seems infeasible for this research project, as there is a time constrain, and it is only the author who would have to conduct the interviews and analyse the data. In addition, it would be very difficult to get approval from any organisations to conduct a longitudinal case study.

3.3.2.4 Cross-Case Analysis

Eriksson and Kovalainen (2008) argued that regardless whether the research is a single-case or multiple-case study design, the analysis must begin with the analysis of each individual case; this technique is called within-case analysis. In multiple-case study, however, “this stage is followed by cross-case analysis” (p.130). Cross-case analysis is an analytical technique that suits multiple-case study, stated Yin (2004, cited in Eriksson and Kovalainen, 2008). However, there are other techniques that suit both single and multiple-case studies, but they don’t seem to fit the purpose of this research. In cross-case analysis a form of comparison will be conducted on both cases investigating any similarities or differences across the cases and against the devised theory, as stated by Eriksson and Kovalainen (2008). Cross case analysis allows researchers to investigate multiple-case studies and it will be adopted to cross analyse the case studies on the selected organisations.

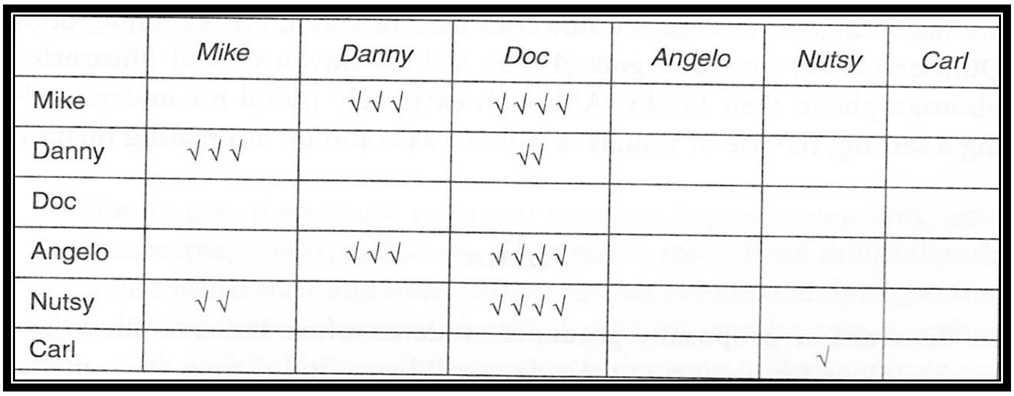
3.3.2.5 Computer-Assisted Qualitative Data Analysis (CAQDAS)

Technology has advanced and has become part of any business and aspect of life in modern times. It has helped researchers in conducting their research in various ways, for example: audio and video recording, saving, creating databases, mapping and handling data. All these technologies are fed into a software application referred to as Qualitative Data Analysis (QDA) as noted by Eriksson and Kovalainen (2008). QDA and CAQDAS both refer to qualitative data analysis; these tools allow researchers to collect data, in recording interviews, note-taking, transcribing, editing and coding. Some of these applications are: NVivo, NUD.IST, and Atlas.ti. These software have been widely used in business research, however, in terms of time and cost, they are not the most efficient, claimed Dolan and Ayland (2001, cited in Eriksson and Kovalainen, 2008). These applications can help with data management, organisation and analysis, as they could handle large amount of data. However, they do not provide analytical frameworks. It is the researcher's responsibility to decide what theoretical and methodology to utilise.

In this research NVivo 8 will be used, which helps in storing and managing large amount of qualitative data through transcribing interviews, coding, classifying themes, sorting data, and examining relationships in the data, according to (Tavalea, 2008). In addition, NVivo helps in searching and retrieving text segments, stimulating interaction with the data, and relationship building within data, as stated by Dembowski and Hanmer-Lloyd (1995, cited in Collis and Hussey, 2009).

3.3.3 Data Visualisation

When case study data is collected and systematically analysed, data is formed in various forms that allow inferences drawing and/or action taking (Denzin & Lincoln, 1998, p. 180). This process entails reduction in the data set based on the coding that should have taken place at earlier stage. Bailey (2007, p. 152) described visual representation “as a means by which the researcher can literally show the results to an audience”. Denzin and Lincoln listed some examples of those visual representation: structured summaries, synopses, (Fischer & Wertz, 1975), vignettes (Erickson, 1986), network-like or other diagram (Carney, 1990; Gladwin, 1989; Strauss, 1987; Werner & Schoepfle, 1987a, 1987b) and matrices with text rather than number in the cells (Eisenhardt, 1989a, 1989b; Miles, Huberman, 1984, 1994). Bailey (2007) also stated that visual presentation could be resembled visually or textually in the final manuscript. Bailey referred similarly to a set of examples of these presentation forms: drawings, conceptual maps, matrices, tables, and charts. Those forms “would serve not only as visual presentation of what one has learned through analysis but also as generative, analytical techniques” argued Bailey (2007, p. 151). Figure 3.1 shows an example of visual representation of data that facilitates coding of the pattern of social influence.



	Mike	*Danny*	*Doc*	*Angelo*	*Nutsy*	*Carl*
Mike		√ √ √	√ √ √ √			
Danny	√ √ √		√√			
Doc						
Angelo		√ √ √	√ √ √ √			
Nutsy	√ √		√ √ √ √			
Carl					√	

Figure 3.2: An Example of Data Visual Representation. (Bailey, 2007, p.151)

Another form of data visualisation is depicted in figure 3.3 that shows sample chart produced in NVivo model explorer.

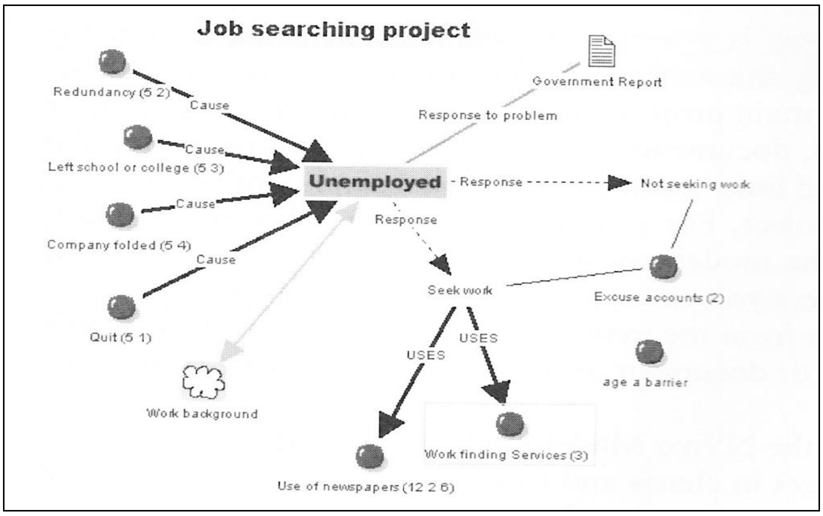


Figure 3.3: A Sample Chart Produced in the NVivo Model Explorer. (Gibbs, 2002)

3.4 RESEARCH METHODOLOGY LIMITATIONS

The selected method for this research has been designed to utilise a case study method of exploratory positivist's paradigm where proposed hypotheses will be tested via the collected and analysed data. Data will be collected in various ways, semi-structured interviews, document collection, diary recording. A multiple-case study is designed to be conducted in two organisations. The design of the case study research and data collection methods was thoroughly discussed by considering internal and external factors. However, there are some limitations as is the case with any research method. Simones (2009, p. 162) stated that "there are strengths and weaknesses in most research approaches and case study research is no exception".

Yin (1984) categorised the case study method limitations as follows: construct validity, internal validity, external validity and reliability. Construct validity is about the validity of building the research methods, and collecting data, where a level of subjectivity is expected, while internal validity relates more to explanatory case study which is out of scope of this research. External validity is about generalising the case study and draws the most criticism on case study method. The last one is reliability that demonstrates the ability to conduct the same case study design and obtain similar results. Other authors (Collis & Hussey, 2009) categorised the limitations as validity, generalisation and reliability, referring to Yin's limitations: construct validity, external validity and reliability, respectively.

This section is set to discuss these limitations of the research; it is structured to review the reliability, validity and generalisation issues in sub-sections 3.4.1, 3.4.2 and 3.4.3 respectively.

3.4.1 Reliability

Reliability, according to (Collis & Hussey, 2009, p. 64) "refers to the absence of differences in the results if the research were repeated". In other words, if another party attempts to conduct the same case study, would they get similar results? Yin (1984, p.45) emphasised on "repeating the same case study, not on replicating the results of one case study by doing another case study". The impact of that is whether to trust the findings of the case study. (Yin, 1984; Simones, 2009) recommended documenting the research procedure so that it can be re-performed again following the same steps that have been done in thefirst run. The aim is to minimise the errors and biases in a study, argued both authors.

Collis & Hussey (2009) claimed that reliability mostly concerns positivist studies, while under interpretive paradigm reliability is of little importance. The same authors added: "The qualitative measures do not need to be reliable in the positivist sense". Although this research is designed to be conducted under positivist paradigm, the collected data are qualitative data. Testing will be performed using quasi-judicial method, where a rational argument is used to interpret the data (see section 3.2.5.1). Collis and Hussey (2009) indicated that for interpreting qualitative data, defined procedures and protocol would ensure authentic results. (Eriksson & Kovalainen, 2008) stated similar stance to Collis and Hussey's view on the need for high reliability for quantitative data, but not so much for qualitative data.

In this research the case study design has been argued and documented at all levels, as demonstrated in the research design section. Further details on coding and thematic framework could be found in Appendix A to ensure all details are captured and can be followed, if required. The author believes that this measure is viable and would mitigate the risk indicated in this type of limitation.

3.4.2 Validity

Yin (1984) refers to this limitation as construct validation and indicates that this is the most problematic aspect of case study research. Criticism has been drawn towards the case study method because investigators fail to develop sufficient operational set of measures, Yin indicated. In addition, there is a high level of 'subjectivity' in data collection. Collis and Hussey (2009, p. 65) define validity as "the extent to which the research findings accurately reflect the phenomena under study". In other words, it reflects how accurate the findings and the drawn conclusions of what has been investigated are and what evidence has been provided to ascertain the results (Eriksson & Kovalainen, 2008). Collis and Hussey refer to what Yin has described as construct validation and indicate their importance to business research. Collis and Hussey (2009) indicated that validity is demonstrated in interpretive paradigm analysing qualitative data, in contrary to the positivist paradigm where high reliability to reproduce similar results is required. Kvale (1996, p. 238) shares the same view with Collis and Hussey (2009), stating that "qualitative research can, in principle, lead to valid scientific knowledge".

The other noted aspect is subjectivity in collecting data and subsequent analysis. While case study opponents base their rejection to the case study subjective judgment, Simones (2009) argued that in qualitative research, including case study, subjectivity is not a negative thing. In addition, subjectivity cannot be totally eliminated, although reducing the subjectivity level would help in gaining more credibility of the research results. To achieve that, a form of triangulation can be adopted, that's collecting various forms of data from different resources and cross checking the outcomes (Yin, 1984). In this research data collection methods have been stated, that should help in cross-checking the collected data. However, as it is only the author who works on the research, there will be a level of subjectivity in analysing and justifying the outcomes. The author will endeavour to provide as much evidence as possible to justify the devised conclusions.

3.4.3 Generalisation

Case study generalisation, or external validity in Yin (1984) definition, is a limitation that was briefly discussed in section 3.2.5.4. Criticism is drawn on how possible it is to generalise findings of one case study to the universe. Yin (1984) argues that the critics are inadequate as they are implicitly making analogy to survey research. Survey research is based on statistical generalisation, while case study research is based on analytical generalisation, asserted Yin. According to (Kvale, 1996, p. 233) 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". The researcher would base their generalisation claims on 'assertational logic' by specifying the supporting evidence, added Kvale.

Gummesson (1991, cited in Collis & Hussey, 2009) argued that interpretivists could generalise their findings from one setting to a similar setting. Similarly, Normann (1970, cited in Collis & Hussey, 2009) stated that it is possible to generalise from few cases, or even from a single case, if the analysis has captured the interactions and characteristics of the phenomena under study.
Generalisation, however, does not take place automatically, argued Yin (1984, p. 44) and asserted that " a theory must be tested through replication of the findings in a second or even a third neighbourhood", or another setting.

Yin's assertion about testing through replication in another setting enhances the credibility of conducting multiple-case study. That should be done in a fashion aiming at replication not sampling, which would increase the findings credibility and generalisation could be justified. Simones (2009, p 164) stated that "cross-case generalisation is commonly adopted in a collective case study". The same author argued several cases could be studied and cross-case analysis is conducted to identify common issues and themes. That would enable the researcher to derive general propositions that generalise across the number of cases studied. In this research, the case study is devised to be conducted in two organisations that have similar settings. Provided the collected data allow testing of the devised hypotheses and the ability to replicate the findings, the researcher is confident to generalise the findings and reduce the impact of this limitation.

3.5 FORECAST RESEARCH OUTCOMES

By conducting this research the researcher aims at finding the answers to the research question and sub-questions. The answers should help identify the business value perceptions in managing IT risk management in control structure environment, and how the business would realise the value. As it was indicated in the literature review, business value comes in many shapes and at different levels within the organisation's business and IT interaction: strategic, financial, and operational. The outcomes could be presented in a matrix that show business and IT perceived values.

Identifying business value would contribute to successfully address other problems raised in the literature review. For example, this could indicate the best practice in keeping effective and efficient IT risk management process that underpins up-to-date IT risk profile, which would ensure secure and reliable IT systems. In addition, it could provide recommendations on how to leverage other activities for example compliance program, internal and external audit cycles. All these could be devised in the form of guidelines that could be presented in a table or an appendix if deemed necessary.

It is not anticipated that this research could quantify business value because of the limited time. However, identifying various value forms could pave the way for future research that would aim at quantifying business value which is highly desirable. Analysis method like content-analysis could be utilised through an in-depth longitudinal case study to achieve that.

3.6 CONCLUSION

The review of problems that have been raised in the literature review helped to identify the key problem for this research. It has been argued that identifying business value gained from managing IT risk in control-based structured environments would help provide answers for other problems raised in the previous Chapter. A selection of case studies that researched subjects in the same domain was reviewed and the adopted research methodologies were examined. Reflection on the main problem, the research question, sub-questions and hypotheses have been presented.

Available research methods for researching IT systems both qualitative and quantitative methods, were reviewed. By reflecting on the reviewed research while examining the research objectives, the research methodology design was devised and justified. It is proposed to utilise case study methods in two large organisations in public sector. By adopting an exploratory and positivist paradigm assertions that have been theorised will be tested through analysing data utilising quasi-judicial method to interpret qualitative data.

Data will be collected in various ways: semi-structured interviews, document collection and diary recording. The case study was designed to be conducted in two companies to validate and replicate the findings through a cross-case analysis. Although the design of the case study and data collection methods were thoroughly discussed by considering internal and external factors, there are some limitations as is the case with any research methods. Chapter 4, reports the results. A thematic analysis will be performed by coding the data utilising CAQDAS - NVivo 8.0 and the outcomes of the field work will also be reported in Chapter 4. In Chapter 5 the analysis and discussion of findings will be presented.

Chapter 4

Research Report

4.0 INTRODUCTION

In Chapter 3, the research method was devised to be a qualitative method by conducting a case study in two large local organisations. The selected research method was reasoned and justified through a systematic development of ideas. A discussion started with exploring a number of research reports on similar topics presented by various researchers. In those papers a case study method was the preferred research method. However, different data collection techniques were utilised, for example single case study versus multiple case studies, surveys versus face-to-face interview. Furthermore, the industry type and length of the research were among the other factors that were examined. Thence, the research problems were discussed again and sorted in relation to the focus of the research. The focus was to be on Identifying Business Value (see section 3.2.2). The research question was formed to focus the research on finding the answer/s from supporting and detracting evidence to the problem-focus of the research. A set of hypotheses were devised to further test the proposed theory utilising the collected and analysed data. At that stage, various research methods were explored in attempt to identify the most suitable research method that would suit the research topic. The research method was developed from the literature as well as the data-collection methods, taking into account the nature of the research and available resources. As a result it was decided to conduct a comparative case study in two organisations. Conducting semi-structured face-to-face interviews was proposed as the main data collection method. Sub-questions were derived to help in directing the semi-structured interviews.

Following the proposed research method, semi-structured interviews were conducted in two organisations in the public sector. Although the selected organisations are in two different industries Health and Media respectively, both organisations have large IT teams and have forms of structured control environments. The interviews were carried out with people in IT, internal Audit, project and program office (IT) as well as business representatives. Documents were collected to further examine the gathered information. In addition some publicly available documents were downloaded from the organisations websites.

This Chapter reports and presents the collected data. The collected data will be coded using NVivo 8, a software package for qualitative data analysis. Thematic analysis will be applied as was proposed in Chapter 3. This chapter is structured as follows: section 4.1 explores the preparations for the field work; section 4.2 outlines the selected case studies, while section 4.3 reports the coded data. Lastly, section 4.4 concludes the Chapter 4. Chapter 5 presents the analysis and discussion of findings.

4.1 FIELD WORK – PREPARATION

Personnel in the two organisations were contacted in compliance with the ethics requirements and interviews were arranged with a number of staff in IT, Audit and Business division. Once the name and contact of the interviewees were decided, communications were initiated between the author and the interviewees. The aim of early communication was to build a rapport with the participants and to convey the purpose of research and an idea of what the interviews were about. In addition, AUT research protocols relating to the confidentiality of the collected data and identity of the organisations as well as the participants were communicated.

The set of interviews were conducted in Company A operating in the Health industry, followed by another set of interviews in Company B, which operates in the Media industry. The break-time between the two sets of interviews helped to identify any pitfalls that had been un-intentionally taken place in the first set of interviews. The learned lessons helped to conduct the second set of interviews in a better way, for example, asking direct questions, and managing the time efficiently. The author spent substantial amount of time rehearsing and preparing for the interviews, in addition to collecting as much information as possible about the organisations from their web site. However, some variations were encountered that had to be dealt with to ensure activities took place as planned.

This section reports the findings of the field work, exploring first the variations to the proposed research method and data collection techniques will be shown in section 4.1.1.

4.1.1 Variation

In reality it is inevitable to execute what has been planned without encountering any issues. When that takes place and in order to to achieve the objectives the plans could require some changes to various degrees. The former statement is prevalent when conducting field work where the researcher has to meet with people from different backgrounds and attempts to solicit information from them within, a limited period of time. Various factors cause that, for example, people are not available because of other work commitments, or are changing jobs. Nevertheless, a researcher should develop an alternative plan with feasible actions to counter those kinds of issues without jeopardising the overall plan. In conducting a case study in two organisations, the author has encountered some issues and had to adjust the original plan. However, the issues were not major and no substantial changes were made to the original plan.

For Company A approval was granted to meet with five people. One staff member, the information security manager, left the organisation before the interview date. In addition, it was not possible to meet with the business representative. However, quality data were gathered from the rest of interviewees, who represented information systems and internal audit. The author planned some questions for the interviewees, aiming at gathering business views on IS performance, and triangulating that with information collected from the IS strategic plan that was downloaded from the organisation web site. Furthermore, one participant who was new on the role, had spent a few months only that did not give them enough time to fully grasp the business and IS environment in the organisation. However, that particular participant's role was managing service desk, application and network support, and proved to be quite informed and contributed very well to the research. Another matter that hindered the data collection was when an interviewee was not prepared to answer a question, or if he/she could not or did not want to answer particular questions.

As it was noted in the opening paragraph of this section, the author communicated with prospective interviewees before the interviews, to build a rapport. However, for each interview it was still necessary to spend several minutes to break the ice before proceeding into the interview itself. That was accommodated by allowing some extra time between interviews. Those breaks were arranged to record some notes, if necessary, and to prepare for the next interview. Not surprisingly, one interviewee came a bit later than the scheduled time, which impacted the next interview. However, the author managed to complete the interviews, and later followed up with the interviewee and collected that data the was needed.

All four interviews were conducted on the same day, and because of the time limit and the nature of the business, it was not possible to stay on the site outside the scheduled time. For that reason, there was not a diary recording in the manner that was proposed in the devised research method. However, the author utilised the diary recording to capture thoughts and ideas around the research topic various aspects. With regards to the organisation documents, only someof the relevant documents were collected, as not all documents are in the public domain. After transcribing the interviews the author raised some questions and sent them in emails to solicit more information. Although not everybody responded overall the responses were sufficient.

In Company B one person had to withdraw from the interviewing process, and the author managed to meet with the same number of people as in Company A. However, for this company a business representative was among the participants. Furthermore, the initial plan to conduct the interviews was delayed for a while as some of the staff went on leave. That put some strain on the research plan, although it was still manageable. Despite Company B having published many documents on their web site, they were not so relevant to IS, as it was the case for Company A. All interviews were conducted on the same day as planned, except one person who turned up a bit late. As that person holds a profile that encompasses IT network, security, and risk management, the author arranged another date and time to further interview that key person. On the other hand, the author managed to get a site tour that provided better understanding on IS-Business engagement. Similar to what had happened in Company A, some questions went without an answer, because either the participant was not ready or they might have felt uneasy to answer. However, that scenario was anticipated to happen especially after the experience in Company A, so it did not cause any concern.

With regards to the diary recording, it was a replica to what had happened with the first company and the author utilised that in noting down thoughts and insights to answer the research question. As for the other type of data collection, the organisation's internal auditor kindly provided many documents. Unfortunately, the needed documents were not in the public domain, for example, IS strategic plan, risk register, incident report samples. For that reason it was not possible to verify some of the claims that were made around IS performance.

For both cases, the author had anticipated meeting 5-6 people, however only 4 people were interviewed from each company. The time constraint caused by managing the access authorisation and ethics processes impacted on subject availability. However, given that the research duration is limited to the academic calendar, the author is satisfied with the outcomes of the data-collection procedures.

4.2 CASE STUDY SELECTION

Lin (1984) indicated that for a comparative case study it is recommended to report the findings of each case study and then to conduct a cross-case analysis, seeking a replica of the first case study findings in the second case study. The author is happy to follow the indicated approach; hence this section will be structured in the following way: Company A will be discussed in section 4.2.1, and Company B in section 4.2.2. The findings for both companies will be reported in section 4.3. As for the cross-case analysis it will be undertaken in Chapter 5. The same data collection procedures were applied for both companies. Furthermore, by analysing the interview transcriptions, common themes were found, and the data were coded around the same themes. However, it is anticipated that the occurrence frequency of some of the evidence would vary from one case to the other. It is worth mentioning that the terms Information Technology (IT) and Information Systems (IS) are used interchangeably, since the author followed the convention used in each company.

4.2.1 Company A

As it was indicated in section 4.1.1, company A is a public-sector health industry organisation in the North Island of New Zealand. It is quite a large corporate organisation with staff totalling 6000, and providing health services for around 8% of New Zealand population, according to their web site. The organisation has an Audit and Risk committee that, among the overall enterprise governance and audit, oversees activities in the IS with regards to auditing, risk management, and IS governance. In addition, there is a Quality and Risk group that manages the overall risk and produces annual risk plan as part of the District plan aligned with the Ministry of Health (MoH) risk management requirements. The organisation coordinates with many government and non-government organisations as part of their business requirements. In addition, the organisation is required to comply with a number of Acts, for example Health and Disability Act 2000, Public Records Act 2005 and Privacy Act 1993.

The organisation has IS team with 100 staff, that could grow to 150 if contractors are taken into account. The IS is headed by a CIO who reports directly to the CEO and to the Audit and Risk committee. The IS is structured in several teams and functions providing the organisation with information services. In addition, the organisation outsources some of its IS functions. A consulting firm provides Company A with services around IT governance, Audit, and risk management.

semi-structured face-to-face interviews were conducted with four people from internal audit coded with Internal Auditor (IA), enterprise architecture coded Enterprise Architect (EA), program office coded Program Office Manger (PM) and desktop and application services coded Desktop Service (DS). Each interview took between 30 and 45 minutes, and was recorded using a digital recorder. The interviews started with brief introduction of the author and the research objectives. The author had spent some time browsing the organisation's web site and gathered as much information as possible, which helped in building the rapport with the interviewees. In addition, the gathered information helped in forming a picture of the environment and, in this case, identifying some issues that the organisation faces. For example, the IS strategic plan document indicated that there are limited resources, and the demand exceeds the supply; also there are many projects that require prioritisation, which does not seem to be business driven. This issue was raised during the interviews and that helped immensely in stirring the conversation and gathering valuable information about a number of underlining issues. While a set of sub-questions, as discussed in Chapter 3, were used to focus the interviews around those questions, some other questions were made on the spot as they were deemed necessary to ask. That helped in interacting with the participants and helped in stirring the interviews and made them thought-provoking conversation. That technique was necessary as one of the objectives is to gather participants' perceptions on various aspects of the researched topic.

Table 4.1 presents the source of data that has been collected from various people and other sources.

Table 4.1: Company A Data Sources Summary. (Author, 2011)

Data source	No. of Items	Details
Recorded interviews	4	Internal Auditor (IA) Enterprise Architect (EA) Program Office Manager (PM) Desktop Service (DS)
Collected documents	4 Documents plus the company's web site	Organisational structure Change Management Assessment worksheet IS structure IS strategic plan
Sighted documents		Some documents (internal use) were sighted, framework diagram, policies.
Diary recording	1 Book	3 days of diary recording, during preparation while and after conducting the interviews.

The interviews were later transferred to the author's PC, who transcribed the sound files after coding them with their respective participant's role-code. Transcription took considerable amount of time, and the generated word documents were revised a number of times to ensure all conversations are captured. A final revision was made to delete the 'noise' like 'um' and 'un' and added some notes when the author was sighting some documents or computer screens. In addition the author made some notes for each interview, which were either added to the document or will be added as a note document into Nvivo8.

4.2.2 Company B

The other public sector firm Company B, operates in the Media industry. A number of face-to-face interviews were conducted in a similar fashion to Company A. The company's premises is in the North Island; however it has many smaller size branches in various locations around New Zealand, although all IT systems and functions are located in the main building. While the total number of staff (940) is smaller than that in Company A, it has similar teams' structure with IT staff number around 73. The company has Audit and Risk committee that oversees the internal audit and IT functions. There are a number of Acts the company is required to comply with, for example: Crown Entities Act 2004, Companies Act 1993. The company is required to file annual reporting, as it was stated in their published documents on their website, Statement of Intent and Interim report.

As it was indicated IT staff is around 73. However, the company did not outsource any of its IT functions, as its intent is to develop and retain in-house expertise. The company, however, does hire specialists to complement their expertise in designing and implementing IT solutions. On the other hand, the company hires a consulting firm to perform their statuary external audit including IT audit. While the notion of developing internal knowledge in best practice and IT control framework has some risks, it is necessary to ensure these practices are embedded within the organisation's culture. The risk in developing such a knowledge and practical experience in those best practices and frameworks is that they require time and long term investment. In addition, implementing a control framework still requires an independent validation.

semi-structured interviews were conducted in the main building where the IT teams and internal audit are based. Four people were interviewed from internal audit coded with Internal Auditor (IA), program office coded Program Office Manger (PM), and information services coded Information Service (IS) and manager of shared services for HR system coded Shared Service – HR (HR). The interviews varied from 25 to 50 minutes. The internal audit and information services managers offered more time as they are more involved in the design, decision making, and monitoring of IT systems functions. During those interviews various documents and charts were collected and some web pages were sighted for non-public documents. Table 4.2 depicts the various data collection methods.

Table 4.2: Company B Data Sources Summary. (Author, 2011)

Data source	No. of Items	Details
Recorded interviews	4	Internal Auditor (IA) Information Services (IS) Program Office Manager (PM) Shared Services - HR (HR)
Collected documents	9 Documents plus the company's web site	Organisational structure Technology chart Audit and Risk Committee – Terms of reference Internal Audit – Objectives document. Directors' Profile – Company's board Company's Operation Policies Company Senior Leadership Team (SLT) chart HR chart Annual report Statement of Intent
Sighted documents		Some documents (internal use) were sighted, policies and procedures, incident reports.
Diary recording	1 Book	3 days of diary recording, during preparation, while and after conducting the interviews.

4.3 FIELD FINDINGS REPORT

The interview transcriptions were reviewed to find common themes that have been expressed by the participants. The themes were coded around the focus of the research with the aim of finding answers to the research question. These are: Establishing risk context is discussed in section 4.3.1, while section 4.3.2 includes finding around how the organisation manages its IT risk. Section 4.3.3 reports the established frameworks and best practices and their status. Section 4.3.4 explores the benefits the organisation gains from implementing those frameworks. The last three sections 4.3.5 and 4.3.6 and 4.3.7 respectively explore the existing challenges, problems and solutions that the participants perceived as necessary to overcome the defined challenges and problems. Table 4.3 summarises the main elements of the findings with their corresponding nodes and page number.

Table 4.3: Fieldwork Findings Summary. (Author, 2011)

Element	Node	Page No.
IT Risk Context	• Business Requirements • Regulatory Requirements	97-
IT Risk Management	• Committee • Roles and Responsibilities • Ad hoc • Process • Risk Management Tool • Risk Register • BCP-DRP	103-
Existing Control-Structures Framework and Best Practices	• COBIT • ITIL • TOGAF • Prince2 – PMI • ISO 27001 • Policies • Others	115-
Benefits from Control-Structure Frameworks and Best Practices	• Business-IT Alignment • Effectiveness • Efficiency • Security • Defined Roles and Responsibilities • Communication • Holistic View - Planning • Increase IT Credibility	123-
Challenges	• Immature IT Risk Standard • Lack of Awareness • Lack of Local Expertise • High Resource Consumption • Lack of Executive Management Support • Business and Technology Demands • Resistance • Complexity • Many Frameworks • Ambiguous Regulatory Directions	141-
Problems	• Business – IT Silos • Business – IT Misalignment	157-

Element	Node	Page No.
	• Business – IT Structures • Risk Management Function • BCP-DRP • Reactive not Proactive • User's Behaviour	
Solutions	• Define Objectives • Consult 3rd Party • Make Use of Major Incidents • Educate and Train • Improve Business – IT Communication • Customise Frameworks to Business Environment • Demonstrate Value to Business • Integrate Frameworks and Best Practices • Co-operate with Internal Audit	165-

4.3.1 IT Risk Context

As discussed in Chapter 2, section 2.1.3.1, it is imperative to define IT risk context in terms of regulatory and business requirements. The findings are categorised in two sections: Business Requirement and Regulatory Requirements.

4.3.1.1 Business Requirements

The following sub-sections present fist the findings about Company A and then about Company B. Each sub-section is to be structured similarly to the end of the Chapter 4. Interviewees are coded according to their role (see table 4.1 and 4.2 for interviewees' coding details).

4.3.1.1.1 Company A

As it was indicated, Company A operates in the public Health sector that requires coordinating and co-operating with a number of District Health Board (DHB) as it was indicated by interviewee DS "Yes, part of the regional DHB, so we work, I don't know how closely it is, with number of DHBs". Participant DS further confirmed that IS should be available as required, which would be quite a challenge.

When asked about the organisation size and number of staff, participant EA replied

> "Between contractors and permanent, there are about 90 staff, but there is also big service contracts with organisations like Gen-i and a 3rd party vendor, so it is actually hard to quantify exactly how many people in IT, at any given time it could be anywhere between 5-30 people of those working on different things, so somewhere between 100-150 IT staff"

Interviewee EA further added that "the helpdesk has not been outsourced, the desktop management has been outsourced", and indicated that outsourcing has risk "it involves a lot of risk, so there is I think, awareness we need to identify risk". In addition, interviewee EA indicated that

> "Up to now, they are worried about clinical risk, health and safety, IS is sort of not really been looked at, Security is been physical security not data security".

That reveals the risk awareness level within the organisation. Furthermore, interviewee EA described one other side of the risk context when talking about the kind of used technologies within the organisation and said:

> "And mobility and the proliferation of mobile devices, people they want to use, effectively people want to bring their own technology and use them at work, the fact that IS would never be able to keep up with the investment that is required so you got to support those emerging technologies in some way but still maintain security, privacy, integrity, the daily challenge."

In line with what EA described the risk status within the organisation, interviewee IA indicated that because of the current Business-IT misalignment there are risks that have not been identified. IA stated "So there is a lot of IT risks out there in the business they know about, but IS don't know about, there is no merging, so there are separate risk registers and risk plans."

Interviewee PM stated that "in this organisation they don't understand the concept of enterprise, you know, a hospital in this case is made of 23 departments and a very thin layer of management who sits on top". PM continued and gave a grim picture of the technology current status by stating

> “the fact the matter is all our technologies need to be replaced in 3-4-5 year time’s span, the volume of change is really plus, we have new requirements that always cascading in we have got stuff that is not needed any more that has to go out. It is a big risk situation”

And further added

> “most of problems we can’t fix, they are around the user’s behaviour, and those kind of top of the hill (hospital) there, are inherently signing off on their bad behaviour, we have been there and fought good fights about unique logins, we took away all the generic login, but they turned on their individual ones generic logins, so we are screwed.”

4.3.1.1.2 Company B

Company B work force is mostly in the North Island and it has about 940 staff with about 73 IT staff members and some contractors brought in when needed. There are smaller offices at various locations around New Zealand. However, all IT operations and functions are centralised in the company’s main building. As a media company, their core business is the content as it was indicated by interviewee IS:

> “Our value is in within the content and taken that content of, as long we have the right controls to ensure that the content is protected and the rights are protected within the content then as far as the business risk is the rest of it is that really just about normal standard sort of cooperate business risk is not that overly needing of strong indoctrinated process or indoctrinated policies that control things to an Nth degree”

IS elaborated further on where most of the funding goes:

> “the majority of the company’s funds focused on content and the right of content the “lion share” of the business revenue of business profitability in that space”

That reflects how important the content is for this company. Similarly, interviewee IS pointed out another angle to the focus of the business in Company

B: “Our key focus on that is transmission and keeping on air, the question always does it keep us on air”. Furthermore, interviewee PM emphasised the same view:

> “News is performance and strategic objectives are being the first if something happens here, it is going to happen to other media company, so we want to be able to get to air first, rather than some other company, if something happens in here”.

For those reasons, interviewee IS identified the main risk here is the content:

> “our biggest risks are, loss of rights and loss of content, if somebody steals materials of one source and puts on their show, before it goes on the air in the US, that would be very poor for us, as poor of reputation that is our biggest dollar value, as known media company brand with high reputation in the industry, and with the general public and the ownership of two TV channels in NZ, so ours have a reputation and strong brand is not damaged by content failure is the most critical one, the other risks from IT point of view, is that access, is the wrong people be able continue to access services that are here”.

On the other hand, the organisation undergoes a major shift in adopted technology as indicated by interviewee IA:

> “We are moving to digital, broadcasting to move away from Analogue, it is called project xyz, so we replaced lots of our stuff, and we are going to end up now, instead of the old fashion VHS tapes, everything is going to be on digital, it would take a bit of time , but that’s we are going “.

Furthermore, interviewee IA pointed out how IT supports the business expansion:

> “They fit in helping the put in place the infrastructure so for example, brand new cameras, they help select all cameras and get the entire network stuff”.

Interviewee HR pointed out the management’s directive to update the financial system on a regular basis:

> “So we were told that we need to upgrade the system quite regularly, like annually, suppose that even there is an assessment of that, Service provider will do, in SLA we can also

> pull in another external party to do a technical audit if we wanted to, we get more of unbiased review of the system".

It was noticed that the culture in Company B is to develop in-house expertise and to reduce contracting as well as outsourcing, as it was described by interviewee PM:

> "No, there is not really a lot outsourced there is few systems that I suppose most of it just vendor, most of the systems we have on site, there used to be data centre with a 3rd party vendor, but not sure if that still in use if you can check with Infrastructure team, but I don't think it is there anymore. There may be some back up, I'm not sure".

4.3.1.2 Regulatory Requirements

4.3.1.2.1 Company A

The other side of the IT risk context relates to government regulations, acts and industrial standards. When asked, interview IA indicated that "I'll say those are the key ones, probably there are other acts". Interviewee PM indicated however, that

> "There are security standards around communication of information using HL7 and the underline infrastructure, but not very well understood or communicated, to be honest, they are probably not that applicable because they are about a piece of technology and trying to solve a very narrowed point or component within the entire IT function across the sector"

Furthermore, interviewee IA indicated that Company A would have to be aligned with MoH directives

> "The ministry have been declaring it is going to be more regionalisation and nationalisation particularly around IT systems and solutions, to the extent that have within the national health board within the MOH they have special IT committee if you call that, and they are going to direct or are directing national solutions, so the DHBs are not going to spend big money in millions on their own solutions without going through

> the national forum or committee and they are expecting them to work towards single national system, say financial and HR, Payroll systems even clinical systems eventually. Because it is going to take long time. They are trying to cover off nationally the risk they are having or these different systems they are not integrated, they are going to bring it together."

This was confirmed by interviewee PM, although the picture was presented slightly differently:

> "MOH have produced recently a national Health IT plan, it is a poorly constructed collection of desperate ideas, that provocatively knit together to meet an equally ill defined set of outcomes by the minister they are all palatable to his political appetite, whatever that means, it boils down to incoherent directions even or less in terms of how it aid by way of standards or policies to help us in decision making"

4.3.1.2.2 Company B

The company is required to comply with a number of regulations, for example: Crown Entities Act 2004, Companies Act 1993. In addition, the company is required to file annual reporting, as it was stated in their Statement of Intent and Interim report, documents published on their web site. That was further confirmed by interviewee IA who indicated that "we are subject to Information Act".

Interviewee PM pointed out the number of Acts and regulations the business applications are required to comply with and stated:

> "business Acts or financial reporting ones, we have got HR system that has to be compliant with HR Act, Employment Act, and Health and Safety, typical generic Acts. Similarly, interviewee HR stated what the financial system is required to comply with "compliant with the legislative changes, tax changes".

On the other hand, as Company B as a government agency the IT team has developed and published a set of IT security policies that are compliant with ISO and governmental security standards as it was mentioned by interviewee IS: "They are compliant with ISO and SIGS"

4.3.2 IT Risk Management

In Chapter 2 section 2.1.3 IT risk management process was discussed with its various elements. Organisations have different ways for managing their risk; in this section the findings are categorised based on how Company A and Company B manages their IT risk, and how this is related to the overall organisation’s risk. This section is arranged in sub-sections (4.3.2.1 – 4.3.2.6) each exploring the various aspects of the IT risk management in the selected case studies.

4.3.2.1 Committee

4.3.2.1.1 Company A

Company A has a Risk and Audit committee as indicated by interviewee EA: “at the board level, IS now has to report IS risks into the risk register – to Risk and Audit committee, so we look at risk from IS perspective”. Similarly, interviewee IA who is in charge of Internal Audit and conducts risk based audit confirmed:

> “Our place within the organisation is: we report directly to the audit committee, and has a dotted line to one the executive manager the director of the director of the board governance - so that we have complete independence so we can review anywhere in the organisation”.

4.3.2.1.2 Company B

Company B has an Audit and Risk committee that oversees the overall organisation risk and internal audit functions. This was confirmed by interviewee IS who indicated: “We have got a risk management framework is approved by the audit and risk committee”

4.3.2.2 Roles and Responsibilities

4.3.2.2.1 Company A

With regards to roles and responsibilities in managing the overall risk or the IT risk, there doesn’t seem to be clearly defined and communicated roles and responsibilities. Interviewee IA indicated that ”what we do is prepare annual internal audit plan that is pretty much risk based, so we either indentify risks throughout the year, if we don't address it immediately, we put in our tentative program for the upcoming finical year”. Interviewee IA further added:

> “When it comes to internal audit, we aren’t expected to know all the risks or the regulatory compliance requirements we expect the management be aware of that and to know that for their area and put their risk plan, we basically leverage of their risk plans and try to identify any gaps they may have and will do our own.”
>
> However, when interviewee DS was asked about who manages the risk, the reply was “Yes I think that IA, just wondering whether IA is part of that risk team. I was aware he was just an auditor he didn’t necessarily follow the looks of risk.”

On the other hand, interviewee EA indicated that: ”what we do now do, so we got the Q and Risk team”, which is a function within Company A that manages the overall organisation’s risk. However, interviewee IA mentioned that:

> ”we do have a quality and risk function here it reports to that role – on a diagram - I think it is quite disjointed so I cannot give good news about it, Quality and Risk are meant to gather all the risk across the organisation and prepare a top level risk plan”

When the author asked interviewee PM if the Quality and Risk function is inactive, PM’s reply was quite cynical: “Gee, you are kind; I call them dead people, than inactive the Quality and risk people. I think they have a pulse at some stage; they do absolutely no quality and risk management around IT”.

4.3.2.2.2 Company B

Interviewee IS from the IT structure holds a portfolio that oversees IT risk and security, as stated by interviewee IS: “in my space I hold BCP, risk and security network and software architecture roles”. Furthermore, interviewee IS indicated that various IT team members would conduct self-test on existing controls to ensure their effectiveness, although it is not part of their core portfolios:

> “It would not be part of their core portfolio, the person who does it on extra-autonomously but they have been given special privileges and special access to able to do that review and

> report, and they have the skills to do it, so rather then bring a 3rd party that have the set of skills we developed the skill internally enabled them with series of tools giving them the access so that they can repeat the processes and in a sense to keep the core team honest".

Part of interviewee IS responsibilities is to create and maintain IT risk register, as it was stated:

> "We have risk register and I update that now every six months, by talking to whole range of top senior managers, we report that to audit and risk committee and effectively to the board"

When the author asked interviewee IS if the internal audit team verifies their self-test process, the answer was positive "It does". Furthermore, it was indicated that the external auditor conducts annual audit as well, as pointed out by interviewee IS "as well as the consulting firm (external auditor), they also check us annually".

On the other hand, interviewee PM manages the project risks: "So I guess one of my objectives is actually, my role quite new role, is actually re-implement that, so reduces risk with project failure".

4.3.2.3 Ad hoc

4.3.2.3.1 Company A

It was interesting to get a different perspective on how well IT risk is managed within Company A, as it was indicated earlier by IA:

> "What we do is prepare annual internal audit plan that is pretty much risk based, so we either indentify risks throughout the year, if we don't addressed immediately, we put in the our tentative program for the upcoming finical year, so we talk to all of our senior and executive managers during planning process, audit planning process, and we suggest topics to them and we talk about risks we know about, we ask them about their risks, we get the risk plan available."

IA further added:

> " Within – Key IT risks – and we spend a good time with CIO about that, so we put together our plan and for the last say half a

> dozen years we generally we always included IT risks in our plans to some extent. This year we've only included one minor IT item because we found when we audited IT to a large degree in the previous years and they (IT) actually put together a work program they want to focus on the next year and a half - so we chose to let them out of the audit plan this year"

IA continued: "Knowing that they have a heck lot of work to do, we let them get on things, and in a year or two we will come and identify other areas of IT risk we want to cover". Interviewee IA described what the Quality and Risk function does and stated:

> "Quality and Risk are meant to gather all the risk across the organisation and prepare a top level risk plan so it meant to come from the bottom up, but we do not have too many bottom level risk plans, they are not that mature they are not sound, I think what happens is they prepare top level risk plan kind of different from the bottom one it is not reformed from the bottom ones, and as I indicated before that IS risk plan and risk management still hasn't got to good standards anyway."

And further added about the overall risk plan:

> "The top level risk plan is framed trying to meet some of these risks the MoH aware off because our top level risk plan goes to them, and our annual plan and strategic plan, the top level risk plan has to echo what MoH expects to see. The low level risk plans are quite different and you mentioned you asked business what are your objectives, what could go wrong that's where I think our business has not matured yet. When they do the risk plan they think of someone trip over the computer wire so fall out of bed. They don't say what are our objectives what are we here to achieve what is going stop us to achieving those goals. Whether IT has gone through the same questioning process I don't know. What IT trying to achieve and what could go wrong, so this might identify risks, so our system going to crash or virus will attack"

Interviewee IA summarised the IT risk status and said: “So there is a lot of IT risks out there in the business they know about, but IS don’t know about, there is no merging , so there are separate risk registers and risk plans”. And further added:

> “I think it has been accepted that the risk management processes within IS are not up to standard, even though the organisation has the systems, tools and processes to facilitate sound risk planning and management. I understand that the IS department is working on this area of their operations”.

When the author directed those questions to the IT managers, answers varied. For example, interviewee EA indicated:

> “I think that, risk awareness of identifying and managing risks is an organisation is starting to grow, up to now, they are worried about clinical risk, health and safety, IS is sort of not really been looked at, Security is been physical security not data security, but there is never been a holistic view of this.”

On the other hand, interviewee DS indicated:

> “Within the area, there is no formal risk management. Let me rephrase that, we have incident management which is handling certain levels of issue, we’ve got change management, which is handling or trying to mitigate the risk to the business from infrastructure point of view, but there is no formal risk management for other areas. What you normally class risk management, there is not any, so, when I first got here, I pointed out that there is not any. And I think, GA (IT security that has left), also was trying implement, some risk management, but it doesn’t seem to go anywhere at the moment. You actually, reminded me, I need to start that again, I drop off my list to do.”

DS further added that:

> “RM, in IT is fairly mature, I’ve been collating risk of issues, which I send to the CIO on a weekly basis with updates, but they are not all of my area I’m responsible for, I’m just highlighting but there is no formal process to go through”.

However, interviewee PM pictured a better view on IT risk management and stated:

> "I think we have always managed our risk , as managers, this is sometime a little bit difficult for people in the business to realise that is we are working on a very short window of life span of our structured we manage and run it and deliver to them, the idea of risk management is second nature, everything we do is about risk management, because the fact the matter is all our technologies need to be replaced in 3-4-5 year time's span, the volume of change is really plus, we have new requirements that always cascading in we have got stuff that is not needed any more that has to go out. It is a big risk situation, and so we've always done that"

It can be concluded that risk is managed within functions and teams but not overall, neither is a holistic view taken when managing IT risk.

4.3.2.3.2 Company B

No reference was found in Company B data for this category.

4.3.2.4 Process

4.3.2.4.1 Company A

Although it has been described in the previous section that IT risk management is managed on an ad-hoc basis, some observations were made that a process for that purpose was being established. Interviewee IA refers to the process as indicated below:

> "There is national (DHB) risk forum that we all areas represented, and they created several years ago on a risk assessment tool. It pretty standard, looks at the probability, consequence, impact and most things, controls, and rates them and scores them, and coming up a scoring per risk, and IT or IS are meant to apply the same tool."

However, interviewee EA has another saying on that: "the risk management tool, is not actually a tool, it is basically a risk management process". Interviewee IA indicated there is a methodical approach that has been advised and followed to initiate adequate risk management process, as it can be seen:

> "to CIO credit, he has taken up on audit review we did probably several years ago around the IT control environment, and I'll show you an approach that was taken for an IT risk management. [IA looking for the document] something I can show you but can't give you – this is the approach we take for external-internal audit service provider, so taken that wheel and spike approach and with carried out our review of that quadrant and we did a deep wide audit how well IT doing in that area , and we are going to move around the wheel in the next maybe six years, 5-6 years trying to cover all those off but also what CIO did after we produced our report on this – we call it quadrant of IT effectiveness review , there were certain several recommendations but the CIO engaged a consulting firm as a consultant to work with IT to try and progress all improvements that need to be made on those areas and what a consulting firm do now they come in once a year and they revise the IT effectiveness by going through a whole series of questions and look at how people are perceiving the state now around those subjects and they rate from one to 1-4, 1 is very poor, and 4 or 5 is the maxim you can achieve the gold star standard, and so CIO or IS , say 4 out 5, we don't want to go to 5 it is too expensive, we try to achieve 4 for these and maybe 3 for some. So CIO gets external consulting firm to assess IS from that regard, try to cover all these risk area"

Interviewee EA stated that project risk is managed within project management framework:

> "So we identify for each project, as part of the project initiation, we identify the risks that project see, now often time that risk are related to dependency, time, people, money, but that the extent of it"

Interviewee PM elaborated more on project risk management and said:

> “What have done in the past we have come with effectively a gradient scale and we looked at things like: are we going kill somebody, then we go OK is it going to stop the service to work effectively, so we work our way down to its a nice to have then what we do, we score the projects and find out where they fit on that. It tends to be quite accurate, and then we draw a line across there, we’ve got bit more sophisticated as we moved on, we’ve said well we want to look at productivity, and with we got a lot better in managing the dependency you can’t do B unless you do A first, so we kind of clustered those projects up and funded them on that basis, then there are just the things that we were told we have to do. Or we have got a risk that it has to be dealt with whether it is of high priority or not, so that’s kind of the other form”

Interviewee PM further added:

> “We have a risk model, it has 8 characteristics, we manage risk quite strongly, in that , all projects have to have risk based lined and risk managed throughout the project, it is reported on a 14 days basis, and expectation basis and is aggregated into program reports”.

When the author asked interviewee PM whether the project risk management would consider the organisation’s risk, the reply was:

> “Unfortunately, no, we kind of, we try to come with a model that reflects what that would look like but the organisation does not have that.”

4.3.2.4.2 Company B

Within Company B there seems to be a number of defined ways for conducting elements of an IT risk management process. For example, when interviewee IS was asked whether they evaluate risk on regular basis, the answer was: “Yes, there is a monthly process, quarterly and 6 monthly”. Furthermore, interviewee IS elaborated in depth on how often security risks are logged, assessed and dealt with. Furthermore, a root cause analysis would be conducted to identify needed remediation, if any. In addition, there is a periodic review conducted by interviewee IS as part of their portfolio, as well as internal audit review.

> "Do we have any security risks or security issues logged and the investigation underneath that was that done to satisfactory level to identify if there is any further enhancement or improvements we can do, and basically I hold that portfolio, so I do that either periodically, 6 monthly, annually, Internal audit keeps us honest, to have a monthly schedule of activity so we go through and check various, IA could talk about that, in depth, one of the team actually go through, and has have a schedule of activity"

In addition, interviewee IS indicated that a further review is done by a 3rd party: "It does, as well as the consulting firm (external auditor), they also check us annually".

On the other hand, interviewee IS pointed out that IT risk is monitored through some IT functions at the operational levels:

> "The risk management entirely is really around going through the change management until we have a structured , we implemented service management reasonably well for incident change, configuration change, problem, and release, so we have a CAB , works on release, predominately on release".

Interviewee HR outlined the performed steps that ensure business applications meet business requirements stipulated by the SLA:

> "with the software provider we got technical reviews of the system, so that's an annual process we have implemented as part of our service level agreement with the Vendor, that probably, they do technical review to ensure the system compliant with what it needs to do"

Similarly, interviewee HR added that internal system check and verify are executed to ensure business risk within financial application is managed, as it is described:

> "The other thing we do, in terms of the content of the system, processing of pay, and variation, employee information, we have audit process checking after, following after fortnightly pays or monthly".

Interviewee PM stated that project risk is managed within project framework that has been established as part of project program: “we have a generic project framework, which includes risk and risk register and how to manage risk within project”. Furthermore, interviewee PM indicated that any project residual risk would be transferred to IT operational teams who would update the risk profile.

> “We have within technology we have got a crises hand book, which basically details what to do within crises within technology department depending on what the scenarios are and what systems”.

4.3.2.5 Risk Management Tool

4.3.2.5.1 Company A

Interviewee IA indicated that there is a tool based on AS/NZS 4360 as noted here: “We have the standard tool at all [DHB- business] use it comes from a document, I’ve got it here, [sound of getting a document] we have a risk module comes out of AS/NZS 4360”. However, interviewee EA described it differently:

> “The risk management tool is not actually a tool, it is basically a risk management process, and at the moment the tool as far I’m aware, we haven’t implemented a tool outside a spreadsheet, OK. I know that one of the guys might have little Access db to keep track of the stuff, but it really it is not a tool that might expect when you would put in the different types of risks and do risk analysis you may do all SOX requirements that you would expect to have project our areas and the vulnerability you that need to be researched, it doesn’t stuff like that, what it really most it does, is keep a list of things that actually have been reviewed”.

4.3.2.5.2 Company B

No reference was found in Company B data for this category.

4.3.2.6 Risk Register

4.3.2.6.1 Company A

As far risk register is concerned, Quality and Risk group prepares it. However there is no consolidated risk register, as it was indicated by interviewee IA: “[IT] risk register is not fed to the Quality and Risk group risk register”.

4.3.2.6.2 Company B

Company B records their business risks in a risk register, however there are other risk registers as outlined by the participants. Interviewee IA indicated how business risk is registered as stated, “risk is anything and everything is just one, technology may operate their own risk register IS may be able to talk about that”

However, interviewee IS indicated that there is one risk register for IT and another for project management:

> “We have in a sense two, one for the project, portfolio project management tool called i-Line, has the rise and manages risks in project, we have an overall IT risk register, these are the one that are generally raised by people through an email or through the server centre”.

Furthermore, interviewee IS pointed out the regular check and the reporting line within the organisation structure as noted:

> “We have risk register and I update that now every six months, by talking to whole range of top senior managers, we report that to audit and risk committee and effectively to the board”.

4.3.2.7 BCP – DRP

4.3.2.7.1 Company A

With regards to BCP-DRP, interviewee EA mentioned that there are no DRP capacities as noted:

> “There is, there is BCP plan from, ah, from the health DHB perspective, I’m not aware of the extent that it covers the IS infrastructure, the reason I say , that is we don’t have a DR capability from IS perspective, so if our core data centre goes down we do not have another data centre to fell over to. So the BCP [business] will have to include a manual processing”.

4.3.2.7.2 Company B

Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) are vital to business survival, although it comes at a cost. Interviewee IA answered positively when asked if there is a BCP and DRP: "Yes, there is, we have that, because it is important and our key focus on that is transmission and keeping on air". Furthermore, interviewee IA elaborated on BCP and DRP capability and testing procedure for the organisation:

> "As part of that project now it has finished that gives us new capability we didn't have before so part of the follow up work is to look again at DRP and BCP; but we do have a formal structure and every business area has a crises plan and crises champion and about every 2 years, we do simulation it is sort of going , last time we went to the hotel abc, they told us somewhere hit by earthquake and people what would I do and they got , main department has box, and supposedly the senior people has got one of those at home, and one of them here, and they got the box out"

On the other hand, when the question was directed to interviewee IS who oversees the BCP within IT functions, the reply was not so positive, as outlined:

> "Oh, it is a big question, from an enterprise level NO, from system specific level we have some, from a business as a company content free delivery television business, and we have some capabilities"

And further added:

> "Right now the company BCP is around resiliency and redundancy within single site we are expanding that out into dual site, so DR, right now we don't have any DR outside the building, we have DR inside the building, there is quite a lot of resiliency dual path-ing, resilience redundant platforms, or pieces of component that we can bring thing to bare".

Interviewee PM confirmed what had been said with regards to the BCP and DRP capability within the organisation, and indicated:

> “We have within technology we have got a crises hand book, which basically details what to do within crises within technology department depending on what the scenarios are and what systems”.

When the author asked if that is kind of a DRP, the answer was “Yes”. Furthermore interviewee PM outlined how the inherent risk is passed on to the operational team as part of the BCP and DRP update, as stated:

> “So within that I suppose to me inherent risk is then passed on to the operational support team and that there is part of the release to production documentation that looks at BCP and DRP processes, have they been documented for the new system or whatever we were doing to pass on to the support”.

4.3.3 Existing Control-Structures Framework and Best Practices

As it was discussed in Chapter 2 section 2.2, there are many IT Control Structure frameworks, standards, and best practices that many organisations could implement to manage their IT systems. Among those control structures are COBIT, ITIL, TOGAF, PMI, Prince2, or some kind of proprietary framework, in addition to defined policies and standards. This section explores the implemented control structures in sub-sections 4.3.3.1 – 4.3.3.7.

4.3.3.1 COBIT

4.3.3.1.1 Company A

There was no clear indication whether COBIT has been implemented fully or partially, as it was described by interviewee IA who indicated that there was an initiative a few years ago to implement COBIT and ITIL:

> “The impression I get is there are certain parts have been implemented, I can remember the term SIMPLE, I think SIMPLE are a service provider, that is meant to an initiative to install COBIT or ITIL, probably the ITIL “.

Furthermore, IA indicated that:

> ” I understand that ex-IS security manager – was trying to implement around those framework model COBIT and ITIL, I

> think CIO has been recognising them as well, because we have a couple of reviews carried out around that subject few years ago".

In addition, interviewee DS stated:

> "There was an audit done by a consulting firm using their mix of COBIT and ITIL, which a fairly standards of what you do, you self assess and then you get certain business people to comment on where they feel you are, creating spider web chart, and using all the colours where you are and where you want to be in few years. We are going through that as well, but there is no, I don't think we are aligned following COBIT methodology, it is a cut down COBIT, that's sort of fused with ITIL, from the consulting firm's perspective" .

Contrary to what had been mentioned previously, interviewee EA's answer was "but we don't use COBIT".

4.3.3.1.2 Company B

Interviewee IA indicated that COBIT is partially implemented within the company, as stated:

> "So, because I talked to them about COBIT, because I quite like the framework and the view is we are aware of it and we'll apply the principles and enough of it to meet our business needs"

Interviewee IA further elaborated on the reason behind implanting a light version of the framework, as noted: "But we are not going to go down the framework roads, because there is no value to the business in terms of doing a lot of detail". Interviewee IS shares the same view, however, it was indicated that COBIT was adopted in conjunction with IS 27001-2 to manage IT security and security governance:

> "So, where it is relevant we linking to it, as far as frameworks we have used both of COBIT and ISO 27001-2 – framework to look security poster and our security governance"

4.3.3.2 ITIL

4.3.3.2.1 Company A

ITIL best practices have been implemented widely within Company A, which is expected as ITIL have become well reputed in many IT operational functions, for example Helpdesk, Change, Release, Problem and Incidents Management. Interviewee IA indicated that there was an initiative a few years ago to implement COBIT and ITIL:

> “the impression I get is there are certain parts have been implemented, I can remember the term SIMPLE, I think SIMPLE are a service provider, that is meant to an initiative to install COBIT or ITIL, probably the ITIL, so we did two reviews about 4-5 years ago around the SIMPLE initiative they trying to install ITIL, I have to think because we are reporting that much, probably big part of it implemented, because it doesn’t come out of our standard audit, that something you have to talk to IT”.

Interviewee PM briefly talked about ITIL “Yes they are bringing ITIL and standardised, business analysis principally in new organisation”. However, interviewee EA elaborated a bit more on ITIL best practices:

> “We got the starting points of a lot of the components of ITIL, from incident management perspective, that’s pretty much embedded, there is the start of looking at problem management process, which has not begun yet, we have done incident management. Change management that has began, and now pretty well embedded, it needs to mature because today it treats them one size fits all where obviously in change that is not the reality. As for planning capacity management, from ITIL is just began so we got the first draft to that process, although the process has been signed off actively now has been kicked off. So that’s from the ITIL perspective, the component there are number of them, say in phase one process in place, that embedded in I think it is fair to say, from a demand list, wait list, planning, the particularly side, there is no really good functioning IS”

Interviewee DS talked in details about ITIL as DS manages the functions that ITIL excels at:

> "There are many different things, from the service desk point of view you are adding more management process how to handle the calls that coming in, making sure you are managing in more effective way and you can report on what is you are receiving that can then feed through into problem management if that's implemented, or you can start reducing or identify the root cause of the incident, so you can start reducing the incident that coming in, as you reduce the number of incidents, people do not need to ring service desk often, so they are generally happier. You have got the change management that you handling the risk, if you make any changes in the application or to the infrastructure or whatever it might be so you are reducing the chance of something going wrong which would reduce the number of incidents. You get to the cycle there. You get the capacity management side of things, which is another thing we started doing, which removes the risk of reaching full capacity before, the demands come there, so you are then improving the perception of IT department in the eyes of the business because you got less delay in implementing new solutions, that then fits in the change management side of things. You got to go through that".

Participant DS further stated:

> "[ITIL] it is providing better control over how the whole areas operating, you demonstrating you know what's going on, you managing it, in a way you are prepared for anything the business throw at you".

4.3.3.2.2 Company B

The IT division within Company B has implemented a number of ITIL functions and processes as it was indicated by interviewee IS:

> " The risk management entirely is really around going through the change management until we have a structured, we

> implemented service management reasonably well for incident change, configuration change, problem, and release, so we have a CAB, works on release, predominately on release”

Interviewee PM confirmed that ITIL best practices are utilised within IT, although as a project manager interviewee PM doesn’t use it as stated: “I’m aware of ITIL, I suppose, I personally don’t use it”

4.3.3.3 TOGAF

4.3.3.3.1 Company A

Interviewee EA indicated that The Open Group Architecture Framework (TOGAF) has been customised to the health industry and have been implemented within Company A, and was to be adopted by other organisations within DHB, as noted below:

> “TOGAF has been adapted for all the architectural work here DHB internally, we have basically taken the ADM module, and modified it for applicability within Health business and we call it health-based standards, so now within the geographic area – all of us have adopted and agreed to use the Health-based , which is the health view of the ADM. We, myself and another colleague are in the process of ruling this out nationally and getting all of the DHBs, outside our region from IS architecture perspective, se we are making progress”.

4.3.3.3.2 Company B

No reference was found in Company B data for this category.

4.3.3.4 Prince2 –PMI

4.3.3.4.1 Company A

In similar fashion to TOGAF, Company A has customised PRojects IN Controlled Environments (Prince2) methodology and called it Company A’s way, as indicated by interviewee EA:

> “We have project management framework, we use Prince2, but we don’t use COBIT, as for Prince2 it is modified to our need and we call it Company A -Way, we have taken Prince2

> methodology and of project management, and said what's applicable for our environment, now that has been rolled out across both health industry in the region, the program offices, have adopted the modified Prince2".

The above statement was confirmed by interviewee PM: "In Prince2 document it says to tailor the methodology to the business need, so we branded our tailored version, and called it Company A's way".

4.3.3.4.2 Company B

Company B has adopted Project Management Institute (PMI) framework for project management best practices, as it was stated by interviewee PM:

> "One of my responsibilities is looking after project management framework, so within that framework, we are trying to follow a standard, PMP or PMI, and Prince2 those two are modified one, but we have a generic project framework which includes risk and risk register and how to manage risk within project"

4.3.3.5 ISO 27001

4.3.3.5.1 Company A

No reference was found for implementing ISO 27001/2.

4.3.3.5.2 Company B

Interviewee IA indicated that the company decided not to become ISO 27001 accredited as noted: "they have taken a view that we don't have to be ISO accredited, to do our business and that it is too detailed and too expensive". However, as it was indicated in the opening of this section, Company B implemented what they found necessary and needed, as it was stated by interviewee IS:

> "An example where do that sort of thing, is like in: policy, [showing policies on the intranet site], this is our technology or IT policies, they are compliant and ISO and SIGS".

Furthermore, interviewee IS added,

> “So, where it is relevant we linking to it, as far as frameworks we have used both of COBIT and ISO 27001-2 – framework to look security poster and our security governance”

4.3.3.6 Policies

4.3.3.6.1 Company A

With regards to the Policies and Procedures, the company has implemented a set of general and IT specific policies and has published them on their Intranet. When the researcher asked interviewee IA about the Policies, the answer was: “Yes, definitely”. Furthermore, the author asked interviewee IA if there are specific IT policies, the reply was: ”we certainly have nearly half a dozen IT policies”, and further added: “ there are categories for different areas, like Internet under security”.

4.3.3.6.2 Company B

Company B has general and IT specific policies and procedures as it was confirmed by interviewee IA, in the following dialogue snippet:

> “Author – I’m sure within the company you have set of Policies and Procedures,
> IA – Yes,
> Author – and there are P and P for IT
> IA- Yes”.
> The same view was confirmed by interviewee IS who stated:
> “An example where do that sort of thing, is like in: policy, [showing policies on the intranet site], this is our technology or IT policies, they are compliant and ISO and SIGS”.

4.3.3.7 Others

4.3.3.7.1 Company A

Interviewee IA had indicated earlier that AS/NZS 4360 has been adopted as risk management methodology: “we have the standard tool at all [DHB- business] use it comes from a document, I’ve got it here, [sound of getting a document] we have a risk module comes out of AS/NZS 4360”. In addition to that, Company A sought an external consulting firm to analyse and advise on applying a systematic method in building IT control-based structured environments:

> “to CIO credit, he has taken up on audit review we did probably several years ago around the IT control environment, and I’ll show you an approach that was taken for an IT risk management. [IA looking for the document] something I can show you but can’t give you – this is the approach we take for external-internal audit service provider, so taken that wheel and spike approach and with carried out our review of that quadrant and we did a deep wide audit how well IT doing in that area , and we are going to move around the wheel in the next maybe six years, 5-6 years trying to cover all those off but also what CIO did after we produced our report on this – we call it quadrant of IT effectiveness review, there were certain several recommendations but the CIO engaged a consulting firm as a consultant to work with IT to try and progress all improvements that need to be made on those areas and what a consulting firm do now they come in once a year and they revise the IT effectiveness by going through a whole series of questions and look at how people are perceiving the state now around those subjects and they rate from one to 1-4, 1 is very poor, and 4 or 5 is the maxim you can achieve the gold star standard, and so CIO or IS, say 4 out 5, we don’t want to go to 5 it is too expensive, we try to achieve 4 for these and maybe 3 for some. So CIO gets an external consulting firm to assess IS from that regard, try to cover all these risk area”.

4.3.3.7.2 Company B

Interviewee IA elaborated on a strategic initiative that the company had developed and communicated to their stakeholders. The initiative outlines the company’s goals and objectives that all business and IT activities should be aligned to the defined goals and objectives, as stated:

> “We have got a strategic initiative I’ll show you, the vision is inspiring NZ on every screen, and then we have got our four key

> pillars and then our strategic [refer to a diagram], and strategic initiatives and everything supposed to go to one of the those pillars and support it, they have go always ask does deliver one of those key pillars, and IT is no different , very much the view is that IT support the business, so we should not do that because it is a good idea for IT, it is because it will support the transmission or support the business area, and that's also a change in culture, to say what is the role of IT and what's role the business owner"

Furthermore, interviewee IA indicated the process for project and case approval that would align to the described strategic initiative:

> "We have a CAPEX committee, so all the projects you want to do, you do a little mini business case, then if it approves, you do a big one, and you have to bring capital back to these initiatives (diagram – pillar) usually there is a formal prioritisation for all projects, and the SLT, which is our senior leadership team, they are the ones who ultimately make the final decision on the big stuff, they are the one who decide actually what we doing and what not, so that how it is managed".

4.3.4 Benefits from Control-Structure Frameworks and Best Practices

Implementing control-structure is a resource intensive task and could take quite a long time to implement appropriately. Organisations face conundrum of investing in establishing costly controls frameworks and best practices, or utilising the resources on improving their information systems that have to realise ROI. As in any business aspects, organisations require to realise gained benefits if they opt to establish those frameworks and/or best practices. In this section, types of benefits are categorised and explored in sub-sections 4.3.4.1- 4.3.4.8.

4.3.4.1 Business - IT Alignment

Business and IT alignment is quite crucial to facilitate IT enablement to the business. Organisations where business – IT alignment is not achieved and retained face never-ending issues with overspending on projects, or implement projects that do not meet business requirements.

4.3.4.1.1 Company A

Interviewee EA was referring to Enterprise Architecture and stated: “the reason, we established an architecture function within a DHB to help bring an action and define the pathway to reach that, which is a big challenge”. In addition, EA said: “The other thing it uses means to communicate and to align everybody to get on the same direction and support that, everybody is moving in the same place”. On the other hand, EA indicated that:

> “99% of organisations only focus the architecture on the IS side, that’s not what TOGAF is about , it is much broader, it actually encompasses the whole thing, with the flavour being that these business vision, drivers, requirements, processes, and from the IS functions, which would deliver the outputs to support whether the strategic direction is around growth, consolidation”.

As the Enterprise Architecture is for the business as well, interviewee EA emphasised that:

> ”The business also needs to understand and buy-in into the architecture. The Enterprise architecture is not about IS, it is about IS, business, process, business analysis, about, continuity, organisational planning, all of that comes together under the umbrella of Enterprise Architecture”.

Interviewee IA shares the same view on that and stated:

> “So we don’t only need structure around that, but structure for business people in the business be able to describe their needs and have one channel so that it goes to channel to IS and they receive the needs and IS can translate that in their terms, but at the moment there is no structure around that”.

4.3.4.1.2 Company B

Business and IT alignment is crucial to business survival and hence it is a daunting task to complete. With business dynamics and ever changing technologies business and IT alignment require on-going monitoring to re-assess and adjust the effort to retain the desired outcomes.

Company B has devised a strategic initiative as outlined by interviewee IA:

> "we have got a strategic initiative I'll show you, the vision is inspiring NZ on every screen, and then we have got our four key pillars and then our strategic [refer to a diagram], and strategic initiatives and everything supposed to go to one of the those pillars and support it, they have to always ask does it deliver one of those key pillars, and IT is no different, very much the view is that IT support the business , so we should not do that because it is a good idea for IT, it is because it will support the transmission or support the business area, and that's also a change in culture, to say what is the role of IT and what's role the business owner".

Interviewee IA further described the procedure of business case approval, which includes IT initiatives that would have to align with the business strategic goals:

> "for capital stuff, we have a CAPEX committee, so all the projects you want to do, you do a little mini business case, then if it approves, you do a big one, and you have to bring capital back to these initiatives (diagram – pillar) usually there is a formal prioritisation for all projects, and the SLT, which is our senior leadership team, they are the ones who ultimately make the final decision on the big stuff, they are the one who decide actually what we doing and what not, so that how it is managed"

In line with this view, interviewee IS indicated how the technology would be aligned to the business strategies, as stated:

> "So the technology will set, a sort of layers, the high level layer, of strategy or set, see how we structure the team behind the strategy, that was in a sense around how we want to operate, and there is a high level strategy on what we want to achieve, so that's what we called a business activity plan, so if we want to become agile or we want to manage to simplify, we want to have increased customer relationship, that's the high level and that 's how we structure the team".

Furthermore, interviewee IS outlined another activity IT do to ensure IT activities aligned with business strategies by periodic review to the division policies, as stated:

> "Do we review the policy annually? Yes; who does that? Me, team leader; what is based on? It is based on feedback from, business engagement and from the service centre call logs, so do we have any security risks or security issues logged and the investigation underneath that was that done to satisfactory level to identify if there is any further enhancement or improvements we can do"

Interviewee IS elaborated on how the defined policies would help IT portray their position in supporting business activities, as stated:

> "The other side, where there is a grayness or where there is an opportunity for flexibility the policy give us guidance, with the explanations and with the connections to other framework supporting documentation, allows us to understand where the policy is trying to drive the requirement of having it and where there risk and where the issue like so it gives us good guidance on where we can make decision and can make exception through an approved process that it is black and white, where it is black and white it gives us the protection layer, it is not us making the decision it is the policy and the flip to us, where there is a gray often we use that as a guide where we shouldn't be making"

That would allow IT division to have the right level of information as outlined by interviewee IS:

> "Well once you got the information you can then, understand, one of the biggest things is to provide evidence and justification for, that helps influence team structures and team designs".

Interviewee IS described an example of what was stated previously:

> "There was a recommendation to reduce by another FTE, so when we looked at the how many calls we were logging and actually what the metrics inside there was, it clearly showed

> evidence that we shouldn't do that, because it would reduce our ability to provide"

Once the right information is obtained, IT is able to respond positively to business demands, as further stated by interviewee IS: "We can justify if there is a value for the business to have the service or the access, this and that, and there is a limited risk for the business in doing that".

That would eventually lead to one of the main IT objectives, which is to enable the business to achieve their goals and objectives, as indicated by interviewee IA: "that is the key word enable, that's the key thing IT enables business".

Interviewee IA talked in much detail about IT improvement since they implemented a set of structures around IT change and release management, as stated:

> " There has been a significant improvement in the IT in the last 4 years, change management moved from being a bit of mess , and now they have got a very a structured process, with a change advisory board that meet weekly, and they are structured and they have got automated workflows, they did not used to have, so that's making a huge difference, it is also giving them building up a body of knowledge base of incidents so they could do reporting and do trend analysis, they couldn't do based on factual things, they have got managers now they are more prepared to be discipline and saying no to business owners, and explain why we can't do things. I think within IT is well they are far more they are support the business area, and it is not often building these marvellous servers, it has always come back to transmission and support the business, there is different attitude now, in terms of getting the balance between, sometimes, the business owner will want to whole lot of things, where have had situations where the business owners gone out and bought a piece of software, and were security people looked at it you can drive a bus through it, and then the technology people they have to do a huge amount of work at

> huge cost, and so one of the things we are looking at is trying to get the costs, to correctly set not just keep piling technology, they are actually charging back to the business areas, so that they are making a better informed decision when the screw up they wear the cost and if they want something expensive which has expensive ongoing cost they have to justify the budget for it, were previously, technology budget used to go up up up like this , and caused a lot of criticisms on technology because the cost gone to the roof, but they really have no control the business owners no 1 made the calls, and IT serviced, and now we are getting the balance, and business manager you need to involve us in terms of us helping you ,develop the spec, and what you want the requirement so that when you go out will help you review them together".

On the other hand, interviewee HR expressed another view on how the structured environment helped IT to review their capability to support business application, as outlined:

> "IT had taken major change and obviously reduced the count so that did not add any value from business owner, but then, 1 year later, they went through a restructure again, it was more around aligning to the strategy and that was about providing not only support to broadcast technology but also to business application technology, e.g. Payroll systems, finance system, so they have recognised there is a gap, that they previously had, so they invested"

Furthermore, interviewee HR shared the same view when the author commented on one of the benefits of the control-based structured environments in this conversation:

> "Author – you have the way the business convey their requirements, and in return IT will say well we can do that, within this time and budget,
>
> HR – Pretty much

> Author – to keep the balance between business requirements/needs and IT capabilities
>
> HR- As well”.

4.3.4.2 Effectiveness

Effectiveness is demonstrated in high performing systems and responding to business demands optimally.

4.3.4.2.1 Company A

Interviewee DS stated:

> “ There are many different things, from the service desk point of view you are adding more management process how to handle the calls that coming in, making sure you are managing in more effective way and you can report on what is you are receiving that can then feed through into problem management if that’s implemented”.

Furthermore, interviewee DS indicated: “You get the capacity management side of things, which is another thing we started doing, which removes the risk of reaching full capacity before, the demands come there”. In addition, interviewee EA indicated:

> “Another way it gives a formal structure to why it is what we do and what we deliver, so in some ways it provides a check list to make sure we that we do thing in similar methodology, the other thing it gives consistency it means to say that we can bring people in and out who can review or contribute in that structured way and we know we are going to get the same output every single time”.

Furthermore, interviewee IA described the benefit in “user support, project management and sound IT services generally, from a proactive perspective rather than reactively”.

4.3.4.2.2 Company B

Interviewee IA indicated how IT change management has improved:

> "There has been a significant improvement in the IT in the last 4 years, change management moved from being a bit of mess , and now they have got a very a structured process , with a change advisory board that meet weekly, and they are structured and they have got automated workflows, they did not used to have, so that's making a huge difference , it is also giving them building up a body of knowledge base of incidents so they could do reporting and do trend analysis, they couldn't do based on factual things".

Similarly, IT were empowered not to accept taking over unfinished projects, as noted by interviewee IA who stated:

> "Previously projects all finished and off we go, and the technology have it suddenly dumped on them, while now they could say no we are not prepared to take it, yet, you have not got the documentation up-to-date, stays in project, so that gives technology some support in terms we will get it and take the responsibility for running it when it is stable ".

In line with that view, interviewee IS described:

> "There is a definite no in certain requests are made, so for example, people want to bring their personal devices and connect to the company's system, the policies allow us to say NO, and it is got , can you , should and shouldn't, it give us the ability to be quite 'autocratic, No' ".

Another example where IT was able to make informed decisions as noted by interviewee IS:

> "There was a recommendation to reduce by another FTE, so when we looked at the how many calls we were login and actually what the metrics inside there was, it clearly showed evidence that we shouldn't do that, because it would reduce our ability to provide".

Interviewee IS described the benefit of real time monitoring and said:

> "So this provides real time monitoring and real time reporting on what is going, if the management were saying continues

> growth and queues not doing this, indication there is a problem, lack of resource or performance. That was big change, so the people did not have the visibility before or it was anecdotal, or I'm busy, OK so we can see what kind of calls that have been logged".

Interviewee PM described part of the project management process and stated:

> " I personally do I think if you have a repetitive task, and you do them then there is a control round them is a lot tidier and if you have an audit function with that as well, within the implementation of one of the control function, definitely helps, more projects are delivered more successfully ."

When the author asked interviewee PM whether 'successful' project means on budget and time, the answer was:

> "Budget and time, actually less important than delivering the scope, delivering the value from that project. If project delivered under budget and on time but it doesn't deliver any value or benefits that originally, than it is a waste of time".

On the other hand, interviewee HR expressed different opinion on IT performance with changes that were observed by other participants and stated:

> "To be honest, interesting you asking me now, IT had taken major change and obviously reduced the count so that did not add any value from business owner, but then, 1 year later, they went through a restructure again, it was more around aligning to the strategy and that was about providing not only support to broadcast technology but also to business application technology, e.g. Payroll systems, finance system, so they have recognised there is a gap, that they previously had, so they invested".

4.3.4.3 Efficiency

Efficiency means reducing cost, time, and staff needed to perform certain tasks and processes without affecting the outcome quality.

4.3.4.3.1 Company A

Interviewee DS described the benefits of applying ITIL incident management practices, and said:

> "You can start reducing or identify the root cause of the incident, so you can start reducing the incident that coming in, as you reduce the number of incidents, people do not need to ring service desk often".

Interviewee EA shed another light on that and said:

> "another way it gives a formal structure to why it is what we do and what we deliver, so in some ways it provides a check list to make sure we that we do thing in similar methodology, the other thing it gives consistency it means to say that we can bring people in and out who can review or contribute in that structured way and we know we are going to get the same output every single time".

Furthermore, interviewee PM indicated:

> "We have a risk model, it has 8 characteristics, we manage risk quite strongly, in that, all projects have to have risk based lined and risk managed throughout the project".

4.3.4.3.2 Company B

Interviewee IS indicated one particular example on sufficiency:

> "We want to reduce the cost of our website delivery , we want to make sure that simplifies and aligned to a smaller team [footprint] then business area activity plan would go, OK what are going to do, we are going to review change out the increased cost or change the outsourced, review and look at the outsourcing commodity components".

Another example from interviewee IS, when the provided information helped the management in making the right decision to retain staff head-count to deliver the required service,

> "There was a recommendation to reduce by another FTE, so when we looked at the how many calls we were login and actually what the metrics inside there was, it clearly showed

> evidence that we shouldn’t do that, because it would reduce our ability to provide”.

Interviewee IA elaborated on how the new structure helped to do adequate costing, as stated:

> “so one of the things we are looking at is trying to get the costs, to correctly set not just keep piling technology, they are actually charging back to the business areas, so that they are making a better informed decision when the screw up they wear the cost and if they want something expensive which has expensive ongoing cost they have to justify the budget for it, were previously, technology budget used to go up up up like this, and caused a lot of criticisms on technology because the cost gone to the roof, but they really have no control the business owners no 1 made the calls, and IT serviced, and now we are getting the balance, and business manager you need to involve us in terms of us helping you ,develop the spec, and what you want the requirement so that when you go out will help you review them together”.

Interviewee PM highlighted the benefits the organisation would gain from project management’s perspective, as stated: “the implementation of one of the control function, definitely helps, more projects are delivered more successfully” and further added:

> “Budget and time, actually less important than delivering the scope. Delivering the value from that project. If project delivered under budget and on time but it doesn’t deliver any value or benefits that originally, than it is a waste of time”.

4.3.4.4 Security

Security of IS is in related to notions of Confidentiality, Integrity, and Availability.

4.3.4.4.1 Company A

Interviewee IA indicated: “there is a huge value from managing IT risk properly, as this would provide enhanced IT environment stability, security / privacy”.

4.3.4.4.2 Company B

Interviewee IS indicated the control-based structured environments helped IT in deciding on use of personal devices, as stated:

> "There is a definite no in certain requests are made, so for example, people want to bring their personal devices and connect to the company's system, the policies allow us to say NO, and it is got, can you, should and shouldn't, it give us the ability to be quite 'autocratic, and say No".

In addition, interviewee IS indicated the value of BCP of DRP,

> "right now the company BCP is around resiliency and redundancy within single site we are expanding that out into dual site, so DR, right now we don't have any DR outside the building, we have DR inside the building, there is quite a lot of resiliency dual path-ing, resilience redundant platforms, or pieces of component that we can bring thing to bare".

Interviewee PM shared the same view on BCP and DRP value to the business, as noted:

> "So the business were involved in them so they definitely see the value in that, for example, news definitely see the value in that having a backup, obviously news is performance and strategic objectives are be the first if something happens here, it is going to happen to other media company, so we want to be able to get to air first, rather than some other company, if something happens in here".

Furthermore, interviewee IA described the formal structure to ensure the BCP-DRP is current:

> "We do have a formal structure and every business area has a crises plan and crises champion and about every 2 years, we do simulation it is sort of going, last time we went to the hotel abc, they told us somewhere hit by earthquake and people what would I do and they got, main department has box, and

> supposedly the senior people has got one of those at home, and one of them here, and they got the box out".

4.3.4.5 Defined Roles and Responsibilities

Framework and best practices define data, functions and processes ownership and level of responsibilities. That clearly states and communicates responsibility and accountability to stakeholders.

4.3.4.5.1 Company A

It was indicated by interviewee EA: **"**the other thing, we try to do, it forms ownership at who is responsible, you think of RACI, you do that at the different stages it helps in form that".

4.3.4.5.2 Company B

Interviewee IS described the business-IT decision-making aspect where roles and responsibilities are defined:

> "So the general manager the owner of all, and myself is the conduit and if you can say, I would be the one who would set the assessment or, whether I do it direct or I bring in someone to do it, or seek guidance or consulting from someone, that it is my responsibility to assess and address and has to assume owner from leadership point of view, that is the really the key governance, so if I make recommendation to we need to go often build something here or change something here, and here is the background or the analysis underneath it, it would be submitted to him, to say yes or no, because he'll hold the financial authorisation".

On the other hand, interviewee IS described how some IT personnel would conduct self-test on existing controls, and stated:

> "They know the pitfalls, to look for, and also know what the exceptions are, so there are always exceptions to the control, and those are generally documented, and therefore they will skip over those areas, rather than drilling in into an area that they

> know there is an exception, the reason is there is an exception, there is a business reason that has been agreed and signed off”.

In addition, when interviewee IS was asked if they apply a sort of role-segregation, the reply was “Yes”.

Furthermore, interviewee HR stated that the IT manager liaises with the business, in addition to specialists who would respond to business-IT related enquires, as noted:

> “Yes there is one business manager, they support the business applications, HR, Finance, so he is the account manager, and under him there will be the technical team the application specialists, so he is got the relationship with me and the specialist understand the technology. We have got the project we have got underway, at the moment, so there is a steering committee that help us drive , we meet monthly , give update on our deliverable so the project manager, myself and the account manager from technology would meet with the steering committee and talk about progress of the project, risks, issues, etc”.

4.3.4.6 Communication

Frameworks and best practices controls improve communication by using common terminologies.

4.3.4.6.1 Company A

Interviewee EA indicated that “It helps in number of ways, first helps with communication, we are speaking the same language, and it should improve the communication”. Interviewee EA iterated: “The biggest thing here is using the same language, producing the same outputs, using the same inputs, we are getting there we are making progress”. Further EA added: “What it will do, it will liaise between the IT functions across the DHB region; they all have the same, speak the same language”.

4.3.4.6.2 Company B

Interviewee IS highlighted the benefit of communicating the right information and stated:

> "Well once you got the information you can then, understand, one of the biggest things is to provide evidence and justification for, that helps influence team structures and team designs".

In addition, interviewee HR expressed their approval of the existing mechanisms that would allow adequate communication between business and IT, as it is exhibited in the dialogue snippet with the author:

> "Author - you have the way the business convey their requirements, and in return they IT, will say well we can do or do that, within this time and budget, and you have got the finance say OK I can't budget this or that, so that's the way the jobs or project got prioritised
> HR – Pretty much
> MA – to keep the balance between business requirements/needs and IT capabilities
> HR- As well".

4.3.4.7 Holistic View – Planning

Frameworks and best practices control-based structured environments provide visibility to the whole system; in other words, it allows a holistic view to the establishment of business and IT systems.

4.3.4.7.1 Company A

Interviewee DS stated that:

> "[ITIL] it is providing better control over how the whole areas operating, you demonstrating you know what's going on, you managing it, in a way you are prepared for anything the business throw at you".

In Company A's IS strategic plan it was noted that "Another weakness, there are too many initiatives, without individual projects, without taking the context of the whole system into account", (Company A Web site). The author commented on that to interviewee EA and emphasised "In a corporate environment, without having the ability to establish the holistic view so many things will be missed out". Interviewee EA responded with:

> "that's exactly right, it comes back to the prioritisation process at the end of the day without understanding the organisation priority without the big view, picture, where this is going to fit in what needs to be fixed, then understand the risk profile and the different portfolios and that brings all of that together".

Furthermore, interviewee EA indicated that Enterprise Architecture helps in planning:

> "From an IS perspective TOGAF is being invaluable in assisting the whole of IS in understanding what we are going to and what's the standard will be what the vision is what is the architecture are to be stated will be and how will look, we can use that in terms of storming sessions, requirement gathering, discussion with business, prioritising and budgeting another planning, and that has been used, it just been used inconsistently, today, to achieve that, but it has been used".

4.3.4.7.2 Company B

Interviewee IA explained the strategic initiative the organisation has and indicated how all business and IT projects and activities should be aligned with one of the strategic streams, as stated:

> "We have got a strategic initiative I'll show you, the vision is inspiring NZ on every screen, and then we have got our four key pillars and then our strategic [refer to a diagram], and strategic initiatives and everything supposed to go to one of the those pillars and support it, they have to always ask does deliver one of those key pillars, and IT is no different , very much the view is that IT support the business, so we should not do that because it is a good idea for IT, it is because it will support the transmission or support the business area, and that's also a change in culture, to say what is the role of IT and what's role the business owner".

Furthermore, interviewee IA emphasised how the IT and business interrelate to each other when serving business goals:

> "I think within IT is well they are far more they are support the business area, and it is not often building these marvellous servers, it has always come back to transmission and support the business, there is different attitude now, in terms of getting the balance between, sometimes, the business owner will want to whole lot of things"

Interviewee IS elaborated on the IT part of that and stated:

> "So the technology will set, a sort of layers, the high level layer, of strategy or set, see how we structure the team behind the strategy, that was in a sense around how we want to operate, and there is a high level strategy on what we want to achieve, so that's what we called a business activity plan"

Further interviewee IS added:

> "We do have a portfolio which is the half of the CAB in the sense should we be doing this, what are the current initiatives in the plate how are they being risk assessed, lot of those are minor no risk, talking about existing frameworks every now and then we have something in lined the file-based change driven project xyz so I did some risk reviews around that, so that's done within the project but rest of it were done as part of CAB and change".

Interviewee IS described another example and stated:

> "So we can actually track where the call is and, so I look at the high level, but each team looks at their queues. So this provides real time monitoring and real time reporting on what is going, if the management were saying continues growth and queues not doing this, indication there is a problem, lack of resource or performance. That was big change, so the people did not have the visibility before or it was anecdotal, or I'm busy, OK so we can see what kind of calls that have been logged".

In addition, interviewee IS indicated the advantage of having the visibility through the information and stated: "Well once you got the information you can then, understand, one of the biggest things is to provide evidence and justification for that".

On the other hand, interviewee HR described another view on how the IT resources plan met business strategic goals, and stated:

> " IT had taken major change and obviously reduced the count so that did not add any value from business owner, but then, 1 year later, they went through a restructure again, it was more around aligning to the strategy and that was about providing not only support to broadcast technology but also to business application technology, e.g. Payroll systems, finance system, so they have recognised there is a gap, that they previously had, so they invested, we realised there is need for more headcount here, , with us still working on the recruitment process"

4.3.4.8 Increase IT Credibility

It is imperative to have healthy work relationship between Business and IT. While it is a collective responsibility, IT should earn business trust by providing the business the required level of support. This section reports the findings on that aspect of IT and business work relationship.

4.3.4.8.1 Company A

In relation to IT credibility within business, interviewee DS stated:

> "Improving the perception of IT department in the eyes of the business because you got less delay in implementing new solutions that then fits in the change management side of things".

And added:

> "You can start reducing or identifying the root cause of the incident, so you can start reducing the incident that coming in, as you reduce the number of incidents, people do not need to ring service desk often, so they are generally happier".

4.3.4.8.2 Company B

Interviewee IA elaborated on how IT has improved in the last few years, which demonstrates the confidence the business has in their IT functions, as noted:

> “There has been a significant improvement in the IT in the last 4 years, change management moved from being a bit of mess , and now they have got a very a structured process , with a change advisory board that meet weekly, and they are structured and they have got automated workflows, they did not used to have, so that’s making a huge difference , it is also giving them building up a body of knowledge base of incidents so they could do reporting and do trend analysis, they couldn’t do based on factual things, they have got managers now they are more prepared to be discipline and saying no to business owners, and explain why we can’t do things”.

In turn, interviewee IS stated how and why IT would respond to business calls: “We can justify if there is a value for the business to have the service or the access, this and that, and there is a limited risk for the business in doing that”

Furthermore, interviewee IS described another example where IT was able to make an informed decision:

> “There was a recommendation to reduce staff by another FTE, so when we looked at the how many calls we were login and actually what the metrics inside there was, it clearly showed evidence that we shouldn’t do that, because it would reduce our ability to provide “.

4.3.5 Challenges

Organisations face many challenges when implementing control-based structured environments, which would increase the cost and mask the benefits from being realised. This section explores the various challenges in sub-sections 4.3.5.1-4.1.3.5.10**.**

4.3.5.1 Immature IT Risk Standard

IT risk management standard and methodologies are fairly immature in comparison to financial and other disciplines. This could become an issue when the standard or methodology is unable to provide answers to certain circumstances or technologies.

4.3.5.1.1 Company A

This view was expressed by interviewee DS who stated "RM, in IT is fairly mature". Furthermore interviewee IA indicated:

> "I can tell you though, the risk assessment and risk management IS overall are not as standards as it should be, the evidence of that, we are going to control self-assessment program at the moment for the whole organisation, and that using a self assessment tool for a whole series of questions around a lot of subjects it's a work shop it takes about 3 hours. We set with IS team, this Monday, went through key business process to assess internal controls, when it comes to risk management it didn't come that well"

4.3.5.1.2 Company B

No reference was found in this category in Company B data.

4.3.5.2 Lack of Awareness

In an organisation where business and IT people do not have the adequate level of understanding of the importance of IT controls in managing IT resources and respond to business demands. That lack of awareness could create many issues when attempting to establish control-based structured environments. For example, business may request a new technology without knowing the benefit or the feasibility of applying such a technology.

4.3.5.2.1 Company A

Interviewee DS has expressed the following concern:

> "While now at the moment the business will come with a solution saying being to a conference, somebody else is using

> this tool, I want that implemented. And you got, you already, on the back foot, because if you turn and say, what's it exactly that you want? A: I want that, Q: but do you want to do, A: I want that, Q: what do you want to do? A: I want what that tool does. If you talk them out of it, you are the bad guy, so you get to spend more time making small changes".

Interviewee PM shares the same view: "That is something business people have always struggled with IT. They don't understand". In addition interviewee PM indicated that user's behaviour causes major issues for IT:

> "Most of problems we can't fix, they are around the user's behaviour, and those kind of top of the hill (hospital) there, are inherently signing off on their bad behaviour, we have been there and fought good fights about unique logins, we took away all the generic login, but they turned on their individual ones generic logins, so we are screwed".

On the other hand, interviewee PM expressed another view on how the organisation considers IT as a back office function with less priority than the core function of the organisation.

> "These organisation are process desert, there is no written process, outside the clinical processes standard operating procedure, that you would expect, it is a bit like in air line industry they have very strict written processes for flying planes, but they don't have many processes for organising it, and that exactly what we have here, because that all considered back office. And back offices' problem, we shouldn't spending any money on any back office, all money should be spent on having many clinicians, if we have enough clinician we are in better position".

Lack of awareness could exist at any level. For example, interviewee IA indicated the lack of awareness among the board members of the IT role in enabling the business and the need to establish right mechanisms for business and IT to communicate their requirements and proposed solutions before they are implemented; as it can be seen in what interviewee IA indicated:

> "So straight after the Virus attack, I arranged for our board member to come to a course effective board of committees and I asked the presenter from the institute of directors to tailor the segment on IT governance, and CIO came along to that course. What that showed, the problem about ITG and IT risk, and what brought to surface that fact that is business struggles to identify their business risk, and struggled to describe their business needs, to IS and IS tried their best to understand these needs, so sometimes IS come up with solution before they know the problem ".

This view is shared by interviewee EA who stated:

> "Yes, and I think that, risk awareness of identifying and managing risks is an organisation is starting to grow, up to now, they are worried about clinical risk , health and safety, IS is sort of not really been looked at, Security is been physical security not data security, but there is never been a holistic view of this. So there is now starting to raise the awareness".

When the author commented "IT people they are very good at doing the technical part but when it comes to process and control and evaluate risk, it took us a while to get them digest what we trying to say", interviewee IA replied: "It is not part of their makeup (process and control for IT)" and added

> "When they do the risk plan they think of someone trip over the computer wire so fall out of bed. They don't say what are our objectives what are we here to achieve what is going stop us to achieving those goals"

Interviewee EA agreed to some extent on that and described the status of risk among the organisation:

> "So there is I think, awareness we need to identify risk, I don't think is necessary good understanding really on how to prioritise, manage, even break apart the risk and have the look at the context of duration, component or risk, all that, you would expect to apply to it, so it looked at an entity as a whole, which could be little hard to swallow".

When attempting to establish framework, security program or enterprise architecture it is imperative to educate stakeholders and send the right message with adequate level of details. Interviewee EA indicated: “So we need to educate the business on TOGAF , or actually on Enterprise Architecture, right now before we can do that, we need to get our house in order “.

4.3.5.2.2 Company B

Interviewee IA discussed the culture within senior management:

> “There is no appetite in this company, to hold a difficult conversation, there is no culture, they talk about generally, in terms of objectives and stuff like that, but when there is none compliance, where I see a lot of it as IA, not a lot happens, and there is conundrum say nice words, and got nice systems in place, but they are not enforced by the senior managers because they don’t want to be held accountable themselves, so sort of fidget”.

4.3.5.3 Lack of Local Expertise

Lack of experience in implementing control framework is another challenge an organisation could face when it intends to establish a control framework. While an organisation could utilise 3rd parties who are specialised in that, however, that comes at a cost and entails a risk in itself.

4.3.5.3.1 Company A

Interviewee IA indicated that at some stage:

> “The impression I get is there are certain parts have been implemented, I can remember the term SIMPLE, I think SIMPLE are a service provider, that is meant to an initiative to install COBIT or ITIL, probably the ITIL, so we did two reviews about 4-5 years ago around the SIMPLE initiative they trying to install ITIL”

Interviewee IA further indicated:

> “ I understand that ex-IS security manager – was trying to implement around those framework model COBIT and ITIL, I

> think CIO has been recognising them as well, because we have a couple of reviews carried out around that subject few years ago".

However, the organisation did not have any replacement for the ex-IS security manager to carry on what has been started. Instead the organisation consults a vendor for that purpose, as noted by interviewee IA: "So CIO gets an external consulting firm to assess IS from that regard, try to cover all these risk area". When the author asked interviewee EA about outsourcing becoming part of life, sometimes it is a good thing to do when you don't have the local expertise but there is another kind of risk interviewee EA's reply was" Yes, exactly, it involves a lot of risk". Interviewee EA shed more light on implementing change management within IT in company A:

> "Change management that has began, and now pretty well embedded, it needs to mature because today it treats them one size fits all where obviously in change that is not the reality".

That demonstrates the level of experience the organisation has in implementing that part of ITIL best practices. However, when developing in-house expertise it is expected to have some learning curve if it could be accommodated and if the risk it might introduce could be managed.

4.3.5.3.2 Company B

Interviewee PM indicated:

> " If you look at the technology, there is no architect within that, so we now actually, basically the governance model for the future architecture within company, so we don't have any architecture as such, they will be contracted when we need them, so there is no enterprise view, in my personal opinion"

Furthermore, interviewee PM commented on the training level of project managers:

> "We have project managers delivering projects that haven't been trained, there is no formal training or informal training within this company, so there is an inherent risk that the project would fail".

4.3.5.4 High Resource Consumption

Implementing adequate control-based structured environments consumes resources and takes a long time to mature.

4.3.5.4.1 Company A

When the author commented “these kinds of projects/solutions, they take long time,” and interviewee DS reply was: “They do”. Furthermore, interviewee DS commented about implementing IT control framework:

> “the part that is not easy, everybody goes OK, what is the time frame this going to be done by, most people say, we are very busy, this is going to take 3 or 4 years, to get to where we want to be, and they get told : yes OK, we will bring some external consultant here to help define the ITIL processes, set things up, in the mean time, IT dept get to carry one and has to handle all the external pressures that are coming in, handling all day to day work , keep the place running help deliver the new solutions , and deliver the changes that need to be put in place to improve so they can deliver, so they could do what need to be done in better way”.

Which is emphasised once more by the DS’s statement:

> “And generally there is underline reason for why we are not doing that properly. Normally , because in this case the IT dept is so over worked and understaffed, and they haven’t got the time to do the things properly in the first place”.

Another reflection on how much time those kind of initiatives could take was provided by interviewee IA:

> “We are going to move around the wheel in the next maybe six years, 5-6 years trying to cover all those off but also what CIO did after we produced our report on this – we call it quadrant of IT effectiveness review , there were certain several recommendations but the CIO engaged a consulting firm as a consultant to work with IT to try and progress all improvements that need to be made on those areas and what a

> consulting firm do now they come in once a year and they revise the IT effectiveness "

Similarly, interviewee EA commented on time expectations:

> "We have been too optimistic in term what we thought we would achieve, because of the pressure of things that happened in the last 12 months, people are tired, whether because their expectation were higher or just feeling down, and the organisation was going backwards".

Furthermore, interviewee EA referred to the cost of those initiatives: " we trying to do that, we got that, so that's another control that's put in place , which is big cost item for the business". EA also Added:

> "It all come to money, and there is probably business expectation that we have that, but there is not funding to support it, so we trying to achieve the similar type of result, without spending more money, we will get there in 3-4 years, but it will be wrong to say from IS perspective that there is a DRP".

However, interviewee DS agreed that implementing IT control structure pays off, but at a cost, "Yes, you will expect in few years, you could reduce the head count, or take on more work to deliver better benefit to the business, you expect that, but it doesn't make that easy at the beginning".

4.3.5.4.2 Company B

Interviewee IA pointed out that implementing COBIT would take quite a long time: "Like COBIT, it is vast thing, if you try to implement all of it; you would spend years tying up knots".

On the other hand, interviewee PM indicated the lack of resource is the reason for not conducting adequate project audit: "There is no real audit function throughout the project at the moment. Again only because we never had the resources"

4.3.5.5 Lack of Executive Management Support

For an initiative like establishing IT control framework, that is resource intensive as was demonstrated in the previous section, executive management's support is vital.

4.3.5.5.1 Company A

Although it was noted in section 4.1.3.5.3 that the CIO is active in implementing such frameworks, there are still issues around the support at board level. It was indicated by interviewee IA: "Some way we are trying to do work around IT risk is I found that Audit committee was not spending the training money, training budget ". On the other hand, interviewee PM stated:

> "We would work with business to determine what's the highest priority and what we get funded, it was never enough money, the business was shocking in supplying any form of priority or direction and at the end we would make an educated guess based on risk. What we perceived a risk".

Interviewee PM indicated that business not so much concerned about IT as it is a back-office function:

> "these organisation are process desert, there is no written process, outside the clinical processes standard operating procedure, that you would expect, it is a bit like in air line industry they have very strict written processes for flying planes, but they don't have many processes for organising it, and that exactly what we have here, because that all considered back office. And back offices' problem, we shouldn't spending any money on any back office, all money should be spent on having many clinicians, if we have enough clinician we are in better position".

4.3.5.5.2 Company B

Interviewee IA described the organisation's culture for setting the objectives and that has been influenced by the senior management to some extent:

> "There is no appetite in this company, to hold a difficult conversation, there is no culture, they talk about generally, in

> terms of objectives and stuff like that, but when there is none compliance, where I see a lot of it as IA, not a lot happens, and there is conundrum say nice words, and got nice systems in place, but they are not enforced by the senior managers because they don't want to be held accountable themselves".

4.3.5.6 Business and Technology Demands

Business and Technology demands on the other hand put a lot of pressure on IT resources.

4.3.5.6.1 Company A

One example is Mobile technology as indicated by interviewee EA:

> "And mobility and the proliferation of mobile devices, people they want to use, effectively people want to bring their own technology and use them at work, the fact that IS would never be able to keep up with the investment that is required so you got to support those emerging technologies in some way but still maintain security, privacy, integrity, the daily challenge".

However, interviewee EA indicated that although there is always a business demand, IT is limited to what they can deliver:

> "That we can only deliver to them what we can get our hands on, we cannot deliver to them technologies that aren't there at the moment and that is a big problem in the sector".

In addition, interviewee EA stated that "we have been too optimistic in term what we thought we would achieve, because of the pressure of things that happened in the last 12 months". Interviewee DS shared the same view that day-to-day operations take time and this doesn't allow IT staff to implement IT control best practice as indicated:

> "IT dept get to carry one and has to handle all the external pressures that are coming in, handling all day to day work, keep the place running help deliver the new solutions, and deliver the changes that need to be put in place to improve so they can deliver, so they could do what need to be done in better way".

Business and technology demands in corporate environment is expected to be high and would require constant attention However, a balance is required to be struck to attend to other demands. Interviewee EA indicated a positive side to technology demand:

> "The fact the matter is all our technologies need to be replaced in 3-4-5 year time's span, the volume of change is really plus, we have new requirements that always cascading in we have got stuff that is not needed any more that has to go out".

4.3.5.6.2 Company B

Interviewee IA indicated that there is more demand than available resources:

> "It can't often, because we have not got the money or the platforms, or people we got more projects then we got people, there is real tension prioritising that and IS would be to talk about that"

Similarly, interviewee HR outlined the current IT capability to support business application:

> "Currently, I don't think our currently technology resource to support well enough, we and a result we had to utilise support from the vendor, the current resource not to the standards we need".

Furthermore, interviewee PM stated:

> "Everyone is running around at the moment, trying to get things delivered, and there is no real planning, other there is planning but it is very reactive rather than proactive".

4.3.5.7 Resistance

Staff resistance to a new set of controls plays a big role in delaying or hindering the process of implementing IT controls framework.

4.3.5.7.1 Company A

Interviewee EA elaborated on that:

> "You got the resistance, you know, you got always the exactly the same , the resistance to change, people who can't wait to

> change , you got the people who would say: we always done it in this way, why wouldn't we keep doing, you've got people who try to sabotage it, ones who cautious who wait and see, you got all sort of this across the board, I think that, I was surprised by that comment, because the individual who made that comment, I would thought they would be very aware of why we need to start planning and preparing and doing things in much more structured way, otherwise, there will be more challenges to look after, so I was surprised by that comments. But saying that, that person of the personality they like to live in chaotic of environment. I don't believe that from an organisation perspective is sustainable that why I believe these methodologies were created."

In another statement interviewee EA mentioned that another reason for why people would resist any changes, was that they don't see any value in that:

> "There is a distorted sale activity is going to happen because no everybody sees the value and benefits in fact I just had a conversation with a colleague today about why do you need the design stuff, we never did this in the old days, and we could have an un-interesting conversation about why we do it, because the old days, what we have got left is the result of no planning from the old day that we have to deal with".

Interviewee IA went further and explained that a staff member does not like to work in a structured way:

> "We need a formal framework, for IS, I think we have, XYZ manager, he is person with a character who doesn't work that well with structure with formal structure, routine and discipline".

On the other hand, interviewee PM attibuted most of the issues to user's behavior:

> "Most of problems we can't fix, they are around the user's behaviour, and those kind of top of the hill (hospital) there, are inherently signing off on their bad behaviour, we have been there and fought good fights about unique logins, we took away

> all the generic login, but they turned on their individual ones generic logins, so we are screwed".

4.3.5.7.2 Company B

Interviewee IA outlined an example of how staff would resist the adoption of some applied measures:

> "You planed work, but we are now getting people to record time, I gather that recorded in two systems, I don't know why, so that causes a lots of frustration, and a lot of them, the technical people they just want to go and fix it, they don't want to go and do the paper work. And so that's something IS might talk about that, nobody likes doing paper work. But for the audit trials we need that done; also so we have to make time for people to do it".

4.3.5.8 Complexity

Implementing control frameworks and coordinating between various best practices implies many details of controls and processes that interact and overlap with each other at various levels.

4.3.5.8.1 Company A

When the author commented: "when you are trying to manage a complicated area, and the complexity, new technology, and business requirements creeping in every day, so to come up with such a solution, it is not easy". Interviewee DS replied "It is not easy". On the other hand, interviewee EA described implementing enterprise architecture and said "We established an architecture function within a DHB to help bring an action and define the pathway to reach that, which is a big challenge". In similar fashion, EA indicated how complicated it is to align ITIL, TOGAF and Prince2:

> "As the PM methodology, so another control has been put in place, another thing, is we are trying to do to show the alignment and hand off between Prince2, ITIL and TOGAF and whether they all fit in the, and it is really difficult to do. It is complicated"

Implementing and coordinating between various controls and processes require a thorough understanding of the system and business themselves, as noted by interviewee EA:

> “At the end of the day without understanding the organisation priority without the big view, picture, where this is going to fit in what needs to be fixed, then understand the risk profile and the different portfolios and that brings all of that together we really are like that says, going down so many rabbit- holes in parallel and just hoping they will lead to the same place, and the reality they will never do”.

4.3.5.8.2 Company B

Interviewee IS indicated a situation where a security process was overly complicated and did not serve the business:

> “We had an approach probably 2-3 years ago that was a consolidation of that that, so we managed that through a dedicated resource who’s focused was on really internal consultant gate –keeper, that did not work for the company, because, I suppose it did not work for two reasons, one was that the process became rigid, to me it was not for business it was, because it required, everything from documentation, briefing sessions, and sign-offs, so that type of structured approach did not fit with business needs, so the business felt, it was restrictive and overly complicated, convoluted and in-efficient”.

On the other hand, interviewee IA pointed out that COBIT T is a vast framework, “Since like COBIT, it is vast thing, if you try to implement all of it; you would spend years tying up knots”.

4.3.5.9 Many Frameworks

One challenge that practitioners and businesses face when attempting to establish control frameworks and best practices, is that there are too many of them.

4.3.5.9.1 Company A

As indicated by interviewee EA: “However, on the flip side of it, there are so many of these which one do you adopt”. It is a valid argument, considering that organisations require to coordinate with other businesses and develop local expertise and train own staff on new processes and controls.

4.3.5.9.2 Company B

Interviewee IA commented on good practices versus best practices and the fact that there are many models and frameworks:

> “People are comfortable with good practice, but best practice, something that there has been some bad experience, with best practices, what is best today not necessarily tomorrow, and one consulting firm have their best, and a consulting firm have their best. And we have got into that mess as well”.

Furthermore, interviewee PM pointed out there are many models, although, from a different view point:

> “I think it needs to be more robust framework to prioritise and optimise the portfolio projects within the company and again linking that to the strategy, there are recognised best practices on how to do that, there is lot of different models”.

4.3.5.10 Ambiguous Regulatory Directions

Some regulatory directions are not clear or are impractical to follow.

4.3.5.10.1 Company A

Interviewee PM explained:

> “The MoH have produced recently a national Health IT plan, it is a poorly constructed collection of desperate ideas, that provocatively knit together to meet an equally ill defined set of outcomes by the minister they are all palatable to his political appetite, whatever that means, it boils down to incoherent directions even or less in terms of how it aid by way of standards or policies to help us in decision making”

That would certainly hinder the organisation's effort to comply with those kinds of instructions. Interviewee PM further described the directions and gave a grim picture of what it looked like:

> "I don't like to call it the traditional top-down bottom-up challenging model, because that inherently means that there is somebody out in the MOH sending things down, if they had clear direction that would be really good, I turned to think of it more in terms of tornado –cyclone side model, where you like spin drier with a guy to put stuff in the top, and goes spin-dry and no one knows, all people know is there are whole of things that are circulating but they don't understand if they come top-down or bottom-up and don't understand how they integrate together but what they do know is there a hell of ball circulating in this spin dry – that's how I think of it".

Similarly, interviewee EA indicated another issue with PIA and stated:

> "PIAs, Privacy Impact Assessment, the problem with PIA cause, they don't necessarily tell you how to address, and what are you going to do about it and it is also reliant on the individual projects, so it needs a thorough job to indentifying all the risk".

Furthermore, EA added:

> "Plus they don't deal very well with likes of mobile workforce that we have that moves, not necessarily out in the wild, but between DHBs, there are still restrictions on certain information on patient info that can be kept and taken and modified. Because of current privacy laws in NZ, so all of that has to be taken into account so we have the PIAs and we use those to the best we can to form some risk and risk assessment".

4.3.5.10.2 Company B

No reference was noted in Company B data.

4.3.6 Problems

Company A and Company B have a number of Problems that were conversed about during the interviews with the participants. The problems vary in their severity and root causes. This section is structured to explore those problems in sub-sections 4.3.6.1 - 4.3.6.7.

4.3.6.1 Business - IT Silos

4.3.6.1.1 Company A

Gaps between Business and IT create a number of problems and evidence for that was observed by interviewee IA:

> “I arranged for our board member to come to a course effective board of committees and I asked the presenter from the institute of directors to tailor the segment on IT governance, and CIO came along to that course. What that showed, the problem about IT G and IT risk, and what brought to surface that fact that is business struggles to identify their business risk, and struggled to describe their business needs, to IS and IS tried their best to understand these needs, so sometimes IS come up with solution before they know the problem”

Interviewee IA indicated that “there [IT] risk register is not fed to the Quality and Risk group risk register”, which is another form of deficiency as risk register should be consolidated at a higher level. Interviewee DS shared the same view and stated: “There is no cohesion in this place of different areas of IS and the business”. DS further elaborated on that and touched upon prioritisation:

> “It doesn’t seem to be cohesion between business units to prioritise any other work, you could have regulatory requirements, and you could have technical risk, or could have part of the business saying we need new system or we need new ED and it seems to be no, group that sit down and say what are our priority here what we need to do, what dependant on something else, I have seen no visibility on that”

Similarly, interviewee PM indicated that business is not providing clear directions regarding prioritisation: “the business was shocking in supplying any form of priority or direction and at the end we would make an educated guess based on risk".

On the other hand, the author asked interviewee PM whether the project risk in considering the whole organisation, in the following little dialogue:

> "Author – I gather that the risk was managed on the project basis, did you have chance to look at the risk within the whole picture
> PM – within the entire organisation?
> Author – Yes,
> PM- Unfortunately, no, we kind of, we try to come with a model that reflects what that would look like but the organisation does not have that".

4.3.6.1.2 Company B

There were no references found in Company B for this category. However, the fact that business-IT misalignment evidence was found indicates the existence of such silos.

4.3.6.2 Business - IT Misalignment

Business - IT silos lead to business and IT misalignment, which in turn leads to various problems, among them prioritisation that has been identified by most of the participants.

4.3.6.2.1 Company A

The author raised a point that was mentioned in the IS strategic plan: that stated that demand exceeds supply, and asked how the organisation prioritises the work, and based on what? Interviewee EA's answer was:

> "Yep, we do, but it's all done wrong. And it seriously is, because today it is IT who set all of that where it is the business who should do the prioritisation, so I mean by views are clears many months, the way we prioritise work outside of IT, i.e. non-IS related work, so the work do on behalf of business, is prioritised in a wrong way".

When the same question was directed to interviewee IA and the author wondered if the prioritisation was done based on business needs, the answer was “You think so, may be not!”

Interviewee PM reasoned this issue and stated: “The business was shocking in supplying any form of priority or direction and at the end we would make an educated guess based on risk”. However, interviewee DS has different view for why this was happening and stated:

> “It doesn’t seem to be cohesion between business units to prioritise any other work, you could have regulatory requirements, and you could have technical risk, or could have part of the business saying we need new system or we need new ED and it seems to be no, group that sit down and say what are our priority here what we need to do, what dependant on something else, I have seen no visibility on that“

Interviewee PM further indicated that business-IT misalignment caused by misunderstanding on the business part of what kind of technology IT are able to deliver, and stated:

> “That we can only deliver to them what we can get our hands on, we cannot deliver to them technologies that aren’t there at the moment and that is a big problem in the sector”.

Interviewee EA, however, indicated:

> “ It comes back to the prioritisation process at the end of the day without understanding the organisation priority without the big view, picture, where this is going to fit in what needs to be fixed, then understand the risk profile and the different portfolios and that brings all of that together”.

4.3.6.2.2 Company B

Interviewee PM pointed out the current gap between business priorities and IT tasks:

> “In the portfolio framework is obviously the business has a lot of ideas and initiatives that they want to implement, at the moment there is bit of gap between that and what our priorities are”

Interviewee PM further added: “At the moment that’s where the gap is, there is not any real prioritisation within the company for the project”. On the other hand, interviewee IA commented on one particular project that went for too long: “Some of it, we had a big project we ended up going, started 2004, we had to de-scope, a lot of the communications were vague, it just went too long”

4.3.6.3 Business - IT Structures

There seem to be a number of issues around business and IT structures, in particular around functions and roles that allow two-way communication, where business requirements are conveyed to IT and IT communicate their concerns.

4.3.6.3.1 Company A

Interviewee DS pointed out that and stated “There is no cohesion in this place of different areas of IS and the business” and further elaborated on that: “It doesn’t seem to be cohesion between business units to prioritise any other work”. Interviewee IA shared the same view:

> “So we don’t only need structure around that, but structure for business people in the business be able to describe their needs and have one channel so that it goes to channel to IS and they receive the needs and IS can translate that in their terms, but at the moment there is no structure around that”.

Similarly, interviewee EA indicated:

> “ I think that’s actually something very prevalent at the moment, what we don’t have, is a lot of organisations large organisations have like service delivery function or client manager type of function we don’t have that function“.

4.3.6.3.2 Company B

Interviewee IA answered a question about whether there is an IT governance structure, and the reply was: “Not really, just uses the manners of the leadership team”. Consequently, interviewee PM pointed out the gap between the business strategy and the implemented projects:

> “What I see the company puts a strategy together, but then we don’t look at how we implement that strategy and how that

> implementation results in what we should be doing, the whole linkage from the strategy to the very much details of the projects we should be doing, and it is not there"

Furthermore, interviewee PM responded to a question around project post-implementation review, where there doesn't seem to be a well defined structure around that:

> "Yes, as part of the framework, we should be doing post implementation and benefit analysis, there used to be PMO outside the technology used to do all of that, now it is fragmented in that, it is not my role to manage at the moment, it is IA to manage the Audit post implementation reviews of project, and there is no real audit function throughout the project at the moment. Again only because we never had the resources and again my new role, it has been left for last year".

4.3.6.4 Risk Management Function

4.3.6.4.1 Company A

It was indicated that the Quality and Risk management function within the organisation is not functioning properly. Interviewee IA elaborated on that function:

> "we do have a quality and risk function here it reports to that role I think it is quite disjointed so I cannot give good news about it, Quality and Risk are meant to gather all the risk across the organisation and prepare a top level risk plan so it meant to come from the bottom up, but we do not have too many bottom level risk plans, they are not that mature they are not sound, I think what happens is they prepare top level risk plan kind of different from the bottom one it is not reformed from the bottom ones, and as I indicated before that IS risk plan and risk management still hasn't got to good standards anyway".

Interviewee PM described a grim picture of how this function is performing

> "I call them dead people, then active then the Quality and risk people. I think they have a pulse at some stage; they do absolutely no quality and risk management around IT."

Interviewee DS shared the same concerns and indicated that:

> "Within the area, there is no formal risk management. Let me rephrase that, we have incident management which is handling certain levels of issue, we've got change management, which is handling or trying to mitigate the risk to the business from infrastructure point of view, but there is no formal risk management for other areas".

Interviewee IA, however, pointed out that IT has not performed this function up to the desired level:

> "I think it has been accepted that the risk management processes within IS are not up to standard, even though the organisation has the systems, tools and processes to facilitate sound risk planning and management. I understand that the IS department is working on this area of their operations".

4.3.6.4.2 Company B

Interviewee IS pointed out that there used to be a dedicated resource to manage security and risk, and that proved to be ineffective:

> "So, we had an approach probably 2-3 years ago that was a consolidation of that that, so we managed that through a dedicated resource who's focused was on really internal consultant gate –keeper , that did not work for the company, because , I suppose it did not work for two reasons, one was that the process became rigid, to me it was not for business it was, because it required ,everything from documentation, briefing sessions, and sign-offs, so that type of structured approach did not fit with business needs, so the business felt, it was restrictive and overly complicated , convoluted and in-efficient ".

However, interviewee IS answered a question about whether the risk register is consolidated in a sense in the following way:

> “We have in a sense two [risk register] , one for the project , portfolio project management tool called i-Line, to rise and manage risks in project , we have an overall IT risk register, these are the ones that are generally raised by people through an email or through the server centre”.

Furthermore, interviewee IS indicated there were not defined objectives as exhibited in the following short dialogue snippet:

“Author – but there is no objectives, like you have set of objectives for each team..

IS - No, in a sense it is a mesh of the whole lot”

And further added:

> “In sense the risk is identified and the action is either could be generally, is risk is acknowledged and would either be addressed in future, like trying to mitigate the risk in the current state because the amount of work required to retrofit something on top of it would be significant and, of limited value, but as we go forward the activity in that area, of that system we would look to, include mitigating the risk, and whether there is a future enhancement or changes”.

Not identifying business objectives was noted by interviewee IA, who stated:

> “There is no appetite in this company, to hold a difficult conversation, there is no culture, they talk about generally, in terms of objectives and stuff like that, but when there is none compliance, where I see a lot of it as IA, not a lot happens”.

4.3.6.5 BCP-DRP

BCP and DRP are quite vital for sustaining businesses. Given the size and type of industry; it is expected to have a high level of BCP and DRP where the IT is the backbone of that planning.

4.3.6.5.1 Company A

Company A does have a form of BCP, but the IT is not part of it. It was indicated by interviewee EA:

> "There is, there is BCP plan from, ah, from the health DHB perspective, I'm not aware of the extent that it covers the IS infrastructure, the reason I say, that is we don't have a DR capability from IS perspective, so if our core data centre goes down we do not have another data centre to fell over to. So the BCP [business] will have to include a manual processing".

Interviewee EA related that to cost as outlined below:

> "It all come to money, and there is probably business expectation that we have that, but there is not funding to support it, so we trying to achieve the similar type of result, without spending more money, we will get there in 3-4 years, but it will be wrong to say from IS perspective,, that there is a DRP"

4.3.6.5.2 Company B

Interviewee IS commented on the current status of BCP-DRP: "It is a big question, from an enterprise level NO, from system specific level we have some". Interviewee IS further elaborated on BCP:

> "Right now the company BCP is around resiliency and redundancy within single site we are expanding that out into dual site, so DR, right now we don't have any DR outside the building, we have DR inside the building, there is quite a lot of resiliency dual path-ing, resilience redundant platforms, or pieces of component that we can bring thing to bare"

4.3.6.6 Reactive not Proactive

In a corporate environment business and technology changes happen often and at various level and scale. Without having adequate mechanisms to monitor and analyse changes and trends the organisation would not have the capacity to respond to those changes accordingly.

4.3.6.6.1 Company A

Interviewee PM described the current monitoring status: "It is appallingly bad; nobody is doing any proactive monitoring it is done in a crises basis".

4.3.6.6.2 Company B

Interviewee PM stated:

> "Everyone is running around at the moment, trying to get things delivered, and there is no real planning, other there is planning but it is very reactive rather than proactive".

4.3.6.7 User's Behaviour

Another reflection of the current status of the user behaviour in terms of using IT systems is presented in the interviewee's responses below.

4.3.6.7.1 Company A

Interviewee PM indicated: "most of problems we can't fix, they are around the user's behavior"

4.3.6.7.2 Company B

Interviewee IA attributed the IT staff response to time-sheeting system:

> "We are now getting people to record time, I gather that recorded in two systems, I don't know why, so that causes a lots of frustration, and a lot of them, the technical people they just want to go and fix it, they don't want to go and do the paper work".

On the other hand, interviewee IA indicated an issue at the senior management level:

> "There is no appetite in this company, to hold a difficult conversation, there is no culture, they talk about generally, in terms of objectives and stuff like that… but not a lot happens".

4.3.7 Solutions

Participants from Company A came from senior IT management as well as from the internal audit function. They suggested remediation to rectify the existing problems that were discussed. This section examines those solutions as they have been classified in sub-sections 4.3.7.1 - 4.3.7.9.

4.3.7.1 Define Objectives

Business units including IT should identify their objectives and assess the associated risk at various levels.

4.3.7.1.1 Company A

It has been indicated by interviewee IA that this would help the business unit identify risk:

> "The low level risk plans are quite different and you mentioned you asked business what are your objectives, what could go wrong that's where I think our business has not matured yet. When they do the risk plan they think of someone trip over the computer wire so fall out of bed. They don't say what are our objectives what are we here to achieve what is going stop us to achieving those goals".

Although, objectives could identified at a higher level, it would be more beneficial to define objectives at the team and/or function level as this would assist in assessing the risk at a granular level.

4.3.7.1.2 Company B

Interviewee IA explained about the organisation strategic initiative:

> "We have got a strategic initiative I'll show you, the vision is inspiring NZ on every screen, and then we have got our four key pillars and then our strategic [refer to a diagram], and strategic initiatives and everything supposed to go to one of the those pillars and support it"

Furthermore, interviewee IA outlined the project approval process:

> "For capital stuff, we have a CAPEX committee, so all the projects you want to do, you do a little mini business case, then if it approves, you do a big one, and you have to bring capital back to these initiatives (diagram – pillar) usually there is a formal prioritisation for all projects, and the SLT, which is our senior leadership team, they are the ones who ultimately make the final decision on the big stuff, they are the one who decide actually what we doing and what not, so that how it is managed"

However, interviewee PM had another view on the current business IT prioritisation:

> “I think at the moment, it is very ad-hoc prioritisation process we shouts louder some times, and every time the wind changes as well, I think it needs to be more robust framework to prioritise and optimise the portfolio projects within the company and again linking that to the strategy”

4.3.7.2 Consult Third Party Experts

When local expertise is not available or not up to the desired level, consulting external specialised parties could be a valuable option to assess the environment and devising a mitigation plan. External parties are utilised to validate internal assessment as well, which would add another layer of protection and validation.

4.3.7.2.1 Company A

Interviewee IA explained how Company A engages with a consulting firm:

> “this is the approach we take for external-internal audit service provider, so taken that wheel and spike approach and with carried out our review of that quadrant and we did a deep wide audit how well IT doing in that area , and we are going to move around the wheel in the next maybe six years, 5-6 years trying to cover all those off but also what CIO did after we produced our report on this – we call it quadrant of IT effectiveness review , there were certain several recommendations but the CIO engaged a consulting firm as a consultant to work with IT to try and progress all improvements that need to be made on those areas and what a consulting firm do now they come in once a year and they revise the IT effectiveness by going through a whole series of questions and look at how people are perceiving the state now around those subjects “

However, interviewee IA made another statement that reflects how a third party opinion helps IT leadership gain executive backing:

> “So it compounds it gets worse and worse, until it is about to collapse, so a consulting firm come in and say you are not

> doing that very well. But that then gives the CIO the opportunity to say to the rest of the executives I need time, money, to address this, because we pay to the consulting firm tell us, whether they told everybody before or not, it doesn't matter. And it allows IT to focus on these areas".

4.3.7.2.2 Company B

Interviewee HR indicated that a third party could help in reviewing the system:

> "In SLA we can also pull in another external party to do a technical audit if we wanted to, so the vendor, we get more of unbiased review of the system"

In addition, interviewee IS commented on third party engagement with the organisation: " as well as the consulting firm (external auditor), they also check us annually ".

However, interviewee IS indicated that third party involvement should be justified to where it could add a value to the business:

> "It has to have the business knowledge, and you wouldn't have that coming from a third party, they have a tendency a structured road and it is one size fits all, that does not really work here, it would in other segments , other companies".

Interviewee PM, gave another example for how third party service could add some value:

> "I think this company when the PMO was outside the technology there was a lot of work done on that project framework, there were couple of external auditors that reviewed the framework, this is few years ago now, it was pretty sound ".

4.3.7.3 Make Use of Major Incidents

When major incidents take place, make use of that to gain more attention from Executive management and raise IT profile.

4.3.7.3.1 Company A

Company A has suffered a virus attack and that raised the executives' awareness of the role IT plays. Interviewee IA indicated what had happened to the organisation when it was hit by a virus and how they capitalised on that and what was identified:

> "One has come out from the board to focus on CIO of IS, that really rose to a higher level when we struck by Conficker (virus) and evidently it was one of the internationally virus, that we had to take the network down for 3 days, luckily it was Friday, but regardless the made the media and caused a whole lot of havoc here, that brought the profile of IS way up , so what happened CIO put a whole program I referred to earlier that would address all our security issues not just what Conficker [the virus] raised, but all other audit reports and other raised by the commission so we helped CIO putting together the report summarised it and prioritised it and sequenced it, and passed it to CIO, stating this what should be the focus in the next 1-2-3 years, and reporting on the to the audit committee as well".

Similarly, interviewee DS commented on the same incident:

> "I'm aware of certain areas that business is focused from technology point of view, just a year ago, the DHB got hit by a Conficker virus that affected the business for several days, so the CEO is very aware of that, aware of that risk or the issue now, he has made the top priority is to make sure this not to have any of those, but then everything else is also top priority"

The author conversed with two other interviewees about the 'positive' side of that incident. Interviewee EA agreed by saying "it works positively", while interviewee PM agreed but cautioned: "True, it is bit tough if you are the person who is taken the material damage".

4.3.7.3.2 Company B

No reference was found in Company B data for this category.

4.3.7.4 Educate and Train

Awareness programs play a vital role in educating users, at all levels, about acceptable use and best practice. In addition, special programs could be designed to target particular groups to raise their awareness of a particular topic. Also, developing in-house expertise on implementing and utilising frameworks and best practices would help immensely in adopting those practices.

4.3.7.4.1 Company A

Interviewee IA commented on how conducting a workshop targeting board members and discussing a specific topic had helped in raising the IT profile:

> "I arranged for our board member to come to a course effective board of committees and I asked the pres from the institute of directors to tailor the segment on IT governance, and CIO came along to that course. What that showed, the problem about IT G and IT risk, and what brought to surface that fact that is business struggles to identify their business risk, and struggled to describe their business needs, to IS and IS tried their best to understand these needs, so sometimes IS come up with solution before they know the problem"

Interviewee EA indicated the importance of educating business on enterprise architecture and what it brings to them: "So we need to educate the business on TOGAF, or actually on Enterprise Architecture, right now before we can do that, we need to get our house in order ". And further added "the business also needs to understand and buying into the architecture". This would help in demonstrating the value to business.

Communicating with business also helps in informing them what IT do, as indicated by interviewee DS:

> "We can go out there and talk to people and explain to them what we are doing, explain, I don't think we do an awful lot of talking to the business, we wait for them to come to us, there is providing hard call facts on the internet"

That would help in what IT could deliver as it was one of the interviewee PM's concerns who stated:

> "That we can only deliver to them what we can get our hands on, we cannot deliver to them technologies that aren't there at the moment and that is a big problem in the sector".

On the other hand, building in-house expertise and training IT staff on implementing best practices and framework, would help in various ways as indicated by interviewee EA:

> "I think the short answer is yes, it would because obviously people have been through training, and understand what's this about, they would have high awareness of what you get, or they see from a far. The short answer is yes, there are also other benefit, from doing that, it would accelerate the adaption, it would also I think, give you a great of pool of people to participate in the activities, it would certainly make communication a lot better as everybody speaks the same language".

4.3.7.4.2 Company B

Interviewee IS outlined the measures taken to keep IT management up to date with best practices:

> "I attend various security forums, IT security summit, meet with industry reps, I personally sign in into different sites that send me emails on what is going on in the world and industry trends and knowledge periodicals as well, I also, we do deal with number of consultancy teams, external firms, they come to us, what the industry are doing, the IA is active, some IT skills and understanding, she attend various forms and send to us stuff if they have some relevance".

Interviewee IS pointed out the benefit of developing in-house expertise:

> "So rather then bring a 3rd party that have the set of skills we developed the skill internally enabled them with series of tools giving them the access so that they can repeat the processes and in a sense to keep the core team honest".

Education and training is necessary to staff at all levels. Interviewee IA outlined the need to target the senior management:

> "There is no appetite in this company, to hold a difficult conversation, there is no culture, they talk about generally, in

> terms of objectives and stuff like that, but when there is none compliance, where I see a lot of it as IA, not a lot happens, and there is conundrum say nice words, and got nice systems in place, but they are not enforced by the senior managers because they don’t want to be held accountable themselves”

However, interviewee PM indicated the importance of training project managers on best methodologies:

> “From the portfolio, from a PM delivering projects, if people following that framework, we had staff made sure they did follow that framework all the time and we had a proper trained project managers to deliver all the projects that would be great”.

4.3.7.5 Improve Business-IT Communication

Establishing better means for IT to communicate with business and vice versa, helps in various ways.

4.3.7.5.1 Company A

Interviewee IA indicated the need to have a mechanism that would allow the business to convey their needs:

> “So we don’t only need structure around that, but structure for business people in the business are able to describe their needs and have one channel so that it goes to channel to IS and they receive the needs and IS can translate that in their terms”.

Interviewee EA identified a current issue and mentioned:

> “I think that’s actually something very prevalent at the moment, what we don’t have , is a lot of organisations large organisations have like service delivery function or client manager type of function we don’t have that function”.

Interviewee EA elaborated further on that:

> “You would expect those delivery manager or client manager whatever you called them will be out there with the business representing IS talking to them gathering requirements and setting expectations, waving the flag, but also conversely coming back, shaking the branch at the IS end and make sure

> the work is performed correctly, in the right time and the right way, so until I think until we get some sort of interface with the business that lives in the business but owned by IS, therefore report back, if you can manage that I think that would help".

In line with interviewee EA's view, interviewee DS indicated that "yes, you need to have service delivery team who are talking to the business understanding what they need, account management basically". In addition, interviewee DS emphasised on the necessity to understand how business assesses IT services and what they expect of them:

> "One of the effective ways, where you consult people from IS and say where are we now, where are we aiming for, but also talk to the business and ask where do you think IS is at, and where do you they should be for, and bringing all these together to know where our target is"

Interviewee PM mentioned that one of the issues with business is they don't realise the IT capability:

> "This is sometime a little bit difficult for people in the business to realise that is we are working on a very short window of life span of our structured we manage and run it and deliver to them".

Furthermore, interviewee PM pointed out another concern:

> "That we can only deliver to them what we can get our hands on, we cannot deliver to them technologies that aren't there at the moment and that is a big problem in the sector".

However, interviewee DS indicated that this concern could be resolved by talking to the business:

> "We can go out there and talk to people and explain to them what we are doing, explain, I don't think we do an awful lot of talking to the business, we wait for them to come to us, there is providing hard call facts on the internet"

On the other hand, interviewee DS indicated that communicating with business builds trust and confidence in IT:

> "The biggest way I found in my previous experiences when you go with the business and getting them to work with you and trust you and all that kind of thing, it is a demonstrator, if you can simple like, if you can demonstrate that on day one, you spent 10 minutes trying to get to the service desk, then it might take 3-4 days before anybody resolves anything, because the way it works, you can demonstrate that people can get to the server within 2 min, and it actually takes let, say 60% to the cause of the call".

4.3.7.5.2 Company B

Interviewee HR outlined the reporting mechanisms between business and IT to support business applications:

> "It if is relating to the s/w as the business owner, say Chris21, we have an account manager , I would liaise with that person to address the issue of this service, is not good enough around the dealing of any issues that come up , and obviously that might even be relying on the 3rd party as well, but it is sort of, making sure they are aware of the service delivery is what we expect, so it is communicate , there is a manger in that area, if there is no real resolution or traction , you would go up a level, etc".

Furthermore, interviewee HR indicated what IT should make sure of:

> "The technology they service us, so they need to make sure they provide the certain level of expertise and we just raised issues with them, as a business owner".

Interviewee IS emphasised the importance of information:

> "Well once you got the information you can then, understand, one of the biggest thing is to provide evidence and justification for, that helps influence team structures and team designs"

Interviewee IS added: "Right so do we have monthly statistics that produces monthly balanced score card, it is not fully BSC, and it is rather a monthly reporting format". Interviewee IS stated the form that business conveys its feedback to IT: "It based on feedback from, business engagement and from the service centre call logs". In addition, interviewee IS elaborated on the way that business conveys their concerns:

> "The way we measure it, would actually be through the customer satisfaction. So whether its anecdotal f/b, as soon as we hear a noise created by complexity and bureaucracy, so if the noise level is reasonable low, we know that we are doing well"

When the author asked interviewee IS how IT would gather the business feedback, the reply was:

> "Fundamentally it is folded into our relationship management structure within the business, so business unit's managers meet with customers on regular basis, and gather that feedback".

However, interviewee PM had a different view on how the communication is conducted among business and IT units:

> "I think at the moment, it is very ad-hoc prioritisation process we shouts louder some times, and every time the wind changes as well, I think it needs to be more robust framework to prioritise and optimise the portfolio projects within the company and again linking that to the strategy"

4.3.7.6 Customise Frameworks to Business Environment

Frameworks and best practices are not one size fits all; therefore it is imperative to apply pragmatic approach in implementing those control frameworks and best practices.

4.3.7.6.1 Company A

Company A has customised TOGAF enterprise architecture to serve the organisation and industry environment as described by interviewee EA:

> "TOGAF has been adapted for all the architectural work here DHB internally, we have basically taken the ADM, and modified it for applicability within Health business and we call it health-based standards, so now within the geographic area – all of us have adopted and agreed to use the Health-based , which is the health view of the ADM".

In addition, interviewee PM indicated that Prince2 methodology has been customised to suit the business context: "In Prince2 document it says to tailor the methodology to the business need, so we branded our tailored version, and called it DHB-way".

Customising control frameworks has to meet business objectives. Interviewee DS indicated the necessity to have business view on IT capability maturity level:

> "I think the way that the assessment that has been done so far with the consulting firm, is one of the effective ways, where you consult people from IS and say where are we now, where are we aiming for, but also talk to the business and ask where do you think IS is at, and where do you they should be for, and bringing all these together to know where our target is, because no point aiming for 5 if it is not needed. It will be waste of everything. But there is not point IS saying we need to get to level 2, or 2.5, if the business if the business call for level 3, 4, so you can't do it in isolation".

4.3.7.6.1 Company B

Interviewee IA described the organisation's approach to adopting control frameworks:

> "They have taken a view that we don't have to be ISO accredited, to do our business and that it is too detailed and too expensive so , because I talked to them about COBIT, because I quite like the framework and the view is we are aware of it and we'll apply the principles and enough of it to meet our business needs, but we are not going to go down the framework roads, because there is no value to the business in terms of doing a lot of detail so there a lot more flexible"

Interviewee IA further elaborated on the capability maturity level that suits the organisation's environment:

> "We have to be pragmatic and practical and appreciate what we used to do a rolls- Royce everything and now we have to get our

> people and of some our specialist more creative program to say you don’t need to be rolls-Royce in everything”.

The pragmatic approach was expressed by interviewee IS as well:

> “We take a reasonable pragmatic approach, because the majority of the Company’s funds focused on content and the right of content the “lion share” of the business revenue of business profitability in that space, so technology has access to those funds, but we take very pragmatic view of services that the business needs”

Interviewee PM shared the same view as it is demonstrated in the following dialogue snippet:

> “Author – some of the framework, you follow best practice, you value these frameworks, but some people see controls, business?
> PM- as business barriers ?
> Author – yes,
> PM- I think quite often it is getting that balance in that pragmatic view so obviously, some projects have an inherent high risk some projects a low risk, so obviously controls around high risk projects should be higher than low risk projects. “

4.3.7.7 Demonstrate Value to Business

Demonstrating value to business increases IT creditability and improves business and IT alignment.

4.3.7.7.1 Company A

Interviewee DS indicated that:

> “The biggest way I found in my previous experiences when you go with the business and getting them to work with you and trust you and all that kind of thing, it is a demonstrator, if you can simple like, if you can demonstrate that on day one, you spent 10 minutes trying to get to the service desk, then it might take 3-4 days before anybody resolves anything, because the way it works, you can demonstrate that people can get to the server within 2 min, and it actually takes let, say 60% to the

> cause of the call, while you are on the phone, rather than 20%, people start trusting it is worth calling IS, because they will do something. You can demonstrate when somebody got an idea, we are listening, we may not always agree with them, we may talk them out of it, but if we can demonstrate we listen we work with them, to understand what is it that they want and we will find a solution for them, a solution might be different to what they thought it was, then now trust , they will think we can be trusted to deliver these things, rather than at the moment, while now at the moment the business will come with a solution saying being to a conference, somebody else is using this tool, I want that implemented. And you got, you already, on the back foot, because if you turn and say, what's it exactly that you want? A:I want that, Q: but do you want to do, A: I want that, Q: what do you want to do? A: I want what that tool does. If you talk them out of it, you are the bad guy, so you get to spend more time making small changes".

Interviewee DS further pointed out what kind of measures can be taken by IT to achieve that:

> "Simple things that can be demonstrated as graphs if we need to, show people how busy it is, and what we are doing, what have done to improve on the interface between the IS and the business which is the service desk. You do all of that, and realising the people attending the session reading the presentation".

In line with that view, interviewee EA commented:

> "The other thing that would help in this space is the will factor, one thing we don't do, we do a lot of work, huge big projects, or other things, happening under the hood, nobody can see, so from the business perspective they never the little small delivery, how I think if we could focus on one or two of those per quarter, the brand goes up and credibility goes up and

> people would go wow, it doesn't have to be big but people would be impressed".

Interviewee EA further elaborated on demonstrating IT value to the business:

> "Well one of those, by spending bit more time with them understand what their main points are and fixing those things, because there is a lot of hanging fruit that just never get deal with because there is so much noise about big piece of work , and as it has been pointed out earlier because of the lack of business involvement in prioritisation of the work we do on their behalf, because if we assume that based on dollars and size that some project are more important than others, then maybe we assume incorrectly, and they business may see more value in those small jobs, that we never get around that, because the long term consume all the resources, and how if you could have the communication and get the prioritisation in place, you would understand, pretty quick and build those bridges, but it is about building new relationship spending time, respecting value in each other and then building from there by delivering".

4.3.7.7.2 Company B

Interviewee IS pointed out the need to identify business value in offered services:

> "We can justify if there is a value for the business to have the service or the access, this and that, and there is a limited risk for the business in doing that"

Furthermore, interviewee IS outlined an example where IT had to take a decision where the value to the business was:

> "One of the biggest thing is to provide evidence and justification for, that helps influence team structures and team designs, so there was a recommendation to reduce by another FTE, so when we looked at the how many calls we were login and actually what the metrics inside there was, it clearly showed evidence that we shouldn't do that, because it would reduce our ability to provide"

Interviewee IS pointed out the usefulness of a monthly report in the form of BSC that is generated to communicate monthly statistics:

> “Right so do we have monthly statistics, that produces monthly balanced score card, it is not fully BSC, it is rather a monthly reporting format but it is in line with what BSC does, so I’ve, we do produce those metrics, talked about [looking at the intranet, viewing steering wheels of various reports]”.

Interviewee PM indicated the importance of implementing projects that deliver value to the business:

> “Budget and time, actually less important than delivering the scope. Delivering the value from that project. If project delivered under budget and on time but it doesn’t deliver any value or benefits that originally, than it is a waste of time”.

4.3.7.8 Integrate Frameworks and Best Practices

Currently, there are many frameworks, standards and best practices that complement each other, where one method is better than the other in the approach or the level. For example, ITIL serves IT operational functions and it tells how to implement certain controls, while COBIT works at the strategic and tactical levels and indicates what needs to be done. Similarly, TOGAF is enterprise architecture and ISO 27001/2 standard is specialised in IT security. When implementing number of these methods, it is important to integrate them to achieve optimal value and eliminate overlapping, which could incur further cost.

4.3.7.8.1 Company A

Interviewee EA indicated the necessity to integrate existing frameworks and best practice, although it is not easy:

> “As the PM methodology, so another control has been put in place, another thing, is we are trying to do to show the alignment and hand off between Prince2, ITIL and TOGAF and whether they all fit in the, and it is really difficult to do. It is complicated “

The author conversed with interviewee DS about that, as noted below:

> “ Author - you use ITIL because it is good in your area, and EA uses kind of tailored Enterprise TOGAVE and PM did modified

> Prince, so all these, everybody is utilising a method or a practice that is best for their areas,
> DS – and they got to melted together
> Author – exactly, that is the framework, some from COBIT is one of
> DS - Yes”

4.3.7.8.2 Company B

Interviewee PM commented on the current prioritisation status: “I think at the moment, it is very ad-hoc prioritisation process”, and added:

> “I think it needs to be more robust framework to prioritise and optimise the portfolio projects within the company and again linking that to the strategy”.

Furthermore, interviewee PM remarked:

> “ I personally do I think if you have a repetitive task, and you do them then there is a control round them is a lot tidier and if you have an audit function with that as well, within the implementation of one of the control function, definitely helps, more projects are delivered more successfully”.

4.3.7.9 Co-operate with Internal Audit

Corporate businesses have internal audit function; however, not all of them have the IT audit capacity. Nevertheless, internal audit could play a vital role in aligning business and IT. In addition, if utilised adequately it could add value to IT in validating IT controls and processes and by elevating IT profile.

4.3.7.9.1 Company A

In Company A the internal auditor IA played a role in raising the Board awareness of IT role and helped to raise the IT profile. Interviewee IA described their position within the organisation:

> “Our place within the organisation is: we report directly to the audit committee, and has a dotted line to one the executive manager the director of the director of the board governance - so

> that we have complete independence so we can review anywhere in the organisation".

Furthermore interviewee IA pointed out how the IT risk is incorporated within the audit plans:

> "And within – Key IT risks – and we spend a good time with CIO about that, so we put together our plan and for the last say half a dozen years we generally we always included IT risks in our plans to some extent".

Another example where internal audit could help IT was given by interviewee IA:

> "when we struck by Conficker (virus) and evidently it was one of the internationally virus, that we had to take the network down for 3 days, luckily it was Friday, but regardless the made the media and caused a whole lot of havoc here, that brought the profile of IS way up , so what happened CIO put a whole program I referred to earlier that would address all our security issues not just what Conficker [the virus] raised, but all other audit reports and other raised by the commission so we helped CIO putting together the report summarised it and prioritised it and sequenced it, and passed it to CIO, stating this what should be the focus in the next 1-2-3 years, and reporting on the to the audit committee as well. "

The level of contact the internal audit has within the organisation assists in raising the awareness. Interviewee IA indicated what was done to achieve that:

> "Some way we are trying to do work around IT risk is I found that Audit committee was not spending the training money, training budget, so straight after the Virus attack, I arranged for our board member to come to a course effective board of committees and I asked the pres from the institute of directors to tailor the segment on IT governance, and CIO came along to that course. What that showed, the problem about IT G and IT risk, and what brought to surface that fact that is business struggles to identify their business risk, and struggled to describe their business needs, to IS and IS tried their best to

> understand these needs, so sometimes IS come up with solution before they know the problem”

4.3.7.9.1 Company B

Interviewee IA elaborated on the internal audit role in the organisation:

> “IA – What we have done, in the last 2-3 years, it has not been as effective as I would like yet, we have our standard annual internal audit plan, and within specific section we call it IT plan, and we put that in place with from our Technology people , so we have distinct area and we say what areas do you want covered whether we got concerned about and specifically put those in, it is within one of IT senior manager, which we were not doing before”.

Interviewee HR outlined the importance of the audit process:

> “I see them as necessary part or the role the audit place, and from around the material we are using the content , that’s important the audit process happens, the following if there is new review of process , audit processes, in my role that have not done a lot recently, but I know it was done before that, so the IA and I work on that, have we got the right audit in place, are they doing what’s required, and that’s what IA and I have been discussing recently”

In addition, interviewee IS described the internal audit role: ”Internal audit keeps us honest, to have a monthly schedule of activity so we go through and check various”.

Interviewee IS elaborated further on the internal auditor within the company:

> “I worked in many companies, I found internal audit in this company probably the best because they understand what the business is trying to do and the business, very diversified you got news, having view of that means someone could bring the e wide balance, I find the internal audit quite useful because the understanding and the perspective that allows it to operate and enable things to happen more freely”

4.4 CONCLUSION

In this Chapter the field work findings were reported, based on the data collection methods that ware developed in Chapter 3. The field work was done by conducting semi-structured interviews in two large local organisations, collecting the relevant documents and logging observations in a log diary. Variations and challenges were reported to indicate if there was a need to adjust the field work plan. The data collection methods proceeded unchanged by recording the interviews and collecting the provided documentation.

The recorded interviews were transcribed and fed into NVivo 8. Nodes were structured to reflect the identified themes and the correlations between various nodes. Data were coded using thematic approach to define common themes. The defined nodes and the associated data were reported in various sections around the research sub-questions. Furthermore, noted challenges, problems and solutions were reported for further cross-case analysis.

The next Chapter 5 will include discussion of the findings and cross-case analysis. It aims to find answers to the research sub-questions, to test the proposed hypotheses and finally to answer the research question.

Chapter 5

Discussion of Findings

5.0 INTRODUCTION

The fact findings of field work conducted in two organisations were reported in Chapter 4. The reported findings were structured around the research sub-questions and other categories that were relevant to the research focus. In the literature review a thorough examination was presented for business value gained from managing IT risk in control-based structured environments. This chapter presents the cross-case study analysis of the findings in an attempt to answer the research question as well as to evaluate the hypotheses that have been devised in Chapter 3. Based on the analysis and evaluation outcomes, a further attempt will be made to outline solutions on how to establish IT risk management in control-based structured environments that would add value to the business.

This chapter is structured in the following ways; section 5.1 reviews the research question and the hypotheses proposed in Chapter 3. Section 5.2 discusses the reported findings with the aim to answer the research sub-questions to test hypotheses and to answer the research question. Section 5.3 includes discussion of the reported challenges and problems. Section 5.4 explores the recommended solutions, and section 5.5 concludes the chapter.

5.1 REVIEW OF RESEARCH QUESTION, SUB-QUESTIONS AND HYPOTHESES

In Chapter 3 the research question was identified. That was used to aid the field work during which collecting data was collected relevant to about the research focus. The research question, as outlined in Chapter 3 is:

How could a business realise the value of managing IT risk in control-based structured environments?

In addition, the following sub-questions were devised to further aid the researcher during the data collection stage:

(1) What is the IT risk context?

(2) How is the IT risk managed?

(3) What are the perceptions of business value derived from implementing IT control frameworks?

(4) What is the business value in managing IT risk in control-based structured environments?

Last is a set of proposed hypotheses that need to be evaluated in order to establish the evidence for answering the research question:

H1: Risk management is an ongoing process rather than a one-off project;

H2: Following a holistic approach in managing risk ensures valid outcomes;

H3: Reducing subjectivity in managing risk produces near factual results;

H4: Activities of other frameworks and best practices can be leveraged by meeting objectives at reduced cost.

5.2 CROSS-CASE ANALYSIS

As outlined earlier in section 4.1 the cross-case analysis will be structured around the research sub-questions. The findings will be discussed in section 5.2.1to answer the sub-questions first, in section 5.2.2 the devised hypotheses will be evaluated. In section 5.2.3 the answer to the research question will be discussed by examining the case study findings.

5.2.1 Research Sub-Questions

The research sub-questions were used during the face-to-face interviews conducted as part of the field work. The aim was to solicit information that would lead to answering the research question. This section is structured in four sub-sections 5.2.1.1-5.2.1.4 that discuss the findings related to the four research sub-questions.

5.2.1.1 Establishing IT Risk Context

As it was indicated in Chapter 2 section 2.1.3, the IT risk context consists of business and regulatory requirements. As it was indicated in section 4.3.1.1.1, Company A is a public-sector Health industry organisation with staff totalling 6000, providing health services for around 8% of New Zealand population. It is required to produce annual risk plan as part of the District plan aligned with the

MoH risk management requirements. The organisation coordinates with many government e.g. (DHB) and non-government organisations as part of their business requirements. In addition, the organisation is required to comply with a number of Acts, for example Health and Disability Act 2000, Public Records Act 2005 and Privacy Act 1993, as noted in Chapter 4 section 4.3.1.2.1. The company has about 90 IT staff on permanent basis and also some contractors whose number changes depending on the company's requirements. The total IT staff could fluctuate around 100-150. To meet various business and IT objectives, Company A has outsourced some of its IT functions, for example helpdesk and desktop management.

It seems though that the organisation's focus is more on the clinical requirements as noted by one of the participants, while IT doesn't get the adequate attention. As a result there is some indication that there are many unidentified IT risks. Furthermore, IT faces a number of challenges when identifying the risk of new technologies, for example mobile devices, as well as when retiring older technologies and introducing new ones. On the other hand, substantial risk exists around users' behavior and lack of defined processes.

The other organisation is Company B, which is a public sector firm, in the Media industry, as noted in Chapter 4 section 4.3.1.1.2. The company's main premises is in the North Island, however it has many smaller size branches in various locations around New Zealand, however, all IT systems and functions are located in the main building. While the total staff member number 940 is smaller than that of Company A, it has a similar IT structure with IT staff number around 73. There is a number of regulations the company is required to comply with, for example: Crown Entities Act 2004, Companies Act 1993. The company is required to file annual reports, as it is stated in their Statement of Intent and Interim report documents published on their web site.

The IT staff is approximately 73, however, the company did not outsource any of its IT functions, as its intent is to develop and retain in-house expertise. The company however, does hire specialists to complement their skills in the design and implementation IT solutions.

As a media company, the core business of Company B is the media content and the right of that is the "Lion share" of the business revenue. The other factor that determines the business priority is ‘transmission’ and to stay on air. On the other hand, adopting a new technology, for example Digital technologies, would impact the risk context by increasing the complexity level. IT functions would have to support the business plans, in terms of expansion and keeping the business application current.

When looking at the two organisations, they seem to have a number of things in common. Both organisations are in the public sector; they have similar IT team structure in supporting business operational and strategic activities, and face similar challenges in adopting new technologies. With regards to regulatory requirements, being public sector organisations, both companies are required to comply with a number of acts. However, as they operate in different industries, each organisations would have to comply with certain acts, for example, Air Code for broadcasting practice, Children Advertisement guidelines for Media, or Health and Disability Act 2000. Company A spans over very a wide geographical area, the number of its staff is almost 6 times the number of staff at Company B. However, their IT staff number is not substantially larger than that of Company B. The reason for that is Company A outsources a number of its IT functions, while Company B prefers to develop and retain in-house skills. Furthermore, Company A is required to coordinate with many government and non-government organisations within the health industry, which increases the complexity level of their IT risk context, while Company B does not have that concern. Table 5.1 summarises the discussed context.

Table 5.1: IT Risk Context in Case study Companies. (Author, 2011)

IT Risk Context	Company A	Company B
Business	A public sector health industry organisation. 6000 staff providing health services for around 8% of NZ population. The company has about 90 IT permanent staff and 10-60 contractors. The company has outsourced some of its IT functions, (helpdesk and desktop management). The organisation coordinates with many government (DHB) and non-government organisations	A public sector firm, in the Media industry, total number of staff 940. It has similar IT structure with IT staff number around 73. The company does not outsource any of its IT functions. Business priority is 'transmission' and to stay on air, news and content are prime concerns.
Regulatory	Health and Disability Act 2000, Public Records Act 2005 and Privacy Act 1993, MoH and DHB.	Crown Entities Act 2004, Companies Act 1993, Air Code for broadcasting practice, Children Advertisement guidelines for Media.

5.2.1.2 IT Risk Management Process

In Chapter 2, section 2.1.3. IT risk management process elements were thoroughly examined. To perform the various tasks and activities that underline the relevant risk management process aspects, organisations adopt different approaches. This section examines how the case study organisations manage their IT risks that have been identified as the outcome of identifying IT risk context.

In section 4.3.2.1 it was reported that Company A has a Risk and Audit committee; similarly Company B has an Audit and Risk committee that oversees the overall organisation's risk and internal audit functions. With regards to defined roles and responsibilities, as it was reported in section 4.3.2.2, there doesn't seem to be a clearly defined ownership in managing overall or IT risk. Company A has a Quality and Risk team that in theory should manage the overall risk, including IT risk, or to some extent coordinate with the IT division to manage IT risk. However, that team is not functioning in an efficient way and IT risk is not managed by that group. Company A used to have an IT security manager that has left the organisation. In comparison, in Company B IT security and risk are part of one of the IT manager's portfolio, who coordinates with other functions and IT staff to ensure IT risks are under control. In addition, in Company B internal and external Auditors do further checks to verify the IT risk status, similarly to what Company A does.

With regards to a defined IT risk management process in Company A, the different answers gathered from the participants demonstrated that there is no fully defined and documented IT risk management process, as reported in section 4.3.2.3. In other words, IT risk is managed on ad-hoc basis, each IT team would manage their risk without taking in consideration the full IT and/or business context. That view was emphasised by one participant who indicated that there are many IT risks that IT is not aware of. Company A, as noted in section 4.3.2.4, is required to adhere to a risk management framework devised by DHB. However, there were no observations on the status of that. IT risk seems to be well managed at project level. However, no comments were made on what mechanisms the organisation has devised to transfer the residual risk, if any, to a unified IT risk register. In contrary, in Company B project risk is managed as part of the project framework based on PMI methodology, and residual risk is transferred to IT risk register. IT risk is regularly reviewed and risk register is updated.

Both companies use a mix of spreadsheets, Access data bases and in-house developed intranet for recording risks and following up on their progress, references found in 4.3.2.5 and 4.3.2.6. As noted earlier, Quality and Risk function at Company A maintains the overall risk register, but not IT risk, which is managed within IT functions. In Company B a web based forms are available to register IT risk, although is not fully consolidated with the overall business risk.

With regards to BCP and DRP capabilities, as reported in section 4.3.2.7., Company A seems to focus on the core business clinical functions, but not so much on IT aspects. Company B has developed some IT DRP based on providing dual systems. As for BCP, there seems to be a business based BCP that has the capability to keep the transmission or on-air status intact, which is vital for the organisation. Overall, both companies seem to have similar levels of BCP and

DRP. Table 5.2 summarises the examined elements of IT risk management process.

Table 5.2:IT Risk Management Process. (Author, 2011)

IT Risk Management	Company A	Company B
Committee	The company has an Audit and Risk committee	The company has an Audit and Risk committee
Defined roles and responsibilities	IT risk is managed at function level. IT security and risk role is vacant.	IT risk is part of one of the IT managers portfolio
Process	IT is implementing a long term road map that would eventually establish IT risk management as part of the whole ITG.. Currently, IT risk is managed at the various IT functions but no defined process of regular assessment, other than internal and external audit.	IT risk is regularly assessed; devised controls are assured through self-test procedure overseen by internal and external audit.
Risk Register	Risk register for each IT function, no consolidated risk register	IT risk register
BCP and DRP	Focus on core business rather than on IT, which has simple form of DRP.	Form of IT DRP, with business BCP.

5.2.1.3 Business Value in Implementing IT Control Frameworks

Organisations opt to implement IT control frameworks for various reasons. Companies A and B have adopted a mixture of frameworks, standards and best practices, as noted in section 4.3.3. This section starts with a summary of the reported findings about existing IT controls and risk management standard used in the case study companies. This is followed by a discussion on the perceived business values gained from implementing recognised IT control frameworks.

Company A has implemented customised enterprise architecture TOGAF as well as Prince2 for project management and ITIL for service desk, change and release management. In addition, the organisation follows the risk management guidelines AS/NZS 4360, and has developed a set of policies for IT in general and

IT security. However, no evidence was found that any of COBIT, Val IT, or ISO 27001 have been implemented or adopted in some form. Company A has made outstanding efforts in customising TOGAF and Prince2 methodologies to fit with the health industry context.

Similarly, Company B has adopted ITIL and PMI and has devised IT security policies based on COBIT, ISO 27001 and SIGS; the latter is based on AS/NZS 4360. Company B approach in implementing those frameworks, standards and best practices is to select what is relevant and would add value to the business, rather than implement fully COBIT or ISO 27001 and become accredited to ISO 27001 standards. Reported implemented IT control frameworks, standards and best practices are summarised in table 5.3.

Table 5.3: Implemented IT Control Frameworks, Standards and Best Practices. (Author, 2011)

IT Control Framework	Company A	Company B
COBIT	None	Partially (security related controls) implemented
ITIL	Change Management, Release Management, problem management, Capacity Management, Incident Management	Change Management, Release Management
ISO 27001	None	Partially implemented
Val IT	None	None
TOGAF	Customised and implemented	None
Prince2-PMI	Customised Prince2	PMI
Policies	General and IT specific policies devised and published	General and IT specific policies devised and published
Others (SIGS, AS/NZS 4360)	AS/NZS 4360	AS/NZS 4360, SIGS

As it was indicated in section 4.3.4, implementing IT control frameworks and best practices is a resource-intensive exercise and could take quite a long time to implement appropriately. However, it is vital to realise the benefits of implementing such frameworks. Organisations face a dilemma whether to invest in implementing costly controls frameworks and best practices, or to utilise the existing resources to improve their information systems by acquiring new technology. In the rest of this section an examination will be conducted of the business value gained from establishing control-based structured IT environments, as it has been reported by participants from the case study companies.

One of the important benefits IT control frameworks produce is business-IT alignment as it was explained in section 4.3.4.1. Within Company A, the perception about implementing enterprise architecture is to bring business-IT decision-making process to defined pathways as well as ensuring everybody is on the same direction. In addition, it was emphasised that TOGAF is about business rather than IS and about business process, business continuity, and ensuring underpinning IT processes and activities are functioning accordingly. Another view was that control frameworks would ensure business requirements are channelled through and interpreted by IT in their terms.

As for Company B, it was indicated that, with business dynamics and ever changing technologies, business and IT alignment requires on-going monitoring to re-assess and adjust the effort to retain the desired outcomes, as reported in section 4.3.4.1.2. The company has devised a strategic plan that has four key pillars; every project/function (business and IT) is supposed to relate to one of those pillars that supports it. In addition, the business-IT alignment was further tuned as the technology teams formed in a sort of layers, the high level layer where IT team is structured to support the business strategy. Furthermore, projects were pipe-lined and prioritised based on business demands, which in turn were based on the strategic pillars that were described earlier. In addition, aligning with strategy was demonstrated by providing support not only to the core business function, which is broadcast technology, but to support business applications as well.

Furthermore, the defined set of policies helped business as well as IT justify their decisions and/or make exception in order to meet business needs. That would eventually lead to one of the main IT objectives, which is to enable the business achieve their goals and objectives.

The other type of benefits is Effectiveness, which is demonstrated in high performing teams, systems and functions. As reported in Chapter 4, section 4.3.4.2, Company A participants indicated this benefit in various forms. For example, from the service desk point of view, implementing ITIL best practices helps to handle service requests they receive effectively. In addition, feeding reports of what has been received by the service desk into the ITIL-problem management process helps identify root cause problems. Furthermore ITIL-capacity management process prevents the systems risk of reaching their full capacity and alerts the system management before the demands increases to an unmanageable level. On the other hand, the control-based structured environments allow consistency across the organisation in terms of providing user support, project management and sound IT services in a proactive rather than reactive fashion.

Interviewee IA from Company B indicated how IT change management has improved and said that effectiveness was gained from implementing ITIL in Company B. That was demonstrated in a significant improvement in IT in the last 4 years; change management became a very structured process that established a change advisory board that meets weekly, and implemented automated workflows. That also enabled IT build up a knowledge-base of incidents so they could do reporting and trend analysis based on factual findings.

Similarly, project management methodologies were defined, which empowered IT to not accept unfinished projects. All that gives technology some support in terms of taking the responsibility of activities when they are complete and stable. Furthermore, project management was seen as crucial for delivering successful projects in with the anticipated value of the project, in terms of scope, quality, on time and within budget.

Efficiency was another form of added value the case study organisations described and reported as described in section 4.3.4.3. With regards to Company A, the benefit of applying ITIL incident management practices is in reducing or identifying the root cause of the incident. That helps to reduce the number of incidents, which in turn reduces the service desk calls. On the other hand, the structured work environment helps to bring in new or temporary staff who can contribute within a short period of time, as they would be able to follow the defined processes. That would surely reduce the staff turnover and would increase staff productivity.

As for Company B, efficiency is demonstrated in a number of ways, for example reducing the cost of website delivery by allocating a smaller team. Another example is when the information provided from managing service desk helped in making the right decision where head-count was retained to deliver the required service. Furthermore, the structured environment helped to do adequate costing and to charge business units that demand new technology or update existing one. The conserned business unit would carry the cost and if they want something expensive that has ongoing cost, they would have to justify the need for it. Similarly, project management's benefits were demonstrated in delivering projects scope, with the right quality, on time and within budget.

Section 4.3.4.4 explores another value aspect: security. Security can be seen in terms of confidentiality, integrity, and availability of information assets and systems. For Company A it was indicated that managing IT risk properly would realize a huge value, as this would provide enhanced IT environment with stability, security and privacy.

Similarly, Company B participants outlined the benefits of control-based structured environments from security point of view. For example, the defined policies helped IT in deciding on the use of personal devices. At some point staff wanted to bring their personal devices and connect them to the company's network system. The policies allowed IT to question that and were able to justify their decision in banning personal devices, which would have created security issues.

In addition, the value of BCP of DRP was mentioned as well. Company B has a formal structure and every business area has a crisis plan and crisis champion, and they test their plan in about every two years. Even though the IT DRP involves providing dual paths resilience redundant platforms in a single building, business definitely sees the value in that. For example, the news team definitely sees the value in having a backup, as news is the performance and strategic objectives for the company.

Framework and best practices define ownership and level of responsibilities for data, functions and processes. That clearly states and communicates responsibility and accountability to stakeholders, as it was emphasised by a Company A participant, as reported in section 4.3.4.5.2. On the other hand, Company B participants described the business-IT decision-making aspect where roles and responsibilities are defined as the IT senior manager makes recommendations and the GM has the financial authorisation. At the operational level, IT personnel would self-test existing controls, as they know the pitfalls and what to look for, and also know what the exceptions are, although that is done with taken into account role-segregation principles. Furthermore, there is an IT manager role that liaises with the business to gather their requirements and supports the business applications for HR and Finance. In addition to the technical team, there are application specialists who would respond to business-IT related enquires.

One highly valuable outcome of implementing IT control framework is enhanced communication. Participants from Company A indicated, as reported in section 4.3.4.6.1, that frameworks help in improving the communication among stakeholders as they use the same terminologies. Using common terminologies among various IT functions and business units has immense impact on the whole process. Business would be able to convey their requirements without any concerns of misinterpretation at the IT side. Similarly, IT would be able to respond accordingly and/or could easily ask for more resources to meet business requirements. In addition, as reported in section 4.3.4.6.2 for Company B, one participant from IT highlighted the benefits of communicating the right information as they would be able to make an informed decision and to provide evidence and justification. In addition, the business representative expressed their approval of the existing mechanisms that would allow adequate communication between business and IT. Good communication helps IT build adequate capabilities and prioritise their tasks according to business demands.

Another valuable benefit that IT control-based structured environments allow is a holistic view to the establishment of business and IT systems. As it can be seen in section 4.3.4.7.1, for Company A it was reported that ITIL best practices provide better control over how the whole operational area functions. That enables IT to provide the business with adequate support in form of quality and time. On the other hand, in Company A’s IS strategic plan, published on its web site, it was noted that “Another weakness, there are too many initiatives... without taking the context of the whole system into account”. That demonstrates the acknowledgment of the necessity of having a holistic view when prioritising their projects. That view was emphasised by one participant who indicated that without having the ability to establish the holistic view, many things will be missed out. Furthermore, the same view was iterated by another participant who indicated that without understanding the full picture, it wouldn't be possible to understand the true priorities of the organisation. Furthermore, it was indicated that TOGAF Enterprise Architecture is invaluable when analysing the whole business-IT interrelation and hence it helps to do adequate planning. TOGAF can be used in terms of brain-storming sessions, requirements gathering, discussion with business, prioritising and budgeting.

For Company B, as reported in section 4.3.4.7.2, it was indicated that the strategic initiative of the organisation stipulated that all business and IT projects and activities should be aligned with one of the strategic streams. That in turn should be aligned with the rest of the plan elements. In other words, IT initiatives should not take place only because they are good ideas for IT, rather they should be implemented because they will be supporting a business area. That view was shared by a business representative who stated that IT has taken a recent restructuring that resulted in providing better support to business applications. That was needed by the business and was valued immensely.

The last value aspect that was reported by the case study companies was increasing IT credibility in the business area. Company A participants elaborated on how ITIL would contribute to this factor, as reported in section 4.3.4.8.1. For example, ITIL – Change Management helps in improving the perception of IT department in the eyes of the business because there will be less delay and least disruption when implementing new solutions. In addition, identifying the root cause of the incident, which is part of ITIL – Incident Management, helps reduce the incident re-occurrence. That would certainly reduce the number of service desk calls and would please the business users of IT services.

With regards to Company B, it was reported in section 4.3.4.8.2 that devising a strategic plan and various ITIL management functions have improved IT performance immensely. That was demonstrated in various ways, for example change management has become a more robust and structured process, along with the establishment of a change advisory board that meets on weekly basis. In addition, incident management process was established and a knowledge base of incidents was built that helps in reporting and conducting trend analysis. On the other hand, IT can justify to the business their decisions that are made based on agreed policies, which increases IT credibility. For example, IT was asked once to reduce head counts. However, the service desk records showed that undertaking the devised reduction would impact on IT performance. It was an informed decision where business and IT aligned their decision to the benefit of the business.

Business values discussed in this section are summarised in table 5.4.

Table 5.4: Business Value in Implementing IT Control Frameworks, Standards and Best Practices. (Author, 2011)

Business value in IT control-based structured environments	Company A	Company B
Business - IT Alignment	Enterprise architecture TOGAF was implemented. TOGAF is about business rather than IS; business process, business continuity, and ensuring underpinning IT processes and activities are functioning accordingly.	The company has devised a strategic plan that has four key pillars, every project/function (business and IT) is supposed to relate to one of those pillars and to support it.
Effectiveness	Implementing ITIL service desk best practices help managing process on how to handle service calls. Capacity management manages business demands. Project management and sound IT services generally, from a proactive perspective rather than reactive.	There was significant improvement in IT in the last 4 years: change management, change advisory board that meets weekly. IT built a knowledge base of incidents so they could do reporting and do trend analysis.
Efficiency	Benefits of applying ITIL incident management practices are in reducing incidents by identifying the root cause.	Reducing the cost of website delivery, by allocating smaller team. The information provided from managing service desk helped in making the right decision where head-count was retained to deliver the required service.
Security (Confidentiality,	Managing IT risk would provide a huge value from	Defined policies helped IT in deciding on use of

Business value in IT control-based structured environments	Company A	Company B
Integrity, and Availability)	managing IT risk properly, as this would provide enhanced IT environment stability, security and privacy.	personal devices. The policies allowed IT to question the request and to justify their decision in banning personal devices, which would have created security issues.
Defined Roles and Responsibilities	Framework and best practices define ownership and level of responsibilities for data, functions and processes. That clearly states and communicates responsibility, accountability to stakeholders	Business-IT decision-making aspects where roles and responsibilities are defined as the IT senior manager makes recommendations and the GM has the financial authorisation. Segregation of roles principles are applied.
Communication	Frameworks help improve the communication among various IT functions and business units as they use common terminologies.	The benefit of communicating the right information as business and IT would make informed decision and be able to provide evidence and justification.
Holistic View – Planning	ITIL best practices provide better control over how the whole business operates. That would enable IT to provide the business with adequate support of the desired quality and time. TOGAF Enterprise Architecture is invaluable in assisting to understand the whole business- IT interrelationship and hence help in adequate planning.	The strategic initiative the organisation has devised stipulated that all business and IT projects and activities should be aligned with one of the strategic streams. That in turn should be aligned with the rest of the plan elements.
Increase IT Creditbility	ITIL – Change Management helps to improve the perception of IT department in the eyes of the business. ITIL – Incident Management helps to reduce the incident re-occurrence. That would reduce service desk calls, and	ITIL change management has become a more robust process, along with establishing of a change advisory board. In addition, incident management process was established and a knowledge base of

Business value in IT control-based structured environments	Company A	Company B
	would please the business users with IT services.	incidents was built. On the other hand, IT have become able to justify their decisions to the business.

5.2.1.4 Business Value in Managing IT Risk in Control-Based Structured Environments

In Chapter 2 it was established that risk exists in every aspect of business at strategic and operational levels. In addition, there are many types of risk, for example, financial risk, environmental risk, and IT risk. Organisations focus on their core business risk, where risk practices and methodologies existed and have matured. As for IT risk, despite the fact that there are some standards and frameworks to manage IT risk, practices have not reached the same maturity level as for other disciplines. Businesses manage their IT risk in various ways and apply different methodologies. This section examines the business value in managing IT risk in the established IT control-based structured environments within the case study companies.

It was reported in Chapter 4 section 4.3.2.1 and was further discussed in section 5.2.1.2 that Company A manages their IT risk in isolation from the whole organisation risk. Furthermore, various IT functions manage their respective risks without takeing into account the whole picture. As it was reported by one of the participants there is no cohesion between IT functions, which results in many un-identified risks. That view was corroborated by another participant (internal auditor) who indicated that there are many IT risks that IT do not know about. Having said that, as noted earlier, IT functions have established TOGAF enterprise architecture which manages IT risks related to business applications and seems to be working well. In addition, ITIL various functions and processes have been well practiced that helps to detect and manag IT operational risk. In addition, it was indicated that anticipating potential risks would help IT service desk respond in timely fashion that would reduce service calls and increase IT credibility. Furthermore, project management methodology Prince2 has been customised and applied accordingly.

It was reported that the project management office has devised a risk model to scale projects based on their business return and implied risk. In each of those main IT functions the recognised business value in managing the associated risk is to avoid undesirable events and/or to capture business opportunity. Despite the positive returns each IT functions individually demonstrated, it was noted in the IT strategic plan that IT functions lack the ability to have a holistic view of the environment. The lack of holistic view has resulted in prioritrising IT projects in inefficient fashion, as it was emphasised by many participants. This could result from a lack of dedicated staff to manage IT risk; it was understood that Company A had previously a security manager who had left the organisation. Part of that role portfolio is managing IT security risk, which could be expanded to include operational IT risk.

The environment in Company B is different from that in Company A, as IT risk is part of one of the IT manager's portfolio who participated in the interviews. Company B has an Audit and Risk committee that oversees the overall organisation risk and internal audit functions. IT risk is regularly reviewed and risk register is updated. Project risk is managed as part of the project framework based on PMI methodology. Should the deliverables of completed projects imply new or residual risk, then the risk is transferred to IT risk register. Furthermore, it was indicated by one of the participants that the control-based structured environments provide factual information that would allow IT to take adequate decisions. Once the right information is obtained, IT is able to respond positively to business demands. That helps to influence team structures and team capabilities. IT will be able to justify if there is a value for the business to have the requested service the access.

Another example for business value in managing IT risk is enabling IT to manage their IT functions more efficiently. To demonstrate that, when IT was asked to reduce FTE (Full Time Employee) number, the management referred to the help-desk records and the metrics inside there. IT management was able to justify their needs to retain team size to continue supporting the business demands.

Table 5.5 summarises business values explored in this section.

Table 5.5: Business Value in Managing IT Risk in Control-Based Structured Environments. (Author, 2011)

Business value in managing IT risk in control-based structured environments	Company A	Company B
Manage Business-IT risk	TOGAF enterprise architecture which manages IT risks relates to business applications. In each of those main IT functions there isrecognised business value in managing the associated risk to avoid undesirable events and/or to capture business opportunity	Control-based structured environments provides factual information. Once the right information is obtained IT is able to respond positively to business demands. IT will be able to justify if there is a value for the business to have the requested service or the access
Managing operational IT risk	ITIL various functions and processes have been well practiced that helped in detecting and managing IT operational risk.	Various ITIL functions were implemented that helped the organisation reduce operational risk and improve performance of day-to-day operations.
Effectiveness and Efficiency	It was indicated that anticipating potential risks helps IT service desk respond in timely fashion that would reduce service calls and increase IT credibility.	The organisation was able to manage their IT functions more efficiently. IT was able to justify their needs to retain team size to continue supporting business demands.
Managing IT project risk	Project management methodology Prince2 has been customised and applied accordingly. It was reported that the project management office has devised a risk model to scale projects based on their business return and implied risk.	Project risk is managed as part of the project framework based on PMI methodology. Should the deliverables of completed projects imply new or residual risk, the risk is transferred to IT risk register.

5.2.2 Hypotheses Evaluation

As it was noted in section 5.1, four hypotheses have been formulated to assert the researcher’s proposed theory developed in the literature review in Chapter 2. In this section an attempt will be made to find relevant evidence within the collected and analysed data from the case study organisations. The evidence will be cross-examined to establish on whether to accept or reject the hypotheses.

The gathered evidence will be presented in text, as demonstrated in table 5.6. The text will be analysed with qualitative approach quasi-judicial method, where a rational argument is used to interpret the data in searching for ‘for’ and ‘against’ statements that refute or prove the hypothesis in question. The qualitative approach does not deliver numbers as quantitative research methods do.

Table 5.6: Hypotheses Evaluation. (Author, 2011)

H1: Risk management is an ongoing process rather than a one-off project.	For	Against
Company A:	In Section 4.3.2.4.1 interviewee IA statement in paragraph 1. In addition, interviewee IE indicated the need to be able to respond to the new and emerging technologies, as noted in section 4.3.5.6.2 ; interviewee PM stated in section 4.3.4.2.1 paragraph 5 that”.. everything we do is about risk management, because the fact the matter is all our technologies need to be replaced in 3-4-5 year time’s span, the volume of change is really plus,..”	No reference found that suggests that IT risk management is a one-off project. The maturity level of IT risk management process is not up to a desirable level as indicated by interviewee IA who stated that in section 4.3.2.3.1 paragraph 6.
Company B:	In section 4.3.2.4.2, interviewee IS stated in paragraph 1 “ they evaluate risk on regular basis,.. there is monthly	No reference found

	process, quarterly and 6 monthly" Furthermore, interviewee PM indicated in paragraph 5 that any project residual risk would be transferred to IT operational teams who would update the risk profile.	
Verdict: Business dynamics and constant change in technologies require continual risk assessment to ensure the risk profile is current. From the evidence obtained, it is evident that IT risk management is a process rather than a one-off project. The verdict is H1 is supported.		
H2: Following a holistic approach in managing risk ensures valid outcomes.	For	Against
Company A:	A reference to Company A's IT strategic plan as well as statement by interviewee EA in section 4.3.4.7.1, paragraphs 1 and 2.	No clear and direct statement that says holistic approach would provide a valid solution.
Company B:	In section 4.3.4.7.2, statements by interviewee IA and IS in paragraphs 1, 2 and 3, 4 respectively.	No clear and direct statement that says holistic approach would provide a valid solution.
Verdict: The existence of many issues regarding business and IT misalignment, in Company A, and the evidence of success in company B, lead to state that H2 is supported.		
H3: Reducing subjectivity in managing risk produces near factual results.	For	Against
Company A:	Section 4.3.4.2.1, interviewee DS stated in paragraph 1, 2.	No clear reference to contradict that.
Company B:	Section 4.3.4.2.2 interviewee IS stated in paragraphs 4 and 5.	No clear reference to contradict that.
Verdict: Given the noted evidence the hypothesis is set to be supported.		

H4: Activities of other frameworks and best practices can be leveraged in meeting objectives with reduced cost.	For	Against
Company A:	In section 4.3.3.2.1 ITIL interviewee IA referenced ITIL in paragraph 1; interviewee EA in section 4.3.3.3.1 refers to TOGAF, paragraph 1. Prince2 was referenced in section 4.3.3.4.1 paragraph 2 by interviewee PM. In section 4.3.3.7.1 AS/NZS 4360 was referenced by interviewee IA in paragraph 1.	In section 4.3.5.8.1 paragraphs 1 and 2, interviewees DS, EA, indicated it is very complicated and difficult to achieve.
Company B:	In section 4.3.3.1.2 COBIT was referenced by interviewee IA in paragraph 1; interviewee IS referred to COBIT and IA and IS referred to ISO 27001, in paragraph 2. ITIL was mentioned in section 4.3.3.2.2 by interviewee IS in paragraph 1 and PMI was indicated in section 4.3.3.4.2, paragraph 1 by interviewee PM	In section 4.3.5.8.2 paragraph 1 and 2, interviewee IS and IA respectively, indicated it is complicated to integrate various frameworks and that there are still some issues in attempt to achieve that.
Verdict: While it is important to integrate the implemented frameworks and best practices it is difficult to achieve. Obtained evidence is not enough to refute or prove this hypothesis, hence it is inconclusive.		

5.2.3 Research Question

In the view of the reported findings, it is evident that business could realise the tangible and intangible values in managing IT risk in control-based structured environments.

From the discussion and analyses in sections 5.2.1 and 5.2.2, it has been demonstrated that establishing IT control-based structured environments that encompasses integrated framework/best practices/standards is resource intensive, costly and faces a number of challenges. However, the return outweighs the cost. The business would have the ability to holistically view the whole business context and analyse IT risk. That would allow the organisation to make informed decisions about how to avoid circumstances with adverse effects or the negative type of risk. On the other hand, should the positive type of risk materialise in forms of opportunities, organisations would have the adequate capacity and capabilities to capture any opportunities and gain business value. Business value comes in forms of security of the organisation assets, true sense of compliance, business and IT alignment, performance and transparency of information.

5.3 CHALLENGES AND PROBLEMS REPORTED IN FIELDWORK FINDINGS

Implementing IT control frameworks and adopting best or good practices in IT systems face various obstacles. The literature reviewed in Chapter 2, section 2.5 a number of challenges were explored, for example business, technology and regulatory changes and demands. This section explores the challenges in the context of the case studies. Sub-section 5.3.1 explores the challenges, and sub-section 5.3.2 examines the problems reported in the field findings in Chapter 4.

5.3.1 Challenges

One of the challenges reported in Chapter 4 section 4.3.5.1 is that IT risk management standards are in their infant stage in comparison to risk management in finance and other disciplines. This could become an issue when the standard doesn’t cover certain environment or technologies. It was reported in section 4.3.5.1.1 by one of Company A’s interviewee who emphasised the same view on the capability maturity level of IT risk standards.

The other important aspect is the lack of awareness of the necessity of applying IT controls to manage IT resources in response to business demands. That could create many issues when attempting to establish control-based structured environments. In section 4.3.5.2.1 some of Company A participants emphasised that business people have always struggled with IT when requesting new technologies. Lack of awareness could exist at any level of business and IT. One interviewee indicated the lack of awareness among board members of the IT role in enabling the business, and the need to establish right mechanisms for business and IT to communicate their requirements.

Another challenge an organisation could face when it intends to establish a control framework is the lack of experience in implementing control frameworks. As it was noted in section 4.3.5.3, while an organisation could outsource that to a specialised vendor, that entails risk in itself. That view was shared by participants from the case study companies.

In the literature review (Chapter 2, section 2.5) it was indicated that it is imperative to respond to business, regulatory and technology demands and changes. The response has to be done in a timely fashion to ensure the devised risk treatment plan is effective and efficient. However, building adequate capabilities that provide desirable outcomes comes at a cost. It was indicated by one of the Company A participants, as reported in Chapter 4 section 4.3.5.4.1, that implementing IT control framework takes long time. Furthermore, it was indicated that generally there is reason for why Company A is not adequately implementing IT control frameworks. That is because the cost in terms or time and resources. Participants from Company B shared the same view and indicated, as reported in section 4.3.5.4.2, that COBIT, for example, would take quite a long time to implement as it is a ‘vast thing’.

It was demonstrated in the previous paragraph that implementing IT control framework is resource intensive. For that reason, executive management’s support is vital for a successful implementation. It was reported by both case study companies, A and B as shown in sub-section 4.3.5.5.

On the other hand, it was discussed in sub-section 4.3.5.6 that business and technology demands put a lot of pressure on IT resources. For example,proliferation of mobile devices as it was indicated by an interviewee from Company A and the fact the company requires replacing many technologies every 3-4 years. Another interviewee described another aspect of the same issue and indicted that day-to-day operations take time and this doesn’t allow IT staff to implement IT control best practice. Similarly, Company B interviewee outlined that the current IT capability to support business applications is not sufficient to provide the required level of support. That creates an environment where everyone is running around trying to get things delivered, without adequate planning. In addition, some ambiguity in regulatory directions could cause another challenge an organisation would have to face, as it was reported in sub-section 4.3.5.10 by Company A participants. However, that challenging aspect did not seem to be a concern for any of Company B's participants. In the literature review, Chapter 2, section 2.5 several business, technology and regulatory changes and demands were explored that come in line with the reported findings from the case study companies. Business, regulatory and technology demands in corporate environment are expected to be high and would require constant attention. However, a balance needs to be struck to attend the other demands, such as strategic and daily operations.

It was indicated in the literature review that implementing IT control environment would take time and effort for the new environment to be adopted by staff and to become part of the organisation's culture. In Chapter 4, sub-section 4.3.5.7, staff resistance to new environment was reported as a challenge, which plays a big role in delaying or hindering the process of implementing IT controls framework. One reason for that, as it was expressed by one of Company A participants is that people would resist any changes if they don't see any value in them. In addition, some staff not liking to work in a structured way is another reason. Similarly, a participant from Company B outlined how staff would resist implementing and applying new measures, and some technical people would like spending time dealing with technical aspects rather than performing administrative and documenting tasks.

The last two challenging aspects an organisation would face are complexity and too many frameworks and standards to implement as it was reported in sub-sections 4.3.5.8 and 4.3.5.9 respectively. It was reported by Company A participants that implementing control frameworks and standards and coordinating between various best practices is a very difficult exercise and was described as a 'big challenge' and 'It is not easy'. One reason for that, as it was reported, is that it requires a thorough understanding of the system and business themselves. Reported findings from Company B show the same view that indicated for example, COBIT framework is vast and would take years to implement. In addition, there are many models and frameworks, as outlined by other participants.

Table 5.7 summarises the discussed challenges.

Table 5.7: Reported Challenges in Implementing IT Control Frameworks. (Author, 2011)

Challenge Category	Description
Immature IT Risk Standard	IT risk management standards are in their infant stage in comparison to risk management in finance and other disciplines.
Lack of Awareness	The lack of awareness of the necessity to apply IT controls for managing IT resources; this could be within IT as well as business and at all levels.
Lack of Local Expertise	Lack of experience in implementing control frameworks is a big challenge; organisation could outsource that to specialised vendors, however, that entails risk in itself.
High Resource Consumption	Building adequate IT control framework and IT risk management capabilities that provide desirable outcomes is time and resource intensive.
Lack of Executive Management Support	Executive management's support is vital for the successful implementation of any frameworks, standards and best practices.
Business and Technology Demands	Business, regulatory and technology demands in corporate environment are expected to be high and would require constant attention. However, a balance needs to be struck to attend to other demands, like strategic and daily operations.
Resistance	Implementing IT control environment would take time to become part of the organisation's culture and could be hindered by staff resistance.
Ambiguous Regulatory Directions	Regulatory directions could be ambiguous, as noted by a Company A interviewee. However, This challenging aspect did not seem to be a concern of any of Company B's participants.
Complexity	Implementing control frameworks and standards and coordinating that with various best practices is a complex exercise as it requires a thorough understanding of all frameworks and the business.
Many Frameworks	There are many models and frameworks: TOGAF, ITIL, ISO 27001, COBIT, AS/NZS 4360, ISO 31000, ValIT, RiskIT. It is a daunting task to build the knowledge and practical experience to implement and integrate those frameworks, best practices and standards.

5.3.2. Problems

In the literature review in Chapter 2, a number of problems were discussed and the research question was derived that is relevant to the research focus problem. Subsequently, the field work was planned to solicit data that could be used to validate the proposed hypotheses and to answer the research question. However, in the course of collecting the data through semi-structured interviews with the case study participants, a number of problems arose. In this section, the problems reported in Chapter 4, section 4.3.6 will be examined.

One of the reported problems relates to business and IT silos. Disjoints between business and IT create a number of problems. As reported by Company A participants in sub-section 4.3.6.1, business struggle to identify their business risk, and struggle to describe their business requirements to IT. That would result in IT producing a solution before they know what the business requirements are, and would have to make an educated guess based on anticipated risk. Furthermore, it was indicated that there was no cohesion between IT functions themselves, which would deepen the gap even further.

As noted in the previous paragraph, Business - IT silos lead to business and IT misalignment, which in turn leads to various problems, among them prioritisation that has been identified by most of the participants. It was indicated by Company A interviewee, as reported in sub-section 4.3.6.2.1, that, without understanding the organisation priorities as a whole there will be a solution that does not fit the true business requirements. Similarly, in sub-section 4.3.6.2.2, findings from Company B indicated that the business has a lot of ideas and initiatives that they want to implement, however, there is no clear sense of prioritisation.

In sub-section 4.3.6.3 it was reported that there seem to be a number of issues around business and IT structures, in particular around functions and roles that allow two-way communication, i.e. where business requirements are conveyed to IT and IT communicate their concerns. This problem could be the root cause for the two reported problems in the previous paragraphs. It was reported by one of Company A participants that there is no cohesion between IT functions themselves and between IT as a whole and business. It was further reported that there doesn’t seem to be cohesion between business units to prioritise their requirements. Similarly, Company B findings, in sub-section 4.3.6.3.2, pointed out the gap between the business strategy and the implemented projects. Furthermore, a task, for example, project post implementation-review is not conducted as it should, and there is no real audit function throughout the project at the moment.

The findings reported for Company A, made many references to Quality and Risk function that should be managing the whole organisation risk, including IT. However, as reported in sub-section 4.3.6.4, this function seems to be underperforming. In addition, the company has a vacant IT security role that should manage IT security risk. That would result in un-identified risks that the organisation is not aware of. However, various IT functions seem to manage their IT risk, although only individually. Findings from Company B, in sub-section 4.3.6.4.2, indicated that business and IT risk are managed in a defined manner. The company had previously a dedicated resource to manage security and risk that proved to be ineffective, so currently IT risk is part of one of IT senior manager’s portfolio. In addition, IT staff at lower levels were trained and equipped with tools and system rights proportionate to their levels of responsibility, to manage and assess security risk.

BCP and DRP are quite vital for sustaining the business. In sub-section 4.3.6.5, the existing level of BCP and DRP in the case study organisations was explored. Company A does have a form of BCP, but IT is not part of it. An important aspect that was highlighted by one participant is that IT is considered a back-office function. Similarly, Company B interviewees stated the status of BCP-DRP that currently exists: the company has an IT DRP at system specific level but not at the enterprise level. Given the size and type of industries in which the two organisations operate, it is expected of them to have a high level of Business Continuity and Disaster Recovery Planning, where IT is the backbone of that. However, as indicated, that was not the case.

In a corporate environment, where business and technology changes happen quite often and at various levels and scales, it is imperative to build adequate capacities and capabilities to monitor and analyse changes and trends that could take place. For Company A, it was concisely and precisely described in sub-section 4.3.6.6.1 by one participant, who stated: “It is appallingly bad;

nobody is doing any proactive monitoring it is done on a crises basis". In Company B, the picture was not better than what was described in the first company.

The other problem was noted in sub-section 4.3.6.7 is user behaviour in terms of using IT systems. A Company A's interviewee indicated that "most of problems we can't fix, they are around user's behavior", while a Company B participant commented on IT staff behavior of not using time-sheeting system as they should. On the other hand, it was indicated that there is an issue at the senior management level, as there is no appetite to hold a difficult conversation, where clear objectives are defined.

The reported and examined problems in this sub-section are summarised in table 5.8.

Table 5.8: Reported Problems in the Case Study Organisations. (Author, 2011)

Problem	Description
Business - IT Silos	Gaps between business and IT create a number of problems. Organisations have difficulties to identify their business risk and struggle to describe their business requirements to IT. That results in IT producing a solution without knowing what the real business requirements are.
Business and IT Misalignment	Business - IT silos lead to business and IT misalignment, which in turn leads to various problems, among them inadequate prioritisation.
Business - IT Structures	Lack of functions and/or roles that allow two-way communication, where business requirements are conveyed to IT and IT communicate their concerns.
Risk Management Function	Organisations need to clearly define risk management functions roles and responsibilities.
BCP-DRP	BCP and DRP are quite vital for business. The existing level of BCP and DRP in the organisations is for the business only but IT is not part of it, because IT is considered a back-office function.
Reactive Not Proactive	In a corporate environment where business and technology changes happen quite often and at various levels and scales, it is imperative to build adequate capacities and capabilities to proactively respond to business and technology changes.
User's Behaviour	User's behaviour in terms of using IT systems was a noted problem by case study organisations. It was indicated that there is an issue at the senior management level as well.

5.4 RECOMMENDED SOLUTIONS

In the previous section patterns for challenges and perceived problems were examined. That demonstrated that although the case study organisations have implemented a mix of enterprise architecture, standards and best practices, the implementation is partial and still has some gaps. In this section an attempt is made to examine the possible solutions that were identified in Chapter 4 section 4.3.7.

The first remedy that has been devised is to define business objectives. Business units including IT should first identify their objectives and assess the risk associated with those objectives. In sub-section 4.3.7.1.1 a participant from Company A indicated that their company, including IT, has not identified their objectives, which in their opinion needs to be done. Furthermore, it was indicated that that would help the business unit identify their risk. Objectives should be identified at all levels, including the division/function levels as this would assist in assessing the risk at a granular level. As for Company B, strategic initiatives have been identified that required all planned projects/tasks to be mapped to a relevant initiative. However, it was indicated by one participant that there is still an issue with prioritising projects, which demonstrates the lack of defined objectives that map to the organisation's strategic goals.

Implementing frameworks and best practices requires certain level of expertise that might not be locally available. Organisations resort to third party vendors seeking their consultation and expertise in establishing IT control-based structured environments. Consulting external specialised parties could be a valuable option to assess the environment and devise a remediation plan. Although outsourcing has a cost and entails risk as well, external parties could be utilised to validate internal assessment. The latter would add another layer of protection and validation. Company A, as reported in sub-section 4.3.7.2.1, has a third party who provides various consulting services in that respect. Furthermore, as it was observed, Company A's IT leadership has utilised the third party advice to gain executive support. On the other hand, Company B, as noted in sub-section 4.3.7.2.2, utilises an external vendor to provide another level of assurance to the robustness of their IT control structures and to review business applications and SLAs. It was emphasised, however, that consulting third party should add value to the business.

For some organisations executive support is not easily obtained. Often IT management would spend time building business cases, but to no avail. IT management could make use of major incidents when they take place, be they local or at another organisation. Major incidents help demonstrate the impact of the incidents in practical terms and exhibit that if it happens elsewhere, it could happen at the same organisation as well. Company A, as it was reported in sub-section 4.3.7.3.1, has suffered from a virus attack and that raised the executives' awareness of the role that IT plays. No similar incident has been noted in Company B reported findings, however, incidents do take place at various organisations and they could reach the media, from where other organisations could learn a lesson.

It has been noted in section 5.3.1 that lack of awareness and/or lack of local expertise would cause a challenge that would hinder the organisation ability to implement IT control frameworks. Educating and training schemes at all levels could play a vital role in overcoming those challenges, as it has been noted in Company A reporting in sub-section 4.3.7.4.1. In addition, special awareness programs could be designed to target particular groups to raise their awareness of particular topics. Similarly, general awareness program would help in training staff on how to comply the organisation's policies and use IT resources responsibly. Furthermore, developing in-house expertise in implementing and utilising frameworks and best practices would help immensely in adopting those practices.

Similar observations were made in Company B. For example, IT and internal audit senior manager are affiliated to professional groups to keep abreast with relevant trends. Education and training is necessary for staff at all levels. This will help to develop in-house expertise and empower staff with the necessary tools so that they can adhere to the organisation polices and procedures.

One vital aspect of business and IT alignment and credible work-relationship is the efficient communication between business and IT. It was reported by Company A's participants, in sub-section 4.3.7.5.1, that good communication would allow business convey to their needs and IT to translate that in technical terms. Organisations should have functions that channel through business requirements to IT and make sure the work is performed correctly, in the right time and design. In addition, these functions should help make the business aware of IT services and existing capabilities and convey to IT how business assesses IT services and what to expect of them. That would surely build trust and confidence between business and IT. Similarly, Company B participants indicated, as noted in sub-section 4.3.7.5.2, that good communication with business helps IT deliver the required services. In addition, effective communication helps IT build adequate capabilities and capacities.

Organisations have various structures and business requirements, and frameworks and best practices are not one size fits all; therefore it is imperative to customise those control frameworks and best practices when applying them. As it was reported in sub-section 4.3.7.6.1, Company A has customised TOGAF enterprise architecture to serve the organisation and industry environments. The company has basically taken the Architecture Development Method (ADM) and modified it to fit the Health industry context and called it health-based standards. That has been adopted by the DHB within the geographic area. All of DHBs have adopted and agreed to use the Health-based TOGAF, which is the health view of the ADM. In addition, the organisation has applied Prince2 methodology that has been customised to suit their business context, and branded the tailored version, as a DHB-way. It has been indicated, however, that customising control frameworks should meet business objectives, which necessitates having business view on IT capability maturity model level. Within Company B, as reported in sub-section 4.3.7.6.1, the organisation's approach in adapting control framework is to apply what is relevant to their context, for example COBIT and ISO 27001. In addition, the organisation sought a capability maturity level of the applied controls that suited the organisation's environment.

Findings reported from case study companies in sub-section 4.3.7.7, show that demonstrating value to business increases IT credibility and improves business and IT alignment. That certainly works in conjunction with effective business –IT communication and contributes to educating business and raising their awareness of IT role as a business enabler. Through an effective communication IT could get the right prioritisation in place, as IT would understand business requirements, build those solutions, and demonstrate the expected value. That should not only take place when implementing long term and strategic solutions, but also in day-to-day operations. Furthermore, IT can demonstrate to business that IT is listening to business new ideas, although IT may not always agree with them. However, that helps understand what business would like to have, and IT could find a feasible solution. That would certainly help build and improve trust in the business-IT relationship. In similar fashion, findings from Company B, reported in sub-section 4.3.7.7.2, emphasised the importance of demonstrating business value. For example, IT could offer certain services, if there is a value for the business to have the service or the access, and there is a limited risk for the business in doing that. Furthermore, IT could justify a decision taken, where there was a value to the business or not.

At present there are many frameworks, standards, and best practice that complement each other, and where one is more applicable than the other. For example, ITIL serves IT operational functions and it instructs how to implement certain controls, while COBIT works at strategic and tactical levels and indicates what needs to be done. Similarly, TOGAF is enterprise architecture while ISO 27001/2 standard is specifically for IT security management. When an organisation opts to implement a number of these methods, it is important to integrate and leverage them to achieve optimal value and eliminate overlapping. However, it is not easy to integrate existing frameworks and best practices, as it was outlined as a challenge in section 5.3.1. That requires thorough knowledge of the frameworks, standards and best practices in question, along with the business context. To carry out such a task it is anticipated to take time and efforts, however, there will be considerable value to the business.

Large organisations have internal audit function; however, not all of them have IT audit capacity. Internal audit could play a vital role in aligning business and IT. Furthermore, as they report directly to the audit committee, that could help to elevate IT profile within the organisation and to attract executive attention to IT role as a business enabler. In addition, internal audit could add value to IT in validating IT controls and processes. Sub-section 4.3.7.9.1 reported Company A's findings in that respect, where internal audit played a crucial role in raising the

Board awareness of IT role and helped to lift IT profile. Similarly, the internal audit in Company B, although it has no IT audit capacity, helps the business and IT alignment, which was praised by business application managers. In addition, IT functions appreciate the value of auditing cycles that ensure validity of their IT controls and processes.

Table 5.9 summarises the solutions recommended in this section.

Table 5.9: Recommended Solutions in the Case Study Organisations. (Author, 2011)

Solution Category	Description
Define Objectives	Business units as well as IT should first identify their objectives and assess the risk associated with those objectives.
Consult 3rd Party Experts	When local expertise is not available or not to the desired level, consulting external specialised parties could be a valuable option to assess the environment and devise a remedy plan.
Make Use of Major Incidents	For some organisations executive support is not easily obtained. IT management could make use of major incidents when they take place and demonstrate the true impact of the incident.
Educate and Train	Educating and training schemes at all levels could play a vital role in overcoming challenges like lack of awareness and/or lack of local expertise, which would hinder the organisation ability to implement IT control frameworks. Awareness programs as well as developing in-house expertise on implementing and utilising frameworks and best practices would help immensely in adapting those practices.
Improve Business-IT Communication	One vital aspect to business and IT alignment and trusting work-relationship is efficient communication between business and IT. Good communication would allow business to convey their needs and IT to translate that in their terms.
Customise Frameworks to Business Environment	Organisations have various structures and business requirements and frameworks and best practices are not one size fits all; therefore it is imperative to apply pragmatic approach in implementing those control frameworks and best practices.
Demonstrate Business Value	Demonstrating business value to the organisation increases IT creditability and improves business and IT alignment. That certainly works in conjunction with effective business–IT communication and contributes to educating management and staff and raising their awareness of IT role as business enabler.

Solution Category	Description
Integrate Frameworks and Best Practices	Currently, there are many frameworks and best practices that complement each other, where one method is better than the other in the approach or the level. When implementing a number of these methods, it is important to integrate and leverage them to achieve optimal value and eliminate overlapping that could incur further cost.
Co-operate with Internal Audit	Large organisations have internal audit function; however, not all of them have IT audit capacity. Internal audit could play vital role in aligning business and IT. Furthermore, as most of them report directly to the audit committee, that could help in raising IT profile in the organisation and attract executive attention to the IT role as a business enabler. In addition, internal audit could add value to IT in validating IT controls and processes.

5.5 CONCLUSION

In this chapter findings reported in Chapter 4 were examined in relation to the research sub-questions devised in Chapter 3. The outcomes provided ground for testing the hypotheses proposed in Chapter 3 as well as answering the research question. Throughout the various sections summary tables were provided to demonstrate findings for each case study organisation as part of cross-case analysis. Testing the hypotheses resulted in validating 3 out of 4, while one of them needs further investigation to obtain enough supporting evidence. Subsequently, the answer to the research question was established. Further discussion was conducted to examine the challenges and problems reported in Chapter 4. When necessary, references were made to the relevant literature and to research methodology sections. In addition, a section was set to discuss solutions for overcoming the challenges and problems discussed in the chapter.

Next chapter will conclude the research with recommendations for further research.

Chapter 6

Conclusion

6.0 INTRODUCTION

In Chapter 5 the reported field work findings were discussed to find answers for the research sub-questions devised in Chapter 3. The discussion examined each case study data and carried some comparison when found beneficial to the research. As the answers to the sub-questions were obtained, the proposed hypotheses were tested utilising qualitative quasi-judicial method**.** At that stage it was viable to discuss and answer the research question. Further discussion was carried out to examine the reported challenges in implementing IT control-based structured environments, when possible a comparison was made to the sections with relevant literature review.

In this Chapter the research will be concluded with a summary of the findings of the case study companies, referencing the theory that was proposed in the literature review. Furthermore, the research question and its answer will be examined again with an emphasis on its importance to business and IT. In addition, there will be a discussion about the relevance of the research question to practitioners and professional service providers in the IT audit, risk management, security and governance fields. Lastly, a set of recommendations will be made for further research.

The chapter is structured as follows: section 6.1 summarises the findings. Section 6.2 discusses answers to the research questions and section 6.3 includes the recommendation for further research. Lastly, section 6.4 concludes the chapter and the thesis.

6.1 SUMMARY OF FINDINGS

Findings of the field work were reported in Chapter 4, where data collection methods devised in Chapter 3 were applied to collect data from two case study organisations. Using NVivo 8 the collected data were coded and nodes were structured around common themes. The two organisations, referenced as

Company A and Company B, are public sector organisations. Company A is a health industry organisation with staff totalling 6000, providing health services for around 8% of New Zealand population. The IT staff number could fluctuate around 100-150. Company A has outsourced some of its IT functions, for example helpdesk and desktop management. On the other hand, Company B operates in the Media industry, with total staff number of 940, which is less than that of Company A. However, Company B has similar teams structure with IT staff number around 73. Company B has not outsourced any of its IT functions; however, they consult third party vendors when necessary.

The data was obtained mainly from conducting face-to-face interviews with participants from the two organisations. The interviewees occupied roles with Audit, IT and Business. Participants from Company A, were Internal Auditor, Enterprise Architect, Program Office Manager and Desktop Service (see full details in table 4.1). Participants from Company B were Internal Auditor, Information Services Manager, Program Office Manager and Shared Services – HR (see full details in table 4.2).

The findings were structured around the research sub-questions that were devised in Chapter 3, where the IT risk context is established in terms of business, technology and regulatory requirements (see table 5.1 for full details). Furthermore, both companies have implemented most of ITIL functions and processes. While Company A has customised TOGAF enterprise architecture as well as Prince2 for project management, Company B has partially implemented COBIT and ISO 27001 covering security aspects and PMI for project management. Both companies have somehow adapted AS/NZS 4360 risk management standard and in addition, both have developed a set of IT policies for general use and for IT security that are published on their intranet sites. Different aspects of the IT risk management process within each company were examined. Company A manages IT risk within IT functions but they are not fully consolidated with the whole business risk, which has been identified as a problem where business is misaligned with IT. On the other hand, IT risk is part of one of IT manager's portfolio, and there is a defined risk management process (see details in table 5.2).

The other sub-questions related to the business value of implementing IT control frameworks and that of managing IT risk in IT control-based structured environments, were answered by analysing the collected data. For example, with regards to business value of IT control frameworks, a number of benefits were identified: Business-IT alignment, Effectiveness, Efficiency, Security, Defined Roles and Responsibilities, Communications, Holistic view Planning and Increase IT Credibility (see full descriptions in table 5.4). With regards to the business value from managing IT risk within business and at strategic, tactical and operational levels, see table 5.5. Organisations focus on their core business risk, where risk practices and methodologies existed for a long time and have matured. As for IT risk, despite the fact that there are many standards and frameworks to manage IT risk, practices are yet to mature.

Organisations face a number of challenges when they opt to implement IT control frameworks and best practices. Some of those challenges have been identified from the analysis of data collected from the case study companies. While both companies have forms of IT control-based structured environments, both have some problems that have been either conveyed directly by the participants or inferred by the author at the data analysis stage. Throughout the interviewees, the author gathered participants' recommended solutions to the existing problems, in addition to what the author has found out through the data analysis and literature review. The challenges, problems and solutions are detailed in tables 5.7, 5.8 and 5.9 respectively, and summarised in table 6.1.

Table 6.1: A Summary of Challenges, Problems and Solutions Reported in Tables 5.7, 5.8 and 5.9. (Author, 2011)

Challenges: Reported challenges organisations would face when implementing IT control-based structured environments through recognised frameworks, standards and best practices.	**Problems:** Reported and observed problems within the case study organisations.	**Solutions:** Recommended solutions by the participants and through the data analysis by the author.
Immature IT Risk Standard	Business - IT Silos	Define Objectives
Lack of Awareness	Business and IT Misalignment	Consult 3rd Party Experts
Lack of Local Expertise	Business - IT Structures	Make Use of Major Incidents
High Resource Consumption	Risk Management Function	Educate and Train
Lack of Executive Management Support	BCP-DRP	Improve Business-IT Communication
Business and Technology Demands	Reactive Not Proactive	Customise Frameworks to Business Environment
Staff Resistance	User’s Behaviour	Demonstrate Value to Business
Ambiguous Regulatory Directions		Integrate Frameworks and Best Practices
Complexity		Co-operate with Internal Audit
Many Frameworks		

6.2 ANSWERS TO RESEARCH QUESTIONS

The outcomes of hypotheses evaluation are three supported hypotheses that have sufficient supporting evidence, with one inconclusive hypothesis that did not have enough supporting evidence. That hypothesis is about integrating IT control frameworks; since the current environments where the case study was conducted had some deficiencies around integrating existing control frameworks and best practices, it was not possible to gather supporting evidence. Integrating implemented frameworks, standards and best practices is important for the benefit of an organisation as it would gain from implementing those frameworks. It is important to further investigate this aspect and gather sufficient evidence. Nevertheless, the remaining supported hypotheses, besides the answers to the research sub-questions emphasised that IT risk management is an on-going process. In other words, it needs to be kept current and in line with the business dynamics, technology and regulatory changes. In addition, to produce optimum results and to avoid problems like business-IT misalignment, the risk management process has to be integrated with the overall business risk. When evaluating risk and devising risk mitigation plan, overall business context has to be taken into account. That leads to the necessity to have an integrated perspective or a holistic view to be able to make informed decisions. To meet these objectives, IT risk should be managed through established IT control-based structured environments, which would ensure consistent use of recognised procedures.

It has been established that constructing IT control-based structured environments through recognised frameworks and best practices outweighs the other option, which is utilising individual accumulated experience. Furthermore, it has also been demonstrated that establishing an IT control-based structured environments that encompasses integrated framework/best practices/standards is resource intensive, costly and faces a number of challenges. Businesses are required to justify the high cost of IT control frameworks implementation. Therefore, realising the business value of establishing those costly frameworks is vital for gaining executive management support. However, realising the business value is not a straight forward process. IT divisions would have to build processes and procedures to be able to measure and communicate the outcome, preferably in quantitative forms, if viable. IT would gain from the measuring procedures, as they would be able to utilise that in managing the performance of their IT divisions. The adequate implementation of the recognised frameworks and best practices enables IT system to measure the business value. Once that is obtained, business value could be demonstrated to the business through established communication channels. The communication channels themselves should be one of the outcomes of the adequate implementation of those IT control structure environments. Besides, identifying business value would allow business–IT alignment, as well to prioritise projects based on the business demands. On the other hand, implementing effective IT control-based structured environments allows business and IT to develop appropriate capabilities. In other words, this would lead to building strategic capabilities that would allow IT to proactively respond to business dynamics and technology changes, as well as would protect the most valuable assets.

When IT controls are designed, the design should be based on cost effective balance between the business value of the controlled assets and the potential risk. However, being able to determine the business value and to estimate the potential risk is not expected to happen from the first implementation cycle. In addition, the estimation criteria need to be regularly re-evaluated, as asset business value and associated risk do change. So once again, the implementation of IT control frameworks should be based on the business value and associated risk to be able to build the environment with an adequate capability maturity model level that matches the business context. The adequate implementation should have mechanisms to ensure the implementation capability maturity level is reviewed on regular basis and/or when updating is required.

Establishing risk-based IT control-based structured environments through integrated recognised frameworks, best practice and standards would ensure a holistic view. That would enable organisations to realise the business value of their IT systems capabilities that underpin various business processes and assets. As a result, organisations would be able to protect their valuable assets with the least cost and to ensure their capabilities are regularly assessed. That should enable organisations to have a sound strategic plan that can be executed with the least deviation and to make informed management decisions to seize any opportunities when they arise, to grow and prosper.

In chapter 2 figure 2.6 the orgnisational environment attributes are depicted to illustrate the various business dynamics, technology changes and political and legislations requirements, where the organisation is required to accommodate, respond and comply with. Figure 6.1 illustrates the identified business and IT values argued in this research. The figure shows that the organisation would be able to respond to business dynamics and technology changes cost effectively while maintaining its valid compliance status with political and legislation requirements.

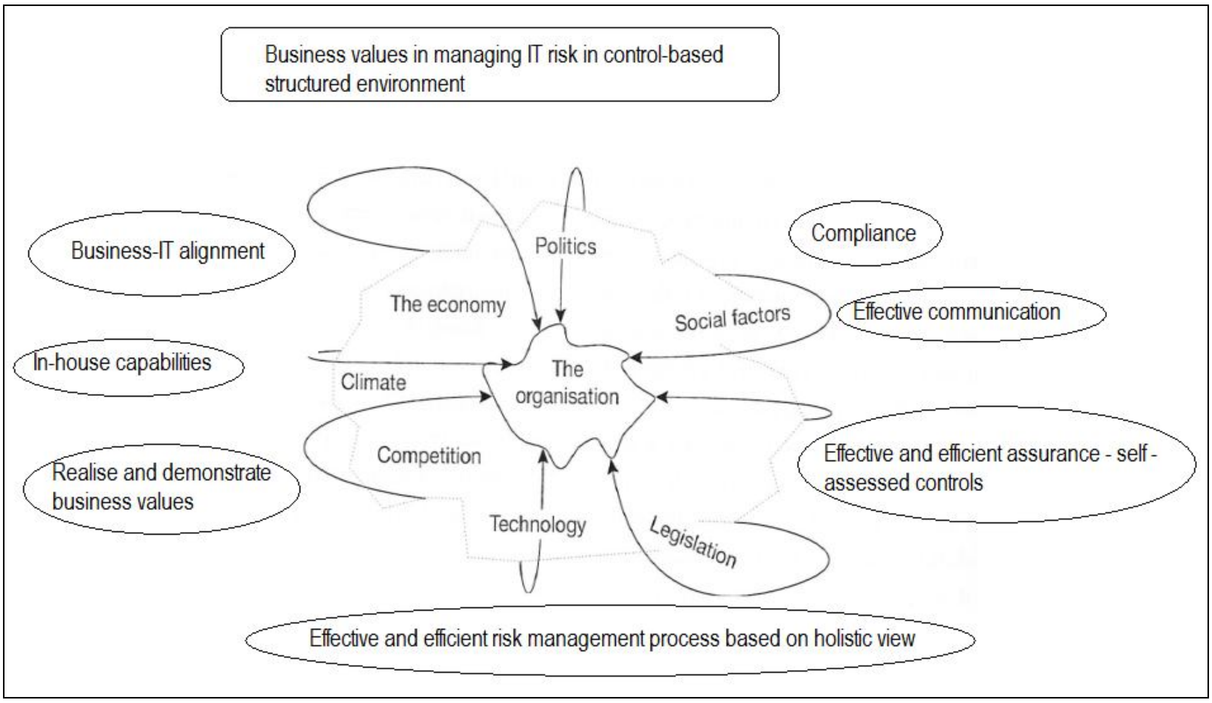

Business values in managing IT risk in control-based structured environment
Business-IT alignment
In-house capabilities
Realise and demonstrate business values
Compliance
Effective communication
Effective and efficient assurance - self - assessed controls
Effective and efficient risk management process based on holistic view
Politics
The economy
Social factors
Climate
The organisation
Competition
Technology
Legislation

Figure 6.1: Business Values and the Organisational Environment. (Author, 2012)

6.3 RECOMMENDATIONS FOR FURTHER RESEARCH

It was indicated in the literature review that when analysing risk, starting with vulnerability and threat assessment an element of subjectivity is applied that would impact the assessment outcome. Thence, the risk is evaluated either qualitatively or quantitatively. The qualitative approach is common, as it is viable to estimate, however, it is subjective, and there will be different views in evaluating the risk. Since, in business value is referenced in monetary figures the question is how qualitative risk could be presented in monetary terms. Although risk practitioners have advised a more granular qualitative approach based on some estimation of likelihood and impact, the outcome remains subjective.

Qualitative method is applied when there is subjectivity which could affect the outcome to a large degree. In contrary, quantifying the subject in financial terms facilitates better evaluation, and hence decisions are made based on factual figures. Qualitative figures do not particularly help in determining the exact value, especially when it comes to risk evaluation and business value in monetary figures. However, it was noted that quantifying IT risk is difficult, if it is possible at all. This seems to be an important area for further research to devise quantitative measures for IT risk and business value. Outcomes of such research would help practitioners apply more accurate evaluations and businesses accordingly could make better decisions.

On the other hand, in the findings reported in Chapter 4, one of the noted problems was that there are too many frameworks, best practices and standards. To establish adequate ITG and risk management process, organisations have no choice but to adopt a mix of frameworks, best practices and standards. The reason for that is either to meet compliance requirements, and/or to complement the applied frameworks, where one framework doesn't cover certain areas of IT. For example, COBIT covers some strategic and tactical objectives, but not operational level objectives. Conversely, ITIL is well known for its operational objectives coverage. On the other hand, ISO 27001-2 is specialised in IT security management aspects; similarly, ISO 31000 standard is for risk management methodologies. Val IT, TOGAF each has special and unique area to cover. Those frameworks, best practices and standards do not antagonise each other, rather they complement each other. However, it is expected to see some overlapping between them that should be identified and reduced to minimum to optimise the cost.

It would be very costly to implement those frameworks, best practices and standards, as this require expertise in all of them; even if a third party is introduced, the cost remains high. The other option is developing local expertise to be able to understand and implement the frameworks and best practices, which is also daunting and costly alternative. To be able to integrate those frameworks, best practices and standards, there needs to be a thorough understanding of the business and all of IT control frameworks in question. The most challenging aspect is the complexity of having a mix of those frameworks, best practices and standards. It is a known fact that establishing a complex IT controls environment could hinder the business, increase the cost, and it could give a false sense of security. Therefore, the author sees that there is very important research opportunity to investigate integrating frameworks, best practices and standards. Practitioners as well businesses would benefit from the outcomes of that kind of research.

6.4 CONCLUSION

This Chapter 6 has concluded the thesis with summarising the findings of the field work and from the analysis of the collected data. The field work and data collection method were devised in the research method that was selected to establish answers to the research identified problems that resulted from the literature review section. Furthermore, the research question was revisited to emphasise the value that the answer adds to the field of ITG, IT risk and security management and business continuity planning. In addition, a couple of recommendations were made for further research that would enable businesses to obtain better value of the implemented IT control-based structured environments.

The literature reviewed in Chapter 2 established the duality of risk and value. Barnier & Fischer (2010, para. 9) stated that “To grow, an enterprise must take risks”. The focus of this research is on IT risk, and in particular the various IT control frameworks including best practice and standards that are advocated to manage IT risk. It has been established that risk is an essential part of any business; if properly managed, it drives growth and opportunity. It has also been established that implementing recognised and risk based IT control frameworks and best practices would enable an organisation to realise the business value from managing IT risk in control-based structured environments. That structure provides a holistic planning, which in turn ensures business-IT alignment and prioritisation are done according to the business requirements. Measuring risk and value could be in either qualitative or quantitative forms; the latter is preferred but proved to be quite difficult to obtain. For that reason, this was recommended for further research. Furthermore, there is no one single framework that covers all aspects of strategic, tactical, operational, and project planning and security for business and IT. Therefore, it is paramount to integrate those frameworks, best practices, and standards, which was identified as another area for further research.

References

Abram, T. (2009). The Hidden Values of IT Risk Management. *ISACA Journal.* 2, 52-56

Ames, M. (2007). *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. (2007). *Risk Management in Context.* Paper presented at the Oceania CACS Conference, 9-12 September, Auckland, New Zealand.

Anderson, K. (2008). A Business Model for Information Security. *ISACA Journal.* 3, 51-52

Arksey, H., & Knight, P. (1999). *Interviewing for Social Scientists.* London: SAGE Publications.

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

Behr, K., Castner, G., Kim, G. (2004). *The Value, Effectiveness, Efficiency and Security of IT Controls*. Paper presented at the IT Governance International Conference, 15-16 November, Auckland, New Zealand.

Benvenuto, N.A., Brand, D. (2005). Outsourcing- A Risk Management Perspective. *ISACA Journal.* 2, 35-40.

Benvenuto, N.A., Brand, D. (2004). Managing the Risks of Outsourcing in a Post-Sarbanes World. *ISACA Journal.* 5, 31-33.

Brand, K., Boonen, H. (2005). *IT Governance based on COBIT 4.0 - A Management Guide*: Van Haren Publishing.

Carnegie Mellon University, Software Engineering Institute. (n.d.). CERT. Retrieved Aug 21, 2010, from: http://www.cert.org/octave/

Cavana, R., Delahaye, B., Sekaran, U. (2001). *Applied Business Research: Qualitative and Quantitative Methods*. Queensland, Australia: John Wiley & Sons.

Chatterji, S. (2007). Bridging Business and IT Streategies with Enterprise Architecture: Realising the Real Value of Business – IT Alignment. Paper presented at the Oceania CACS Conference, 9-12 September, Auckland, New Zealand.

Clifford, S. (2005). *So Many Standards to Follow, so Little Payoff*. Retrieved 6th September, 2010, from Inc magazine: http://www.inc.com/magazine/20050501/management.html

Collis, J., & Hussey, R. (2009). *Business Research* (3nd ed.): Palgrave Macmillan.

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.

Denzin, K., Lincoln, Y. (1998). *Collecting and Interpreting Qualitative Materials*. SAGE Publication Ltd

Design-Oriented Web Applications. *Journal of Computing Science in Colleges*. 24(4), 54-60

Dilworth, J., (1992). *Operations Management*. New York: McGraw-Hill.

Dowse, A., Lewis, E. (2006). *Whatever happened to Alignment?*. Paper presented at the IT Governance International Conference, 13-15 November, Auckland, New Zealand.

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.

Dul, J., Hak, T. (2008). Case Study Methodology in Business Research: Elsevier Ltd.

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

Flick, U., von Kardorff, E., Steinke, I. (2004). *A Companion to Qualitative Research.* SAGE Publications Ltd.

Futcher, L., von Solms, R. (2008). *Guidelines for Secure Software Development.* Nelson Mandela Metropolitan University

Gibbs, G., R. (2002*). Qualitative Data Analysis Exploration with NVivo.* Wiltshire, UK: The Cronwell Press.

Gillham, B. (2000). *Case Study Research Methods*. London, England: Eontinuum

Grover, N. (2009). *Banking Regulations, Mortgages, Recession and Accounting Imbroglios*. Retrieved 10th October, 2010, from: http://www.glgroup.com/News/Banking-Regulations-Mortgages-Recession-and-Accounting-Imbroglios-34087.html

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.

Huang, C., Goo, J., (2009). Rescuing IT Outsourcing: Strategic Use of Service-Level-Agreements. IT Porofessional. Vol. 11
No. 1, pp. 50-58. Jan. 2009

Hu, W. (2009). Internet-Enabled Handheld Devices, Computing, and Programming: Mobile Commerce and Personal Data Applications. USA: University of North Dakota.

Huff, S., Maher, M., Murno, M. (2004). *The IT Attention Deficit: Information Technology and Board of Directors.* Paper presented at the IT Governance International Conference, 15-16 November, Auckland, New Zealand.

IT Governance Institute. (2001). *Board Briefing on IT Governance*: IT Governance Institute.

ISACA. (2009). Introduction to Business Model for Information Security. ISACA

ISACA. (2009). *The Risk IT Framework Excerpt* [power point]. ISACA.

ISACA. (2007). *CISM review manual*, ISACA.

ISACA. (2006). *Val IT Brochure*, ISACA.

ISACA. (2009). Val IT Overview [power point]. 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.

Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Veen, A., Verheijen, T. (2009). *ITIL V3 Foundation Exam – The Study Guide*: Van Haren Publishing

Kennedy, S. (2004). Best Practice for Wireless Network Security. *ISACA Journal.* 3, 36-38

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.

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 8th August, 2010, from: http://www.casact.org/research/erm/overview.pdf

Murphy, T. (2002). Achieving Business Value from Technology: A practical guide for Today's Executive. N.J: John Willey & Sons, Inc.

NIST. 2002. Risk Management Guide for Information Technology Systems. NIST Special Publication 800-
Retrieved 19th September, from: http://csrc.nist.gov/publications/nistpubs/800-30/NIST-SP800-30.pdf on 23 August 2010

North, M., North, M., North, S. (2009). *Security from the Bottom-UP*: Compliance Regulations And The Trend Toward

Ogren, E. (2009). *HIPAA changes force healthcare to improve data flow.* Retrieved 21st September, from: http://searchsecurity.techtarget.com/news/column/0,294698,sid14_gci1349580,00.html?track=NL-102&ad=691251&asrc=EM_NLN_6005064&uid=5500366

Pironti, J. (2006). Information Security Governance: Motivations, Benefits and Outcomes. *ISACA Journal.* 4, 45-48

Ramakrishnan, G. (2001). Risk Management for Internet Banking. *ISACA Journal*. 1, 48-50.

Ramirez, D. (2008). Risk Management Standards: The bigger picture. *ISACA Journal*. 4, 38-40.

Raval, V. (2010). Risk Landscape of Cloud Computing. *ISACA Journal.* 1, 26-30.

Scott, H. (2005). Capital Adequacy beyond Basel. Oxford University Press, Incorporated 2005

Shin, N. (2003). Creating Business Value with Information Technology: Challenges and Solutions.

Shortreed, J. (2008). *Risk Management best practice is ISO 31000.* Retrieved 11th July 2010, from: http://www.irr-neram.ca/pdf_files/May9-2008/shortreed.pdf

Simones, H. (2009). *Case Study Research in Practice.* SAGE Publications Ltd.

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.

Stanley, R. (2004). Security, Audit, and Control Issues for Managing Risk in the Wireless LAN Environment. *ISACA Journal.* 3, 23-25.

Stockman, A. (1996). *Introduction to Microeconomics.* USA:The Dryden Press.

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.

Thorp, J. (2009). Val IT Overview [power point]. ISACA

Trivedi, T. (2007). 10 Things to Consider When Off-Shoring Operations. *ISACA Journal*. 5, 49-50.

Voon, P., Salido, J. (2009). *Trustworthy Computing Group*, Microsoft Corporation

Weerakkody, V., Irani, Z., (2010). A Value and Risk Analysis of Offshore Outsourcing Business models: an exploratory study.
International Journal of Production Research. Vol. 48, no. 2, pp. 613-634

Westerman, G., Hunter, R. (2007). IT Risk: Turning Business Threats into Competitive Advantage

White, G., Conklin, A., Couthern, C., Davis, R., Williams, D. (2003). *Security+ Certification Exam Guide*. New York: McGraw Hill

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.

Appendix A – Thematic Coding Methodology

The Thematic coding methodology was used in coding and analysing data collected from face-to-face semi-structured interviews with participants from case study organisations. In addition, data were extracted from some of the collected documents or from information obtained from the organisations' web sites.

In Chapter 3, where the research methodology was discussed and devised, thematic analysis was considered as a method for indentifying and analysing themes in data. Thematic coding is a process that is used within qualitative research methodologies. It has been argued by reputed authors that thematic analysis is a tool that can be used across different methods. The flexibility of thematic analysis contributes to the richness of its analysis. A thematic order emphasises themes, issues, actors, and conceptual categories. The objective of this assertion is to form a holistic configuration by associating empirical patterns (theme, events, and processes) to each other. Coding means that features, instances, issues and themes in empirical data are classified and given a specific label. The process involves associating and analysing data that share the same themes, ideas, concepts, and propositions. While the initial data were vague and appear incoherent, when processed they are refined, expanded, and maybe discarded. It was indicated that in a case study research predefined proposition are established and systematic coding is pre-planned and used to test the asserted propositions. The predefined propositions would become a basis for a pre-developed thematic coding scheme to be sued when collecting and analysing the empirical data.

Although there are specific rules for thematic analysis, some authors suggested some useful tips to help produce better results. One of the research method limitations was the possibility to produce similar results should the research method be conducted on another case study. Because of the subjectivity of the topic, producing similar results seems a challenging task to perform. This appendix is to outline the steps performed in the thematic analysis that was followed by the author in the process of analysing the obtained data and constructing the resulted themes.

These steps begin by organising all collected empirical data into a primary resource package, which is called a case record. The most important feature of that record is manageability. This implies that there will be some data reduction, where ‘background noise’ like repetitions, digressions, and any other irrelevant data are left out. Next step is to construct categories around the research sub-questions that were used in the semi-structured interviews, sort these categories and look for any similarities in themes or substantive statements that can be combined. The next step is to revise the transcripts and associate the relevant statements to those categories again to ensure that nothing important is missed. Then, review the transcripts and highlight any further substantive categories that would add value to the research focus. Review the transcript and associate any statements that are relevant to the new categories. Review the transcripts again and assign the highlighted substantive statements according to relevant categories. Review the created codes/nodes and write up memos describing any relationships between those nodes, for example dependency, exacerbated by, caused by.

Should there be more than one case study subject then repeat the indicated steps for the other organisations. Note that while transcriptions for all organisations should have the same categories, the same sub-questions would be asked. However, some sub-categories might not have relevant substantive statements because the two companies do not have identical environments.

The thematic analysis was conducted with the aid of one of the CAQDAS software programs called ‘NVivo Version 8’. The NVivo software enables the author to manage, organise, and analyse qualitative data more effectively through transcribing, coding, classifying themes, sorting data, and examining relationships in the collected data. CAQDAS is very useful for analysing large volume of qualitative data. In addition, CAQDAS does not provide any theoretical or analytical framework; however, the researcher has to decide on the theoretical and analytical framework that should be employed in the study. Obviously, thematic analysis is the analytical framework used for this research.

Appendix B – Ethic Approval

AUT
UNIVERSITY
TE WĀNANGA ARONUI O TAMAKI MAKAU RAU

MEMORANDUM

Auckland University of Technology Ethics Committee (AUTEC)

To: Brian Cusack

From: **Dr Rosemary Godbold and Madeline Banda** Executive Secretary, AUTEC

Date: 27 May 2011

Subject: Ethics Application Number 11/52 **Risk based assessment of IT controls frameworks: a case study.**

Dear Brian

Thank you for providing written evidence as requested. We are pleased to advise that it satisfies the points raised by the Auckland University of Technology Ethics Committee (AUTEC) at their meeting on 28 March 2011 and that on 16 May 2011, we approved your ethics application. This delegated approval is made in accordance with section 5.3.2.3 of AUTEC's *Applying for Ethics Approval: Guidelines and Procedures* and is subject to endorsement at AUTEC's meeting on 13 June 2011.

Your ethics application is approved for a period of three years until 16 May 2014.

We advise that as part of the ethics approval process, you are required to submit the following to AUTEC:

- A brief annual progress report using form EA2, which is available online through http://www.aut.ac.nz/research/research-ethics/ethics. When necessary this form may also be used to request an extension of the approval at least one month prior to its expiry on 16 May 2014;

- A brief report on the status of the project using form EA3, which is available online through http://www.aut.ac.nz/research/research-ethics/ethics. This report is to be submitted either when the approval expires on 16 May 2014 or on completion of the project, whichever comes sooner;

It is a condition of approval that AUTEC is notified of any adverse events or if the research does not commence. AUTEC approval needs to be sought for any alteration to the research, including any alteration of or addition to any documents that are provided to participants. You are reminded that, as applicant, you are responsible for ensuring that research undertaken under this approval occurs within the parameters outlined in the approved application.

Please note that AUTEC grants ethical approval only. If you require management approval from an institution or organisation for your research, then you will need to make the arrangements necessary to obtain this.

When communicating with us about this application, we ask that you use the application number and study title to enable us to provide you with prompt service. Should you have any further enquiries regarding this matter, you are welcome to contact Charles Grinter, Ethics Coordinator, by email at ethics@aut.ac.nz or by telephone on 921 9999 at extension 8860.

On behalf of AUTEC and ourselves, we wish you success with your research and look forward to reading about it in your reports.

Yours sincerely

Dr Rosemary Godbold and Madeline Banda

Executive Secretary

Auckland University of Technology Ethics Committee

Cc: Maher Al-Khazrajy maher_a@xtra.co.nz