

University of Tasmania Open Access Repository

Cover sheet

Title

Investigating COBIT for information technology audit in the Tasmanian public sector

Author

Gerke, L

Bibliographic citation

Gerke, L (2005). Investigating COBIT for information technology audit in the Tasmanian public sector. University Of Tasmania. Thesis. <https://doi.org/10.25959/23210051.v1>

Is published in:

Copyright information

This version of work is made accessible in the repository with the permission of the copyright holder/s under the following,

Licence.

Rights statement: Copyright 2005 the Author

If you believe that this work infringes copyright, please email details to: oa.repository@utas.edu.au

Downloaded from University of Tasmania Open Access Repository

Please do not remove this coversheet as it contains citation and copyright information.

University of Tasmania Open Access Repository

Library and Cultural Collections

University of Tasmania

Private Bag 3

Hobart, TAS 7005 Australia

E oa.repository@utas.edu.au

CRICOS Provider Code 00586B | ABN 30 764 374 782

utas.edu.au

Investigating COBIT for Information Technology Audit in the Tasmanian Public Sector

*Dissertation submitted in partial fulfilment of the requirements for the
degree of Bachelor of Information Systems (Honours)*

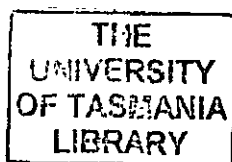
By

Lynne Gerke, BCom BIS



Submitted to the School of Information Systems, University of Tasmania
October 2005

Cent
Thesis
GERKE
BIS(Hons.)
2005



Statement of Authenticity

To the best of my knowledge and belief, this dissertation contains no material accepted for the award of any degree or diploma in any university, except where stated. All material obtained from previously published or written sources has been referenced in the text of the dissertation.

This dissertation may be made available for loan and limited copying in accordance with the Copyright Act 1968.

Lynne Gerke

October 2005

Abstract

There has been worldwide interest in corporate governance because of the high profile corporate collapses of the early 2000s. The use of control frameworks has been mandated in the United States of America through the Sarbanes Oxley Act of 2002. One of the popular frameworks adopted is the Control Objectives for Information and Related Technologies (COBIT).

Organisations have shown an increasing interest in using COBIT both as an IT governance framework and also for IT audit because of its focus on the alignment of business and IT goals and processes. The COBIT framework is massive, so there is a need for research to determine the most important IT processes in public sector organisations in order to reduce the number of audit areas included in an abbreviated COBIT IT audit instrument while retaining relevance. There is a large body of published work available for COBIT, however, much of this has originated within the domain of the practitioner and is aimed at a similar readership, with little, if any, academic research that has considered the effectiveness of the framework. Prior research has been conducted in the national and international arenas, but it is unclear if this can be extended to the Tasmanian public sector.

This research used a survey methodology to obtain ratings from selected Tasmanian public sector organisations for each of the high level IT control objectives in the COBIT framework. These ratings were compiled to form a ranked list of the most important IT processes for the Tasmanian public sector. Audit measures were selected for the key IT processes, then validated by a senior public sector IT audit professional and the instrument subsequently trialled on a range of Tasmanian public sector organisations. An evaluation of the IT audit process using COBIT was also undertaken.

The instrument developed contained seven IT control objectives and was successfully trialled in nine public sector organisations of all possible levels. The results obtained indicated that Tasmanian public sector organisations perceived ensuring security of their systems to be the most important IT process. Of the seven IT control objectives audited, five were also considered important in national and international studies.

The results obtained suggests that use of the COBIT-derived instrument for public sector IT audit provided a insight into the IT governance and control within these

organisations as well as indicating the degree to which the goals and governance of the organisation and the organisation were aligned, neither of which was available with the use of the previous instrument. The use of COBIT for IT audit in this case was considered to be effective and provides some validation in one public sector context of the extensive use of COBIT by practitioners.

Acknowledgements

The past five years have been a rollercoaster ride of triumphs and crashing disappointments, although fortunately more of the former than the latter. I would like to pay tribute to my inspiration and role model, my mother. Without your encouragement and support I would not have made it this far.

To Gail, thanks for persuading me that IT audit was an appropriate domain for me to research. Thank you for your unending patience, for being there and encouraging me when I didn't think I could continue. I don't think I could have picked a better supervisor, but I think you may have created a monster.

The support received from the Tasmanian Audit Office has been amazing. To Christina, thanks for your insights, for providing documentation, contacts and support; without you much of this project would not have been possible. Also to Kate, thank you for your support, for clarifying terminology and for being an admirable stand in when Christina was not available.

Without the co-operation of the managers who participated in the audit phase I would only have had half a project. Thanks to Jane, Jo, Andrew, Iain, Michael, Richard, Scott, Sean and Sen for taking the time out of their busy schedules.

To my patient and supportive colleagues at Roses Newsagency, thanks for understanding when I had assignments, exams and assorted other emergencies. Special thanks to Margaret for stepping in when disaster struck last year and when the going got hard this year. I must now surely be the most overqualified paper girl in the state.

Finally, I would like to dedicate this work to my father. I spent the first thirty years of my life trying so hard not to be like you. Fortunately I grew up. I know that although you may not have said it, you were proud of my achievements. This is for you.

Copyright Acknowledgement

Includes excerpts from COBIT: *Control Objectives for Information and Related Technology* (3rd Edition). ©1996, 1998, 2000 IT Governance Institute (ITGI). All rights reserved. COBIT is a registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute. Used by permission.

Table of Contents

CHAPTER 1 - INTRODUCTION	1
1.1 Introduction	1
1.2 Background.....	1
1.2.1 Governance	1
1.2.1.1 The United States Response.....	1
1.2.1.2 The Australian Response	2
1.2.2 COBIT.....	3
1.3 Information Technology Audit.....	4
1.4 Research Objective.....	4
1.5 Research Significance.....	5
1.5.1 Researchers	5
1.5.2 Practitioners	6
1.6 Thesis Structure.....	6
1.6.1 Chapter 1 - Introduction	6
1.6.2 Chapter 2 - Literature Review	6
1.6.3 Chapter 3 - Methodology	6
1.6.4 Chapter 4 - Results and Analysis	6
1.6.5 Chapter 5 - Conclusions	6
1.6.6 Appendices.....	7
CHAPTER 2 - LITERATURE REVIEW	8
2.1 Introduction	8
2.2 Governance	8
2.2.1 Corporate Governance and IT Governance.....	8
2.2.2 What is Information Technology Governance?	9
2.2.3 IT Governance.....	9
2.2.3.1 IT Strategic Alignment.....	10
2.2.3.2 IT Value Delivery.....	11
2.2.3.3 Risk Management.....	11
2.2.3.4 Performance Measurement.....	12
2.3 Statutory Requirements.....	12
2.3.1 Australia	12

2.3.2	United States of America	12
2.3.3	IT Frameworks	13
2.3.4	Summary	13
2.4	COBIT	14
2.4.1	Introduction	14
2.4.2	<i>The Framework</i>	14
2.4.3	The Control Objectives	16
2.4.3.1	<i>High Level Control Objectives</i>	16
2.4.3.2	<i>Detailed Control Objectives</i>	19
2.4.4	The Management Guidelines	19
2.4.4.1	<i>Maturity Models</i>	20
2.4.5	The Audit Guidelines	20
2.4.6	Prior Research on COBIT	21
2.4.7	Summary	22
2.5	Information Technology Audit.....	22
2.5.1	Introduction	22
2.5.2	ANAO	23
2.5.3	Tasmanian Audit Office.....	25
2.5.4	EUROSAI Self Assessment Project.....	26
2.5.5	Summary	26
2.6	Summary	26
2.7	The Research Question	27
CHAPTER 3 - METHODOLOGY		28
3.1	Introduction	28
3.2	Ethics	28
3.3	Research Aims	28
3.3.1	Aim 1	28
3.3.2	Aim 2	28
3.4	Research Philosophy	29
3.4.1	Ontology	29
3.4.1.1	<i>Objectivism</i>	29
3.4.1.2	<i>Subjectivism</i>	29
3.4.2	Epistemology	30
3.4.2.1	<i>Audit and accounting</i>	30

3.4.3	Research Philosophy Used	31
3.5	Research Methods	31
3.5.1	Phase 1	32
3.5.1.1	Survey.....	32
3.5.1.2	Survey Scope	32
3.5.1.3	Survey Instrument.....	32
3.5.1.4	Pilot testing	33
3.5.1.5	Questionnaire distribution.....	33
3.5.1.6	Follow up.....	33
3.5.1.7	Hypothesis Testing.....	34
3.5.2	Phase 2	34
3.5.2.1	Audit.....	34
3.5.2.2	Maturity Levels	34
3.5.2.3	Scope.....	35
3.6	Reliability and Validity	35
3.6.1	Reliability.....	35
3.6.2	Validity	35
3.6.2.1	Validity of the study	36
3.7	Analysis of Data	37
3.7.1	Phase 1	37
3.7.1.1	The issue of non-response bias.....	38
3.7.1.2	Determination of a ranked list.....	38
3.7.2	Phase 2	38
3.7.2.1	Justification of Choice of Audit Measures	39
3.7.2.1.1	Inclusions by agreement between sources	39
3.7.2.1.2	Exclusion by designation of originating organisation.....	40
3.7.2.1.3	Exclusion through necessity to look outside the organisation	40
3.7.2.1.4	Exclusion through non-applicability	41
3.7.2.1.5	Exclusion through potential inappropriateness	41
3.7.2.1.6	Exclusion through non-specificity	41
3.7.2.1.7	Validation of selected measures.....	42
3.7.2.2	Audit.....	42
3.7.2.3	Documentation.....	42
3.7.3	Processing	43
3.8	Evaluation of Use of Instrument	45
3.8.1	Duration of audit interview	45

3.8.2	Independent evaluation	45
3.8.3	Linkage of IT process to business goals.....	45
3.8.4	Relevance of instrument.....	45
3.8.5	Benchmarking	46
3.9	Summary	46
CHAPTER 4 - RESULTS AND ANALYSIS		47
4.1	Introduction	47
4.2	Phase 1 Survey of Tasmanian Audit Office Clients	47
4.2.1	Response Rate	47
4.2.2	Representativeness of the Data	47
4.2.2.1	<i>Organisational type.....</i>	<i>48</i>
4.2.2.2	<i>Respondent's Position</i>	<i>48</i>
4.2.2.3	<i>Familiarity with IT Processes</i>	<i>49</i>
4.2.2.4	<i>Familiarity with Business Objectives.....</i>	<i>50</i>
4.2.2.5	<i>Summary of Demographic Data</i>	<i>50</i>
4.2.3	Control Objective Rating Results.....	50
4.2.4	Comparison with previous studies	52
4.2.4.1	<i>Explanation of Table.....</i>	<i>53</i>
4.2.4.2	<i>Discussion.....</i>	<i>54</i>
4.2.5	Associated detailed control objectives	54
4.2.5.1	<i>Validation of selected measures.....</i>	<i>55</i>
4.3	Phase 2 Audit of Selected Public Sector Organisations	55
4.3.1	DS5 Ensure Systems Security	56
4.3.1.1	<i>Assigned Maturity Ratings for DS5 Ensure Systems Security.....</i>	<i>56</i>
4.3.1.2	<i>Interpretation of Results for DS5 Ensure Systems Security.....</i>	<i>57</i>
4.3.1.3	<i>Further Discussion.....</i>	<i>58</i>
4.3.2	DS4 Ensure Continuous Service	59
4.3.2.1	<i>Assigned Maturity Ratings for DS4 Ensure Continuous Service.....</i>	<i>59</i>
4.3.2.2	<i>Discussion of Results for DS4 Ensure Continuous Service.....</i>	<i>60</i>
4.3.3	PO1 Define a Strategic Information Technology Plan.....	61
4.3.3.1	<i>Assigned Maturity Ratings for PO1 Define a Strategic Information Technology Plan</i>	<i>61</i>
4.3.3.2	<i>Discussion of Results for PO1 Define a Strategic Information Technology Plan</i>	<i>63</i>
4.3.4	DS11 Manage Data	65

4.3.4.1	<i>Assigned Maturity Ratings</i>	65
4.3.4.2	<i>Interpretation of Results</i>	66
4.3.5	DS12 Manage Facilities	67
4.3.5.1	<i>Assigned Maturity Ratings for DS12 Manage Facilities</i>	67
4.3.5.2	<i>Discussion of Results for DS12 Manage Facilities</i>	70
4.3.6	AI6 Manage Changes	71
4.3.6.1	<i>Assigned Maturity Ratings</i>	71
4.3.6.2	<i>Discussion of Results for AI6 Manage Changes</i>	72
4.3.7	PO8 Compliance with External Requirements	73
4.3.7.1	<i>Assigned Maturity Ratings</i>	73
4.3.7.2	<i>Preliminary Discussion of Results for PO8 Compliance with External Requirements</i>	74
4.3.7.3	<i>Elimination of audit measures</i>	74
4.3.7.4	<i>Revised Assigned Maturity Ratings</i>	75
4.3.7.5	<i>Interpretation of Revised Results for PO8 Ensure Compliance with External Requirements</i>	75
4.3.8	Summary of Audit Results	77
4.3.9	Comparison with previous studies	78
4.3.9.1	<i>Limitations</i>	80
4.3.10	Evaluation of the Instrument	81
4.3.10.1	<i>Duration of Audit Interviews</i>	81
4.3.10.2	<i>Independent Evaluation of Audit Instrument</i>	81
4.3.10.3	<i>Linkage of IT Process and Business Goals</i>	81
4.3.10.4	<i>Base of the Instrument</i>	81
4.3.10.5	<i>Benchmarking</i>	82
4.3.10.6	<i>Summary</i>	82
CHAPTER 5 - CONCLUSION		83
5.1	Introduction	83
5.2	Research Objectives	83
5.3	Research Significance	84
5.3.1	Practitioners	84
5.3.2	Academics	85
5.4	The Research Questions	85
REFERENCES		88

APPENDIX A - COBIT PRIMARY REFERENCE MATERIAL 94

APPENDIX B – ETHICS APPROVAL FOR PROJECT 100

APPENDIX C – INFORMATION SHEET FOR PHASE ONE..... 103

APPENDIX D – INFORMATION SHEET FOR PHASE TWO 106

**APPENDIX E – STATEMENT OF INFORMED CONSENT FOR PHASE TWO
..... 109**

**APPENDIX F – COPYRIGHT PERMISSION FOR USE OF COBIT CONTROL
OBJECTIVES..... 112**

APPENDIX G – QUESTIONNAIRE, PHASE ONE 115

APPENDIX H – REFERENCE GUIDE, PHASE ONE 127

APPENDIX I - T TEST RESULTS..... 148

APPENDIX J – AUDIT WORKING PAPERS..... 157

APPENDIX K – COLLATED AUDIT RESPONSES..... 170

**APPENDIX L – FREQUENCY TABLES FOR ASSIGNED MATURITY LEVELS
..... 182**

Tables

Table 4.1: Type of organisation in which respondents are employed-----	48
Table 4.2: Position titles of respondents-----	49
Table 4.3: Familiarity with IT processes-----	49
Table 4.4: Familiarity with business objectives-----	50
Table 4.5: Ratings for Control Objectives from Phase One of study-----	51
Table 4.6: Comparison of control objectives identified as being important (source Guldentops et al 2002, Liu & Ridley, 2005, EUROSAT, 2005) -----	53
Table 4.7: Maturities assigned for DS5 Ensure Systems Security-----	56
Table 4.8: Minimum and Maximum Means for DS5 Ensure Systems Security-----	57
Table 4.9: Maturities assigned for DS4 Ensure Continuous Service-----	59
Table 4.10: Minimum and Maximum Means for DS4 Ensure Continuous Service -----	60
Table 4.11: Maturities assigned for PO1 Define a Strategic Information Technology Plan-----	62
Table 4.12: Minimum and Maximum Mean Assigned Maturity Levels for PO1 Define a Strategic Information Technology Plan -----	63
Table 4.13: Maturities assigned for DS11 Manage Data-----	65
Table 4.14: Minimum and Maximum Mean Assigned Maturity Levels for DS11 Manage Data -	66
Table 4.15: Maturities assigned for DS12 Manage Facilities -----	68
Table 4.16: Minimum and Maximum Mean Assigned Maturity Levels for DS12 Manage Facilities -----	70
Table 4.17: Maturities assigned for AI6 Manage Changes-----	71
Table 4.18: Maximum and Minimum Mean Assigned Maturity Levels for AI6 Manage Changes	72
Table 4.19: Maturities assigned for PO8 Compliance with External Requirements-----	74
Table 4.20: Revised Maturities for PO8 Ensure Compliance with External Requirements-----	75
Table 4.21: Maximum and Minimum Mean Assigned Maturity Levels for PO8 Ensure Compliance with External Requirements -----	76
Table 4.22: Summary of Mean Assigned Maturity Level Data for All Control Objectives on the Audit Instrument-----	77
Table 4.23: Maturity level means for common control objectives (source of Australian and International Data, Liu, 2003)-----	78

Figures

Figure 2.1 COBIT Conceptual framework (source ITGI, 2000a, p16).....	15
Figure 2.2: The COBIT cube (source: ITGI, 2000, p 16).....	15
Figure 2.3: Relationship between control objectives and the three perspectives of the COBIT cube (Source ITGI, 2000a, p 20).....	17
Figure 2.4: Template for presentation of high level control objectives (source: ITGI, 2000b p 21).....	18
Figure 2.5: Example of COBIT control objective documentation (adapted from ITGI, 2000b)....	18
Figure 2.6: Detailed Control Objective (adapted from ITGI, 2000b).....	19
Figure 2.7: Auditing the IT process, adapted from ITGI, 2000.....	21
Figure 2.8: ANAO's COBIT-based audit framework (Source ANAO, 2004)	24
Figure 3.1: Generic Maturity Model. Sourced from COBIT Management Guidelines (ISACA, 2000)	44
Figure 4.1: Frequency of Assigned Maturity Ratings by Audit Measure for PO1 Define a Strategic Information Technology Plan.....	62
Figure 4.2 Frequency of Assigned Maturity Ratings by Organisation for PO1 Define a Strategic Information Technology Plan.....	63
Figure 4.3: Frequency of Assigned Maturity Ratings by Audit Measure for DS12 Manage Facilities.....	69
Figure 4.4: Frequency of Assigned Maturity Levels by Organisation for DS12 Manage Facilities	69
Figure 4.5: Frequency of Assigned Maturity Levels for PO8 Ensure Compliance with External Requirements.....	76
Figure 4.6: Frequency of Assigned Maturity Levels by Audit Measure for PO8 Ensure Compliance with External Requirements.....	77
Figure 4.7: Comparison between Tasmanian, Australian and International Maturity Levels (source data, current research, and Liu (2003)	79

Chapter 1 - Introduction

1.1 Introduction

This chapter introduces and supports the research documented in this thesis, providing a background to the research problem before outlining the research objectives. It also looks at the significance of the research, and the contribution it makes. The chapter concludes with a brief outline of the structure of the thesis.

1.2 Background

This section looks at the background to the research. It gives an overview of the issues surrounding information technology governance, the Control Objectives for Information and Related Technologies (CobiT) framework and the general field of information technology audit.

1.2.1 Governance

Corporate governance has been a recent focus, because of the high profile corporate collapses of the early 2000s, including giants such as Enron and WorldCom in the United States of America, and HIH Insurance and OneTel in Australia. As part of that focus on corporate effectiveness, the governance of information technology (IT) within corporations has been subject to scrutiny.

1.2.1.1 The United States Response

Responses by governments to the collapse of such corporate giants varied. In the United States of America legislation was enacted in the form of the Sarbanes Oxley Act which prescribed the use of a corporate governance framework that must be followed by all corporations listed with the New York Stock Exchange. Many of the larger companies operating within Australia either offshore subsidiaries of American companies, or have American subsidiaries, and as such are indirectly exposed to the requirements of the Sarbanes Oxley Act.

The use of a governance framework is mandatory under the requirements of the Sarbanes Oxley Act; however, the legislation does not specify exactly which framework should be used. This is a decision made within each organisation. The framework

developed by the Committee of Sponsoring Organisations of the Treadway Commission (COSO) is often used to meet the requirements of the Sarbanes Oxley Act, but this framework does not specifically cover the use of IT.

1.2.1.2 The Australian Response

In Australia there is no requirement to use a framework to guide either corporate or information technology governance. The Australian government approached the collapse of HIH by instituting a Royal Commission, a high level enquiry headed by a leading judicial figure, to examine the circumstances surrounding the collapse. Justice Neville Owen delivered his report in April 2003, and was damning in his criticism of the information technology and systems employed by HIH and their deceptive approach to governance. The Australian Securities and Investments Commission has instituted legal action against many of the leading figures involved in the management of both HIH and OneTel, the other large company to collapse in Australia.

Despite the number of investors who lost significant amounts of money, there was no tightening of the regulatory requirements surrounding corporate or information technology governance. A voluntary best practice standard (AS8015 – 2005 Corporate Governance of Information and Communication Technology) has released by Standards Australia, and the Australian Stock Exchange Corporate Governance Council released its Principles of Good Corporate Governance and Best Practice Recommendations in March 2003, which are also only intended as a guide.

Within the public sector there are few restrictions on governance. Public sector organisations are largely funded by the taxpayer (or ratepayer in the case of local government) and answerable to the government of the day. Governance structures vary widely across the sector and are subject to change according to the wishes of the political masters. Stewardship of public monies is audited by the relevant public audit authority, some of which are also starting to audit governance, and more particularly the governance of information technology.

1.2.2 COBIT

There are numerous IT management frameworks available. Some, such as the Information Technology Infrastructure Library (ITIL) have a long history; however their focus is on the promotion of best practice rather than IT control. Control Objectives for Information and Related Technologies (COBIT), is widely used throughout the world for the examination of IT control and audit. COBIT is derived from many reputable sources, including the Committee of Sponsoring Organisations of the Treadway Commission (COSO), ITIL and Capability Maturity Model Integration (CMMI).

The framework is massive, consisting of thirty four high level control objectives grouped into 4 domains. Each high level control objectives is associated with between three and thirty detailed control objectives, producing a comprehensive framework of some three hundred and eighteen detailed control objectives.

The COBIT framework is increasingly being used to meet the requirements of the Sarbanes Oxley Act, particularly, as noted above, since it has been partly based on and mapped to the COSO framework. It is also being used in many other countries, including Australia. An increasing interest in the alignment of business and IT goals and processes has also contributed to the uptake of the COBIT framework. COBIT is increasingly being used to bring about better IT governance in organisations. IT auditors have also started to use COBIT to guide the IT audit procedure.

There is a large body of literature based around COBIT, as the framework is of particular interest to practitioners, who have been the source of much of this work. It must be noted that many publications about CobiT emanate from the Information Systems Audit and Control Association (ISACA) or the Information Technology Governance Institute (ITGI) the organisations that developed and distribute CobiT, or people closely linked to these organisations. However, there is lack of scholarly research into the framework to evaluate its effectiveness for IT governance or IT audit.

The COBIT framework is large. The Australian National Audit Office, which has IT specialists integrated into its audit teams (ANAO, 2000), does not use the framework in

its entirety for its IT audit program, preferring to use a customised program derived in part from COBIT.

1.3 Information Technology Audit

Whilst there are no regulatory requirements for IT governance measures to be in place in Australia as there are in some other nations, a growing number of private companies voluntarily undertake audits of their IT governance practices. These audits are conducted by the larger accounting firms, as well as IT consultancies. Within the Australian public sector the Australian National Audit Office (ANAO) and the Tasmanian Audit Office (TAO) were the first to use audit programs derived, at least in part, from the COBIT framework for undertaking IT audits (C. Buell, personal communication, 22 September, 2005).

The Tasmanian Audit Office (TAO) is the independent agency responsible for upholding public integrity within the state of Tasmania. Its primary function is to audit the financial statements of public sector organisations within the State. The TAO has expanded its audit scope to include IT audit and it currently employs one senior EDP auditor and an EDP audit cadet. Currently IT audits use a program devised by a private consultant and although interest has been expressed in using the COBIT framework, budgetary restraints of both time and money ensure that this is not feasible due to COBIT's size.

This section has reviewed the areas of corporate governance, the CobiT framework and the field of information technology audit. The research documented in this thesis is grounded in these areas. The research objective is outlined in the next section.

1.4 Research Objective

Because of the size of the framework and the limited time available to perform IT audits, there is a need for research to determine the most important IT processes from the COBIT framework in order to give guidance as to which areas IT audits should cover. The only prior research into the IT processes considered to be the most important comes from an international survey, which may not prove to be appropriate in the Tasmanian

public sector. Moreover, it was not specifically developed for the public sector, but for a range of industries.

1.5 Research Significance

The widespread use of the COBIT framework and the lack of rigorous research into its effectiveness should ensure that this research will be viewed as significant in a number of contexts. Given the use of COBIT internationally for both audit and governance this research should be of interest to practitioners in these fields. The lack of scholarly publications around the framework should ensure the interest of those engaged in research.

1.5.1 Researchers

There has been found to be a predominance of practitioner-based literature surrounding the CobiT framework (Ridley *et al*, 2004). Much of this emanates from ISACA and ITGI, as the custodians of COBIT, as well as people closely related to the development of the framework. In their conclusions Ridley *et al* indicate from the very few academically focused papers, they located only two focused on the COBIT framework, and they call for “rigorous research in the area” (p21) identifying it as having “considerable potential for future work” (p21).

This research will enable a comparison of the COBIT control objectives perceived to be the most important to be made against the international study of Guldentops *et al* (2002), and the national study by Liu & Ridley (2005). These studies both used the same ranking of control objectives compiled by an expert panel, rather than asking the organisations who subsequently assessed their maturity against control objectives on the list. An additional comparison with the control objectives identified by the self assessment project of the European Organisation of Supreme Audit Institutions (EUROSAI) IT Working Group will also be made. Making a comparison of control objectives identified by world experts, or national public sector audit organisations from Europe, to those identified by public sector managers in Tasmania will demonstrate the common concerns and potentially highlight any issues specific to the local industry.

1.5.2 Practitioners

As indicated in 1.5.1 above, much of the literature surrounding COBIT is of a practitioner-based nature and emanates from the source of the COBIT framework or people closely related to it. Ridley *et al* found that most of these publications detailed COBIT implementations. The comparatively large volume of practitioner-based COBIT literature suggests that practitioners are vitally interested in the framework. For the IT audit professional this research will give a unique insight into the IT processes considered to be important within the Tasmanian public sector.

1.6 Thesis Structure

1.6.1 Chapter 1 - Introduction

This chapter provides an overview of the research, providing a brief background and looking at issues directly relating to the research including objectives, significance and the research question, before giving an overview of the structure of the dissertation.

1.6.2 Chapter 2 - Literature Review

Chapter 2 reviews relevant literature giving a background on corporate governance, specifically Information Technology (IT) governance, the COBIT framework, including the existing body of literature about the framework, and the field of IT audit.

1.6.3 Chapter 3 - Methodology

Chapter 3 examines matters relating to the methodology by which this research was undertaken. It looks at the ethical considerations, the research aims, philosophical considerations, the research methods, the issues of reliability and validity as well as methods of analysis for data collected.

1.6.4 Chapter 4 - Results and Analysis

Chapter 4 explores the results of the research. The results from both phases of the study are presented, interpreted and discussed.

1.6.5 Chapter 5 - Conclusions

Chapter 5 presents and discusses the conclusions drawn from the research.

1.6.6 Appendices

The appendices contain material that adds richness to the content of the text of this dissertation, while not necessarily being directly important to the content.

Chapter 2 - Literature Review

2.1 Introduction

This chapter examines the existing body of literature with regard to the concepts that underpin the research project. The research draws on literature from both corporate and information technology governance, the COBIT framework and the growing field of information technology audit and so it is these areas that this review will cover.

2.2 Governance

With the increased focus on Corporate Governance, the use of information technology (IT) within organisations has come under closer scrutiny. IT is now considered to be pervasive in the current business environment (van Grembergen *et al*, 2004). It has been suggested (Epstein & Rejc, 2005) that IT decisions have been made on the basis of compelling arguments or keeping up with the competition rather than sound fiscal grounds and that the costs associated with technology and conversion to a new system are higher than projected while the benefits are lower and harder to achieve.

2.2.1 Corporate Governance and IT Governance

Corporate governance can be viewed as dealing with “the ways in which suppliers of finance assure themselves of getting a return on investment” (Schliefer & Vishny, 1997, p 737). Businesses are now so dependent on information technology that IT governance must be considered in tandem with corporate governance (van Grembergen *et al*, 2004). Information Technology is able to influence the strategic opportunities available to the business and provide critical input to the enterprise’s strategic plan. Through such a mechanism, IT governance allows the entity to fully leverage its information thus acting as a driver for enterprise governance.

The interdependence between enterprise or corporate governance and IT governance ensures that neither should be considered in itself to be a pure discipline (van Grembergen *et al* 2004). Several authors (Guldentops, 2003; ITGI, 2003; Peterson, 2003) have noted the requirement for IT governance to be included in the overall corporate governance structure of an entity.

Investors are willing to pay a premium for the shares of well governed companies (KPMG Belgium, 2005). While a definitive figure cannot be placed on such a premium it is an acknowledged fact that good governance does make a difference to corporate value.

2.2.2 What is Information Technology Governance?

“IT governance is a hot topic, though no one seems to be sure exactly what it is or how to explain it” (Broadbent, 2003, p1).

If corporate governance is the way in which investors are assured of a return on investment, then IT governance can be viewed in a similar manner. It can be viewed as the mechanisms and processes the board, executive and IT management ensure that IT strategy is formulated and implemented to ensure that both the business and IT functions are aligned. (ITGI, 2001; van Grembergen, 2002; Standards Australia, 2005).

The Tasmanian Audit Office (TAO) recognises the importance of linking both enterprise and IT governance in its decision to implement IT audits as a part of its routine procedures.

2.2.3 IT Governance

There has been a global focus on corporate governance, because the high profile corporate collapses of the early part of this decade. The collapse of Enron and WorldCom in the United States led to the introduction of the Sarbanes Oxley Act in that country, while in Australia both HIH and OneTel collapsed and Harris Scarfe required a radical restructuring of its ownership and massive changes to its way of conducting business. The statutory reaction in Australia was not as severe as that in the US where the Sarbanes Oxley Act was drafted and enacted to require oversight of corporate governance. The Australian approach was a series of best practice guidelines, which are not mandatory.

In Australia the Corporations Act underwent revision and a series of corporate governance standards were developed, (AS 8000 to AS 8004) dealing with corporate governance in 2003 and AS8015 dealing with corporate governance of Information and Communication Technology (ICT) in 2005. Further standards are being drafted to

encompass ICT projects and ICT operations. Additionally the Australian Stock Exchange formed the ASX Corporate Governance Council in 2002 with that body subsequently releasing its *Principles of Good Corporate Governance and Best Practice Recommendations* in March 2003. In his final report from the Royal Commission into the HIH collapse Justice Neville Owen found failures in governance and oversight structures at every level of the organisation along with failures in information management systems, which effectively resulted in decision makers being denied information. Justice Owen found that HIH was plagued with both management and IT problems; this was in spite of the company declaring in its annual reports that it had a corporate governance model (Owen, 2003).

Problems with corporate governance practices existed long before the corporate collapses of the early 2000s; the corporate excesses of the 1980s and resulting corporate collapses are probably the most recent. Peter Drucker (1989, p26) predicted the rise of corporate governance saying "... the governance of business ... is likely to become an issue throughout the developed world."

The annual spending for the Australian IT industry was estimated to be \$80 billion in 2002, worldwide at the same time the figure was estimated to be \$3 trillion (Lateline, 2002). With Boards of Management becoming increasingly aware of their fiduciary duties as highlighted by the corporate collapses mentioned previously, large capital expenditures can no longer be delegated to the IT department with the vague hopes that it will be utilised wisely and the company will benefit.

Some of the more important aspects of IT governance are the alignment of the goals of both the information technology and business functions (IT strategic alignment), the addition of value to a business through the use of IT (IT value delivery), the management of the risk associated with the IT function (risk management) and the measurement of performance against either industry benchmarks or projected targets (performance measurement). These aspects are now briefly examined in turn.

2.2.3.1 IT Strategic Alignment

One of the important aspects of IT governance is that of the alignment of the goals of both Information Technology and the business. IT strategic alignment is a complex and

multifaceted process that can be considered to be the means by which IT value is delivered (van Grembergen *et al*, 2004). One study (Burn & Szeto, 2000) indicated that only 50% of business managers and 60% of IT managers considered such alignment to be either successful or highly successful in their organisation. While total alignment may never be achieved it can be considered a worthy ambition as there exists a real concern about the value of IT investments (ITGI, 2003; Broadbent & Weill, 1998).

Aligning the goals of both IT and the business can lead to improved value delivery in the IT function as outlined in the following section.

2.2.3.2 IT Value Delivery

The addition of value to a business through the use of IT can be considered to be directly related to the alignment of IT and business goals and the way in which IT meets the expectations of the business (ITGI, 2003). The value derived from IT investments will be perceived differently by differing levels of the organisation, from users through to the various levels of management (Broadbent & Weill, 1998).

When creating business value, the organisation's appetite for risk must be considered. A brief outline of risk management is outlined in the next section.

2.2.3.3 Risk Management

In contrast to value delivery, where the focus is on creation of business value, risk management can be considered to be focused on the preservation of business value (van Grembergen *et al*, 2004). Risk management is driven by establishing accountability within the organisation (ITGI 2003). Essential to the management of risk is a sound understanding of the organisation's appetite for risk and its exposure to it. This then determines management's options in the management of risk by such means as mitigation, transfer and acceptance strategies (ITGI 2003).

When assessing organisational performance, the performance of the IT function can affect the overall business performance due to the large investment in IT infrastructure and operating costs in many organisations. The following section considers performance measurement.

2.2.3.4 Performance Measurement

Performance measurement is considered to be essential in the modern organisation. One such measurement system is through the use of Balanced Scorecards through which relationships and knowledge based assets are assessed, rather than the traditional accounting measures. Guldentops (2003) considers that IT should have its own scorecard and notes that a linkage between scorecards for both IT and the business as a whole is a strong method of alignment. An alternate method is that of assessing an organisation's "maturity" against a set of standards such as those in the Capability Maturity Model Integration (CMMI) or COBIT frameworks, both of which will be considered in sections 3 and 4 respectively.

The next section examines the statutory requirements for IT governance.

2.3 Statutory Requirements

Statutory requirements for IT governance vary between nations, according to the general approach to corporate governance. In Australia, the approach is more according to the spirit of legislation, whereas in the United States of America the letter of the law is applied.

2.3.1 Australia

There are no statutory requirements within Australia with regards to IT governance at the time of writing. Australian Standard AS 8015 Corporate Governance of Information and Communication Technology was released at the end of January 2005. However, the standard does not contain any mandatory elements and remains simply a pointer to best practice in the field. In terms of private organisations this means there is no requirement to follow any form of IT governance practices. As noted earlier, investors are willing to pay a premium for shares in well governed companies (KPMG Belgium, 2005) and this, along with a vague hope that companies will exercise good corporate citizenship, carries the field of IT governance forward in the private sector in Australia.

2.3.2 United States of America

Probably the most notable statutory requirements for IT governance are those in place in the United States of America. IT governance is covered by the Sarbanes Oxley Act

which regulates corporate governance as a whole in that country. The act requires the use of a framework within which corporate governance is administered. The framework used is not specified and while many organisations have opted for the framework from the Committee of Sponsoring Organisations of the Treadway Commission (COSO), this framework does not provide guidelines for the governance of information technology and thus other frameworks are also being adopted. One such framework is the Control Objectives for Information and Related Technologies (COBIT) focuses on the alignment of both IT and business strategy and function.

2.3.3 IT Frameworks

The most commonly mentioned frameworks in the practitioner literature are the Control Objectives for Information and Related Technologies (COBIT), the Information Technology Infrastructure Library (ITIL), the integrated Capability Maturity Model (CMMi), Six Sigma and the International Standards Organisation (ISO) Standards number 17799 and 9000 (Spafford, 2003; Anthes, 2004; Violino, 2005). The different frameworks have evolved to meet specific needs. ITIL was developed to implement best practice in IT service management. CMMi was originally designed as an aid to improving processes in software development. Six Sigma also focuses on process improvement, but from a statistical point of view. ISO 17799 is a detailed security standard establishing best practices, while ISO 9000 is one of three standards published by ISO guiding quality management systems. COBIT will be considered in detail in Section 2.4.

2.3.4 Summary

While IT governance is currently topical, it seems that it has many different meanings, with differences particularly obvious between academic, practitioner and statutory sources. It places the responsibility for the governance of IT squarely at the feet of the board, rather than in the hands of the IT department, as has been the case in the past in many organisations. It covers the drivers of strategic alignment and performance measurement and the outcomes of value delivery and risk mitigation. While this discussion of IT governance has focused predominantly on private companies, it could

be argued that it applies equally to public sector organisations as there is a move within some sectors to have greater accountability.

As indicated in Sections 2.3.2 and 2.3.2 above, COBIT is one of the frameworks within which organisations are aligning their IT and business governance.

2.4 COBIT

2.4.1 Introduction

The Control Objectives for Information and Related Technologies (COBIT) framework was developed in response to a perceived need for a framework for the internal control of IT governance. It was built upon best practice and has been maintained and upgraded to reflect the changes in such practices. The current version (version 3) is about to be superseded by a new version. COBIT documentation has been published in a number of forms to meet the needs of different members of an organisation. A broad overview is available in the form of the Executive Summary, while the more detailed Framework, Control Objectives, Implementation Tool Set offer an in depth guide to the IT practitioner suited to their level of need. The Management Guidelines are specifically designed for the executive management of the organisation offering a means to monitor organisational achievement against goals. All these documents are available for download from the Internet at no charge. Additionally, a set of Audit Guidelines is available. However, these are restricted to audit practitioner download only. Much of the literature published about COBIT can be traced back to the two organisations that are the custodians and distributors of the framework, the Information Systems Control and Audit Association (ISACA) or the Information Technology Governance Institute (ITGI); or to the people closely associated with these organisations.

2.4.2 The Framework

The conceptual framework of CobiT is complex. At the bottom of the framework are activities and tasks that can be grouped into processes which in turn are grouped to form domains. The official CobiT documentation represents it as depicted in Figure 2.1. The domains within the conceptual framework are given labels with which management

would be familiar: planning and organisation, acquisition and implementation, delivery and support and monitoring.

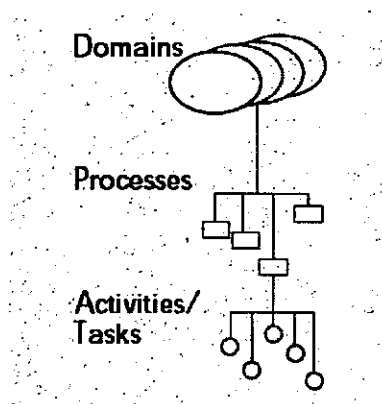


Figure 2.1 COBIT Conceptual framework (source ITGI, 2000a, p16)

The conceptual framework can be considered from three perspectives as depicted in Figure 2.2. From the information criteria perspective the important aspects are those of quality, fiduciary requirements (those of confidence or trust) and security. The information technology resource perspective emphasises people, application systems, technology, facilities and data. The third perspective is that of information technology processes encompasses the activities, processes and domains approach.

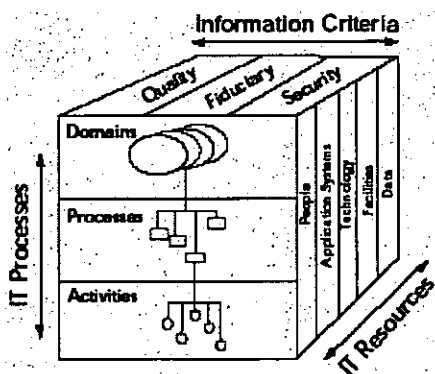


Figure 2.2: The COBIT cube (source: ITGI, 2000, p 16)

The conceptual framework outlines the broader perspectives of COBIT. IT processes are encapsulated by the control objectives.

2.4.3 The Control Objectives

2.4.3.1 High Level Control Objectives

The COBIT Framework (ITGI, 2000a) document details the thirty four high level control objectives within the four domains. The control objectives are defined in such a way as to be non-specific to the technical platform, but also recognising that some specialised technology environments will require different control objectives.

Each control objective is labelled as to its domain and assigned a number within that domain as well as a descriptive title (eg the first control objective in the Planning and Organisation domain is referred to as PO1 Define a Strategic Information Technology Plan). Control objectives are also related to the set of information criteria outlined in the Framework section above, with the relationship being classed as either primary or secondary. In addition, the control objectives are related to the IT resources (People, Applications, Technology, Facilities and Data) specified in the COBIT cube. Figure 2.3 illustrates these relationships.

DOMAIN	PROCESS	Information Criteria							IT Resources				
		effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	people	applications	technology	facilities	data
Planning & Organisation	PO1 Define a strategic IT plan	P	S						✓	✓	✓	✓	✓
	PO2 Define the information architecture	P	S	S	S					✓			✓
	PO3 Determine technological direction	P	S								✓	✓	
	PO4 Define the IT organisation and relationships	P	S						✓				
	PO5 Manage the IT investment	P	P					S	✓	✓	✓	✓	
	PO6 Communicate management aims and direction	P					S		✓				
	PO7 Manage human resources	P	P						✓				
	PO8 Ensure compliance with external requirements	P					P	S	✓	✓			✓
	PO9 Assess risks	P	S	P	P	P	S	S	✓	✓	✓	✓	✓
	PO10 Manage projects	P	P						✓	✓	✓	✓	✓
	PO11 Manage quality	P	P		P			S	✓	✓	✓	✓	✓
Acquisition & Implementation	A11 Identify automated solutions	P	S							✓	✓	✓	✓
	A12 Acquire and maintain application software	P	P		S		S	S		✓			
	A13 Acquire and maintain technology infrastructure	P	P		S						✓		
	A14 Develop and maintain procedures	P	P		S		S	S	✓	✓	✓	✓	
	A15 Install and accredit systems	P			S	S			✓	✓	✓	✓	✓
	A16 Manage changes	P	P		P	P		S	✓	✓	✓	✓	✓
Delivery & Support	DS1 Define and manage service levels	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS2 Manage third-party services	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS3 Manage performance and capacity	P	P			S				✓	✓	✓	
	DS4 Ensure continuous service	P	S			P			✓	✓	✓	✓	✓
	DS5 Ensure systems security			P	P	S	S	S	✓	✓	✓	✓	✓
	DS6 Identify and allocate costs		P					P	✓	✓	✓	✓	✓
	DS7 Educate and train users	P	S						✓				
	DS8 Assist and advise customers	P	P						✓	✓			
	DS9 Manage the configuration	P				S		S		✓	✓	✓	
	DS10 Manage problems and incidents	P	P			S			✓	✓	✓	✓	✓
	DS11 Manage data				P			P					✓
	DS12 Manage facilities				P	P					✓		
	DS13 Manage operations	P	P		S	S			✓	✓		✓	✓
Monitoring	M1 Monitor the processes	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	M2 Assess internal control adequacy	P	P	S	S	S	P	S	✓	✓	✓	✓	✓
	M3 Obtain independent assurance	P	P	S	S	S	P	S	✓	✓	✓	✓	✓
	M4 Provide for independent audit	P	P	S	S	S	P	S	✓	✓	✓	✓	✓

(P) primary (S) secondary (✓) applicable to

Figure 2.3: Relationship between control objectives and the three perspectives of the COBIT cube (Source ITGI, 2000a, p 20)

Each objective is documented according to template illustrated in Figure 2.4.

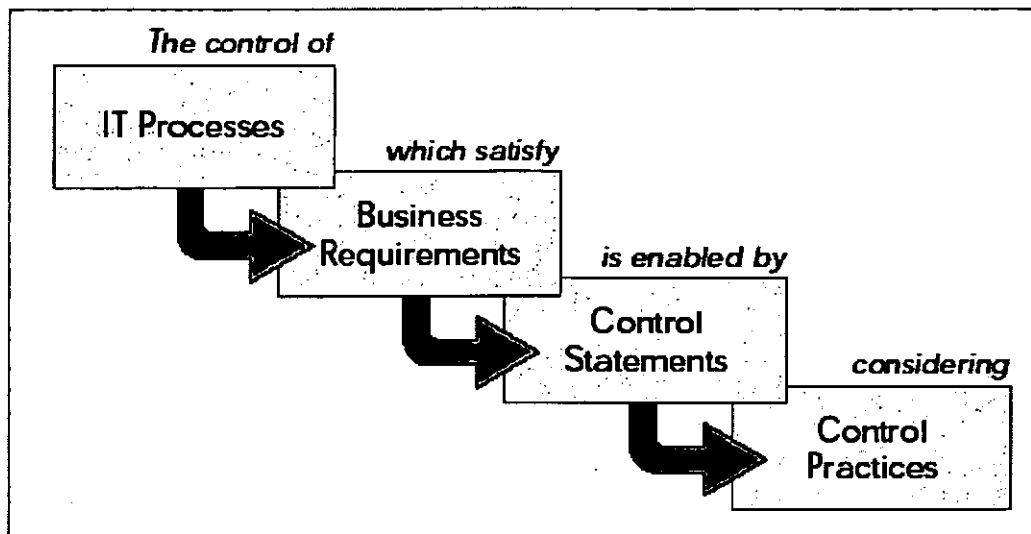


Figure 2.4: Template for presentation of high level control objectives (source: ITGI, 2000b p 21)

Using the first control objective (PO1 Define a Strategic Information Technology Plan) from the Planning and Organisation domain as an example, Figure 2.5 gives an illustration of such documentation.

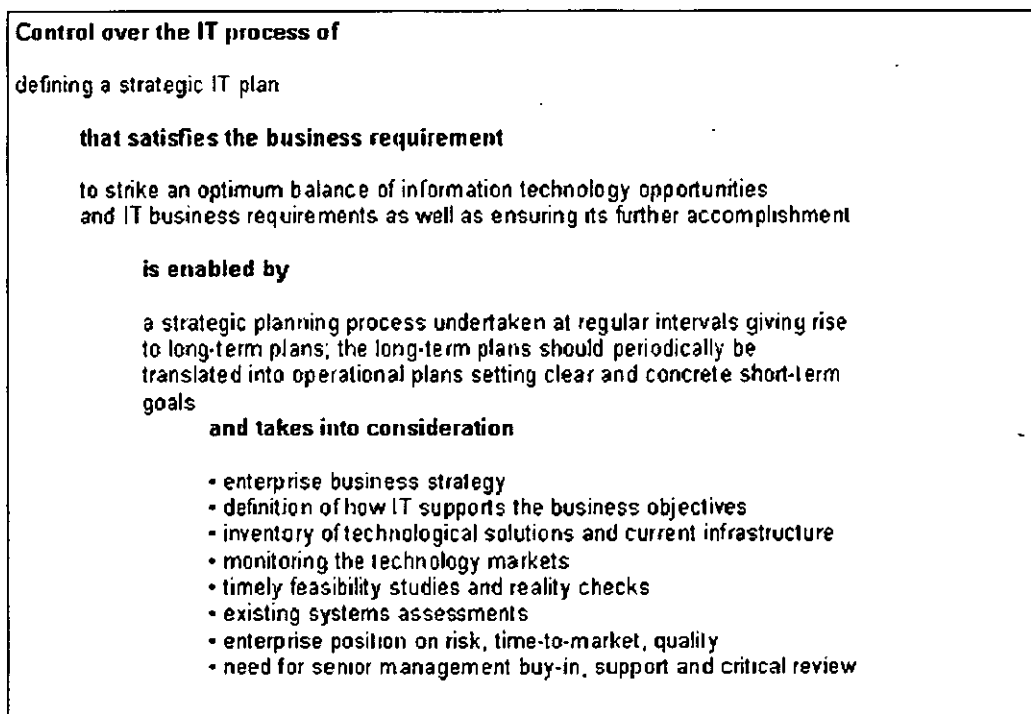


Figure 2.5: Example of COBIT control objective documentation (adapted from ITGI, 2000b)

Additionally each high level control objective is associated with at least three more detailed control objectives.

2.4.3.2 Detailed Control Objectives

While the section above details the thirty four high level control objectives, there exists a further, more detailed set of control objectives associated with each of the IT processes. Each high level control objective is related to between three and thirty detailed control objectives, producing a total of three hundred and eighteen detailed objectives.

The detailed control objectives are drawn from forty one primary sources of both legislated and non legislated international standards and regulations (see Appendix A). The individual control objectives are statements of desired results or purposes to be achieved through their implementation within an IT activity thus providing both policy and best practice for IT control (ITGI, 2000b).

An illustration of a single detailed control objective from the high level control objective PO1 – define a strategic Information Technology Plan is illustrated in Figure 2.6. This is only one of eight detailed control objectives for this high level objective.

Detailed Control Objectives

1 Define a Strategic Information Technology Plan

1.1 IT as Part of the Organisation's Long- and Short-Range Plan

Control Objective

Senior management is responsible for developing and implementing long- and short-range plans that fulfil the organisation's mission and goals. In this respect, senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organisation's long- and short-range plans. IT long- and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the organisation.

Figure 2.6: Detailed Control Objective (adapted from ITGI, 2000b)

It can be seen from the above discussion that the CobiT framework is both long and complex. In order to make the framework more accessible and understandable to managers, a set of management guidelines are provided.

2.4.4 The Management Guidelines

Within COBIT there exists a series of measures by which management can measure the performance of their organisation against the COBIT control objectives. Some of these

measures are not integral to this research project and as such will not be covered in great detail in this review. Specifically the measures that are not considered in this overview are: Critical Success Factors (CSF), Key Goal Indicators (KGI) and Key Performance Indicators (KPI).

2.4.4.1 Maturity Models

The maturity models are a means of scoring the organisation's performance on a Likert-type scale with six potential values ranging from 0 (non-existent) to 5 (optimised). Specific maturity models are available for each individual high level control objective for the framework. These are derived from a generic model which is discussed in more detail in Section 3.7.3.

In addition to the internal or self assessment tools provided by the Management Guidelines, CobiT also produces a set of audit guidelines.

2.4.5 The Audit Guidelines

The final product in the COBIT suite is a set of audit guidelines. These guidelines are not as freely available as the remainder of the COBIT documentation as they are restricted to audit professionals only. These guidelines provide the IT audit professional with a framework within which to conduct audits. The guidelines outline the audit of the IT process are depicted in Figure 2.7.

These guidelines are supplemented by a set of standards, procedures and additional guidelines as well as a code of ethics and IS control professionals standards, the latter forming the basis for the classification of such audit practitioners as a profession. ISACA also run a certification program for audit professionals awarding those successfully fulfilling the requirements a designation of Certified Information Systems Auditor or CISA.

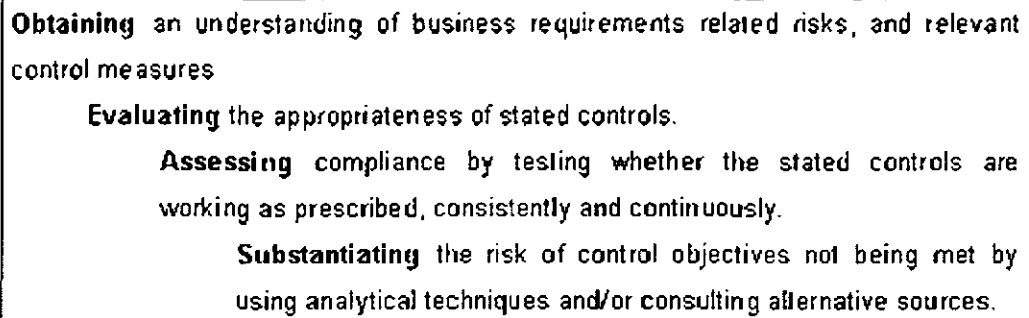


Figure 2.7: Auditing the IT process, adapted from ITGI, 2000

Having examined the various components of the COBIT framework and outlining some of the alternative frameworks, the existing body of research that surrounds the COBIT framework is discussed in the next section.

2.4.6 Prior Research on COBIT

Much of the vast quantity of literature available about the COBIT framework has been produced by practitioners, for practitioners (Ridley *et al*, 2004). While this in itself is not necessarily a problem it indicates a potential gap in the academic literature, but Ridley *et al* (2004) suggest that such a widely adopted framework should be the subject of more rigorous research and state there is “considerable potential for future work” (p21). Liu & Ridley (2005) assert that the widespread international adoption of COBIT in both the public and private sectors is illustrative of its acceptance and credibility. Sallé (2004) goes even further suggesting that COBIT is becoming a de facto standard for IT governance.

One international study particularly of note in this research (Guldentops, *et al*, 2002) examined the high level control objectives perceived by a panel of senior IT experts as being most important, and then had organisations assess their performance against these in the form of maturity scales. The high level control objectives identified by the expert panel are detailed in Table 2.1 below. The same list of control objectives was used by Liu & Ridley (2005) to examine the self-assessed maturity of Australian public sector organisations. While the list has been examined in the broader Australian context, it was drawn up for research published in 2002, given the pace of change in the IT sector, such a list may well no longer be relevant.

Table 2.1: COBIT control objectives identified by Guldentops *et al* (2002)

COBIT Control Objective
PO1 Define a Strategic Information Technology Plan
PO3 Determine Technological Direction
PO5 Manage the IT Investment
PO10 Manage Projects
AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI5 Install and Accredited Systems
AI6 Manage Changes
DS1 Define and Manage Service Levels
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS10 Manage Problems and Incidents
M1 Monitor the Processes

2.4.7 Summary

While not being the only IT framework available, COBIT is certainly one of the most comprehensive and widely used frameworks available to examine the IT governance of an organisation. It has the added advantage of having a formal set of IT audit guidelines and a certification course for auditors using the framework in the conduct of such audits. Despite its use in many countries throughout the world, including Australia, there is a lack of published scholarly research around the effectiveness of the COBIT framework.

The broader field of information technology audit, with a specific focus on public sector organisations will now be examined.

2.5 Information Technology Audit

2.5.1 Introduction

The corporate governance of Australian corporate entities is regulated by the Corporations Act (2001). Auditing of financial statements is one way in which

corporate governance is assessed. In the public sector financial audit is also used to introduce accountability for public money. Given that there is a large capital investment in IT infrastructure and an even larger operating expenditure associated with information and communications technologies (ICT) in the Australian public sector (see Section 2.5.2), the public also need assurance that this investment is sound.

The upcoming sections examine the audit of IT governance in the Australian public sector both at a national level through the Australian National Audit Office and at a state level through the Tasmanian Audit Office. The use of the COBIT framework in a self assessment project for European audit institutions will also be examined.

2.5.2 ANAO

The Australian National Audit Office is the independent audit authority of the Australian Federal Government. It provides audit services to the Federal Parliament and to Commonwealth public sector agencies and statutory bodies. The ANAO claim some 300 government bodies as clients including agencies that deliver core services and are dependent on the Federal Government for funding through the annual budget, and also commercially oriented entities (ANAO, 2000). The ANAO allow approximately 400 hours per audit performed. This figure encompasses time spent auditing both financial statements as well as Information Technology systems controls (C Buell, personal communication, 17/03/2005).

The Australian Government spent an estimated 3.11 billion dollars on ICT operating expenditure and an additional 1.10 billion dollars on ICT capital expenditure in 2002 – 2003. This was an increase of approximately 52% on the 1999 – 2000 figures (ANAO, 2005). With such massive expenditure it is essential that the public is assured that the expenditure is both prudent and beneficial. In the year ending 30 June 2005 the ANAO performed COBIT type audits on five entities: the Australian Taxation Office; Centrelink; Department of Health and Ageing; Department of Veterans' Affairs; and the Health Insurance Commission (ANAO, 2005), with a focus on financial management information systems, specifically SAP.

The ANAO's IT systems controls audit framework, shown in Figure 2.8, is derived in part from the COBIT maturity model. The ANAO recognise that implementing COBIT

in full raises issues of relevance, time and cost, and prefer to audit only those controls critical to the business of the organisation being audited (ANAO, 2002). It is not clear exactly how the ANAO derived their framework.

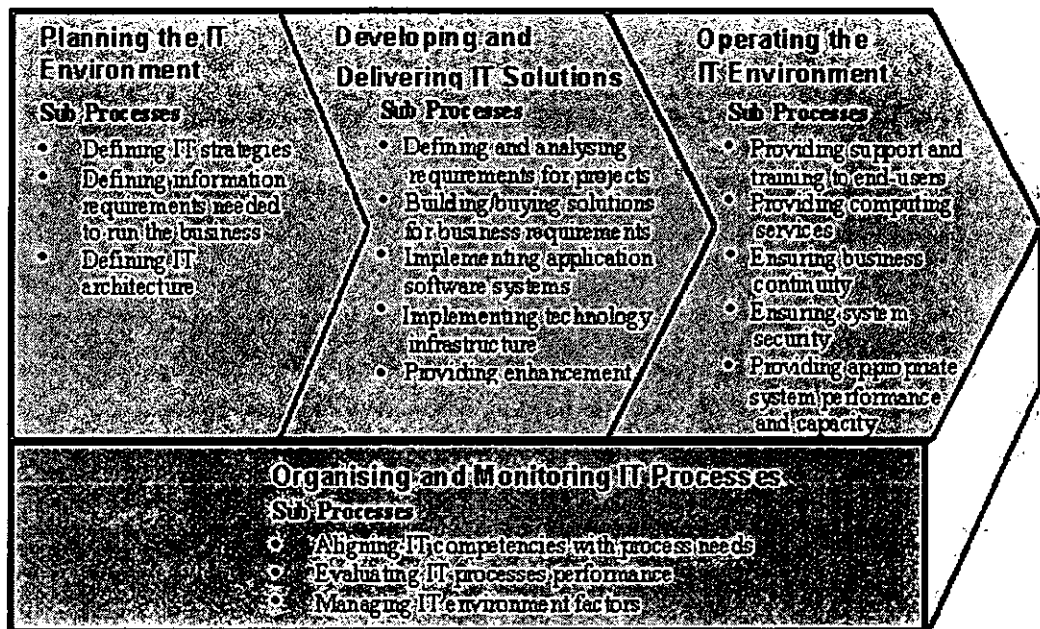


Figure 2.8: ANAO's COBIT-based audit framework (Source ANAO, 2004)

The General Controls Review audit program document for Operating the IT Environment is one example of the way in which the ANAO have based their audit program around CobIT. This document lists ten unique control objectives (not based on COBIT) which have an associate 35 controls or control activities and 167 individual program steps. The ANAO control objectives are related within the program matrix to 68 of the COBIT detailed control objectives.

The ANAO framework uses six potential levels of maturity, based on those from the COBIT framework. The ANAO specify a minimum baseline category at which it is considered that suitable IT governance practices are in place, although there are certain exceptions to the case (ANAO, 2004). It is important to note that as the only systems assessed are those related to financial statement audits undertaken by the ANAO (ANAO, 2004), potentially only a small proportion of the information systems within the agencies are being assessed.

2.5.3 Tasmanian Audit Office

The Tasmanian Audit Office (TAO) is the independent authority charged with upholding public integrity within Tasmania (TAO, 2004). Audits performed by the TAO embrace three major areas, Financial Audit, Regularity Audit and Performance Audit. The IT Audit section falls under the management of Financial Audit Services. The TAO typically allows approximately between twenty and sixty hours per audit, for all aspects of audit. Usually the majority of the allotted time is required to perform the financial audit requirements (C Buell, personal communication, 17/03/2005).

The IT audit section is headed by the most senior external IT auditor in the Tasmanian public sector who holds bachelors degrees in Commerce and Information Systems (with honours) as well as professional qualifications in accounting (CPA) and information systems audit (CISA). She has five years experience in the role. IT audits are currently undertaken according to an audit program devised by an external consultant. This program focuses entirely on the IT function without considering the way in which it integrates with the overall business of the organisation being audited. In addition to conducting IT audits, the senior IT auditor is also expected to undertake financial audit work.

Given the time constraints within which the TAO is forced to operate, it is impossible to implement an audit framework the size of COBIT, particularly in its entirety. The TAO is very keen to employ an abbreviated version of CobiT, particularly with the section of its clientele that is categorised as either key or large clients. Such a designation for clients is made according to the size of their “financials” (or budget) and their political importance. Thus it is possible for an agency that operates on a small budget but is considered to be politically important to be considered a key client by the TAO.

COBIT’s monitoring domain is considered by the Tasmanian Audit Office (TAO) to be one of the most important (C. Buell, personal communication, 21/9/2005) and figures prominently in the results of the European Organisation of Supreme Audit Institutions (EUROSAI, 2005).

2.5.4 EUROSAI Self Assessment Project

The European Organisation of Supreme Audit Institutions is the peak body comprising 45 “External Control Institutions” from the European continent. It is a regional group of the International Organisation of Supreme Audit Institutions (INTOSAI) which groups the Supreme Audit Institutions (SAIs) of 183 countries and acts as an advisory body to the United Nations (EUROSAI, undated).

EUROSAI has an associated IT Working Group. This group has undertaken a project to design a self-assessment tool for SAIs based on the COBIT framework. Individual self assessments are carried out as workshops to determine the 10 to 15 key business processes in achieving the goals of the SAI, the importance of IT support for such processes, the quality of the present IT support and the maturity level of the IT processes seen by the IT department to be the most important. Workshops are undertaken with an independent moderator and vary in length from one to one and a half days (EUROSAI IT Working Group, undated a). Up to February 14, 2005, 12 self assessments were performed and the framework has been updated to a new version to integrate these pilot assessments (EUROSAI IT working group, 2005).

The questionnaire structure used to elicit the perceived importance in the EUROSAI project was the basis for the rating system used in the questionnaire in this research.

2.5.5 Summary

Information Technology Audit is a field still in its infancy through much of the developed world. The COBIT framework is potentially of great benefit since it has a focus on aligning the business and IT goals and processes of an organisation. Additionally it can provide an entire framework for use or a base from which to derive an abbreviated framework if constraints prevent the application of COBIT in its entirety. The focus within COBIT on the alignment of is also seen as desirable by many practitioners.

2.6 Summary

This chapter has examined the available literature in relation to Information Technology Governance, COBIT and other IT frameworks and Information Technology Audit to

provide a background from which to develop the research project. The next chapter will address methodological considerations.

2.7 The Research Question

Which of the high level control objectives from the COBIT framework do Tasmanian public sector organisations perceive to be the most important? How feasible is it to use COBIT to conduct IT audits in Tasmanian public sector organisations?

Chapter 3 - Methodology

3.1 Introduction

This chapter deals with the following issues as they relate to the research project: philosophical stance, ethics, research aims, research methods and, reliability and validity.

3.2 Ethics

Prior to the commencement of the research it was necessary to obtain approval from the Human Research Ethics Committee (Tasmania). The letter of approval from the Human Research Ethics Committee (Tasmania) is located in Appendix B. Appendices C and D are the Information Sheets for Phases One and Two respectively and Appendix E contains the informed consent pro forma.

3.3 Research Aims

There are two major aims of this study.

3.3.1 Aim 1

Determine the control objectives from the COBIT framework that are perceived by selected Tasmanian Audit Office clients to be the most important. This was done in part to reduce the overall number of areas to be audited. The COBIT framework is so large that it is impractical to conduct a single audit that covers all the areas it prescribes. This aim also builds on work done in an international study by Guldentops *et al*, 2002 by examining the control objectives considered to be important in the context of the Tasmanian public sector.

3.3.2 Aim 2

The second aim was, through using the list of IT processes collectively regarded by the TAO clients to be the most important, to derive an abbreviated instrument from the COBIT framework. This instrument was subsequently to be trialled and evaluated on key and large clients of the TAO. Maturity ratings will be assigned from a generic

maturity model sourced from the COBIT framework. These maturity levels were then compared with those obtained by Guldentops *et al* (2002) and Liu & Ridley (2005).

3.4 Research Philosophy

There are two elements to a research philosophy, ontology and epistemology.

3.4.1 Ontology

The Oxford English Dictionary online defines ontology as the “science or study of being.” It is concerned with the way in which the researcher assumes the physical and social world operates (Avison & Fitzgerald, 1995; p 420). The two most common ontological stances used in Information Systems research are those of objectivism and subjectivism.

3.4.1.1 Objectivism

Objective research ontology assumes that the empirical world (or reality) is independent of the researcher (Orlikowski & Baroudi, 1991). The objective researcher assumes there is only one reality, and that can be measured and described in an accurate manner. In undertaking research under this stance the researcher places themselves outside of the phenomenon being studied and claims to have no impact on that which is being studied.

3.4.1.2 Subjectivism

Subjectivism assumes that the world exists only through human experience (Orlikowski & Baroudi, 1991). A subjective researcher interprets meaning in the interactions between people. This stance acknowledges that there are many versions of reality that are dependent on both people and context. The subjective researcher acknowledges that their very presence in the field of research changes the reality being experienced and as such will affect the outcome of the research itself.

Given that audit is a sub-field of accounting, a discipline that has its roots in the “mathematical science of values” (Office, 1887, p 103) and as such does not lend itself well to examination under a subjective stance, it was considered appropriate to conduct this research under an objective ontology.

Ontology and epistemology are closely linked. The selection of an objective ontology then influences the selection of an epistemology.

3.4.2 Epistemology

Epistemology is defined in the online version of the Oxford English Dictionary as “the theory or science of the method or grounds of knowledge.” It is concerned with the nature of the relationship between the researcher and the world (Guba, 1990; p 18) or the way in which the researcher knows things (Hirschheim, 1992; Trochim 1999). There are three major epistemological stances adopted within Information Systems research: positivism, interpretivism (Orlikowski & Baroudi, 1991) and critical social science (Ridley & Keen 1998).

Epistemologically, positivism is founded in the empirical examination of theories, usually requiring such theories to be either verified or falsified. Primarily, positivist researchers use a deductive approach and seek to discover causal relationships that can be generalised (Orlikowski & Baroudi, 1991).

3.4.2.1 Audit and accounting

Chua (1986, p 606) indicates that research in “mainstream accounting” adopts a belief in physical realism in which an objective reality exists independent of the researcher and that reality has a limited or distinct nature that is essentially knowable. Realism, according to Chua, is linked to the relationship between subject and object, in that the object (world) is presumed independent of the subject (researcher) and that knowledge is achieved when the researcher correctly reflects and “discovers” the objective reality.

Accounting and auditing research utilises a view in which there is a world of observation that is separate from the world of theory, and that the world of observation can be used to attest to the scientific validity of the world of theory, a view closely aligned with positivism (Chua, 1986). There is a perception within the accounting profession that numbers (quantitative measures) are more precise and “scientific” than qualitative evidence and even among those who are aware that numbers may be imprecise, the public debate is organised around the numbers, as it is perceived to be the “proper arena for discussion” (Chua, 1986, p 617/18). While interpretivism remains

unpopular as an epistemology in accounting, critical studies are becoming more popular (Lodh & Gaffikin, 1997).

The choice of a positivist epistemology for this research project can only be supported by the dominant use of positivist epistemology in the literature body for accounting, particularly that of auditing.

3.4.3 Research Philosophy Used

The research philosophy of a study is the underlying belief system adopted by the researcher in the course of the particular study at hand.

This study utilised an objective ontology, a positivist epistemology and quantitative methods. This stance was adopted for a number of reasons. The majority of literature and research currently available within the IT governance/audit field is practitioner based, positivist in nature and utilises quantitative methods; in order to be well accepted and relevant to those in the field, it is desirable use a similar philosophy. The Tasmanian Audit Office (TAO) has expressed an interest in utilising the framework derived in the first phase of the study as a basis for IT audits in the public sector in Tasmania; for reasons elaborated above the TAO practices under a predominantly objective, positivist philosophy. The development and use of an instrument under the same philosophy adds to the credibility of the findings.

The underlying research philosophy then largely dictates the research methods employed.

3.5 Research Methods

This section will outline the methods applied by the researcher in the context of this study. Cooper & Schindler (2003) indicated there are two major methods of gathering primary data; the first is observation, the second communication. This study will utilise both methods; communication (via survey) in Phase One and observation (via audit) in Phase Two.

3.5.1 Phase 1

This phase of the study consisted of the development and administration of a survey instrument to the target participants.

3.5.1.1 Survey

Surveys are used to gather information from individuals using a formally designed list of questions, commonly called a questionnaire. Ticehurst and Veal (2000) indicate it to be arguably the most commonly used technique in management research and it is ideal to provide quantified information. The use of a questionnaire provides transparency in how the data has been collected and analysed; it provides the potential for others to re-analyse the same data, extend the research or provide an alternative interpretation. Additionally surveys are useful in collating a diverse range of complex information. Questionnaires are commonly applied to only a proportion (sample) of the population to be studied. The findings from a properly derived sample can be subsequently generalised to the whole population. This research surveyed the total population of 30 organisations and achieved a response rate of over 83%. Consequently, the findings are considered to be representative of the entire population (Baruch, 1999).

3.5.1.2 Survey Scope

This survey encompassed the current key and large clients of the Tasmanian Audit Office (TAO). The TAO assigns client status through a consideration of the size of the organisation's budget (its "financials") and its perceived political importance. The inclusion of political importance means that organisations that are physically small in terms of numbers and required funding, may still be considered to be important.

3.5.1.3 Survey Instrument

Brief details about organisational type, participant's role title and a ranking of familiarity with both organisational and IT goals on a five point Likert-type scale were sought. The main section of the survey instrument asked participants to rate the 34 high level control objectives from the COBIT framework according to their importance to their agency on a Likert-type scale. Permission to use the text of the COBIT Control Objectives is located in Appendix F. This scale was derived from the European

Organisation of Supreme Audit Institutions (EUROSAI) IT working group's Self Assessment project which uses a five point Likert-type scale with a sixth point offset to the left of the main scale for indication that the respondent was not sure. The main scale boxes were labelled from 1 to 5 and the sixth box labelled "N," a key indicating the exact rating for each box was located at the top of each page. The questionnaire was distributed with a reference guide that contained the full text of each of the 34 high level control objectives. A copy of the questionnaire is located in Appendix G and the reference guide in Appendix H.

3.5.1.4 Pilot testing

A pilot test of the questionnaire was administered to managers in 5 organisations within the Tasmanian public sector that were not designated by the TAO as either key or large. These organisations were contacted through the TAO, who forwarded the questionnaires and reply paid envelopes (for return of the questionnaires) on behalf of the researcher. The questionnaires were directed to IT managers or senior business managers with the primary responsibility for IT. The use of organisations outside of the target population preserved that small population to be surveyed for the main survey. Pilot surveys are an important aid in testing various aspects of the questionnaire including wording, sequencing, layout and analysis techniques, as well as estimating completion times (Ticehurst & Veal, 2000)

3.5.1.5 Questionnaire distribution

The Human Research Ethics Committee (Tasmania) requires that a third party may not supply a list of potential subjects for research; rather the researcher may request the third party to distribute questionnaires on their behalf. These organisations were contacted through the TAO, who forwarded the questionnaires and reply paid envelopes (for return of the questionnaires) on behalf of the researcher. The questionnaires were again directed to IT managers or senior business managers with the primary responsibility for IT.

3.5.1.6 Follow up

Questionnaires, due to their nature, often do not return particularly good response rates. It was anticipated that the co-operation of the TAO would improve the response rate in

this case. The TAO also followed up with the organisations on behalf of the researcher to encourage non-respondents to participate.

3.5.1.7 Hypothesis Testing

In quantitative research it is usual to form hypotheses to postulate the relationships between variables and subsequently test the validity of such relationships. Hypothesis formation is generally grounded in the existing literature or on the basis of informal observation. In this case there was not a significant body of research to draw on for hypothesis formation. The audit phase of the study may be considered to be a series of case studies in the effective application of the derived instrument, in which case the development of hypotheses is not appropriate. Given the exploratory nature of Phase One, the case-study nature of Phase Two and the dearth of existing academic literature in which to ground hypothesis formation, hypothesis testing was not done.

3.5.2 Phase 2

The second phase of the study involved the derivation, from the ranked listing of control objectives, obtained from the first phase of the study, of an abbreviated instrument from the COBIT framework and subsequent trial of the instrument with key and large clients of the TAO.

3.5.2.1 Audit

Auditing is a process whereby the practitioner seeks evidences to confirm claims made by an organisation. In the auditing of financial statements such claims are about the financial status of the company. In IT audit using the COBIT framework, the organisation makes claims about the way in which both high level and detailed control objectives are met. The auditor finds such evidence through the examination of documents, and interviews with key personnel amongst other processes.

3.5.2.2 Maturity Levels

Maturity levels are assessed in much the same way as an audit, in that evidences are sought to assess the level of compliance with the individual high level control objective. The exact method is outlined in the COBIT Management Guidelines (ITGI, 2000c). Levels are assessed from 0 (non existent) to 5 (optimised). A more detailed discussion

of maturity levels can be found in Section 2.4.4.1. The process used to assign maturity levels in the audit phase of this research varied from the self assessment usually associated with the COBIT model and is outlined in Section 3.7.3.

3.5.2.3 Scope

The high level control objectives from the COBIT framework are composed of a series of detailed control objectives, with each high level control objective having links with between three to thirty detailed control objectives (ITGI, 2000). The number and nature of the control objectives perceived by the participating agencies as the most important then dictated the size of the abbreviated instrument and consequently the time to complete an audit using such an instrument. It was not possible to audit all agencies that were involved in the first phase of the study as time was a constraining factor.

3.6 Reliability and Validity

Reliability and validity are two of the most important aspects underpinning any research. In terms of this research there are two aspects of validity to be considered, that of the overall validity of the research, and the validity of the survey. More importance is placed on the issues of reliability and validity in the first phase of the study as the use of the control objectives in the second phase of the study is, in itself, an aid to ensuring reliability.

3.6.1 Reliability

Reliability is generally concerned with repeatability of results (Ticehurst & Veal, 2000). In order to be considered to be reliable it is necessary to obtain similar results if the study were to be repeated at a different point in time, or with a different sample group. Conducting a pilot survey (see Section 3.5.1.4 above) will aid in the assessment of reliability in the case of this study. The results of the pilot study were considered to reinforce the reliability of the survey instrument (Neuman, 2000).

3.6.2 Validity

Validity is mainly concerned with the accuracy of the means of measurement, and whether the researcher is actually measuring that which they intended to measure (Winter, 2000).

Data gathering by survey poses a unique set of threats to validity. It is possible that respondents may have answered in a way in which they felt they should, rather than indicating the situation as it really was. For example, an IT manager may have drawn his ratings of the control objectives from his agency's written policies and procedures rather than indicating the actual focus and emphasis placed by his department. Ticehurst and Veal (2000) indicate that there is evidence that even factual survey data must be treated with caution. They indicate that the best forms of protection against potential threats to questionnaire validity are careful attention to both the research process and questionnaire design and the conduct of a pilot survey.

3.6.2.1 Validity of the study

Threats to validity fall into two main categories, internal and external.

Internal validity

Internal validity is concerned with the possibility that changes in the dependent variable can be attributed solely to manipulation of the independent variable and not a different variable. Studies with high internal validity meet this requirement. Studies with low internal validity do not meet such a requirement (Ticehurst & Veal, 2000).

There are several threats to in the internal validity of a research project; these include history, maturation, testing, instrumentation, selection, and experimental mortality. History, maturation and mortality were not a threat in this instance as the duration of the study was less than one month; additionally the involvement of the TAO also helped limit the effects of experimental mortality. Testing was not seen as a threat to internal validity as the pilot survey was administered to a different set of organisations than those who participated in the main study. The use of a single researcher in the second phase of the study addressed some instrumentation threats, which are generally due to inconsistency or unreliability in measuring instruments or observation procedures. The potential of selection issues to affect internal validity was covered by selecting the entire population of key and large clients of the TAO to participate in the study.

External validity

The degree to which the results of a study can be generalised to other settings and situations is its external validity. Usually, in quantitative studies, the researcher is seeking to be able to generalise their findings to other groups, other geographical locations or at a later point in time (Ticehurst & Veal, 2000). However, in this study the researcher is examining a discrete population, the key and large client base of the TAO, and generalisability is not being sought.

Threats to external validity include the reactive effects of: testing, selection and experiment setting. The reactive effects of testing are due to repeated exposure of subjects to the content of the testing instrument. There was no repeated exposure to the questionnaire, thus this was not considered to be an issue. The effects of selection are concerned with the ability to generalise results drawn from a sample to an entire population. In this study the entire population was surveyed, thus eliminating the effect of selection on external validity. It is difficult to control the reactive effects of experiment setting. It was possible that participants in the survey responded in a way in which they thought the researcher wanted them to, an action that would be hard to replicate in the second phase of the study where documents and other audit evidence either existed or did not.

While the questions of philosophy and research methods are important, the way in which the data are to be analysed is equally important since incorrect analysis can affect the research findings.

3.7 Analysis of Data

3.7.1 Phase 1

Data collected in Phase One of the study included a series of ratings on a Likert-type scale and so was quantitative in nature. Before statistical testing began it was essential to consider the issue of non-response bias.

3.7.1.1 The issue of non-response bias

Non response bias is introduced to a survey when the responses of participants differ in a consistent manner from those of non participants. This study had the assistance of the TAO and as such enjoyed a good response rate. It was considered that with a response rate of 83% and only 8%, or two, of those being late responses it was not necessary to consider non-response bias (Bergk *et al*, 2005).

3.7.1.2 Determination of a ranked list

The questionnaire was divided into two sections. The first section contained the demographic data. This was entered into a Microsoft Excel spreadsheet. The organisational type and position title information was summarised into percentages, while the familiarity with business and IT goals information was processed to produce a mean figure for both questions. The second section required the participants to rate the importance of the 34 high level control objectives from the COBIT framework to their organisation on a Likert-type scale. The codes of the high level control objectives (eg DS5) were entered into a Microsoft Excel spreadsheet and the ratings were entered as responses were received. The ratings were summed to give a total for each high level control objective; the data were then sorted in descending order on the basis of these totals. Any control objectives with the same totals were subjected to a second sort on control objective code into simple alphabetical order.

The totals were then subjected to statistical testing to determine points at which significant differences existed. The results of the t-tests performed are found in Appendix I. The repetitive use of a statistical test can lead to the introduction of an increased level of error (University of New England School of Psychology, 2000). To minimise the effect of this, a Bonferroni adjustment should be used.

3.7.2 Phase 2

Phase Two of this project was the development, trial and subsequent evaluation of the abbreviated COBIT instrument in audits among key and large clients of the TAO. The COBIT Audit Guidelines contain a comprehensive listing of the audit measures required to fully audit the IT control of an organisation. To conduct a comprehensive audit of all the high level control objectives on the abbreviated list derived in Phase One using all

the measures would take many days of interviews and investigations, so it was necessary to select only those considered to be the most essential and applicable. The abbreviated list contained three tiers of control objectives, with the first tier containing only DS5 Ensure Systems Security. Given that one control objective was insufficient for the audit program and seventeen was too many, two tiers of control objectives were used, numbering seven high level control objectives in all.

3.7.2.1 Justification of Choice of Audit Measures

The listing of possible audit measures for the trial instrument, comprising seven control objectives, was at least 180 individual measures. The list of possible audit measures for each control objective was drawn from three sources. The first source was the General Controls Review (ANAO, 2004), a document from the ANAO listing all the audit measures to be investigated while auditing operations in the IT environment (the audit program). The second source document was a TAO document provided by the Senior EDP auditor. The third source was the COBIT Audit Guidelines (ITGI, 2000), which were used when there were insufficient measures obtained from the first two sources.

The use of the three sources provided a comprehensive listing of audit measures for most high level control objectives. Given that the aim of the Phase Two was to trial the abbreviated instrument in as many organisations as possible, while still providing meaningful results, it was decided to limit the number of audit measures to a number that could be reasonably examined in an interview of approximately two hours duration. The three sources provided more audit measures than could be audited in such an interview, and so it was necessary to eliminate some measures in order to obtain a suitably sized listing. This was done in two ways: by looking for points of similarity that would indicate a measure should be included in the final listing, and secondly by applying exclusion criteria. The means of inclusion and exclusion are described in Sections 3.7.2.1.1 to 3.7.2.1.2 below.

3.7.2.1.1 Inclusions by agreement between sources

The list for each control objective was examined for points of agreement between items appearing in the listings of both the ANAO and the TAO, where there were measures available from both sources. Agreement between the two audit offices was considered

to be confirmation of the importance of a measure and on this basis the measures were included. An example of inclusion by agreement was the inclusion of the use, granting, modification, removal, control and review of remote access in the measures relating to DS5 Ensure Systems security, which appeared in both sources.

The inclusion of measures on the basis of agreement between audit offices did not include sufficient measures in the final listings to enable a realistic audit opinion to be formed. A meaningful audit opinion requires more than a cursory investigation of a limited number of audit measures, thus additional measures were required to be added to the final framework. Considering each high level control objective in turn, the measures remaining on the comprehensive listing were examined and subjected to scrutiny against five criteria: the designation of mandatory or in scope for measures from the ANAO document, the need to look outside the organisation, reference to organisation type which would not be found within the population, the potential that it covered an area which would not be found, and the nature of the measure (i.e. its specificity).

3.7.2.1.2 Exclusion by designation of originating organisation

Some measures listed within the ANAO document were designated by that office as either mandatory or in scope. Measures with this designation were included in the comprehensive listing but subjected to the remaining criteria for exclusion from the final listing. It was considered that if the ANAO considered measures to be either optional (i.e. not mandatory) or out of scope, they were not relevant in the context of this research. An example of exclusion on such grounds is the control activity 8.2 of the ANAO document specified as “Management has implemented procedures to ensure that all data is classified and ownership has been assigned,” which was derived from COBIT detailed control objective DS5.8 Data Classification. All five points in this control activity were omitted from the comprehensive listing as ANAO designate the overall category to be either neither mandatory or in scope.

3.7.2.1.3 Exclusion through necessity to look outside the organisation

Measures which required the researcher to look outside of the organisation were excluded simply on the basis of the time required to examine external data. For example, one of the audit measures from the ANAO in reference to PO8 Ensure

Compliance with External Requirements was: “Data being transmitted across international borders does not violate export laws.” In order to adequately audit on such a measure, the researcher would have to ascertain if data were transmitted across international borders and then determine the pertinent laws in both Australia (as the source country) and the destination country. This could potentially be a time consuming process if the language of the destination country were anything other than English. Furthermore the task would depend upon specific circumstances.

3.7.2.1.4 Exclusion through non-applicability

The use of documents from the ANAO and the COBIT Audit Guidelines saw the inclusion in the comprehensive listings of measures relating specifically to either Commonwealth or private organisations. Since neither type of organisation would be encountered in the audits, such measures were specifically excluded from the abbreviated list. For example, the ANAO measures include “Identify who is responsible for PSM (Protective Security Manual) compliance.” The PSM is unique to Commonwealth organisations and thus to include such a measure in audits of Tasmanian public sector organisations is unnecessary.

3.7.2.1.5 Exclusion through potential inappropriateness

Some measures from the ANAO document indicated they may not be relevant in all situations by stating specific action should be done “... where appropriate.” Since it is likely that these measures will not be relevant across all organisations to be audited, they were omitted from the final listing for the sake of brevity and the time taken to complete an audit. For example, in the comprehensive listing for DS5 Ensure Systems Security is the measure “Where appropriate perform security configuration review i.e. RACF, Win, Unix.” The wording of this measure implies that it will not be necessary in all situations, and thus it was decided to omit such a measure from the final listing.

3.7.2.1.6 Exclusion through non-specificity

Some measures on the comprehensive listing were broad in nature. This may indicate some relevance across a number of detailed control objectives; however, broad non-specific measures that were unable to be related to detailed control objectives were omitted as including such measures may lead to an incomplete or inaccurate audit opinion being formed. An example of a measure excluded on this basis is the measure

“Consideration has been given to optimising current and future IT investments” from the comprehensive list for PO1 Define a Strategic Information Technology Plan which could not be related specifically to any of the 8 detailed control objectives.

3.7.2.1.7 Validation of selected measures

In order to validate the researcher’s selected measures the selected audit measures were then forwarded to a senior public sector external IT auditor for their comment and input. In line with the feedback, minor revisions were made. The full listing of audit measures included in the trial instrument can be found in Appendix J.

3.7.2.2 Audit

In undertaking the audit procedure the researcher conducted highly structured interviews, assessing performance against a series of processes and requirements, as well as examining documentation such as policies and written procedures.

The organisations were approached by the TAO to participate in the audit phase as the ethical considerations prevented the researcher from obtaining a list of potential participants from that agency and approaching organisations directly. The TAO selected these organisations within two constraints (1) to examine the more complex IT infrastructures and (2) to complete as many audits as possible in a limited time frame. As some of the organisations from Phase One did not have complex IT infrastructures, the Senior EDP Auditor considered audit to be unnecessary. Other organisations were located in regional or rural centres which would have required considerable time spent in travelling.

3.7.2.3 Documentation

In Australia, an auditing standard (AUS 208 Documentation) issued by the Australian Accounting Research Foundation (AARF) requires the auditor in the audit process to document matters that are “important in providing evidence to support the audit opinion” (AUS 208.02, AARF, 2002). This documentation is known as the audit working papers. Working papers are defined in by the Australian Accounting Research Foundation in Auditing and Assurance Standard AUS208 as any material “prepared by and for, or obtained and retained by the auditor in connection with the performance of

the audit.” It is specifically noted that the papers “may be in the form of data stored on paper, film, electronic media or other media.”

In order to facilitate the collection of information in the audit interviews a working paper template was drawn up for each control objective listing the audit measures selected in the process outlined in Section 3.7.2.1. A copy of the template is located in Appendix J.

3.7.3 Processing

The handwritten notes from the audit working papers were summarised by taking the key concepts and directly relevant evidences and presenting them in tabular form (Appendix K). The data were then assessed against the Generic Maturity Model (Figure 3.1) from the COBIT Management Guidelines (ITGI, 2000), seeking key aspects of each level (see discussion below) in the evidences obtained through the audit procedure.

Each audit measure was assigned a “maturity level” to indicate the level to which the measure was met. This “maturity level” was not directly related to the compliance with the individual audit measures. It was used purely as a tool to enable a quantitative comparison of audit outcomes for individual measures between different organisations. An additional benefit to the assigning of “maturity levels” was that it facilitated a comparison with previous studies.

Any audit measure that the organisation indicated as not relevant to their circumstances or not met was assigned level 0 (Non-Existent). Measures addressed indirectly, such as policy that was incorporated in an ad hoc manner in other organisational documentation, or issues dealt with on a case by case basis was assigned level 1 (Initial). Measures which were dealt with under informal or undocumented policies were assigned level 2 (Repeatable) while measures that were addressed by documented policies and formalised training were assigned level 3 (Defined). In the course of the audit interviews many managers indicated that a particular measure was met by their organisation with a simple yes or no response, which in some cases was entirely appropriate. For example, a password policy either specifies restrictions on length or it does not.

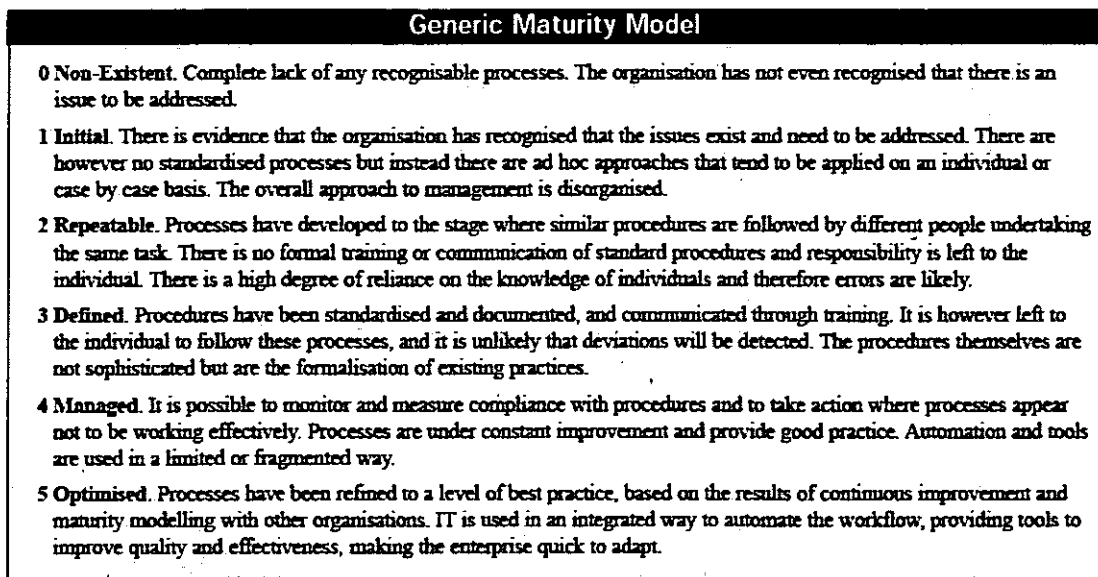


Figure 3.1: Generic Maturity Model. Sourced from COBIT Management Guidelines (ISACA, 2000)

It is entirely appropriate that an auditor use the work of specialists or experts in the formation of an audit opinion. It is covered in auditing standards such as AUS 806 (paragraphs 21 and 22) and AUS 808 (paragraphs 23 to 26). While AUS 808 indicates that the expert should be objective and independent (AUS 808.26) the subjective nature of the “experts” used in these audits is acknowledged and a degree of scepticism is indicated by the assigning maturity level 3 (Defined) rather than a higher level which may be more appropriate. If a clarification was sought the maturity level was assigned on the basis of the clarification supplied.

Measures assigned as level 4 (Managed) were those that had formal documentation and/or training, subject to continuous monitoring and improvement, and may have involved a limited amount of automation. Examples of this are the use of a VESDA system to monitor a server room for smoke, or the use of automated alerts on systems logs. Level 5 (Optimised) was assigned in few cases; the Generic Maturity Model indicates that it should be assigned in cases where the organisation has adopted industry best practice. Level 5 (Optimised) was assigned in measures within DS12 Manage Facilities where certain audit measures were either met or not met, for example the building being locked outside of business hours (or in the case of one organisation, continuously manned). Outside of this level 5 (Optimised) was assigned if the

organisation met the requirements of level 4 (Managed) for a particular audit measure and also included elements of automated workflow.

3.8 Evaluation of Use of Instrument

The use of the instrument will be evaluated in a number of ways.

3.8.1 Duration of audit interview

The duration of the audit interview will be a key evaluation point for the derived audit instrument. If too many audit measures are included the interview will be lengthy and may result in audits not being fully completed. It was anticipated in this study that the audit interviews would be approximately two to three hours in duration. This allows enough time to gather vital information, without intruding excessively on the time of the participating IT manager.

3.8.2 Independent evaluation

Subjecting the derived audit instrument to independent validation by the most senior external public sector IT auditor will also assist in evaluation of the instrument. The audit professional who validates the instrument is also the one who organised the audit interviews. The TAO would not allow a researcher with in invalid or faulty audit instrument access to their clients.

3.8.3 Linkage of IT process to business goals

The audit instrument currently used for IT audit in the Tasmanian public sector is based around low level IT processes. The instrument was not derived to be able to examine linkages between key IT processes and the business goals of the organisation. A properly derived instrument from the COBIT framework will allow such linkages, where they exist, to be examined.

3.8.4 Relevance of instrument

The instrument derived through the method outlined in this chapter will be highly relevant to the organisations being audited as they will have had the opportunity to

participate in rating the control objectives. These ratings will then determine the composition of the derived instrument, making it current and relevant.

3.8.5 Benchmarking

As part of the process in which the instrument is derived, audit measures from other public sector audit organisations are considered for inclusion. This is a form of benchmarking with best practice options able to be included.

3.9 Summary

This chapter has covered issues of ethics, research aims, research philosophy, research methods, reliability, validity and analysis as they apply to the research project.

Chapter 4 - Results and Analysis

4.1 Introduction

This chapter examines the results for both phases of the study. Within each phase of the study the results are presented, interpreted and analysed in sequence. The aggregated structure has been designed to make it easier for the reader to follow the study through both phases to its logical conclusion.

4.2 Phase 1 Survey of Tasmanian Audit Office Clients

4.2.1 Response Rate

From the original thirty questionnaires originally mailed out by the TAO, twenty three were returned by mail. Two respondents requested electronic copies of the questionnaire, which were returned by e-mail. This gives a response rate of 83.3%. The response rate for top managers or representatives of organisations is usually 36%, and for mid-level managers about 60% (Baruch, 1999). Baruch (1999) also suggests response rates more than one standard deviation (13% in the first instance and 20% in the second) from these levels should be explained. The high response rate in this case may be attributable to the facilitating role of the TAO, the documents for the survey were distributed by the TAO and the advance notice of the distribution was done by TAO staff members. Therefore the study was seen by participants as credible and relevant.

4.2.2 Representativeness of the Data

Generally with survey research a questionnaire is distributed among a proportion of a population (a sample). To be able to claim the results of such a survey are representative of the entire population it is sometimes necessary to test for any potential difference between respondents and non-respondents. This presents a problem for the researcher as there are no data available from non-respondents. In such a case it is usual to divide the responses received into two categories, early and late respondents. Representativeness is then tested on multiple perspectives using a statistical test such as the Chi-square. Response rates over 70% are considered to be "very good" (Babbie,

1990). Since this survey was distributed to the entire population of TAO clients designated as either key or large, and the response rate was over 80%, it was considered unnecessary to test the responses for whether they were representative of the whole population.

4.2.2.1 Organisational type

The results for the type of organisation in which the respondents worked are presented in Table 4.1. Only one respondent selected “Other” for their organisational type and specified GBE. This was interpreted as “Government Business Enterprise” and incorporated in the “Government Owned Business/Public Trading Enterprise” category. No respondents reported working for a Government Agency. From a total of 25 respondents, 44%, or 11 respondents, reported they worked for a Government Owned Business or Public Trading Enterprise, 24%, or 6 respondents, worked for a Government Department, 20%, or 5 respondents, for a Local Government Body and only 12%, or 3 respondents worked for a Statutory Body.

Table 4.1: Type of organisation in which respondents are employed

<i>Organisational Type</i>	<i>Freq</i>	<i>%</i>
Government Department	6	24%
Government Owned Company/Public Trading Enterprise	11	44%
Statutory Body	3	12%
Local Government Body	5	20%

It should be noted that although no respondents specified their organisations to be government agencies, this term has a specific meaning that is enshrined in legislation. All government departments and certain other organisations laid out in the relevant legislation are considered to be agencies.

4.2.2.2 Respondent's Position

The results for the position title for the respondents are presented in Table 4.2. Three respondents specified “Other” for their position type, two of which were Finance Managers and one Director Corporate Support. These positions were included in the table while the positions of CEO and IT/IS Director were omitted as no respondents

claimed such titles. From the 25 responses received, 76%, or 19 respondents, specified IT/IS Manager, 8%, or 2 respondents each specified Chief Information Officer (CIO) and Finance Manager, while 4%, or one respondent each specified Business Manager and Director Corporate Support.

Table 4.2: Position titles of respondents

<i>Respondent's Position</i>	<i>Freq</i>	<i>%</i>
CIO	2	8%
IT/IS Manager	19	76%
Business Manager	1	4%
Finance Manager	2	8%
Director Corporate Support	1	4%

4.2.2.3 Familiarity with IT Processes

The results for the ratings of familiarity with IT processes are presented in Table 4.3. Of the 25 responses received, 76%, or 19 respondents, claimed to be “Very familiar” with the IT processes of their organisation, 16%, or 4 respondents, claimed to be “Familiar” with IT processes while 8%, or 2 respondents, claimed to be “Very Unfamiliar” with the IT processes of their respective organisations. The claim by two respondents to being very unfamiliar with the IT processes of their organisations was unexpected, particularly as both respondents in question occupied positions of IT/IS Manager. Any attempt to justify such a response would be mere speculation. However it is possible that both respondents were new to both their position and organisation.

Table 4.3: Familiarity with IT processes

<i>IT Processes</i>	<i>Freq</i>	<i>%</i>
Very unfamiliar	2	8%
Familiar	4	16%
Very familiar	19	76%

4.2.2.4 Familiarity with Business Objectives

The results for the respondents' rating of their familiarity with the business objectives of their organisations are presented in Table 4.4. From the 25 responses, 52%, or 13 respondents, rated themselves as very familiar with the business objectives, 36%, or 9 respondents, claimed to be familiar, 8%, or 2 respondents, considered themselves to be very unfamiliar and 4%, or a single respondent, rated themselves as neither familiar nor unfamiliar with the business objectives of their organisation. Again these ratings were surprising in that two respondents claimed to be very unfamiliar with their organisations' business objectives. Interestingly it was the same two respondents who claimed unfamiliarity with the IT processes of the organisations, lending credence to the possibility that they were new to both their role and their organisation.

Table 4.4: Familiarity with business objectives

<i>Business Objectives</i>	<i>Freq</i>	<i>%</i>
Very unfamiliar	2	8%
Neither familiar nor unfamiliar	1	4%
Familiar	9	36%
Very familiar	13	52%

4.2.2.5 Summary of Demographic Data

The demographic data derived from the first section of the questionnaire comprised organisational type, respondent's position, familiarity with IT processes and familiarity with the business goals of the organisation. This provides a context for the data obtained from the second section of the questionnaire, the rating of the high level COBIT control objectives.

4.2.3 Control Objective Rating Results

The second section of the questionnaire asked participants to rate the importance of the 34 high level control objectives from the COBIT framework to their organisation on a Likert-type scale. The ratings were collated as responses were received, producing a ranked list that is presented in Table 4.5.

Table 4.5: Ratings for Control Objectives from Phase One of study

	Response Number																									Total
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
DS5	5	5	4	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	4	4	4	5	5	5	120
DS4	4	5	5	5	5	4	4	5	5	5	5	5	4	5	5	4	5	5	5	4	4	4	4	4	4	114
PO1	5	4	4	5	5	4	4	4	5	4	5	5	5	4	5	5	5	5	5	5	3	4	5	5	3	113
DS11	5	5	5	5	4	5	5	5	5	5	5	5	5	4	4	4	4	3	4	4	4	4	4	5	4	112
DS12	5	5	4	5	5	5	5	4	5	5	3	5	4	4	4	4	4	4	5	4	4	4	4	5	4	110
AI6	5	4	4	5	5	4	5	4	5	5	4	4	5	4	4	4	4	5	5	4	4	4	4	4	4	109
PO8	5	5	3	5	5	4	4	5	5	5	3	5	4	4	5	4	5	5	4	4	4	4	4	5	3	109
PO5	5	4	4	5	4	4	5	5	5	5	4	5	4	4	4	4	4	5	5	4	3	4	4	4	4	108
AI3	5	4	3	5	4	4	5	5	5	5	3	5	4	4	4	4	4	4	4	4	4	5	4	5	4	107
PO6	5	4	4	4	5	4	5	4	5	4	4	5	5	4	4	4	4	5	5	4	4	4	5	3	3	107
DS10	5	4	4	4	5	4	4	4	5	4	4	4	4	4	4	4	5	5	5	4	4	4	4	4	4	106
DS9	4	4	4	4	4	4	5	4	5	5	5	5	4	4	4	4	5	5	4	4	4	3	4	4	4	106
AI2	5	4	3	4	4	4	4	5	5	5	3	5	4	4	4	4	4	4	5	4	4	5	4	5	4	105
AI5	4	4	4	4	5	4	5	5	5	5	3	4	4	5	4	3	4	4	5	4	4	4	4	5	3	105
PO9	4	4	4	5	5	4	5	4	5	4	4	5	5	4	4	4	4	4	4	4	3	4	4	4	4	105
DS8	3	5	4	4	4	4	5	4	5	4	4	5	4	4	4	3	5	4	5	4	4	4	4	4	4	104
PO4	5	4	4	5	4	4	5	4	5	4	4	4	4	5	4	4	4	4	5	4	3	4	4	4	3	104
AI4	5	4	4	4	4	4	4	4	4	5	3	5	4	4	4	4	4	4	5	4	4	4	4	4	4	103
DS13	3	4	3	4	4	4	4	4	5	5	4	4	4	5	4	4	4	4	5	4	4	5	4	4	4	103
PO10	5	4	4	5	4	4	0	5	5	5	4	5	4	5	4	4	4	4	4	3	4	4	5	5	3	103
PO3	5	4	4	4	4	4	4	3	5	4	5	4	4	3	5	4	4	5	5	4	3	4	4	5	3	103
PO7	4	4	4	4	4	5	3	5	4	4	5	4	4	4	4	4	4	5	5	3	4	4	4	4	4	103
PO11	5	4	3	4	5	4	4	5	4	4	5	4	3	4	4	4	4	4	5	4	3	4	4	4	4	102
DS3	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4	5	4	2	3	4	5	4	101
M2	3	4	3	4	5	4	5	4	5	4	5	5	4	4	4	4	4	4	4	4	4	3	3	4	4	101
PO2	5	4	4	4	4	4	4	4	5	4	4	4	4	3	5	4	4	4	5	4	2	4	4	4	4	101
DS7	4	4	4	4	5	4	4	4	5	4	3	4	4	4	4	4	4	3	4	4	4	4	4	4	4	100
AI1	4	4	3	3	4	4	4	4	5	4	4	4	4	3	4	4	4	4	4	4	4	3	4	5	4	98
DS2	5	5	0	5	4	5	4	2	4	4	5	4	4	5	4	4	4	4	5	4	3	3	4	4	3	98
M1	3	4	0	4	4	4	4	3	5	4	5	4	4	4	5	4	4	4	4	4	3	3	4	4	4	95
DS1	4	4	0	5	5	3	4	4	5	4	4	4	4	4	4	4	3	5	5	4	2	3	3	4	3	94
DS6	3	4	3	4	5	4	4	4	5	4	3	3	4	4	4	3	4	3	3	5	2	4	4	4	4	94
M4	2	3	3	4	4	4	4	3	4	3	3	5	4	3	4	4	3	4	4	3	2	3	3	3	4	86
M3	2	3	4	4	4	3	4	3	4	2	3	4	4	3	3	4	3	3	4	3	2	3	2	3	0	77

----- Indicates groupings of 10

————— Indicates statistically identified groupings

Beginning at the highest ranked control objective, the means were analysed using the paired sample Student's t-test to find significant differences in the means. While it would be usual to implement a Bonferroni adjustment to counter the effects of repeated statistical testing, when testing was performed with $\alpha = 0.005$, the testing was found to be too rigorous so a sensitivity level (α) of 0.05 was used. The first significant difference in the list was found between list items 1 (DS5) and 2 (DS4), (@ df 24, $t = 0.0154$, $p < 0.05$). This was not a feasible point at which to form the abbreviated list as a single item cannot be considered to be a list. Given that one of the stated aims of this

research was to develop and trial an abbreviated instrument for IT audit, a single item is particularly inappropriate as a single aspect is not an adequate test of IT control within an organisation. Any further t-tests performed against the rating for item 1 (DS5) would also be significant, thus testing recommenced against item 2 (DS4). The next point of significance was between items 2 (DS4) and 8 (PO5) (@ df 24, $t = 2.009$, $p < 0.05$), indicating a second tier from item 2 (DS4) to item 7 (PO8). Testing again recommenced against list item 8 (PO5) arriving at a further significant difference (@ df 24, $t = 2$, $p < 0.05$) at list item 18 (AI4), indicating that list item 17 (PO4) was the last member of the third tier. The fourth tier was determined by t-tests against list item 18 (AI4), with the last item (@ df 24, $t = 4.239$, $p < 0.05$) of the tier being list item 32 (DS6). The bottom two list items were determined to be statistically different (@ df 24, $t = 1.984$, $p < 0.05$) thus they formed the fifth (M4) and sixth (M3) tiers.

As there were several points at which an abbreviated list could be formed, it was decided to consult previous studies to determine an appropriate list size. The international study by Guldentops et al (2002) used a list of 15 control objectives, while the study by Liu & Ridley (2005) used the same list. The EUROSAT IT working group recommended forming a list of 10 to 15 control objectives (EUROSAT, undated). These sources suggested the creation of an abbreviated list using the first three tiers of control objectives giving a size of 17 control objectives.

4.2.4 Comparison with previous studies

The seventeen control objectives included in the abbreviated list was ideal for a comparison with the list of 15 control objectives used by both Guldentops *et al* (2002) and Liu & Ridley (2005) as well as the control objectives identified by the EUROSAT project identified as being either “most important” (8 control objectives) or “also important” (8 control objectives). These lists are presented in Table 4.6 below.

Table 4.6: Comparison of control objectives identified as being important (source Guldentops *et al* 2002, Liu & Ridley, 2005, EUROSAl, 2005)

<i>Current Study</i>	<i>Guldentops & Liu & Ridley</i>	<i>EUROSAl</i>
PO1	PO1	PO1
PO9	PO9	PO9
AI2	AI2	AI2
AI6	AI6	AI6
DS4	DS4	DS4
DS5	DS5	DS5
DS10	DS10	DS10
DS11	DS11	DS11
PO5	PO5	AI3
AI5	AI5	PO3
AI3	PO3	M1
PO4	M1	PO2
PO6	PO10	PO10
PO8	AI1	AI1
DS8	DS1	AI4
DS9		DS7
DS12		

4.2.4.1 Explanation of Table

There are eight control objectives common to all three sources of data comprising:

PO1 Define a Strategic Information Technology Plan,

PO9 Assess Risks,

AI2 Acquire and Maintain Application Software,

AI6 Manage Changes, DS4 Ensure Continuous Service,

DS5 Ensure Systems Security,

DS10 Manage Problems and Incidents; and

DS11 Manage Data.

These are in the top eight positions in Table 4.6 and are bounded with a solid line. The two control objectives common to both the current research and to the list used by

Guldentops *et al* (2002) and Liu & Ridley (2005) were PO5 Manage the IT Investment and AI5 Install and Accredited Systems. These control objectives are shown in Table 4.6 bounded by a dashed line. An additional control objective (AI3 Acquire and Maintain Technology Infrastructure) was common to both the current research and EUROSAT (2005) lists. This is shown in Table 4.6 as bounded by a dotted line.

4.2.4.2 Discussion

To have 11 of 17 control objectives common to at least one other list indicates that the perception of the most important IT controls is not dependent on local conditions. The control objectives uniquely identified by the current research were PO4 Define the Information Technology Organisation and Relationships, PO6 Communicate Management Aims and Direction, PO8 Ensure Compliance with External Requirements, DS8 Assist and Advise Customers, DS9 Manage the Configuration and DS12 Manage Facilities. Since the list of 17 control objectives compiled in this study is longer than both other lists, Guldentops *et al* (2002) / Liu & Ridley (2005) listed fifteen control objectives while the combined EUROSAT (2005) lists contained 16 control objectives, it was inevitable that unique control objectives would be identified. However, the uniquely identified control objectives originate from only two COBIT domains, indicating that IT professionals within the Tasmanian public sector are actively concerned with the planning and organising as well as the delivery and support domains. There was no focus on monitoring identified in the Tasmanian data, while both other sources identified one control objective from the monitoring domain, M1 Monitor the Processes, was not positioned within the abbreviated list of 17 IT control processes, nor indeed near the top of the next tier.

4.2.5 Associated detailed control objectives

The seventeen high level control objectives in the final instrument had a list of 180 associated detailed control objectives. To adequately audit such a list would make the audit highly labour intensive in both fieldwork and documentation. For the sake of brevity it was decided to audit only the top two tiers of high level control objectives, a total of seven in all. Furthermore, it was seen as appropriate to trial the audit of IT control processes that were common to the most important identified by Guldentops *et*

al (2002), Liu & Ridley (2005) and EUROSAI (2005). Audit measures were selected for these seven high-level control objectives as described in 3.7.2.1.1 to 3.7.2.1.6.

4.2.5.1 Validation of selected measures

In order to validate the researcher's selected measures the selected audit measures were then forwarded to the senior professional external IT auditor in the Tasmanian public sector for their comment and input. In line with her suggestions, minor revisions were made. The full listing of audit measures included in the trial instrument can be found at Appendix K.

Once the audit measures were finalised, the trial audits were organised and conducted as outlined in Section 4.3.

4.3 Phase 2 Audit of Selected Public Sector Organisations

A total of nine organisations accepted the invitation to be a part of the audit phase of the research. Of these, four were agencies as defined in the State Service Act 2000, two were government business enterprises, two were statutory bodies and one was a local government body. Only one of these organisations had not participated in Phase One of the study. That particular organisation did, however, participate in the pilot study and was included in Phase Two on the recommendation of the Senior EDP auditor from the TAO, as it had an IT infrastructure of an appropriate size. It should be noted that four organisations that participated in the audit phase are designated as government agencies according to legislation. In tables throughout section 4.3 these organisations will be marked with an asterisk (*). Each category of organisational type that participated in the survey, also participated in the audit phase.

The audits took the form of an interview with a senior manager or person in charge of information technology within each organisation. These interviews, conducted onsite at the premises of the organisations, ranged in duration from approximately 40 minutes for the smallest organisation, to 100 minutes for the organisation with the most complex IT infrastructure. In the course of the interview the participating manager provided evidence of the way in which the organisation addressed the individual audit measures.

The working papers were subjected to the analysis outlined in Section 3.7.3 and the collated results can be seen for each control objective in Sections 4.3.1 to 4.3.7.

4.3.1 DS5 Ensure Systems Security

The most highly ranked control objective, DS5 Ensure Systems Security, is concerned with the business goal of “safeguarding information against unauthorised use, disclosure or modification, damage or loss” (ITGI, 2000, p70) and is enabled by “logical access controls which ensure that access to the systems, data and programmes is restricted to authorised users” (ITGI, 2000, p70).

4.3.1.1 Assigned Maturity Ratings for DS5 Ensure Systems Security

Table 4.7 displays the maturity levels assigned to each audit measure on the basis of compliance with the control objective DS5 Ensure Systems Security for each participating organisation, the corresponding means for individual measures and organisations as well as a mean for the overall control objective.

Table 4.7: Maturities assigned for DS5 Ensure Systems Security

Measure	Organisation (* denotes agency status)									
	1*	2*	3	4	5*	6	7*	8	9	Mean
1	4	4	0	1	4	4	4	4	2	3.00
2	3	4	2	4	4	4	4	3	3	3.44
3	4	4	3	4	4	4	4	3	3	3.67
4	4	4	2	4	3	2	3	3	2	3.00
5	4	4	4	4	4	4	3	4	4	3.89
6	4	4	4	4	4	4	2	4	4	3.78
7	4	4	0	3	4	3	2	3	0	2.56
8	2	3	4	0	4	2	4	0	4	2.56
9	4	4	2	4	4	2	4	4	4	3.56
10	4	4	0	4	2	4	4	4	4	3.33
11	1	4	0	1	1	1	4	4	0	1.78
12	4	4	4	4	4	4	4	4	4	4.00
Mean	3.50	3.92	2.08	3.08	3.50	3.17	3.50	3.33	2.83	3.21

Maturity ratings assigned to measures within this control objective varied from a low of 0 (non-existent) to 4 (managed). No organisations were assessed as attaining 5 (optimised) for any of the audit measures. The minimum and maximum means for both

organisations and audit measures along with their respective organisation and measure numbers (bracketed) are shown in Table 4.8. The overall mean assigned maturity level for DS5 Ensure Systems Security was 3.21 across all audit measures and organisations. Tables showing the frequencies of maturity ratings for organisations and for individual audit measures are located in Appendix L.

Table 4.8: Minimum and Maximum Means for DS5 Ensure Systems Security

	Lowest mean	Highest mean
Organisation	2.08 (3)	3.92 (2)
Measure	1.78 (11)	4.00 (12)

4.3.1.2 Interpretation of Results for DS5 Ensure Systems Security

These results were surprising given that DS5 Ensure Systems Security was overwhelmingly rated as the most important to the organisations participating in the Phase One of this study. For organisational means to range between a level designated as repeatable (level 2) and defined (level 3) was unexpected for a range of processes considered to be so important. It must be noted that while individual aspects of the control objective were assessed as being managed (level 4) but the overall means were lower than was anticipated.

The highest mean maturity rating for an audit measure across all the organisations was for measure 12, which relates to the *existence and communication of policies around the use of Internet, e-mail and file sharing*. The lowest mean maturity rating for an audit measure across all the organisations was for measure 11, which relates to the *revision of audit trails of access and activity on a daily or weekly basis*.

The low means for some individual audit measures may indicate that there is an overall deficiency in the way that some aspects of this control objective were being addressed within these organisations. Six organisations were assigned maturity levels or either non-existent (0) or initial (1) for the way in which they addressed the audit measure (11) of *daily or weekly reviews of audit trails of access or activity*. This audit measure would seem to be critical to the underlying principles of this control objective, as outlined in the introductory remarks for this control objective (see 4.3.1 above).

4.3.1.3 Further Discussion

The Tasmanian Government, through the Information Security Charter 2003, requires all public sector organisations designated as “Agencies” (see Section 4.2.2.1) by legislation to have in place an Information Security policy. This requirement is relatively recent, and many agencies are still in the process of implementing it. A 2004 internal government document, “Information Security Project – Implementation by agencies progress report,” indicated that not all agencies had security policies in place at the time of publication (August 2004). However, all organisations audited that were required by the Charter to have an information security policy in place, were found to have done so by the time of the audits. Of the other organisations, two had security policies in place, one had various elements of a security policy incorporated in other policy documents, one is currently developing a security policy and one did not have a security policy and had no plans to develop such a policy.

The organisations designated as agencies (those required by the Charter to have security policies) had higher organisational mean maturities (ranging from 3.50 to 3.92) than all the other organisations (ranging from 2.08 to 3.33) for DS5 Ensure Systems Security. These means are significantly different ($p = 0.00097$, at $\alpha = 0.05$). This may indicate that the process of developing a security policy encouraged the organisation to examine procedures and processes that affect the security of information. The organisations that had security policies in place, although not having a formal requirement under the charter, also had higher organisational mean maturities than those that did not have one, regardless of whether the organisation was currently developing such a policy. These results appear to support the argument that the development of a security policy was beneficial for individual organisations’ systems security.

The approaches to the audit measure (12) assessing the *need to formally indicate the user’s acceptance of policies around Internet and e-mail usage*, varied from formal sign off to no requirement to indicate acceptance, although this did not affect the maturity level assigned since all organisations had such policies and communicated them. It was indicated by several participants that formal sign off on such policies is not used, on legal advice. Many organisations close to government, predominantly the agencies, are balancing the demands of one department for such formal acceptance to be used, with

the advice of another that acceptance, either in the form of a signature on a policy or a button on a screen that appears while the system is loading (a splash screen), is not enforceable within the legal system.

DS5 Ensure Systems Security was found to have the highest self assessed maturity levels of all the most high level control objective on the lists of Guldentops *et al* (2002) and Liu & Ridley (2005), it was also included in the “most important” list from the EUROSAI Self Assessment project. This is indicative of the importance attributed to DS5 Ensure Systems Security from state through to international levels.

4.3.2 DS4 Ensure Continuous Service

The Control Objective DS4, Ensure Continuous Service, is concerned with the business goal of “making sure IT services are available as required and ensuring a minimum business impact in the event of a major disruption” (ITGI, 2000, p68). DS4 Ensure Continuous Service is enabled by “having an operational and tested IT continuity plan which is in line with the overall business continuity plan and its related business requirements” (ITGI, 2000, p68).

4.3.2.1 Assigned Maturity Ratings for DS4 Ensure Continuous Service

Table 4.9 displays the maturity levels assigned to each audit measure on the basis of compliance with the control objective DS4 Ensure Continuous Service for each participating organisation, the corresponding means for individual measures and organisations as well as a mean for the overall control objective.

Table 4.9: Maturities assigned for DS4 Ensure Continuous Service

Organisation (* denotes agency status)										
Measure	1*	2*	3	4	5*	6	7*	8	9	Mean
1	3	3	3	4	4	4	4	4	0	3.22
2	4	4	5	4	4	4	4	4	3	4.00
3	4	4	3	3	3	4	4	3	3	3.44
4	3	3	4	4	2	4	4	3	2	3.22
5	4	4	3	4	4	4	4	4	4	3.89
6	4	4	4	4	4	4	4	4	4	4.00
7	3	3	3	3	3	3	3	3	3	3.00
Mean	3.57	3.57	3.57	3.71	3.43	3.86	3.86	3.57	2.71	3.54

Maturity ratings assigned to measures within DS4 Ensure Continuous Service ranged from 0 (non-existent) to 5 (optimised) with the majority either 3 (defined), or more commonly, 4 (managed). Tables showing the frequencies of maturity ratings for both organisations and for individual audit measures are located in Appendix L. The minimum and maximum means for both organisations and audit measures along with their respective organisation and measure numbers (bracketed) are shown in Table 4.10. The overall mean assigned maturity rating was 3.54 across all organisations and all audit measures.

Table 4.10: Minimum and Maximum Means for DS4 Ensure Continuous Service

	Lowest mean	Highest mean
Organisation	2.71 (9)	3.86 (6 & 7)
Measure	3.00 (7)	4.00 (2 & 6)

4.3.2.2 Discussion of Results for DS4 Ensure Continuous Service

The lowest mean assigned maturity ratings for the individual audit measures was 3.00, for the audit measure (7) relating to the *matching of media at offsite locations to appropriate media management systems*. The highest mean assigned maturity rating assigned was 4.00, for the audit measure (2) relating to *publication policy with particular regard to publishing to the Internet* and also for that relating to *types of backups, their performance according to a schedule and the storage of backups in appropriate locations* (measure 6).

Within the thirteen detailed control objectives associated with DS4 Ensure Continuous Service are six that specifically refer to a continuity plan within their titles. Therefore, DS4 Ensure Continuous Service places an emphasis on such a plan existing. Only one organisation had no business continuity plan and no disaster recovery plan. Since there were no plans in place, a maturity level of 0 (non-existent) was assigned. However, it was indicated that there was an imminent meeting at which formation of these plans was to be considered. Should the outcome of that meeting be the formation of such plans, the assigned maturity level would rise. One organisation considered its long and short range plans to be business continuity and disaster recovery plans, a situation that might be considered to be less than ideal.

Many organisations indicated that the organisation's Internet publication policy was not the responsibility of the Information Technology department. However most managers were able to indicate that the relevant policies were in place and the organisation had strict controls over such publication.

DS4 Ensure Continuous Service was also found on the lists of Guldentops et al (2002), Liu & Ridley (2005) and the EUROSAI project (2005). This indicates that the provision of continuous support is considered to be an important factor at a state, national and international level.

4.3.3 PO1 Define a Strategic Information Technology Plan

The Control Objective PO1 Define a Strategic Information Technology Plan is concerned with the business goal of "striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment" (ITGI, 2000, p24). PO1 Define a Strategic Information Technology Plan is enabled by "a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals" (ITGI, 2000, p24).

4.3.3.1 Assigned Maturity Ratings for PO1 Define a Strategic Information Technology Plan

Table 4.11 displays the maturity levels assigned to each audit measure on the basis of compliance with the control objective PO1 Define a Strategic Information Technology Plan for each participating organisation, the corresponding means for individual measures and organisations as well as a mean for the overall control objective.

Table 4.11: Maturities assigned for PO1 Define a Strategic Information Technology Plan

Organisation (* denotes agency status)										
Measure	1*	2*	3	4	5*	6	7*	8	9	Mean
1	3	3	3	3	3	3	3	3	0	2.67
2	1	3	2	3	3	2	2	2	2	2.22
3	3	2	3	3	3	3	3	3	2	2.78
4	3	2	3	3	3	3	3	3	1	2.67
5	3	2	3	4	3	3	3	3	3	3.00
6	3	3	3	3	3	3	2	3	3	2.89
7	3	3	2	3	3	3	3	3	3	2.89
8	3	3	3	3	3	3	3	3	3	3.00
Mean	2.75	2.63	2.75	3.13	3.00	2.88	2.75	2.88	2.13	2.76

The maturity ratings assigned to the audit measures within PO1 Define a Strategic Information Technology Plan ranged from 0 (non-existent) to 4 (managed) assigned to a single organisation for one audit measure, with the vast majority (58 occurrences or 79.45%) of ratings being 3 (defined). There were no ratings of 5 (optimised) assigned within this control objective. Tables showing the frequencies of maturity ratings for both organisations and audit measures are located in Appendix L and the data are displayed graphically in Figures 4.1 and 4.2.

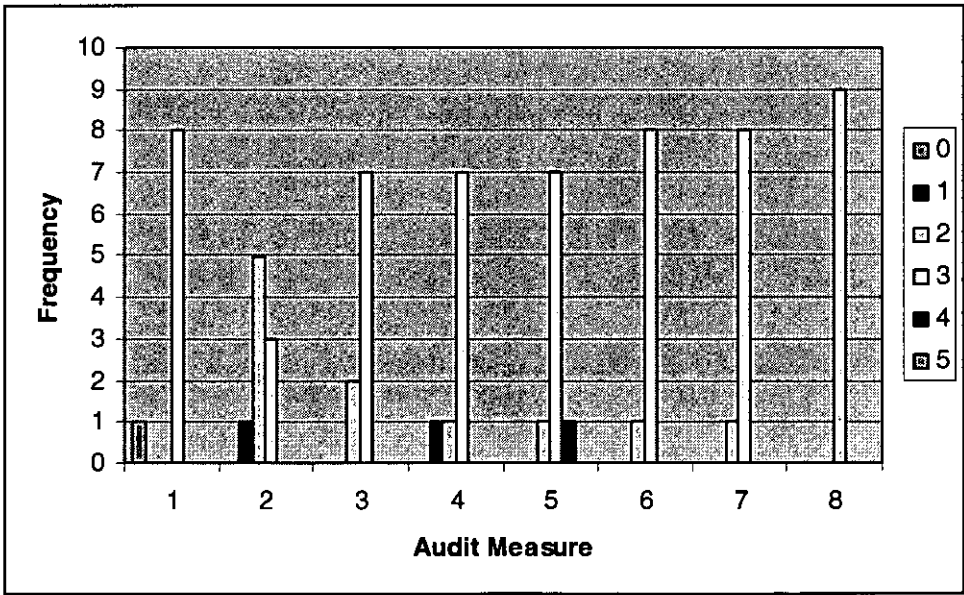


Figure 4.1: Frequency of Assigned Maturity Ratings by Audit Measure for PO1 Define a Strategic Information Technology Plan

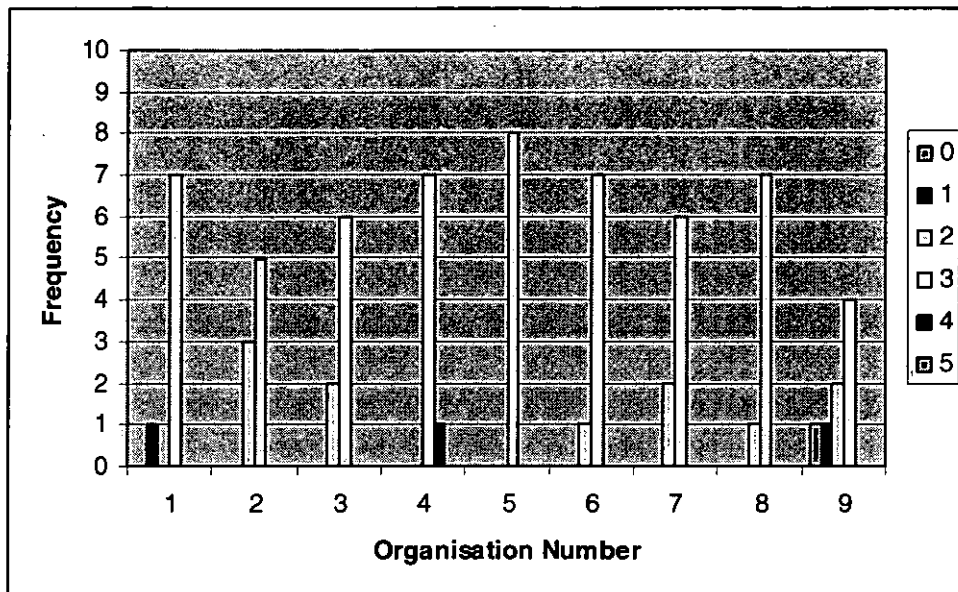


Figure 4.2 Frequency of Assigned Maturity Ratings by Organisation for PO1 Define a Strategic Information Technology Plan

The mean assigned maturity level across all audit measures and all organisations was 2.76. The minimum and maximum mean assigned maturity levels with their corresponding organisations and audit measure numbers.(bracketed) are shown in Table 4.12.

Table 4.12: Minimum and Maximum Mean Assigned Maturity Levels for POI Define a Strategic Information Technology Plan

	Lowest mean	Highest mean
Organisation	2.13 (9)	3.13 (4)
Measure	2.22 (2)	3.00 (5 & 8)

4.3.3.2 Discussion of Results for PO1 Define a Strategic Information Technology Plan

The lowest mean maturity level for audit measures calculated across all organisations was 2.22 for the *inclusion of relevant IT initiatives in the IT long and short range plans* (measure 2). The highest mean maturity level was 3.00 for measures 5, *consistency of the IT long and short range plans with the long and short range plans of the organisation*, and 8, *the existence of tasks to implement the IT long and short range plans*. The greatest fluctuation among assigned maturity ratings in individual audit measures was in measure 1, relating to the *existence of minutes from an IT planning or*

steering committee. This can be directly attributed to the fact that one organisation did not have an IT planning or steering committee and was consequently assigned a rating of 0 (non-existent).

The greatest fluctuation of assigned maturity levels within an organisation was again in organisation 9 with a range from a single occurrence of level 0 (non-existent) for measure 1 to four occurrences of 3. This can be seen in Figure 4.2, where there are four bars on the chart relating to Organisation 9. The most consistent organisation in terms of assigned maturity ratings for PO1 Define a Strategic Information Technology Plan, was Organisation 5, which was assigned 3 (defined) for all measures, this can be seen by the single bar relating to Organisation 5 on the chart at Figure 4.2. Across all organisations and all audit measures, the mean assigned maturity rating was 2.76, which is lower than the overall means for both DS5 Ensure Systems Security and DS4 Ensure Continuous Support. This may indicate a focus on the more practical objectives to the detriment of management based objectives such as planning.

As mentioned in Section 4.3.3.2 one organisation did not have an IT planning or steering committee. This organisation was consistently assigned lower maturity ratings with the lowest mean assigned maturity for both DS4 Ensure Continuous Support and PO1 Define a Strategic Information Technology Plan, while having the second lowest mean assigned maturity level for DS5 Ensure Systems Security. This result may be due to the organisational type, as the organisation in question being a local government body, the only one to be audited in this study.

Information obtained during the audit indicated that linkage of both long and short range IT plans to the long and short range plans of the business was approached in different ways across the organisations. In one organisation the IT plans were an integral part of the business plans. A second organisation used an overarching departmental initiative to dictate the broad direction of the IT plans, which was perceived by the manager who participated in the audit as being helpful.

PO1 Define a Strategic Information Technology Plan was also included in the lists of Guldentops et al (2002), Liu & Ridley (2005) and the EUROSAI project (2005), where it was nominated in the “most important” category.

4.3.4 DS11 Manage Data

The Control Objective D11 Manage Data is concerned with the business goal of “ensuring that data remains complete, accurate and valid during its input, update and storage” (ITGI, 2000, p82). It is enabled by “an effective combination of application and general controls over the IT operations” (ITGI, 2000, p82).

4.3.4.1 Assigned Maturity Ratings

Table 4.13 displays the maturity levels assigned to each audit measure on the basis of compliance with the control objective DS11 Manage Data for each participating organisation, the corresponding means for individual measures and organisations as well as a mean for the overall control objective.

Table 4.13: Maturities assigned for DS11 Manage Data

Measure	Organisation (* denotes agency status)									Mean
	1*	2*	3	4	5*	6	7*	8	9	
1	4	1	3	3	0	3	3	1	3	2.33
2	4	4	3	3	0	3	3	3	1	2.67
3	1	1	1	3	3	1	1	3	3	1.89
4	1	1	1	3	0	3	3	3	0	1.67
5	1	1	3	3	0	3	3	3	0	1.89
6	1	3	3	4	3	3	3	3	3	2.89
7	4	3	0	0	1	0	2	2	0	1.33
8	1	1	1	1	1	2	1	1	0	1.00
9	3	0	3	4	0	4	3	3	0	2.22
10	4	4	4	4	4	4	4	4	4	4.00
11	3	3	3	3	3	3	3	3	3	3.00
12	3	3	3	3	3	1	0	0	3	2.11
13	4	4	3	3	3	3	3	3	0	2.89
14	4	4	3	4	4	3	3	3	3	3.44
15	3	0	1	3	0	3	0	3	3	1.78
16	1	3	3	3	1	2	4	3	3	2.56
17	3	0	1	4	0	3	0	3	3	1.89
18	1	4	3	3	0	3	1	3	3	2.33
Mean	2.56	2.22	2.33	3.00	1.44	2.61	2.22	2.61	1.94	2.33

The maturity ratings assigned for the control objective DS11 Manage Data ranged from 0 (non-existent) to 4 (managed). No organisation was assigned a maturity rating of 5 (optimised) assigned within DS11 Manage Data. The minimum and maximum mean

assigned maturity levels are presented with their associated Organisation and Audit Measure numbers (bracketed) in Table 4.14.

Table 4.14: Minimum and Maximum Mean Assigned Maturity Levels for DS11 Manage Data

	Lowest mean	Highest mean
Organisation	1.44 (5)	3.00 (4)
Measure	1.00 (8)	4.00 (10)

4.3.4.2 Interpretation of Results

The mean assigned maturity ratings within the individual audit measures range from 1.00 for Audit Measure 8, *mitigating procedures to address the risk of misaddressing messages, particularly by fax and e-mail*, to 4.00 for Measure 10, *the training provided to operations staff with regard to backup, archiving and restore procedures*. This is the largest variation seen in the top 4 control objectives of the trial instrument and indicates a wide variation in the way in which the management of data is approached within the organisations participating in the audit trial.

For individual organisations the mean assigned maturity ratings ranged from 1.44 to 3.00 (see also Table 4.13). The mean assigned maturity rating for two organisations was less than 2 (repeatable). Eight of the nine organisations had assigned maturity ratings ranging between 0 (non-existent) and 4 (managed). The remaining organisation had assigned maturity ratings ranging between 1 (initial) and 4 (managed). The overall mean assigned maturity rating for DS11 Manage Data was 2.38, which was the equal lowest of all the control objectives in the audit along with AI6 Manage Changes.

Many of the audit measures for the Manage Data control objective were considered by IT managers to be not applicable in their organisations. The wide variation among assigned maturity ratings within DS11 Manage Data may indicate an inconsistent approach to the management of data within individual organisations. This conclusion is supported by the indication from the managers that many of the audit measures were addressed on a case by case basis by individual systems administrators or business units.

The *integrity, confidentiality and non-repudiation of sensitive messages transmitted over public networks such as the Internet* was managed poorly by many organisations as

evidenced by the assignment of maturity ratings of either 0 (non-existent) or 1 (initial) in over half the organisations audited. One manager believed sending sensitive messages was not done within their organisation, while another provided advice not to do it. The *risk of misaddressing messages by letter, fax or e-mail* was indicated by many as almost impossible to mitigate. Most organisations addressed the problem for e-mail by use of a global address book and the government directory where possible, but in most cases the responsibility was left to individual users.

DS11 Manage Data is not found in the lists of Guldentops et al (2002) and Liu & Ridley (2005). It is listed among the “also considered to be important” control objectives from the EUROSAI self assessment project (2005). With the equal lowest mean assigned maturity level across both organisations and audit measures, there is a great deal of scope for the improvement in the way that the requirements of DS11 Manage Data are addressed within the Tasmanian public sector.

4.3.5 DS12 Manage Facilities

The Control Objective DS12 Manage Facilities is concerned with the business goal of “providing a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards” (ITGI, 2000, p84). It is enabled by “the installation of suitable environmental and physical controls which are regularly reviewed for their proper functioning” (ITGI, 2000, p84).

4.3.5.1 Assigned Maturity Ratings for DS12 Manage Facilities

Table 4.15 displays the maturity levels assigned to each audit measure on the basis of compliance with the control objective DS12 Manage Facilities for each participating organisation, the corresponding means for individual measures and organisations as well as a mean for the overall control objective.

Table 4.15: Maturities assigned for DS12 Manage Facilities

Measure	Organisation(* denotes agency status)									Mean
	1*	2*	3	4	5*	6	7*	8	9	
1	5	5	5	5	5	5	5	5	5	5.00
2	5	5	5	5	5	5	5	5	5	5.00
3	5	3	1	5	5	5	5	5	5	4.33
4	4	4	4	4	4	4	4	4	4	4.00
5	5	5	4	4	5	1	1	4	4	3.67
6	4	4	3	3	3	3	3	3	3	3.22
7	5	5	3	3	3	4	4	4	3	3.78
8	4	3	3	3	3	3	3	3	3	3.11
9	4	2	2	0	0	0	0	0	0	0.89
10	3	3	0	3	3	1	0	3	1	1.89
11	3	3	3	4	3	0	4	3	1	2.67
12	3	4	4	4	4	3	4	4	4	3.78
13	4	4	4	3	4	3	3	3	3	3.44
14	3	4	3	4	3	4	4	4	4	3.67
15	4	3	2	2	3	3	4	3	3	3.00
16	4	4	4	4	4	4	4	4	4	4.00
17	3	3	3	3	3	3	3	3	3	3.00
18	4	5	3	3	3	3	3	3	3	3.33
19	4	0	4	3	1	3	3	3	3	2.67
20	4	1	3	3	4	3	4	3	4	3.22
Mean	4.00	3.50	3.15	3.40	3.40	3.00	3.30	3.45	3.25	3.38

The assigned maturity ratings for DS12 Manage Facilities range from 0 (non-existent) to 5 (optimised). The consistent assigning of a single maturity level for five audit measures can be seen in Figure 4.3.

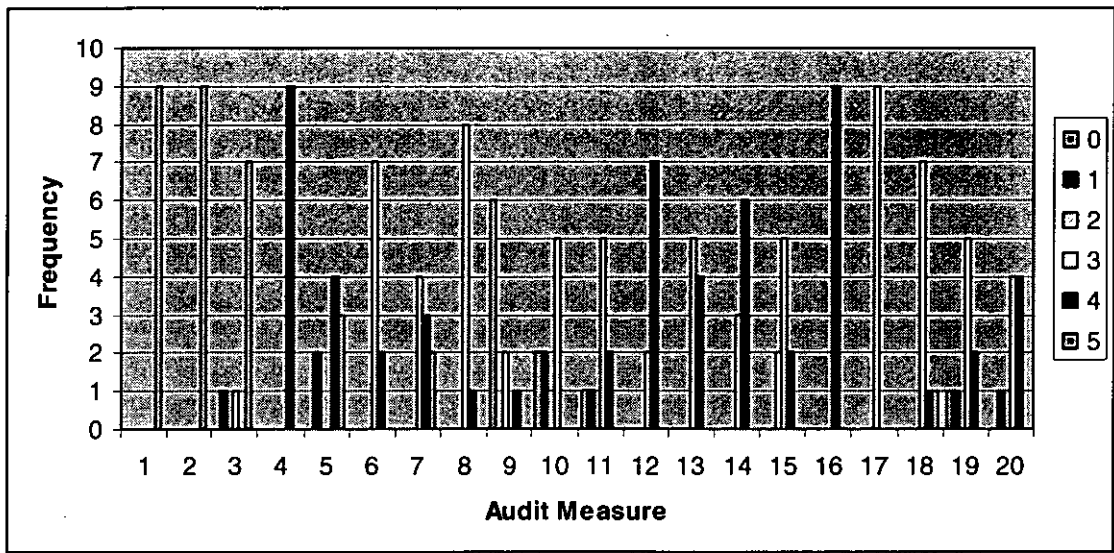


Figure 4.3: Frequency of Assigned Maturity Ratings by Audit Measure for DS12 Manage Facilities

The range of maturity levels assigned across the audit measures within each organisation can be seen graphically in Figure 4.4. The presence of bars for all six possible maturity levels for two organisations indicates a potentially inconsistent approach to the management of facilities.

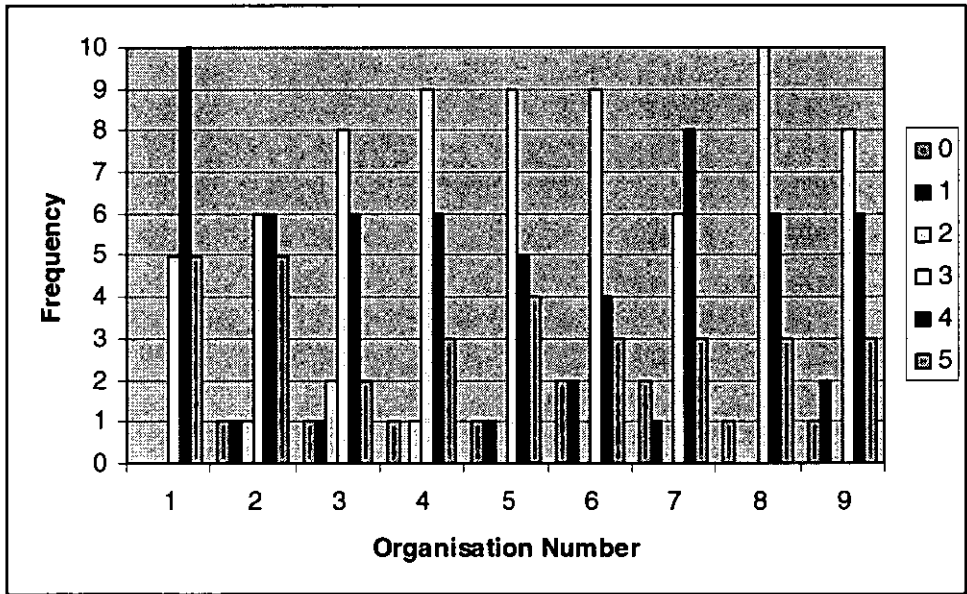


Figure 4.4: Frequency of Assigned Maturity Levels by Organisation for DS12 Manage Facilities

The mean assigned maturity level across the whole control objective DS12 Manage Facilities was 3.38. Table 4.16 displays the minimum and maximum mean assigned maturity levels for both organisations and audit measures.

Table 4.16: Minimum and Maximum Mean Assigned Maturity Levels for DS12 Manage Facilities

	Lowest mean	Highest mean
Organisation	3.00 (6)	4.00 (1)
Measure	0.89 (9)	5.00 (1 & 2)

4.3.5.2 Discussion of Results for DS12 Manage Facilities

There was less variation in the mean assigned maturity ratings across the organisations with the lowest being 3 and the highest 4. Only one organisation was not assigned maturity level 0 (non-existent), with the remaining organisations all being assigned maturity ratings from 0 (non-existent) to 5 (optimised) for audit measures within DS12 Manage Facilities. It is important to note that of the eight organisations assigned a level 0 (non-existent), only two were assigned such a rating for more than one audit measure.

Most organisations had well developed policies and procedures around the management of their physical premises. All facilities were locked over night, with the exception of one, which was manned at all times. In most cases access to the IT department was through both reception and security where it was necessary to sign in to the organisation's premises, with the security aspect being provided either by security personnel or through the use of programmable devices such as proxy cards or small plastic coated capsule like devices, commonly called dongles. The programmable devices are used in most cases to access the premises after hours. In all but one case the reception logs were not examined by the IT department to review departmental visitors. Only one organisation required visitors to the computer facilities to sign in, but in all cases access to the server room was restricted to those who were accompanied by an authorised member of staff or those who had been issued with appropriate access privileges. All the server rooms were located on floors above ground level and flooring varied widely. One organisation had both raised flooring and anti-static matting, four organisations had server rooms with no special considerations made, and others had

rubber matting on ordinary flooring. One IT manager indicated that they considered Uninterruptible Power Supply (UPS) to be unnecessary and used it only on critical machines, justifying this stance by declaring that modern machines cope far better with loss of power than previously.

DS12 Manage Facilities was one of the six control objectives unique to the Tasmanian listing of 17 control objectives. Using the mean assigned maturity level as a metric, the processes around DS12 Manage Facilities were at a consistently higher standard, since the mean assigned maturity level across both organisations and audit measures was the highest for this control objective.

4.3.6 AI6 Manage Changes

The Control Objective AI6 Manage Changes is concerned with the business goal of “minimising the likelihood of disruption, unauthorised alterations and errors” (ITGI, 2000, p58). It is enabled by “a management system which provides for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure” (ITGI, 2000, p70).

4.3.6.1 Assigned Maturity Ratings

Table 4.17 displays the maturity levels assigned to each audit measure on the basis of compliance with the control objective AI6 Manage Changes for each participating organisation, the corresponding means for individual measures and organisations as well as a mean for the overall control objective.

Table 4.17: Maturities assigned for AI6 Manage Changes

Measure	Organisation (* denotes agency status)									Mean
	1*	2*	3	4	5*	6	7*	8	9	
1	3	3	1	3	3	4	4	3	2	2.89
2	3	3	1	3	3	4	4	3	2	2.89
3	1	4	0	2	0	2	1	2	0	1.33
4	3	4	0	3	1	3	4	3	1	2.44
5	4	0	0	3	3	3	4	3	3	2.56
6	3	0	0	3	1	3	1	3	3	1.89
Mean	2.83	2.33	0.33	2.83	1.83	3.17	3.00	2.83	1.83	2.33

Assigned maturity levels for AI6 Manage Changes varied from 0 (non-existent) to 4 (managed). No organisation was assigned a maturity rating of 5 (optimised) for any of

the audit measures in this control objective. The most commonly assigned maturity level was 3 (defined) with 24 occurrences (54%). Tables showing the frequencies of assigned maturity ratings for organisations and for individual audit measures are located in Appendix L.

The overall mean assigned maturity level for AI6 Manage Changes was 2.33, which was the equal lowest mean assigned maturity level for all control objectives with DS11 Manage Data. The minimum and maximum mean assigned maturity levels for both organisations and audit measures along with the respective organisation and measure numbers (bracketed) are shown in Table 4.18.

Table 4.18: Maximum and Minimum Mean Assigned Maturity Levels for AI6 Manage Changes

	Lowest mean	Highest mean
Organisation	0.33 (3)	3.17 (6)
Measure	1.33 (3)	2.89 (1)

4.3.6.2 Discussion of Results for AI6 Manage Changes

Within individual audit measures the mean assigned maturity levels varied from 1.33 for measure 3, *the adequacy of IT libraries and existence of base line code levels*, to 2.89 for measures 1 and 2, both based around the *documentation of change*. There were no audit measures for which organisations were assigned ratings of a consistent level indicating a much more inconsistent approach across all the organisations to the processes around the management of change.

There was much more variation of mean assigned maturity ratings across the individual organisations. These ranged from a low of 0.33 to a high of 3.17. Three organisations were assigned maturity ratings across all audit measures that varied by only one level indicating a consistent approach to these processes. One of these organisations failed to gain a maturity rating higher than 1 (initial) for any audit measure, indicating an immature organisational approach to the management of change.

One manager considered that most of the change management audit measures were not applicable to their organisation as no coding takes place within the organisation, as

many of the audit measures examined for AI6 Manage Changes were based around making changes to program code. The same manager had previously indicated that the organisation was looking to appoint a programmer. When such an appointment is made and internal development and change processes begin it is essential that the organisation re-consider its position in respect of such audit measures. Several organisations indicated that code was kept by individual vendors or contractors and thus could not comment on the adequacy of such code libraries. Most managers considered users to be aware of and understand the need for formal change control procedures at some level.

AI6 Manage Changes was one of the eight control objectives found on the lists of Guldentops et al (2002) and Liu & Ridley (2005) while the EUROSAT project (2005) included it in the listing of control objectives considered to be the “most important.” In this research it was shown to be managed in an inconsistent and under-developed manner within the Tasmanian public sector.

4.3.7 PO8 Compliance with External Requirements

The Control Objective PO8 Compliance with External Requirements is concerned with the business goal of “meeting legal, regulatory and contractual obligations” (ITGI, 2000, p38). It is enabled by “identifying and analysing external requirements for their IT impact, and taking appropriate measures to comply with them” (ITGI, 2000, p38).

4.3.7.1 Assigned Maturity Ratings

Table 4.19 displays the maturity levels assigned to each audit measure on the basis of compliance with the control objective PO8 Compliance with External Requirements for each participating organisation, the corresponding means for individual measures and organisations as well as a mean for the overall control objective.

Table 4.19: Maturities assigned for PO8 Compliance with External Requirements

Measure	Organisation (* denotes agency status)									Mean
	1*	2*	3	4	5*	6	7*	8	9	
1	2	3	3	3	3	4	4	3	0	2.78
2	4	4	4	4	4	4	4	4	4	4.00
3	3	3	2	3	3	3	3	3	3	2.89
4	4	3	0	3	3	4	3	0	3	2.56
5	3	0	0	3	1	0	3	0	3	1.44
6	3	0	0	0	0	4	3	0	0	1.11
Mean	3.17	2.17	1.50	2.67	2.33	3.17	3.33	1.67	2.17	2.46

Assigned maturity ratings for PO8 Compliance with External Requirements varied from 0 (non-existent) to 4 (managed). No organisation was assigned a maturity rating of 5 (optimised) for any of the audit measures. The most commonly assigned maturity rating was 3 (defined) with 18 occurrences (50%).

4.3.7.2 Preliminary Discussion of Results for PO8 Compliance with External Requirements

Across individual audit measures the mean assigned maturity levels ranged from 1.11 for measure 6, *compliance of EDI processes with policies, procedures and contracts*, to 4.00 for measure 2, *reviews of safety and health and any necessary corrective actions*. Organisational approaches to occupational health and safety saw a maturity rating of 4 (managed) assigned across all organisations indicating a consistent approach to this external requirement. Audit measure 3, *compliance with documented privacy and security policies and procedures*, was also approached in a consistent manner across all organisations with a variation of only one level in maturity, as all organisations were assigned either level 2 (repeatable) or level 3 (defined).

4.3.7.3 Elimination of audit measures

With 10 responses (from a possible 18) of not applicable and thus assigned a maturity level of 0 (non-existent) audit measures five and six were considered by many of the managers to be irrelevant. Four organisations considered the question of insurance to be irrelevant, with one manager indicating the government chooses to be self-insured in most cases. Only four organisations indicated that organisational policies and insurance contracts were aligned with a fifth indicating that not much insurance was held in respect of IT. Six of the nine organisations did not have Electronic Document

Interchange (EDI) processes. One organisation had implemented a system to retrieve data from remote worksites and distribute this among various clients and contractors. This system was the nearest to an EDI described to the researcher. In view of the fact that the majority of organisations did not have insurance contracts in place or specific EDI processes there are grounds for eliminating these audit measures from the results.

4.3.7.4 Revised Assigned Maturity Ratings

The revised mean maturity levels, after removing audit measures 5 and 6, for PO8 Ensure Compliance with External Requirements are presented in Table 4.20. This table varies from Table 4.19 in that the mean assigned maturity ratings for individual organisations are consistently higher due to the elimination of maturity ratings of 0 in ten out of eighteen instances. The mean assigned maturity level for the entire control objective is also higher for the same reason.

Table 4.20: Revised Maturities for PO8 Ensure Compliance with External Requirements

Measure	Organisation (* denotes agency status)									Mean
	1*	2*	3	4	5*	6	7*	8	9	
1	2	3	3	3	3	4	4	3	0	2.78
2	4	4	4	4	4	4	4	4	4	4.00
3	3	3	2	3	3	3	3	3	3	2.89
4	4	3	0	3	3	4	3	0	3	2.56
Mean	3.25	3.25	2.25	3.25	3.25	3.75	3.50	2.50	2.50	3.06

4.3.7.5 Interpretation of Revised Results for PO8 Ensure Compliance with External Requirements

The assigned maturity ratings have not changed in their range, still varying from a low of 0 (non-existent) to a high of 4 (managed) with no rating of 5 (optimised) being assigned. The elimination of audit measures 5, *insurance contracts*, and 6, *EDI processes*, did not affect the mean assigned maturity levels of the remaining four audit measures.

The mean assigned maturity level for PO8 Ensure Compliance with External Requirements has been revised upward to 3.06. The maximum and minimum means for both audit measures and organisations along with the respective organisation and audit measure numbers (bracketed) are shown in Table 4.21.

Table 4.21: Maximum and Minimum Mean Assigned Maturity Levels for PO8 Ensure Compliance with External Requirements

	Lowest mean	Highest mean
Organisation	2.25 (3)	3.75 (6)
Measure	2.56 (4)	4.00 (2)

The frequency of assigned maturity levels against organisations is displayed graphically in Figure 4.5 and against audit measures in Figure 4.6.

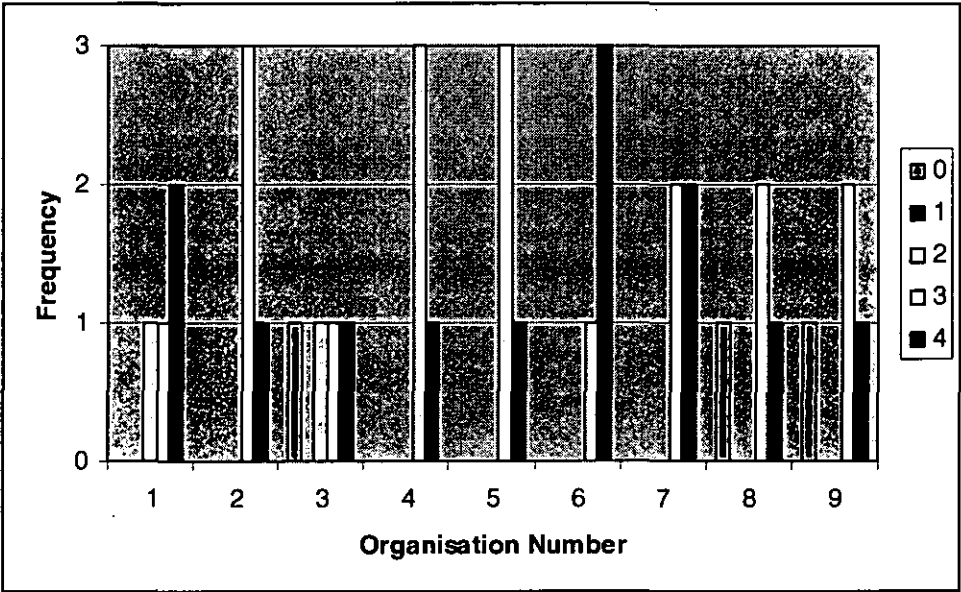


Figure 4.5: Frequency of Assigned Maturity Levels for PO8 Ensure Compliance with External Requirements

PO8 Ensure Compliance with External Requirements was one of the control objectives identified as being unique to the Tasmanian listing. After eliminating the audit measures that were considered to be not applicable in many organisations the mean assigned maturity level rose to above 3 (defined).

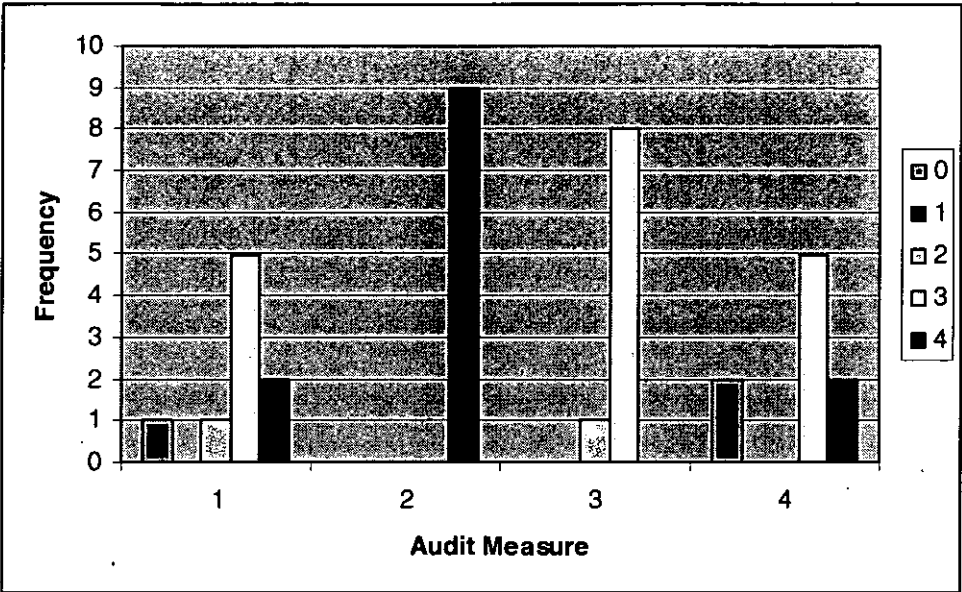


Figure 4.6: Frequency of Assigned Maturity Levels by Audit Measure for PO8 Ensure Compliance with External Requirements

4.3.8 Summary of Audit Results

The data discussed in Sections 4.3.1 to 4.3.7 above can be summarised and presented as in Table 4.22. This presents the control objectives in order of their mean assigned maturity level and shows the average mean maturity level for each organisation against each control objective.

The presentation of the number of observations indicates the number of audit measures for each control objective multiplied by a factor of 9. Clearly then DS12 has the greatest number of audit measures (20) while PO8 Ensure Compliance with External Requirements contains the least (4).

Table 4.22: Summary of Mean Assigned Maturity Level Data for All Control Objectives on the Audit Instrument

Measure	Organisation Number									Average	Std Dev	N
	1	2	3	4	5	6	7	8	9			
DS4 Average	3.57	3.57	3.57	3.71	3.43	3.86	3.86	3.57	2.71	3.54	0.74	63
DS12 Average	4.00	3.50	3.15	3.40	3.40	3.00	3.30	3.45	3.25	3.38	1.25	180
DS5 Average	3.50	3.92	2.08	3.08	3.50	3.17	3.50	3.33	2.83	3.21	1.25	108
PO8 Average	3.25	3.25	2.25	3.25	3.25	3.75	3.50	2.50	2.50	3.06	1.09	36
PO1 Average	2.75	2.63	2.75	3.13	3.00	2.88	2.75	2.88	2.13	2.76	0.59	72
AI6 Average	2.83	2.33	0.33	2.83	1.83	3.17	3.00	2.83	1.83	2.33	1.33	54
DS11 Average	2.56	2.22	2.33	3.00	1.44	2.61	2.22	2.61	1.94	2.33	1.34	162

4.3.9 Comparison with previous studies

In Chapter 3 it was stated that the results of this research would be compared with that of previous studies by both Guldentops *et al* (2002) and by Liu & Ridley (2005) and the self assessment project facilitated by the European Organisation of Supreme Audit Institutions (EUROSAI). The methodologies employed by the studies involved organisations assessing their own maturity against the COBIT maturity models for each of fifteen high level control objectives from the framework. The EUROSAI project used a rating system much the same as employed in the first phase of this study to determine the most important control objectives before self assessing maturity against ten to fifteen of the top rated objectives, depending on the ratings assigned by the individual organisations. Of the seven control objectives considered in the audit phase of this research, five were included in the both previous studies and the EUROSAI project. This comparison is provided while acknowledging certain limitations.

Unfortunately mean maturity levels were not available for the EUROSAI project and thus no comparison can be made at this level. The maturity level means of the common control objectives from each of the three studies are displayed in Table 4.23. Unweighted averages only are indicated for the international study data, as full statistics were not available. The international results relate to the public sector. The means are also graphically displayed in Figure 4.7.

Table 4.23: Maturity level means for common control objectives (source of Australian and International Data, Liu, 2003)

Control Objective	Mean and Standard Deviation for Maturity Level				
	Tasmania		Australia		International
	Mean	Std Dev	Mean	Std Dev	Mean
DS5	3.21	1.25	3.40	0.96	2.66
DS4	3.54	0.74	3.24	1.06	2.32
PO1	2.76	0.59	2.91	1.26	2.17
DS11	2.33	1.34	3.06	1.02	2.48
AI6	2.33	1.33	3.18	1.05	2.40

The control objectives in the table are listed in the order in which they appear on the ranked list from Phase One of this study. It can be seen that this does not entirely correspond with the mean assigned maturity level as the mean for DS4 Ensure Continuous Service is larger than that of DS5 Ensure Systems Security.

The standard deviations from this research are also interesting. Standard deviations are a measure of “spread” of data. The standard deviations for this research were lower than those from Liu (2003) for DS4 Ensure Continuous Service, and PO1 Define a Strategic Information Technology Plan, and higher than those from Liu (2003) for DS5 Ensure Systems Security, DS11 Manage Data and AI6 Manage Changes. The last two control objectives (DS11 Manage Data and AI6 Manage Changes) had the lowest mean assigned maturity levels. When comparing the two studies it is important to remember that this study obtained 25 responses, whereas Liu (2003) obtained 102 responses due to a larger scope. The smaller number of responses will impact on the any statistical analysis performed.

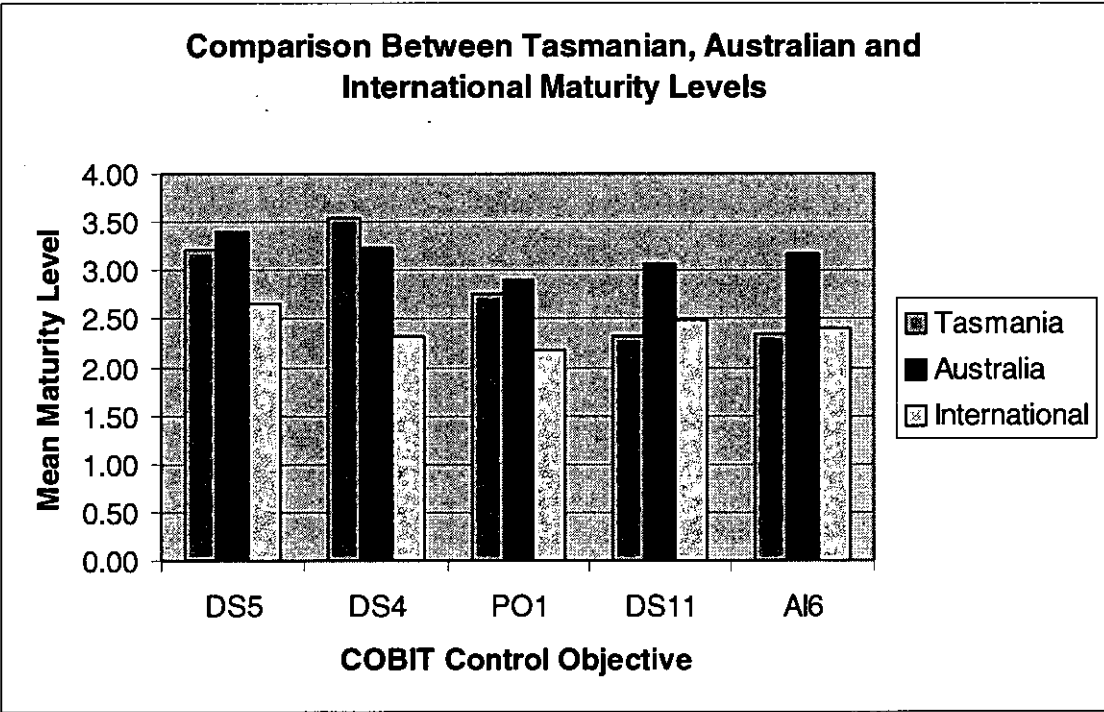


Figure 4.7: Comparison between Tasmanian, Australian and International Maturity Levels
(source data, current research, and Liu (2003))

DS5 Ensure Systems Security was rated as the most important control objective. The difference between the rating for DS5 Ensure Systems Security and DS4 Ensure Continuous Service was statistically significant (Section 4.2.3). The Tasmanian means were assessed as being lower for four out of the five control objectives (DS5, PO1, DS11, AI6) and lower than the international means for only two of the control objectives (DS11 and AI6).

When considering the mean assigned maturity levels the Tasmanian public sector can be considered to be performing best in DS4 Ensure Continuous Service, followed by DS5 Ensure Systems Security, PO1 Define a Strategic Information Technology Plan, and both DS11 Manage Data and AI6 Manage Changes with equal mean assigned maturity levels. For any system a continuity plan is essential in order to provide a reliable service to the user. These plans are usually well developed and practiced, this may account for the departure of the data from the expected. In contrast, security has only recently become a focus within the Tasmanian public sector, and then, only within specific sections of that sector. The organisations that were not required to have a security plan and policy in place outnumbered the agencies and could therefore adversely affect the mean assigned maturity level in this case.

4.3.9.1 Limitations

The maturity models used in the previous studies (Guldentops *et al*, 2002; Liu & Ridley, 2005) and in the EUROSAT project were specific to the individual control objectives being assessed. This gave specific guidance to the person undertaking the assessment as to what should be considered in each control objective. This study used a generic maturity model to assign maturity ratings to each of the audit measures. This generic model, while being the foundation of the specific maturity models used by the others, did not give as much specific guidance in terms of considerations to be made thus requiring a degree of interpretation by the researcher when assigning the maturity levels.

The assessment of maturity in the studies by Guldentops *et al* (2002) and Liu & Ridley (2005) was by individuals employed within the organisations being assessed. In this research the researcher assessed maturity using evidences obtained in the audit phase. Given the assessment was made by an independent third party it could be seen to be

more objective thus potentially lowering the assigned maturities. Moreover, the EUROSAT project the individuals participating in the assessments were, at least in part, trained auditors (EUROSAT, undated). It is anticipated that a greater degree of objectivity would be exercised by these professionals than by managers of organisations such as those who participated in the other studies. As noted above in Section 4.3.8, mean maturity ratings were not available for the EUROSAT project thus a comparison on this basis is not possible.

4.3.10 Evaluation of the Instrument

The instrument can be evaluated by using the criteria outlined in Section 3.8.

4.3.10.1 Duration of Audit Interviews

The longest audit interview was approximately 100 minutes. This is less than the projected maximum of 150 to 180 minutes. The ability to complete the audit interview within the specified time frame is considered to be one element in the validation of the derived audit instrument.

4.3.10.2 Independent Evaluation of Audit Instrument

The abbreviated instrument used for the conduct of IT audits was evaluated by the most senior external public sector IT auditor in Tasmania. There were very few suggested changes, all of which were implemented. The willingness of the auditor to organise the audit interviews was seen as further validation of the instrument.

4.3.10.3 Linkage of IT Process and Business Goals

Using the abbreviated instrument resulted in a direct linkage of the IT processes audited and the business goals of the organisations. This was evidenced by the requirement to produce organisational policy documents as well as through anecdotal evidence from the managers being interviewed.

4.3.10.4 Base of the Instrument

The instrument contained the seven most highly ranked control objectives from Phase One of the study. These rankings were obtained by summing the ratings for each

control objective. This ensured that the audit covered areas that were relevant and important to the organisations.

4.3.10.5 *Benchmarking*

The instrument includes measures obtained from two external sources, as well as from the COBIT Audit Guidelines. These sources were the TAO and the ANAO, both of which have active IT audit programs. The measures obtained from the ANAO program are considered to be validation of the audit instrument since they are mapped back to the individual detailed control objectives.

4.3.10.6 *Summary*

It can be seen that the derived audit instrument has been validated in many ways, both through practice and reference to external documents and practitioners.

Chapter 5 - Conclusion

5.1 Introduction

Chapter One outlined the basic motivation for the study and its aims and objectives. Chapter Two provided a background to the study by looking at the existing body of knowledge surrounding both corporate and IT governance, IT frameworks, with a focus on CobiT and the field of IT governance, with particular reference to both the Tasmanian and Australian public sectors. Chapter Three examined the methodology, under which the research was conducted, while Chapter Four presented and discussed the findings.

5.2 Research Objectives

This research set out to satisfy two objectives. The first was to identify the control objectives from the COBIT framework that were perceived by IT managers within Tasmanian public sector organisations as being important to their organisation at the time of the survey. From the most important processes an abbreviated audit instrument was to be developed and validated by a senior public sector IT audit professional. The second objective was to trial the abbreviated audit instrument on selected Tasmanian public sector organisations and subsequently evaluate its effectiveness.

The study addressed all the research objectives. The excellent response rate of 83% for the survey to determine the most important control objectives ensured that the results were representative of the whole population. The control objectives identified as being most important were drawn from three of the four broad domains in the COBIT framework (Planning and Organisation, Acquisition and Implementation, Delivery and Support and Monitoring, with the Monitoring domain seen as irrelevant. The control objective seen to be most important, DS5 Ensure Systems Security, was the same as that identified by prior national and international studies. The abbreviated instrument finally derived contained five control objectives identified by both the previous studies, and only two control objectives unique to the Tasmanian public sector. The control objectives common to both the previous studies and the final instrument used for audit in this study were:

DS5 Ensure Systems Security

DS4 Ensure Continuous Support

PO1 Define a Strategic Information Technology Plan

DS11 Manage Data

AI6 Manage Changes

The control objectives unique to the final audit instrument in this study were DS12 Manage Facilities and PO8 Ensure Compliance with External Requirements.

The audit instrument was evaluated by the most senior public sector IT external auditor in Tasmania. The quality and appropriateness of the instrument developed is evidenced by the very few amendments that were suggested before implementation and the authority given by the Tasmanian Audit Office to the researcher to undertake the audits. Furthermore the outcomes of this research will be used by the Tasmanian Audit Office to inform future IT audits in the Tasmanian public sector.

The trial audits showed that the instrument contained very few audit measures that were not relevant to the Tasmanian public sector. This is most likely because the selection process was appropriate. The validation of the TAO will also have assisted in this area. It also indicated that there was a wide variation in the approaches to IT governance within the sector. This can largely be attributed to the organisational size and type.

5.3 Research Significance

It is considered that the outcomes of this research will be of interest to both practitioners and academics.

5.3.1 Practitioners

Practitioner based COBIT literature can be considered from two perspectives, that of IT audit practitioners, and of IT professionals. Much of the existing literature published in the practitioner domain with respect to the COBIT framework and aimed at the IT professional is focused around implementation. It provides a sound methodology for identifying the most important control objectives in other public sector groupings.

For the IT audit practitioner the methodology used for deriving, validating and testing an abbreviated instrument will be of interest. Given that until recently only two public sector audit organisations within Australia had implemented COBIT based IT audit frameworks, it has the potential to be used by other public sector audit organisations to implement the COBIT framework. It also has the potential to be the basis for application to IT audits performed within an organisation by specialist IT audit practitioners.

For the Tasmanian Audit Office it provides a viable alternative to the existing audit program and a methodology to reassess the instrument at a future point, when it may no longer be as relevant because of environmental changes. It shows the most important IT processes and evaluates performance through seeking evidences. It also reveals which processes are done well as well as those not done well. Additionally it enables benchmarking between the processes with other public sector entities.

5.3.2 Academics

This research is of interest for researchers as it extends existing work providing a comparison with studies conducted both within Australia and in the international arena. It is of great value in this context as there are very few academic studies in the area. There are many reports of implementations but very few evaluations.

5.4 The Research Questions

The research questions identified were:

1. Which of the high level control objectives from the COBIT framework do Tasmanian public sector organisations perceive to be the most important?
2. How feasible is it to use an instrument derived from COBIT to conduct IT audits in the Tasmanian public sector?

These questions have been answered through the course of this document and are reviewed here.

The control objectives from the COBIT framework identified as being most important to Tasmanian public sector organisations are:

PO1 Define a Strategic Information Technology Plan
PO4 Define the Information Technology Organisation and Relationships
PO5 Manage the Information Technology Investment
PO6 Communicate Management Aims and Directions
PO8 Ensure Compliance with External Requirements
PO9 Assess Risks
AI2 Acquire and Maintain Application Technology
AI3 Acquire and Maintain Technology Infrastructure
AI5 Install and Accredited Systems
AI6 Manage Changes
DS4 Ensure Continuous Support
DS5 Ensure Systems Security
DS8 Assist and Advise Customers
DS9 Manage the Configuration
DS10 Manage Problems and Incidents
DS11 Manage Data
DS12 Manage Facilities

These 17 control objectives can be grouped in three tiers. Of these 17, eight were common to at both of the following sources, an international study by Guldentops et al (2002), a listing that was subsequently utilised by Liu & Ridley (2005) within Australia, or the EUROSAI self assessment project presentation (drawing results from Europe) as at February 2005. These eight control objectives were:

PO1 Define a Strategic Information Technology Plan
PO9 Assess Risks
AI2 Acquire and Maintain Application Technology
AI6 Manage Changes
DS4 Ensure Continuous Support
DS5 Ensure Systems Security
DS10 Manage Problems and Incidents
DS11 Manage Data

The following control objectives were common to both the current research and at least one of the above mentioned sources:

PO5 Manage the Information Technology Investment

AI5 Install and Accredited Systems

AI3 Acquire and Maintain Technology Infrastructure

The control objectives unique to the current study were drawn entirely from the domains of Planning and Organisation as well as Delivery and Support, indicating a focus within the Tasmanian public sector on these particular areas. It is important to note that objectives from the Monitoring domain were not perceived to be important with the highest rated control objective from that domain appearing at position 25 on the overall rankings; the next highest rated Monitoring control objective appeared at position 29, while the remaining two appeared in positions 33 and 34.

The use of the COBIT-derived instrument was also considered to be effective. A number of factors can be seen as evidence of this effectiveness. The audit instrument was benchmarked against the audit instrument of the Australian National Audit Office (ANAO). The audit instrument required only minor changes when it was validated by the most senior external IT auditor in the Tasmanian public sector. The audit instrument was tested through the conduct of nine audits on organisations ranging in size from government departments to local government bodies. The managers involved in these audits were positive about the instrument, with one even noting that the questions covered areas not previously covered in external audits. The ability of the researcher to conduct nine audits within three days indicates the size of the instrument is appropriate. The audit report that was prepared from the audit working papers was far more comprehensive than those prepared previously, with the Senior EDP Auditor from the TAO requesting copies of these reports to form part of the background information for formal IT audits conducted by that office.

References

ANAO, (2000) Australian National Audit Office Homepage accessed 12/7/2005 at <http://www.anao.gov.au/>

ANAO (2001) Untitled Speech Draft, accessed 27/10/2005 at: [http://www.anao.gov.au/website.nsf/publications/4a256ae90015f69b4a256ae9007d73d8/\\$file/acag%20handout%20at%205%20october.doc](http://www.anao.gov.au/website.nsf/publications/4a256ae90015f69b4a256ae9007d73d8/$file/acag%20handout%20at%205%20october.doc)

ANAO (2004) Auditing in an Evolving Environment (A Focus on Auditing Standards and Framework), address to the Institute of Certified Public Accountants and CPA Australia, CPA Forum 2004 accessed 12/7/2005 at: <http://www.anao.gov.au/WebSite.nsf/Publications/1164451EDE34619DCA256EF3000152DC>

ANAO (2005) Interim Phase of the Audit of Financial Statements of General Government Sector Entities for the Year Ending 30 June 2005, Audit report No 56 2004-2005 accessed 12/7/2005 at <http://www.anao.gov.au/WebSite.nsf/Publications/A13BF977D6FF7E2CCA257027007C715A>

Anthes, G. H. (2004) Model Mania, *Computerworld*, Vol 38, No. 10, pp41 – 45.

Australian Stock Exchange, (2003) Principles of Good Corporate Governance and Best Practice Recommendations, accessed 24/05/2005 at <http://www.shareholder.com/visitors/dynamicdoc/document.cfm?documentid=364&companyid=ASX>

Avison, D. E., & Fitzgerald, G. (1995). *Information Systems Development: Methodologies, Techniques and Tools*, 2nd edition, McGraw Hill, Maidenhead, England.

Baruch, Y (1999) Response rate in academic studies – A comparative analysis, *Human Relations*, Vol 52, No 4, pp 421 - 438

Broadbent, M. (2003) The Right Combination, *CIO*, 11/4/2003 accessed 13/7/2005 at <http://www.cio.com.au/index.php?id=1043227491>

Broadbent, M. and Weill, P. (1998) *Leveraging the New Infrastructure* Harvard Business School Press

- Burn, J.M. and Szeto, C. (2000) A comparison of the views of business and IT management on success factors for strategic alignment, *Information & Management*, Vol 37, No 4, pp 197 - 216
- Chua, W. F. (1986) Radical Developments in Accounting Thought, *The Accounting Review*, Vol 61, No 4 pp 601 – 632.
- Cooper, D. R. & Schindler, P. S. (2003). Business Research Methods, 8th edition, McGraw Hill, New York.
- Drucker P. (1989) The futures that have already happened, *The Economist*, Vol 313, No 7625, p 27
- Epstein, M. J. & Rejc, A. (2005) How to measure and improve the value of IT, *Strategic Finance*, Vol 87, No 4 pp 34 - 41
- EUROSAI (undated) *EUROSAI Institutional Information* webpage, accessed 12/7/2005 at http://www.eurosai.org/Ingles/info_inst.htm
- EUROSAI IT Working Group (undated a) IT Self Assessment Flyer, accessed 11/07/2005 at http://www.eurosai-it.org/9282000/d/flyer_it.pdf
- EUROSAI IT Working Group (2005) *IT Self Assessment Project, Current Results and Next Steps*, presentation by Michel Huissoud, Cyprus, 14 February, 2005
- Guldentops, E., (2003) Governing Information Technology through COBIT. In W. Van Grembergen (Ed.), *Strategies for Information Technology Governance*. Hershey, PA: Idea Group Publishing.
- Guldentops, E., van Grembergen, W., and de Haes, S., (2002) Control and governance maturity survey: Establishing a reference benchmark and a self-assessment tool, *Information Systems Control Journal*, Vol 6, 2002.
- Guba, E.G., (1990) The Alternative Paradigm Dialog, in *The Paradigm Dialog*, E.G. Guba (ed) Sage, Newbury Park, USA.

Hirschheim, R. A. (1992) Information Systems Epistemology: An Historical Perspective, in *Information Systems Research: Issues, methods and Practical Guidelines* Galliers, R. Oxford: Blackwell Scientific Publications: pp 28 – 60 accessed 14/6/2005 at <http://www.bauer.uh.edu/rudy/ISEpistemology.pdf>

ITGI (2000) CobiT: Governance, Control and Audit for Information and Related Technology, as cited by van Grembergen, W, de Haes, S. and Guldentops, E., (2004) Structures, Processes and Relational Mechanisms for IT Governance. . In W. Van Grembergen (Ed.), *Strategies for Information Technology Governance*. Hershey, PA: Idea Group Publishing.

ITGI (2000a) CobiT 3rd Edition Framework, available online at http://www.isaca.org/Template.cfm?Section=Obtain_COBIT

ITGI (2000b) CobiT 3rd Edition Control Objectives, available online at http://www.isaca.org/Template.cfm?Section=Obtain_COBIT

ITGI (2000c) COBIT 3rd Edition Management Guidelines, available online at http://www.isaca.org/Template.cfm?Section=Obtain_COBIT

ITGI (2000d) CobiT 3rd Edition Audit Guidelines, available online (for audit professionals) at http://www.isaca.org/Template.cfm?Section=Obtain_COBIT

ITGI (2000e) CobiT 3rd Edition Executive Summary, available online at http://www.isaca.org/Template.cfm?Section=Obtain_COBIT

ITGI (2003) Board Briefing on IT Governance. Accessed online 13/7/2005 at: http://www.itgi.org/Template_ITGI.cfm?Section=Recent_Publications&CONTENTID=15994&TEMPLATE=/ContentManagement/ContentDisplay.cfm

KPMG, Belgium (2005) Corporate Governance, KPMG Belgium accessed 19/9/2005 at: www.kpmg.be/index.thtml/en/Topics/Corpgov/

Lateline (segment: Clinton tackles world poverty at IT talks) 2002, television program, ABC television, Sydney, 28 February

- Liu, Q (1993) A Preliminary Benchmark of IT Control in the Australian Public Sector, MIS thesis, University of Tasmania
- Liu, Q., and Ridley, G., (2005) IT Control in the Australian Public Sector: An International Comparison, *Proceedings of European Conference on Information Systems*, Regensburg, Germany, May 26 - 28, 2005
- Lodh S.C. & Gaffikin M.J.R (1997) Critical Studies in Accounting Research, Rationality and Habermas: A Methodological Reflection, *Critical Perspectives on Accounting*, vol. 8, no. 5, pp. 433-474(42), accessed 20/6/2005 at <http://panopticon.csustan.edu/cpa96/pdf/lodh.pdf>
- McMillan, K.P. (1998), The Science of Accounts: Bookkeeping Rooted in the Ideal of Science, *The Accounting Historians Journal*, Vol 25, No 2, p 1.
- Office (1887), Mathematical Elucidation of Accounts, Vol 2 No 13: 103. Packard, S. S, (1991), Philosophy in Book-keeping", *Book-keeper*, Vol 3, No 33: 131-132; reprint, see Brief (1989).
- Orlikowski, W.J. and Baroudi, J.J. (1991) Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research* 2:1 pp 1 – 28
- Owen, N. (2003) Report of the HIH Royal Commission, accessed online on (19/11/2005) at: www.hihroyalcom.gov.au/finalreport/index.htm
- Peterson, R.R. (2003). Information Strategies and tactics for Information Technology governance. In W. Van Grembergen (Ed.), *Strategies for Information Technology Governance*. Hershey, PA: Idea Group Publishing.
- Ridley, G., & Keen, C. (1998) Epistemologies in Use in Information Systems Research: Divergence or Change? *Proceedings of the Ninth Australasian Conference on Information Systems*, pp 847 - 849 Accessed 14/6/2005 at http://is.lse.ac.uk/Support/AMCIS/AMCIS1998/pdffiles/papers/t20_14.pdf

Ridley, G. Young, J. and Carroll, P. (2004) "COBIT and its Utilization: A framework from the literature", *Proceedings of the 27th Hawaii International Conference on System Science (HICSS)*, 5 – 8 Jan., Big Island, Hawaii, 2004.

Schliefer, A. and Vishny, R.W. (1997) A Survey of Corporate Governance, *Journal of Finance*, Vol 52, No 2, pp 737 – 783 accessed 26//2005 at <http://links.jstor.org/sici?sici=0022-1082%28199706%2952%3A2%3C737%3AASOCG%3E2.0.CO%3B2-V>

Spafford, G. (2003) "The Benefits of Standard IT Governance Frameworks", on Datamation Internet website, last viewed 21 March 2005, available at: <http://itmanagement.earthweb.com/netsys/article.php/2195051>

Standards Australia (2003) AS 8000 – 2003 Australian Standard on Good Governance Principles accessed online at <http://online.standards.com.au/online/autologin.asp>

Standards Australia (2005) AS 8015 - 2005 Australian Standard on Corporate Governance of Information and Communication Technology accessed online at <http://online.standards.com.au/online/autologin.asp>

TAO (2004) Tasmanian Audit Office webpage "Who We Are and What We Do" accessed 12/7/2005 at <http://www.audit.tas.gov.au/aboutus/whowhat.html>

Ticehurst, G. W. & Veal, A. J. (2000). *Business Research Methods: A Managerial Approach*, Addison Wesley Longman, Australia.

Trochim, W. M. K. (1999) Research Methods Knowledge Base. Accessed 14/6/2005 at <http://trochim.human.cornell.edu/kb.positivsm.htm>

University of New England School of Psychology (2000) WebStat: Chapter 7 Analysing Data Part IV: Analysis of Variance, University of New England School of Psychology, viewed 26/9/2005 at http://www.une.edu.au/WebStat/unit_materials/c7_anova/oneway_bonferroni_adjust.htm

van Grembergen, W. (2002). Introduction to the Minitrack: IT governance and its Mechanisms. *Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS)*

van Grembergen, W, De Haes, S. and Guldentops, E., (2004) Structures, Processes and Relational Mechanisms for IT Governance. In W. Van Grembergen (Ed.), *Strategies for Information Technology Governance*. Hershey, PA: Idea Group Publishing.

Violino, B., (2005) IT Frameworks Demystified, *Network World*, Vol 22, No 7, pp S18 – 20.

Winter, G. A (2000). Comparative Discussion of the Notion of ‘Validity’ in Qualitative and Quantitative Research, *The Qualitative Report*, Vol 4, No.s 3/4, accessed 10/6/2005 at <http://www.nova.edu/ssss/AR/AR4-3/winter.html>

Appendix A - CobiT Primary Reference Material

COSO: Committee of Sponsoring Organisations of the Treadway Commission. *Internal Control — Integrated Framework*. 2 Vols. American Institute of Certified Accountants, New Jersey, 1994.

OECD Guidelines: Organisation for Economic Co-operation and Development. *Guidelines for the Security of Information*, Paris, 1992.

DTI Code of Practice for Information Security Management: Department of Trade and Industry and British Standard Institute. *A Code of Practice for Information Security Management*, London, 1993, 1995.

ISO 9000-3: International Organisation for Standardisation. *Quality Management and Quality Assurance Standards — Part 3: Guidelines for the Application of ISO 9001 to the development, supply and maintenance of software*, Switzerland, 1991.

An Introduction to Computer Security: The NIST Handbook: NIST Special Publication 800-12, National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, 1995.

ITIL IT Management Practices: Information Technology Infrastructure Library. Practices and guidelines developed by the Central Computer and Telecommunications Agency (CCTA), London, 1989.

IBAG Framework: Draft Framework from the Infosec Business Advisory Group to SOGIS (Senior Officials Group on Information Security, advising the European Commission), Brussels, 1994.

NSW Premier's Office Statements of Best Practices and Planning Information Management and Techniques: *Statements of Best Practice #1 through #6*. Premier's Department New South Wales, Government of New South Wales, Australia, 1990 through 1994.

Memorandum Dutch Central Bank: *Memorandum on the Reliability and Continuity of Electronic Data Processing in Banking*. De Nederlandsche Bank, Reprint from Quarterly Bulletin #3, Netherlands, 1998.

EDPAF Monograph #7, EDI: An Audit Approach: Jamison, Rodger. *EDI: An Audit Approach*, Monograph Series #7, Information Systems Audit and Control Foundation, Inc., Rolling Meadows, IL, April 1994.

PCIE (President's Council on Integrity and Efficiency) Model Framework: A Model Framework for Management Over Automated Information Systems. Prepared jointly by the President's Council on Management Improvement and the President's Council on Integrity and Efficiency, Washington, DC, 1987.

Japan Information Systems Auditing Standards: Information System Auditing Standard of Japan. Provided by the Chuo Audit Corporation, Tokyo, August 1994.

CONTROL OBJECTIVES Controls in an Information Systems Environment: Control Guidelines and Audit Procedures: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Fourth Edition, Rolling Meadows, IL, 1992.

CISA Job Analysis: Information Systems Audit and Control Association Certification Board. "Certified Information Systems Auditor Job Analysis Study," Rolling Meadows, IL, 1994.

IFAC International Information Technology Guidelines—Managing Security of Information: International Federation of Accountants, New York, 1998.

IFAC International Guidelines on Information Technology Management—Managing Information Technology Planning for Business Impact: International Federation of Accountants, New York, 1999.

Guide for Auditing for Controls and Security, A System Development Life Cycle Approach: *NIST Special Publication 500-153*: National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, 1988.

Government Auditing Standards: US General Accounting Office, Washington, DC, 1999.

SPICE: Software Process Improvement and Capability Determination. A standard on software process improvement, British Standards Institution, London, 1995.

Denmark Generally Accepted IT Management Practices: The Institute of State Authorized Accountants, Denmark,

DRI International, Professional Practices for Business Continuity Planners: Disaster Recovery Institute International. *Guideline for Business Continuity Planners*, St. Louis, MO, 1997.

IIA, SAC Systems Audibility and Control: Institute of Internal Auditors Research Foundation, *Systems Audibility and Control Report*, Altamonte Springs, FL, 1991, 1994.

IIA, Professional Practices Pamphlet 97-1, Electronic Commerce: Institute of Internal Auditors Research Foundation, Altamonte Springs, FL, 1997.

E & Y Technical Reference Series: Ernst & Young, *SAP R/3 Audit Guide*, Cleveland, OH, 1996.

C & L Audit Guide SAP R/3: Coopers & Lybrand, *SAP R/3: Its Use, Control and Audit*, New York, 1997.

ISO IEC JTC1/SC27 Information Technology — Security: International Organisation for Standardisation (ISO) Technical Committee on Information Technology Security, Switzerland, 1998.

ISO IEC JTC1/SC7 Software Engineering: International Organisation for Standardisation (ISO) Technical Committee on Software Process Assessment. *An Assessment Model and Guidance Indicator*, Switzerland, 1992.

ISO TC68/SC2/WG4, Information Security Guidelines for Banking and Related Financial Services: International Organisation for Standardisation (ISO) Technical Committee on Banking and Financial Services, Draft, Switzerland, 1997.

Common Criteria and Methodology for Information Technology Security Evaluation: CSE (Canada), SCSSI (France), BSI (Germany), NLNCSA (Netherlands), CESG (United Kingdom), NIST (USA) and NSA (USA), 1999.

Recommended Practice for EDI: EDIFACT (EDI for Administration Commerce and Trade), Paris, 1987.

TickIT: *Guide to Software Quality Management System Construction and Certification.* British Department of Trade and Industry (DTI), London, 1994

ESF Baseline Control—Communications: European Security Forum, London. *Communications Network Security*, September 1991; *Baseline Controls for Local Area Networks*, September, 1994.

ESF Baseline Control—Microcomputers: European Security Forum, London. *Baseline Controls Microcomputers Attached to Network*, June 1990.

Computerized Information Systems (CIS) Audit Manual: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Rolling Meadows, IL, 1992.

Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1): US General Accounting Office, Washington, DC 1999.

Guide for Developing Security Plans for Information Technology: NIST Special Publication 800-18, National Institute for Standards and Technology, US Department of Commerce, Washington, DC, 1998.

Financial Information Systems Control Audit Manual (FISCAM): US General Accounting Office, Washington, DC, 1999.

BS7799-Information Security Management: British Standards Institute, London, 1999.

CICA Information Technology Control Guidelines, 3rd Edition: Canadian Institute of Chartered Accountants, Toronto, 1998.

ISO/IEC TR 1335-n Guidelines for the Management of IT Security (GMITS), Parts 1-5: International Organisation for Standardisation, Switzerland, 1998.

AICPA/CICA SysTrust™ Principles and Criteria for Systems Reliability, Version 1.0: American Institute of Certified Public Accountants, New York, and Canadian Institute of Chartered Accountants, Toronto, 1999.

Appendix B – Ethics Approval for Project



HUMAN RESEARCH ETHICS COMMITTEE (TASMANIA) NETWORK

MINIMAL RISK APPLICATION APPROVAL

8 June 2005

Dr Gail Ridley
Information Systems
Private Bag 87
Hobart

H8399:

An investigation of the application of the Control Objectives for Information and Related Technologies (COBIT) framework in the Tasmanian public sector.

Dear Dr Ridley

Acting on a mandate from the Tasmania Social Sciences HREC, the Chair of the committee considered and approved the above project on 08 June 2005. When the second stage of study is submitted and a questionnaire is developed, this is to be presented to ethics office as an Amendment to existing project file.

All committees operating under the Human Research Ethics Committee (Tasmania) Network are registered and required to comply with the *National Statement on the Ethical Conduct in Research Involving Humans 1999* (NHMRC guidelines).

Therefore, the Chief Investigator's responsibility is to ensure that:

- 1) All researchers listed on the application comply with HREC approved application.
- 2) Modifications to the application do not proceed until approval is obtained in writing from the HREC.
- 3) The confidentiality and anonymity of all research subjects is maintained at all times, except as required by law.
- 4) Clause 2.37 of the National Statement states:
An HREC shall, as a condition of approval of each protocol, require that researchers immediately report anything which might warrant review of ethical approval of the protocol, including:
 - a) *Serious or unexpected adverse effects on participants;*
 - b) *Proposed changes in the application; and*
 - c) *Unforeseen events that might affect continued ethical acceptability of the project.*

The report must be lodged within 24 hours of the event to the Ethics Executive Officer who will report to the Chairs.

- 5) All participants must be provided with the current Information Sheet and Consent form as approved by the Ethics Committee.
- 6) The Committee is notified if any Investigators are added to, or cease involvement with, the project.
- 7) This study has approval for four years contingent upon annual review. An *Annual Report* is to be provided on the anniversary date of your approval. Your first report is due 08 June 2006. You will be sent a courtesy reminder by email closer to this due date.
Clause 2.35 of the National Statement states:
As a minimum an HREC must require at regular periods, at least annually, reports from principal researchers on matters including:
 - a) *Progress to date or outcome in case of completed research;*
 - b) *Maintenance and security of records;*
 - c) *Compliance with the approved protocol, and*
 - d) *Compliance with any conditions of approval.*
- 8) A *Final Report* and a copy of the published material, either in full or abstract, must be provided at the end of project.

Yours sincerely



for Amanda McAulley
(Executive Officer)

Appendix C – Information Sheet for Phase One



Information Sheet

Title

An investigation of the application of the *Control Objectives for Information and Related Technologies* (COBIT) framework in the Tasmanian public sector.

COBIT is an Information Technology (IT) control framework designed to assist organisations in the management of IT.

Chief Investigator

Dr Gail Ridley, School of Information Systems, University of Tasmania.

Primary Researcher

Lynne Gerke, Honours student, School of Information Systems, University of Tasmania.

Purpose of this study

The first objective of this study is to determine the importance of each of the 34 high level control objectives from the COBIT framework to large Tasmanian public sector organisations. A survey will be used to achieve this purpose, in which the public sector organisations will be asked to rank the control objectives. A second objective is to investigate the feasibility of undertaking an audit of those objectives perceived by the majority of organisations to be the most important.

Benefits of this study

The results of this study will indicate whether it is feasible for the Tasmanian Audit Office (TAO) to use COBIT to streamline IT audits in the Tasmanian government, which will benefit both the TAO and the organisations.

The findings will be of interest to both academics and practitioners. The results will enable a comparison with an international study, allowing an understanding of whether the control objectives can be universally ranked, or whether there are differences along geographical and business sector lines.

As a consequence of the involvement of the Tasmanian Audit Office in this study, it is likely that the results will be of interest to public sector audit authorities both within Australia and internationally.

Study procedures

Your organisation has been selected to take part in this study based on its size, and relationship with the Tasmanian Audit Office. The questionnaire and related documentation have been forwarded by the TAO, and the researchers have not been provided with any private contact details by the TAO. Participation in this study is entirely voluntary. If your organisation is willing to participate, please complete the enclosed questionnaire, which is expected to take approximately 10 minutes to complete by your internal IT auditor, or equivalent officer. For your convenience, a reply paid, self addressed envelope is provided for the return of the questionnaire. As the first phase of the study does not require you to identify you or your organisation, the identity of the survey respondents will not be known from the responses

The second phase of the study is an audit of the control objectives perceived to be the most important across all the responding organisations. The number of organisations to be approached for the second phase of the study, and the identity of the organisations to be selected, will not be known until after the results of the first phase are known, as the decision will depend upon how many control objectives are considered to be the most important and the

nature of those selected. For example, if only a few of the control objectives are highly ranked, and those control objectives will require only a brief time to investigate, then it is likely that all the organisations involved in the first phase will be approached for the second phase. If your organisation is selected to participate in the second phase of the study, you will be approached a second time, seeking your involvement. Although your organisation will be known from the second phase of the study, neither you or your organisation will be identifiable from any publications arising from either phase of the study, as the results will be aggregated.

Confidentiality

Any information you provide will be treated in the strictest confidence. The only people who will have access to the questionnaires will be the Chief Investigator and the Primary Researcher. The electronic form of the data will be stored on a secured computer server within the School of Information Systems. These files will be password protected to prevent unauthorised access. The completed questionnaires will be secured in locked storage accessible only by the Chief Investigator and the Primary Researcher. The data relating to the first phase of the study will be kept for five years, after which it will be destroyed under appropriate supervision.

Note that working papers from the second audit phase of the study will be shared with the Tasmanian Audit Office, as the primary researcher will be acting as an agent of the TAO.

Contact Persons

The contact persons for questions relating to this study are:

Dr Gail Ridley	03 6336 6275	Gail.Ridley@utas.edu.au	University of Tasmania
Lynne Gerke	0409 238 499	lgerke@utas.edu.au	University of Tasmania
Christina Buell	03 6226 0100	C.Buell@audit.tas.gov.au	Tasmanian Audit Office

Approval

This research has received ethical approval from the Human Research Ethics Committee (Tasmania) Network. If you have any concerns of an ethical nature about this research you can contact the Executive Officer of the Human Research Ethics Committee (Tasmania) Network, Amanda McAully (Ph 03 6226 2763).

Results of this investigation

The overall results of the study will be compiled as part of the Honours Dissertation to be finalised in November 2005. Access to the findings of the study can be obtained by making a request to Lynne Gerke, using the contact details provided above.

Signature of Chief Investigator

Signature of Primary Researcher/Student

Dr Gail Ridley

Lynne Gerke

Appendix D – Information Sheet for Phase Two

**Information Sheet**

An investigation of the application of the *Control Objectives for Information and Related Technologies* (COBIT) framework in the Tasmanian public sector.

COBIT is an Information Technology (IT) control framework designed to assist organisations in the management of IT.

Chief Investigator

Dr Gail Ridley, School of Information Systems, University of Tasmania.

Primary Researcher

Lynne Gerke, Honours student, School of Information Systems, University of Tasmania.

The objective of this phase of the study is to investigate the feasibility of undertaking an audit of control objectives, from the COBIT framework, that were perceived by the majority of organisations in Phase 1 of the study to be the most important. The study is being undertaken as part of the requirements for an honours degree in Information Systems.

The results of this phase of the study will indicate whether it is feasible for the Tasmanian Audit Office (TAO) to derive from COBIT a framework for IT audits in the Tasmanian government, which will benefit both the TAO and the organisations.

The research findings will be of interest to both academics and practitioners. The results will enable a comparison with an international study, allowing an understanding of whether the control objectives can be universally ranked, or whether there are differences along geographical and business sector lines. As a consequence of the involvement of the Tasmanian Audit Office in this study, it is likely that the results will be of interest to public sector audit authorities both within Australia and internationally.

Your organisation has been selected to take part in this study based on its size and relationship with the Tasmanian Audit Office. This phase of the study is an IT audit of the control objectives from the COBIT framework perceived to be the most important across all the responding organisations. It is planned that the audit will be conducted within your organisational offices, with the assistance of an IT employee of your organisation. A paper based record of the audit results will be made.

Your organisation participated in the first phase of this study, in which the most important control objectives were identified. The number of organisations to be approached for Phase 2 of the study, the duration of the IT audit and the identity of the organisations to be selected, were dependent on the results of Phase 1, as they were determined by how many control objectives were considered to be the most important and the nature of those selected. However, as the questionnaires from Phase 1 were returned anonymously, your organisation's individual ranking of the control objectives is not known. Although your organisation will be known from undertaking Phase 2 of the study, neither you nor your organisation will be identifiable from any publications produced by the researchers arising from either phase of the study, as the results will be aggregated. No payment will be made for your involvement in the study.

No personal risks to the participants are anticipated as a result of involvement in the study. Some of the information obtained during the study may be viewed as sensitive to the organisation if disclosed. However, procedures taken to ensure confidentiality and protection of information, as described below, have been designed to reduce the risk of any adverse consequences.

Any information you provide will be treated in the strictest confidence. The only people who will have access to the working papers from the audit will be the Chief Investigator, the Primary

Researcher, and the Tasmanian Audit Office. Working papers from this audit phase of the study will be shared with the Tasmanian Audit Office, as this study has support from the TAO. The electronic form of the data will be stored on a secured computer server within the School of Information Systems. These files will be password protected to prevent unauthorised access. The data will be kept by the University of Tasmania for five years, after which it will be destroyed under appropriate supervision. The Tasmanian Audit Office will keep documentation relating to audit for seven years before destruction under appropriate supervision.

Contact Persons

The contact persons for questions relating to this study are:

Dr Gail Ridley	03 6336 6275	Gail.Ridley@utas.edu.au	University of Tasmania
Lynne Gerke	0409 238 499	lbgerke@utas.edu.au	University of Tasmania
Christina Buell	03 6226 0100	C.Buell@audit.tas.gov.au	Tasmanian Audit Office

This research has received ethical approval from the Human Research Ethics Committee (Tasmania) Network. If you have any concerns of an ethical nature about this research you can contact the Executive Officer of the Human Research Ethics Committee (Tasmania) Network, Amanda McAully (Ph 03 6226 2763).

The overall results of the study will be compiled as part of the Honours Dissertation to be finalised in November 2005. Access to the findings of the study can be obtained by making a request to Lynne Gerke, using the contact details provided above.

Note that although your participation is entirely voluntary, and you may withdraw from the study at any time without effect or explanation, you will be asked to sign a separate consent form if you agree to participate. You should retain this Information Sheet.

Signature of Chief Investigator

Signature of Primary Researcher/Student

Dr Gail Ridley

Lynne Gerke

Appendix E – Statement of Informed Consent for Phase Two

**CONSENT FORM**

An investigation of the application of the Control Objectives for Information and Related Technologies (COBIT) framework in the Tasmanian public sector (Phase 2).

1. I have read and understood the 'Information Sheet' for this study.
2. The nature and possible effects of the study have been explained to me.
3. I understand that this phase of the study involves the following procedures: an audit of several Information Technology control objectives within my organisation
4. I understand that the following risks are involved: data collected during this phase of the study may be considered to be sensitive for my organisation. However, only the researchers and the Tasmanian Audit Office will have access to the data that will be securely stored. Publications deriving from the research will not identify individuals or your organisation, and will report aggregated data.
5. I understand that all research data will be securely stored on the University of Tasmania premises for a period of 5 years. The data will be destroyed at the end of 5 years. I understand that this phase of the study is an IT audit by the researcher with the support of the Tasmanian Audit Office and that working papers relating to this audit will be shared with the Tasmanian Audit Office.
6. Any questions that I have asked have been answered to my satisfaction.
7. I agree that research data gathered for the study may be published (provided that neither I nor my organization can be identified as a participant).
8. I understand that my identity will be kept confidential and that any information I supply to the researcher(s) will be used only for the purposes of the research study.
9. I agree to participate in this investigation and understand that I may withdraw at any time without any effect, and if I so wish, may request that any personal data gathered be withdrawn from the research.

Name of participant _____

Signature of participant _____ Date _____

Statement by investigator:

10. I have explained this project and the implications of participation in it to this volunteer and I believe that the consent is informed and that he/she understands the implications of participation.

Name of investigator _____

Signature of investigator _____ Date _____

Appendix F – Copyright Permission for use of COBIT Control Objectives



3701 ALGONQUIN ROAD, SUITE 1010

TELEPHONE:

ROLLING MEADOWS, ILLINOIS 60008, USA

847.253.1545

FACSIMILE:

847.253.1443

Web Site: www.isaca.org

26 July 2005

Lynne Gerke
University of Tasmania
GPO Box 252-87
Hobart Tas 7001
Australia

Dear Lynn:

Thank you for your email dated 26 July requesting permission to use the high level Control Objectives from COBIT: *Control Objectives for Information and related Technology* as the basis for a questionnaire to collect and analyze data for your university honors dissertation. Permission is granted given the following requirements:

1. Permitted use is limited to the 34 high level Control Objectives from COBIT solely for conducting research, collecting data and writing your honors dissertation as referenced in your email, a copy of which is attached hereto. Permission also includes that right to incorporate the Control Objectives in the accompanying reference guide to your research solely as it relates to your academic studies.
2. Permission does not extend to any non-academic or commercial purposes nor does it include the right to grant others permission to photocopy or otherwise reproduce, redistribute or sell this material.
3. The dissertation must include the following attribution: "Includes excerpts from COBIT: *Control Objectives for Information and Related Technology* (3rd Edition). ©1996, 1998, 2000 IT Governance Institute (ITGI). All rights reserved. COBIT is a registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute. Used by permission."
4. This permission is for the English language only.
5. This permission does not include any rights to make commercial and/or educational presentations incorporating this material beyond the uses stated above.

6. Should any of the above limitations be breached, this permission is automatically be revoked as of the date of the breach.

We appreciate your support and interest of the IT Governance Institute and wish you much success in the completion of your dissertation in information systems.

If you have any questions regarding permissions, please call me at 847-253-1545, ext. 457 or contact me by e-mail jskiba@isaca.org.

Sincerely,

Joann Skiba
Director, IP & Business Product Development

cc: Dr. Gail Ridley, University of Tasmania

Appendix G – Questionnaire, Phase One

COBIT Survey

**Use of the Control Objectives for Information
and Related Technologies (COBIT) framework
for IT audits in the Tasmanian Public Sector**



School of Information Systems
University of Tasmania
Hobart TAS 7001
Phone (03) 6226 6200
Fax (03) 6226 6211

The Control Objectives for Information and Related Technologies (COBIT) framework forms the basis for Part 2 of this questionnaire. COBIT is an Information Technology (IT) control framework designed to assist organisations in the management of IT.

This questionnaire collects information about you, the respondent, and your organisation. The information from Part 1 will be used to examine whether factors such as your position and length of service affect the way in which the control objectives are rated. The information gathered from Part 2 will be used to compile a set of the high level control objectives from the COBIT framework that are seen as the most relevant to public sector organisations within Tasmania. This can then be used as the basis for a comparison with studies done both globally and also in Europe. The information will also be used to form an abbreviated instrument from the COBIT framework that may subsequently be used by the Tasmanian Audit Office as a basis for Information Technology audits.

Includes excerpts from COBIT: *Control Objectives for Information and Related Technology* (3rd Edition). ©1996, 1998, 2000 IT Governance Institute (ITGI). All rights reserved. COBIT is a registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute. Used by permission.

Part 1 Demographic Details

Q1. Which of the following best describes the function of your organisation in the public sector? *(Please tick one box)*

- ☐ Government Department (*Example Department of Education*)
- ☐ Government Agency (*Example Tasmanian Industrial Commission*)
- ☐ Government Owned Company/Public Trading Enterprise (*Example Hydro Tasmania*)

Q2. What is your position in your organisation? *(Please tick one box)*

- ☐ CEO
- ☐ CIO
- ☐ IT/IS Director
- ☐ IT/IS Manager
- ☐ Business Manager
- ☐ Other (Please specify) _____

The following scale should be used in completing questions 3 and 4 of Part A only.

- 1 Very unfamiliar
- 2 Unfamiliar
- 3 Neither familiar nor unfamiliar
- 4 Familiar
- 5 Very familiar

Q3. How familiar are you with the IT processes in your organisation? *(Please tick one box)*

- | | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 1 | 2 | 3 | 4 | 5 |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Q4. How familiar are you with the business objectives of your organisation? *(Please tick one box)*

- | | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 1 | 2 | 3 | 4 | 5 |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Part 2 Control over IT processes

With respect of their importance to your organisation, please rate the following 34 control objectives by ticking the appropriate box on the scale. The descriptions of the scale are outlined below. The control objectives cover four domains, planning and organisation, acquisition and implementation, delivery and support, and monitoring.

The scale:

N	Not sure	3	Neither important nor unimportant
1	Very unimportant	4	Important
2	Unimportant	5	Very important

Planning and Organisation (PO)

PO1. Define a strategic IT plan with the business goal of striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PO2. Define the information architecture with the business goal of optimising the organisation of the information systems. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PO3. Determine the technological direction with the business goal of taking advantage of available and emerging technology to drive and enable business strategy. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PO4. Define the IT organisation and relationships with the business goal of delivering the right IT services. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PO5. Manage the IT investment with the business goal of ensuring funding and controlling disbursement of financial resources. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The scale:

N	Not sure	3	Neither important nor unimportant
1	Very unimportant	4	Important
2	Unimportant	5	Very important

PO6. Communicate management aims and direction with the business goal of ensuring user awareness and understanding of those aims. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PO7. Manage human resources with the business goal of maximising personnel contributions to the IT processes. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PO8. Ensure compliance with external requirements with the business goal of meeting legal, regulatory and contractual obligations. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PO9. Assess risks with the business goal of supporting management decisions in achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PO10. Manage projects with the business goal of setting priorities and delivering on time and within budget. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PO11. Manage quality with the business goal of meeting the IT customer requirements. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The scale:

N	Not sure	3	Neither important nor unimportant
1	Very unimportant	4	Important
2	Unimportant	5	Very important

Acquisition and Implementation (AI)

AI1. Identify automated solutions with the business goal of ensuring the best approach to satisfy the user requirements. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

AI2. Acquire and maintain application software with the business goal of providing automated functions, which effectively support the business process. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

AI3. Acquire and maintain technology infrastructure with the business goal of providing the appropriate platforms for supporting business applications. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

AI4. Develop and maintain procedures with the business goal of ensuring the proper use of the applications and the technological solutions put in place. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

AI5. Install and accredit systems with the business goal of verifying and confirming that the solution is fit for the intended purpose. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

AI6. Manage changes with the business goal of minimising the likelihood of disruption, unauthorised alterations and errors. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The scale:

N	Not sure	3	Neither important nor unimportant
1	Very unimportant	4	Important
2	Unimportant	5	Very important

Delivery and Support (DS)

DS1. Define and manage service levels with the business goal of establishing a common understanding of the level of service required. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DS2. Manage third-party services with the business goal of ensuring that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DS3. Manage performance and capacity with the business goal of ensuring that adequate capacity is available and that best and optimal use is made of it to meet required performance needs. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DS4. Ensure continuous service with the business goal of making sure IT services are available as required and ensuring a minimum business impact in the event of a major disruption. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DS5. Ensure system security with the business goal of safeguarding information against unauthorised use, disclosure or modification, damage or loss. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DS6. Identify and allocate costs with the business goal of ensuring a correct awareness of the costs attributable to IT services. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The scale:

N	Not sure	3	Neither important nor unimportant
1	Very unimportant	4	Important
2	Unimportant	5	Very important

DS7. Educate and train users with the business goal of ensuring that users are making effective use of technology and are aware of the risks and responsibilities involved. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DS8. Assist and advise customers with the business goal of ensuring that any problem experienced by the user is appropriately resolved. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DS9. Manage the configuration with the business goal of accounting for all IT components, prevent unauthorised alteration, verify physical existence and provide a basis for sound change management. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DS10. Manage problems and incidents with the business goal of ensuring that problems and incidents are resolved, and the cause investigated to prevent any recurrence. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DS11. Manage data with the business goal of ensuring that data remains complete, accurate and valid during its input, update and storage. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DS12. Manage facilities with the business goal of providing a suitable physical surrounding which protects the IT equipment and people against manmade and natural hazards. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The scale:

N	Not sure	3	Neither important nor unimportant
1	Very unimportant	4	Important
2	Unimportant	5	Very important

DS13. **Manage operations** with the business goal of ensuring that important IT support functions are performed regularly and in an orderly fashion. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Monitoring (M)

M1. **Monitor the processes** with the business goal of ensuring the achievement of the performance objectives set for the IT processes. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

M2. **Assess internal control adequacy** with the business goal of ensuring the achievement of the internal control objectives set for the IT processes. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

M3. **Obtain independent assurance** with the business goal of increasing confidence and trust among the organisation, customers and third-party providers. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

M4. **Provide for independent audit** with the business goal of increasing confidence levels and benefit from best practice advice. *(Please tick one box)*

N	1	2	3	4	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

If you have any comments you would like to make about IT control in your organisation, please write them on this page.

Your contribution to this survey is greatly appreciated.

Please return your questionnaire in the reply paid envelope provided by
26/08/2005

If the envelope has been mislaid, please forward the questionnaire to:

Attention: Miss L Gerke
Private Bag 87
School of Information Systems
University of Tasmania
Hobart, TAS 7001

Appendix H – Reference Guide, Phase One

Reference Guide

accompanying

COBIT Survey

**Use of the Control Objectives for Information
and Related Technologies (COBIT) framework
for IT audits in the Tasmanian Public Sector**



**School of Information Systems
University of Tasmania
Hobart TAS 7001
Phone (03) 6226 6200
Fax (03) 6226 6211**

The Control Objectives for Information and Related Technologies (COBIT) framework forms the basis for Part 2 of this questionnaire. COBIT is an Information Technology (IT) control framework designed to assist organisations in the management of IT. While the questionnaire uses abbreviated versions of the individual control objectives, this Reference Guide lists the full text versions of the control objectives in order to provide additional clarity if it is required.

Includes excerpts from COBIT: *Control Objectives for Information and Related Technology* (3rd Edition). ©1996, 1998, 2000 IT Governance Institute (ITGI). All rights reserved. COBIT is a registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute. Used by permission.

PO1 Define a strategic Information Technology Plan

Control over the IT process of defining a strategic plan that satisfies the business requirement of striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment is enabled by a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long term plans should periodically be translated into operational plans setting clear and concrete short-term goals and takes into consideration

- enterprise business strategy
- definition of how IT supports the business objectives
- inventory of technological solutions and current infrastructure
- monitoring the technology markets
- timely feasibility studies and reality checks
- existing systems assessments
- enterprise position on risk, time-to-market, quality
- need for senior management buy-in support and critical review

PO2 Define the Information Architecture

Control over the IT process of defining the information architecture that satisfies the business requirement of optimising the organisation of the information systems is enabled by creating and maintaining a business information model and ensuring appropriate systems are defined to optimise the use of this information and takes into consideration

- automated data repository and dictionary
- data syntax rules
- data ownership and criticality/security classification
- an information model representing the business
- enterprise information architectural standards

PO3 Determine Technological Direction

Control over the IT process of determining technological direction that satisfies the business requirement to take advantage of available and emerging technology to drive and make possible the business strategy is enabled by creation and maintenance of a technological infrastructure plan that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms and takes into consideration

- capability of current infrastructure
- monitoring technology developments via reliable sources
- conducting proof-of-concepts
- risk, constraints and opportunities
- acquisition plans
- migration strategy and roadmaps
- vendor relationships
- independent technology reassessment
- hardware and software price-performance changes

PO4 Define the Information Technology Organisation and Relationships

Control over the IT process of defining the IT organisation and relationships that satisfies the business requirement to deliver the right IT services is enabled by an organisation suitable in numbers and skills with roles and responsibilities defined and communicated, aligned with the business and that facilitates the strategy and provides for effective direction and adequate control and takes into consideration

- board level responsibility for IT
- management's direction and supervision of IT
- IT's alignment with the business
- IT's involvement in key decision processes
- organisational flexibility
- clear roles and responsibilities
- balance between supervision and empowerment
- job descriptions
- staffing levels and key personnel
- organisational positioning of security, quality and internal control functions
- segregation of duties.

PO5 Manage the Information Technology Investment

Control over the IT process of managing the IT investment that satisfies the business requirement to ensure funding and to control disbursement of financial resources **is enabled by** a periodic investment and operational budget established and approved by the business **and takes into consideration**

- funding alternatives
- clear budget ownership
- control of actual spending
- cost justification and awareness of total cost of ownership
- benefit justification and accountability for benefit fulfilment
- alignment with enterprise business strategy
- impact assessment
- asset management

PO6 Communicate Management Aims and Direction

Control over the IT process of communicating management aims and direction that satisfies the business requirement to ensure user awareness and understanding of those aims **is enabled by** policies established and communicated to the user community; furthermore, standards need to be established to translate the strategic options into practical and usable user rules **and takes into consideration**

- clearly articulated mission
- technology directives linked to business aims
- code of conduct/ethics
- quality commitment
- security and internal control policies
- security and internal control practices
- lead-by-example
- continuous communications programme
- providing guidance and checking compliance

PO7 Manage Human Resources

Control over the IT process of managing human resources that satisfies the business requirement to acquire and maintain a motivated and competent workforce and maximise personnel contributions to the IT processes is enabled by sound, fair and transparent personnel management practices to recruit, line, vet, compensate, train, appraise, promote and dismiss and takes into consideration

- recruitment and promotion
- training and qualification requirements
- awareness building
- cross-training and job rotation
- hiring, vetting and dismissal procedures
- objective and measurable performance evaluation
- responsiveness to technical and market changes
- properly balancing internal and external resources
- succession plan for key positions

PO8 Ensure Compliance with External Requirements

Control over the IT process of ensuring compliance with external requirements that satisfies the business requirement to meet legal, regulatory and contractual obligations is enabled by identifying and analysing external requirements for their IT impact, and taking appropriate measures to comply with them and takes into consideration

- laws, regulations and contracts
- monitoring legal and regulatory developments
- regular monitoring for compliance
- safety and ergonomics
- privacy
- intellectual property

PO9 Assess Risks

Control over the IT process of assessing risks that satisfies the business requirement of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors **is enabled by** the organisation engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks **and takes into consideration**

- risk management ownerships and accountability
- different kinds of IT risks (technology, security, continuity, regulatory, etc)
- defined and communicated risk tolerance profile
- root cause analyses and risk brainstorming sessions
- qualitative and/or quantitative risk measurement
- risk assessment methodology
- risk action plan
- timely reassessment

PO10 Manage Projects

Control over the IT process of managing projects that satisfies the business requirement to set priorities and to deliver on time and within budget **is enabled by** the organisation identifying and prioritising projects in line with the operational plan and the adoption and application of sound project management techniques for each project undertaken **and takes into consideration**

- business management sponsorship for projects
- program management
- project management capabilities
- user involvement
- task breakdown, milestone definition and phase approvals
- allocation of responsibilities
- rigorous tracking of milestones and deliverables
- cost and manpower budgets, balancing internal and external resources
- quality assurance plans and methods
- program and project risk assessments
- transition from development to operations

PO11 Manage Quality

Control over the IT process of managing quality that satisfies the business requirement to meet the IT customer requirements **is enabled by** the planning, implementing and maintaining of quality management standards and systems providing for distinct development phases, clear deliverables and explicit responsibilities **and takes into consideration**

- establishment of a quality culture
- quality plans
- quality assurance responsibilities
- quality control practices
- system development life cycle methodology
- programme and system testing and documentation
- quality assurance reviews and reporting
- training and involvement of end user and quality assurance personnel
- development of a quality assurance knowledge base
- benchmarking against industry norms

AI1 Identify Automated Solutions

Control over the IT process of identifying automated solutions that satisfies the business requirement of ensuring an effective and efficient approach to satisfy the user requirements **is enabled by** an objective and clear identification and analysis of the alternative opportunities measured against user requirements **and takes into consideration**

- knowledge of solutions available in the market
- acquisition and implementation methodologies
- user involvement and buy in
- alignment with enterprise and IT strategies
- information requirements definition
- feasibility studies (costs, benefits, alternatives, etc.)
- functionality, operability, acceptability and sustainability requirements
- compliance with information architecture
- cost-effective security and control
- supplier responsibilities

AI2 Acquire and Maintain Application Software

Control over the IT process of acquiring and maintaining application software that satisfies the business requirement to provide automated functions which effectively support the business process **is enabled by** the definition of specific statements of functional and operational requirements, and phased implementation with clear deliverables **and takes into consideration**

- functional testing and acceptance
- application controls and security requirements
- documentation requirements
- application software life cycle
- enterprise information architecture
- system development life cycle methodology
- user-machine interface
- package customisation

AI3 Acquire and Maintain Technology Infrastructure

Control over the IT process of acquiring and maintaining technology infrastructure **that satisfies the business requirement** to provide the appropriate platforms for supporting business applications **is enabled by** judicious hardware and software acquisition, standardising of software, assessment of hardware and software performance, and consistent system administration **and takes into consideration**

- compliance with technology infrastructure directions and standards
- technology assessment
- installation, maintenance and change controls
- upgrade, conversion and migration plans
- use of internal and external infrastructures and/or resources
- supplier responsibilities and relationships
- change management
- total cost of ownership
- system software security

AI4 Develop and Maintain Procedures

Control over the IT process of developing and maintaining procedures **that satisfies the business requirement** to ensure the proper use of the applications and the technological solutions to be put in place **is enabled by** a structured approach to the development of user and operations procedure manuals, service requirements and training materials **and takes into consideration**

- business process re-design
- treating procedures as any other technology deliverable
- timely development
- user procedures and controls
- operational procedures and controls
- training materials
- managing change

A15 Install and Accredite Systems

Control over the IT process of installing and accrediting systems that satisfies the business requirement to verify and confirm that the solution is fit for the intended purpose **is enabled by** the realisation of a well-formalised installation migration, conversion and acceptance plan **and takes into consideration**

- training of user and IT operations personnel
- data conversion
- a test environment reflecting the live environment
- accreditation
- post-implementation reviews and feedback
- end user involvement in testing
- continuous quality improvement plans
- business continuity requirements
- capacity and throughput measurement
- agreed upon acceptance criteria

A16 Manage Changes

Control over the IT process of managing changes that satisfies the business requirement to minimise the likelihood of disruption, unauthorised alterations and errors **is enabled by** a management system which provides for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure **and takes into consideration**

- identification of changes
- categorisation, prioritisation, and emergency procedures
- impact assessment
- change authorisation
- release management
- software distribution
- user of automated tools
- configuration management
- business process re-design

DS1 Define and Manage Service Levels

Control over the IT process of defining and managing service levels **that satisfies the business requirement** to establish a common understanding of the level of service required **is enabled by** the establishment of service-level agreements which formalise the performance criteria against which the quantity and quality of service will be measured **and takes into consideration**

- formal agreements
- definition of responsibilities
- response times and volumes
- charging
- integrity guarantees
- non-disclosure agreements
- customer satisfaction criteria
- cost/benefit analysis of required service levels
- monitoring and reporting

DS2 Manage Third Party Services

Control over the IT process of managing third-party services **that satisfies the business requirement** to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements **is enabled by** control measures aimed at the review and monitoring of existing agreements and procedures for their effectiveness and compliance with organisation policy **and takes into consideration**

- third-party service agreements
- contract management
- non-disclosure agreements
- legal and regulatory requirements
- service delivery monitoring and reporting
- enterprise and IT risk assessments
- performance rewards and penalties
- internal and external organisational accountability
- analysis of cost and service level variances

DS3 Manage Performance and Capacity

Control over the IT process of managing performance and capacity that satisfies the business requirement to ensure that adequate capacity is available and that best and optimal use is made of it to meet required performance needs **is enabled by** data collection, analysis and reporting on resource performance, application sizing and workload demand **and takes into consideration**

- availability and performance requirements
- automated monitoring and reporting
- modelling tools
- capacity management
- resource availability
- hardware and software price/performance changes

DS4 Ensure Continuous Service

Control over the IT process of ensuring continuous service that satisfies the business requirement to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption **is enabled by** having an operational and tested IT continuity plan which is in line with the overall business continuity plan and its related business requirements **and takes into consideration**

- criticality classification
- alternative procedures
- back-up and recovery
- systematic and regular testing and training
- monitoring and escalation processes
- internal and external organisational responsibilities
- business continuity activation, fallback and resumption plans
- risk management activities
- assessment of single points of failure
- problem management

DS5 Ensure Systems Security

Control over the IT process of ensuring systems security that satisfies the business requirement to safeguard information against unauthorised use, disclosure or modification, damage or loss **is enabled by** logical access controls which ensure that access to systems, data and programmes is restricted to authorised users **and takes into consideration**

- confidentiality and privacy requirements
- authorisation, authentication and access control
- user identification and authorisation profiles
- need-to-have and need-to-know
- cryptographic key management
- incident handling, reporting and follow-up
- virus prevention and detection
- firewalls
- centralised security administration
- user training
- tools for monitoring compliance, intrusion testing and reporting

DS6 Identify and Allocate Costs

Control over the IT process of identifying and allocating costs that satisfies the business requirement to ensure a correct awareness of the costs attributable to IT services **is enabled by** a cost accounting system which ensures that costs are recorded, calculated and allocated to the required level of detail and to the appropriate service offering **and takes into consideration**

- resources identifiable and measurable
- charging policies and procedures
- charge rates and charge-back process
- linkage to service level agreement
- automated reporting
- verification of benefit realisation
- external benchmarking

DS7 Educate and Train Users

Control over the IT process of educating and training users that satisfies the business requirement to ensure that users are making effective use of technology and are aware of the risks and responsibilities involved is enabled by a comprehensive training and development plan and takes into consideration

- training curriculum
- skills inventory
- awareness campaigns
- awareness techniques
- use of new training technologies and methods
- personnel productivity
- development of knowledge base

DS8 Assist and Advise Customers

Control over the IT process of assisting and advising customers that satisfies the business requirement to ensure that any problem experienced by the user is appropriately resolved is enabled by a help desk facility which provides first-line support and advice and takes into consideration

- customer query and problem response
- query monitoring and clearance
- trend analysis and reporting
- development of knowledge base
- root cause analysis
- problem tracking and escalation

DS9 Manage the Configuration

Control over the IT process of managing the configuration that satisfies the business requirement to account for all IT components, prevent unauthorised alterations, verify physical existence and provide a basis for sound change management **is enabled by** controls which identify and record all IT assets and their physical location, and a regular verification programme which confirms their existence **and takes into consideration**

- asset tracking
- configuration change management
- checking for unauthorised software
- software storage controls
- software and hardware interrelationships and integration
- use of automated tools

DS10 Manage Problems and Incidents

Control over the IT process of managing problems and incidents that satisfies the business requirement to ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence **is enabled by** a problem management system which records and progresses all incidents **and takes into consideration**

- audit trails of problems and solutions
- timely resolution of reported problems
- escalation procedures
- incident reports
- accessibility of configuration information
- supplier responsibilities
- coordination with change management

DS11 Manage Data

Control over the IT process of managing data that satisfies the business requirement to ensure that data remains complete, accurate and valid during its input, update and storage **is enabled by** an effective combination of application and general controls over the IT operations **and takes into consideration**

- form design
- source document controls
- input, processing and output controls
- media identification, movement and library management
- data back-up and recovery
- authentication and integrity
- data ownership
- data administration policies
- data models and data representation standards
- integration and consistency across platforms
- legal and regulatory requirements

DS12 Manage Facilities

Control over the IT process of managing facilities that satisfies the business requirement to provide a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards **is enabled by** the installation of suitable environmental and physical controls which are regularly reviewed for their proper functioning **and takes into consideration**

- access to facilities
- site identification
- physical security
- inspection and escalation policies
- business continuity planning and crisis management
- personnel health and safety
- preventive maintenance policies
- environmental threat protection
- automated monitoring

DS13 Manage Operations

Control over the IT process of managing operations that satisfies the business requirement to ensure that important IT support functions are performed regularly and in an orderly fashion **is enabled by** a schedule of support activities which is recorded and cleared for the accomplishment of all activities **and takes into consideration**

- operations procedure manual
- start-up process documentation
- network services management
- workload and personnel scheduling
- shift hand-over process
- system event logging
- coordination with change, availability and business continuity management
- preventive maintenance
- service level agreements
- automated operations
- incident logging, tracking and escalation

M1 Monitor the Processes

Control over the IT process of monitoring the processes that satisfies the business requirement to ensure the achievement of the performance objectives set for the IT processes **is enabled by** the definition of relevant performance indicators, the systematic and timely reporting of performance and prompt acting upon deviations **and takes into consideration**

- scorecards with performance drivers and outcome measures
- customer satisfaction assessments
- management reporting
- knowledge base of historical performance
- external benchmarking

M2 Assess Internal Control Adequacy

Control over the IT process of assessing internal control adequacy hat satisfies the business requirement o ensure the achievement of the internal control objectives set for the IT processes **is enabled by** the commitment to monitoring internal controls, assessing their effectiveness, and reporting on them on a regular basis **and takes into consideration**

- responsibilities for internal control
- ongoing internal control monitoring
- benchmarks
- error and exception reporting
- self-assessments
- management reporting
- compliance with legal and regulatory requirements

M3 Obtain Independent Assurance

Control over the IT process of obtaining independent assurance that satisfies the business requirement to increase confidence and trust among the organisation, customers, and third-party providers is enabled by independent assurance reviews carried out at regular intervals and takes into consideration

- independent certifications and accreditation
- independent effectiveness evaluations
- independent assurance of compliance with laws and regulatory requirements
- independent assurance of compliance with contractual commitments
- third-party service provider reviews and benchmarking
- performance of assurance reviews by qualified personnel
- proactive audit involvement

M4 Provide for Independent Audit

Control over the IT process of providing for independent audit that satisfies the business requirement to increase confidence levels and benefit from best practice advice is enabled by independent audits carried out at regular intervals and takes into consideration

- audit independence
- proactive audit involvement
- performance of audits by qualified personnel
- clearance of findings and recommendations
- follow-up activities
- impact assessments of audit recommendations (costs, benefits and risks)

Appendix I - T Test Results

Tier One

t-Test: Paired Two Sample for Means

	<i>DS5</i>	<i>DS4</i>
Mean	4.8	4.56
Variance	0.166666667	0.256666667
Observations	25	25
Pearson Correlation	0.362620334	
Hypothesized Mean Difference	0	
df	24	
t Stat	2.295276167	
P(T<=t) one-tail	0.015380154	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.030760308	
t Critical two-tail	2.063898547	

Tier 2

t-Test: Paired Two Sample for Means

	<i>DS4</i>	<i>POI</i>
Mean	4.56	4.52
Variance	0.256666667	0.426666667
Observations	25	25
Pearson Correlation	0.216564922	
Hypothesized Mean Difference	0	
df	24	
t Stat	0.272165527	
P(T<=t) one-tail	0.393911265	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.78782253	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>DS4</i>	<i>DS11</i>
Mean	4.56	4.48
Variance	0.256666667	0.343333333
Observations	25	25
Pearson Correlation	0.039301042	
Hypothesized Mean Difference	0	
df	24	
t Stat	0.526741538	
P(T<=t) one-tail	0.301604019	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.603208038	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>DS4</i>	<i>DS12</i>
Mean	4.56	4.4
Variance	0.256666667	0.333333333
Observations	25	25
Pearson Correlation	0.056980288	
Hypothesized Mean Difference	0	
df	24	
t Stat	1.072240924	
P(T<=t) one-tail	0.147137926	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.294275852	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>DS4</i>	<i>A16</i>
Mean	4.56	4.36
Variance	0.256666667	0.24
Observations	25	25
Pearson Correlation	0.161164593	
Hypothesized Mean Difference	0	
df	24	
t Stat	1.549193338	
P(T<=t) one-tail	0.067211198	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.134422396	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>DS4</i>	<i>PO8</i>
Mean	4.56	4.36
Variance	0.256666667	0.49
Observations	25	25
Pearson Correlation	0.347774467	
Hypothesized Mean Difference	0	
df	24	
t Stat	1.414213562	
P(T<=t) one-tail	0.085070777	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.170141553	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>DS4</i>	<i>PO8</i>
Mean	4.56	4.36
Variance	0.256666667	0.49
Observations	25	25
Pearson Correlation	0.347774467	
Hypothesized Mean Difference	0	
df	24	
t Stat	1.414213562	
P(T<=t) one-tail	0.085070777	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.170141553	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>DS4</i>	<i>PO5</i>
Mean	4.56	4.32
Variance	0.256666667	0.31
Observations	25	25
Pearson Correlation	0.372240581	
Hypothesized Mean Difference	0	
df	24	
t Stat	2.00932406	
P(T<=t) one-tail	0.027938375	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.05587675	
t Critical two-tail	2.063898547	

Tier Two ends after AI6 Manage Changes

Tier 3

t-Test: Paired Two Sample for Means

	<i>PO5</i>	<i>AI3</i>
Mean	4.32	4.28
Variance	0.31	0.376666667
Observations	25	25
Pearson Correlation	0.580411849	
Hypothesized Mean Difference	0	
df	24	
t Stat	0.371390676	
P(T<=t) one-tail	0.356802561	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.713605122	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>PO5</i>	<i>DS10</i>
Mean	4.32	4.24
Variance	0.31	0.19
Observations	25	25
Pearson Correlation	0.357103779	
Hypothesized Mean Difference	0	
df	24	
t Stat	0.699854212	
P(T<=t) one-tail	0.245373514	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.490747028	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>PO5</i>	<i>AI2</i>
Mean	4.32	4.2
Variance	0.31	0.333333333
Observations	25	25
Pearson Correlation	0.44070447	
Hypothesized Mean Difference	0	
df	24	
t Stat	1	
P(T<=t) one-tail	0.163643441	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.327286881	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	PO5	DS8
Mean	4.32	4.16
Variance	0.31	0.306666667
Observations	25	25
Pearson Correlation	0.232435828	
Hypothesized Mean Difference	0	
df	24	
t Stat	1.162803799	
P(T<=t) one-tail	0.128170602	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.256341204	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	PO5	AI4
Mean	4.32	4.12
Variance	0.31	0.193333333
Observations	25	25
Pearson Correlation	0.517402027	
Hypothesized Mean Difference	0	
df	24	
t Stat	2	
P(T<=t) one-tail	0.028469924	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.056939847	
t Critical two-tail	2.063898547	

Tier 3 ends after PO4 Define the IT Organisation and Relationships

Tier 4

t-Test: Paired Two Sample for Means

	<i>A14</i>	<i>PO11</i>
Mean	4.12	4.08
Variance	0.193333333	0.326666667
Observations	25	25
Pearson Correlation	0.457606369	
Hypothesized Mean Difference	0	
df	24	
t Stat	0.371390676	
P(T<=t) one-tail	0.356802561	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.713605122	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>A14</i>	<i>DS3</i>
Mean	4.12	4.04
Variance	0.193333333	0.373333333
Observations	25	25
Pearson Correlation	0.136480208	
Hypothesized Mean Difference	0	
df	24	
t Stat	0.569494797	
P(T<=t) one-tail	0.2871563	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.5743126	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>A14</i>	<i>DS7</i>
Mean	4.12	4
Variance	0.193333333	0.166666667
Observations	25	25
Pearson Correlation	0.232119173	
Hypothesized Mean Difference	0	
df	24	
t Stat	1.140703651	
P(T<=t) one-tail	0.132624387	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.265248774	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>A/4</i>	<i>A/1</i>
Mean	4.12	3.92
Variance	0.193333333	0.243333333
Observations	25	25
Pearson Correlation	0.046104767	
Hypothesized Mean Difference	0	
df	24	
t Stat	1.549193338	
P(T<=t) one-tail	0.067211198	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.134422396	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>A/4</i>	<i>M1</i>
Mean	4.12	3.8
Variance	0.193333333	0.916666667
Observations	25	25
Pearson Correlation	-0.13856633	
Hypothesized Mean Difference	0	
df	24	
t Stat	1.444630237	
P(T<=t) one-tail	0.080745951	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.161491902	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>A/4</i>	<i>DS1</i>
Mean	4.12	3.76
Variance	0.193333333	1.19
Observations	25	25
Pearson Correlation	0.149413677	
Hypothesized Mean Difference	0	
df	24	
t Stat	1.616447718	
P(T<=t) one-tail	0.05953396	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.119067919	
t Critical two-tail	2.063898547	

t-Test: Paired Two Sample for Means

	<i>A14</i>	<i>M4</i>
Mean	4.12	3.44
Variance	0.193333333	0.506666667
Observations	25	25
Pearson Correlation	0.090528044	
Hypothesized Mean Difference	0	
df	24	
t Stat	4.238975338	
P(T<=t) one-tail	0.000143799	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.000287597	
t Critical two-tail	2.063898547	

*Tier 4 ends after DS6 Identify and Allocate Costs****Tier 5***

t-Test: Paired Two Sample for Means

	<i>M4</i>	<i>M3</i>
Mean	3.44	3.08
Variance	0.506666667	0.91
Observations	25	25
Pearson Correlation	0.436904874	
Hypothesized Mean Difference	0	
df	24	
t Stat	1.983739568	
P(T<=t) one-tail	0.029418326	
t Critical one-tail	1.710882067	
P(T<=t) two-tail	0.058836652	
t Critical two-tail	2.063898547	

*Tier 5 ends after M4 Provide for Independent Audit**Tier 6 contains last control objective M3 Obtain Independent Assurance*

Appendix J – Audit Working Papers

DS5 Ensure Systems Security

Audit Measure	Conclusion
<p>Has the organisation developed a security statement and policy?</p> <ul style="list-style-type: none"> ✧ Confirm the statement and/or policy exists, is endorsed and communicated. ✧ Confirm that the policy/plans/procedures are current. 	
<p>Determine whether remote access is used in the organisation.</p> <ul style="list-style-type: none"> ✧ Identify policy and procedures over the granting, modifying and removal of remote access. ✧ Determine how the organisation controls this access. ✧ Confirm that remote access is regularly reviewed 	
<p>Are there formalised procedures in place for the granting, modifying and removal of user access privileges?</p> <ul style="list-style-type: none"> ✧ Are requests for user access documented? ✧ What is the approval process for granting access? ✧ Is access removed for users that have left the organisation? ✧ How is IT staff made aware of staff leavers? ✧ Is removal of system's access done in a timely manner? ✧ What are the procedures for granting and removing emergency/ temporary access? ✧ Are periodic reviews of user access conducted? ✧ Are periodic reviews conducted of user profiles to ensure appropriate access rights? 	
<p>Confirm that review of users have been undertaken on regular basis, and all exceptions actioned.</p>	
<p>How are users uniquely identified to the each system components (ie. Unique user Id and password)?</p>	

Audit Measure	Conclusion
<p>Does the agency have a password policy that incorporates the following:</p> <ul style="list-style-type: none"> ✧ Minimum and maximum length; ✧ Special restrictions in the setting of passwords (ie at least one numeric character); ✧ System forced change ✧ History preventing/limiting reuse; ✧ Lockout after number of unsuccessful attempts; ✧ System timeouts. 	
<p>Review system configuration and confirm that password policy has been set and this is consistent with Security policy and procedures</p>	
<p>Identify whether multiple layers of passwords are required for sensitive functions application ie SU to root, Firecall etc.</p>	
<p>Are there network access logs?</p>	
<p>Are these logs regularly reviewed by appropriate staff?</p>	
<p>An audit trail of access/activity is reviewed daily or weekly.</p>	
<p>Are there formal policies in regard to:</p> <ul style="list-style-type: none"> ✧ Internet use ✧ Email use ✧ File Sharing <p>How are these disseminated amongst staff, particularly new users?</p> <p>Do staff members have to agree with these policies?</p>	

DS4 Ensure Continuous Support

Audit Measure	Conclusion
Verify the existence of a current and endorsed IT continuity plan. Determine if the key business stakeholders have provided input to the continuity plan	
Review publication policy, eg management required to approve all Internet content.	
Evaluate how the agency ensures the backup/archiving has completed correctly (eg. Are tapes readable?)	
Does the agency periodically check data maintained to ensure integrity and correctness?	
Review and evaluate standard backup and archiving procedures	
For each system, what types of backups are performed (Consider frequency, cycle and rotation)? Are these backups performed in accordance with the predetermined backup schedule? Are the backups/archives stored in appropriately secure, on-site and off-site, locations?	
Determine if media at off-site location are matched to appropriate media management system	

DS11 Manage Data

Audit Measure	Conclusion
For a selected sample of source documents consistency is evident with respect to stated procedures relating to authorisation, approval, accuracy, completeness and receipt by data entry and data entry is timely.	
Audit trails are provided to facilitate the tracing of transaction processing and the reconciliation of disrupted data.	
Error handling procedures and actions comply with established policies and controls.	
Output reports are secured awaiting distribution, as well as those already distributed to users in compliance with established procedures and controls.	
Disposed sensitive information procedures and actions comply with established policies and controls.	
Media storage sites are physically secure and inventory current.	
Adequate protections ensure integrity, confidentiality and non-repudiation of sensitive messages transmitted over the Internet or any other public network.	
The risk of misaddressing messages (by letter, fax or e-mail) is mitigated by appropriate procedures.	
Controls that are normally applied to a specific transaction or process, such as faxing or automatic telephone message answering, also apply to computer systems that support transaction or process (e.g., fax software on a personal computer).	

Audit Measure	Conclusion
Obtain a copy of backup and archiving policy and procedures.	
Determine what training has been provided to operations staff with regard to backup/archiving and restore procedures?	
Determine if the backup and restore procedures been documented sufficiently to allow someone other than the primary IT resource to perform the necessary tasks.	
Is test data protected and controlled: <ul style="list-style-type: none"> ✧ minimise use of personal information for test purposes ✧ If used the data should be depersonalised before use 	
Strict controls in place over access to a programs source library.	
Data security function: <ul style="list-style-type: none"> ✧ The function is staffed with sufficient personnel of appropriate expertise and experience. User and group profiles should be defined to reflect CIS and user department organisation ensuring that appropriate segregation of duties is maintained. ✧ Profile attributes and special authorities should reflect users' business functions. 	
Access to on-line editors which have capabilities to replace/modify file contents, internal storage areas or programs is limited through access control software or security profiles to system administrator or other authorised personnel.	
Audit trail of all changes is kept.	
Direct editing is approved and fully documented.	
Audit trails of changes to transaction files and master files are kept.	

DS12 Manage Facilities

Audit Measure	Conclusion
The building is locked down overnight (outside of business hours).	
Building visitors are monitored by reception and security.	
Restriction beyond the reception area is restricted via locks (i.e. proxy cards).	
Access outside of business hours requires appropriate privileges upon proxy cards.	
Video/sensor monitors in place throughout the building	
Adequate procedures are in place for providing and terminating staff members' physical access.	
<p>The server room is physically locked (i.e. proxy cards).</p> <p>Access to the room is restricted to relevant staff (i.e. IT Staff Only).</p> <p>Adequate procedures are in place for providing and terminating staff members' physical access</p> <p>Video camera's monitor the entry points to the server room.</p> <p>The room is within sight of IT staff.</p> <p>No other access risks (windows etc).</p>	
Is there a signing in procedure for visitors entering the computer facilities?	
Are reviews conducted of the visitor registration log book?	

Audit Measure	Conclusion
Is there a long term plan for the facilities required to support the agency's computing environment?	
Are periodic review of access privileges and profiles conducted?	
Adequate fire devices in place: <ul style="list-style-type: none"> ✧ Air Conditioning Unit ✧ Humidity/Temperature monitors ✧ Fire/Smoke Alarms/Sensors ✧ Fire Extinguishers 	
Temperature and humidity is controlled and monitored (I.e. air conditioner unit, vesda system).	
Is the server room adequately located? Consider: <ul style="list-style-type: none"> ✧ Other business operations nearby ✧ Areas prone to natural disaster ✧ The type of business conducted, that may pose risk of terrorism ✧ Nearby water risks (I.e. running water pipes etc) 	
Appropriate floors - anti static.	
Boxes are all racked and raised.	
All components of the communication network under the organization control are physically secured.	
Appropriate back-up or alternative routing for key elements in communications networks exists.	

Audit Measure	Conclusion
Access to terminals which may have network master terminal status is restricted.	
All boxes feature UPS. UPS are regularly tested. Appropriate shutdown & battery time.	

PO1 Define a Strategic Information Technology Plan

Audit Measure	Conclusion
Minutes from IT planning/steering committee meetings reflect the planning process.	
Relevant IT initiatives are included in the IT long- and short- range plans (i.e., hardware changes, capacity planning, information architecture, new system development or procurement, disaster recovery planning, installation of new processing platforms, etc.).	
IT initiatives support the long- and short-range plans and consider requirements for research, training, staffing, facilities, hardware and software.	
Consideration has been given to optimising current and future IT investments.	
IT long- and short-range plans are consistent with the organisation's long- and short-range plans and organisation requirements.	
Plans have been changed to reflect changing conditions.	
IT long-range plans are periodically translated into short-range plans.	
Tasks exist to implement the plans.	

PO8 Ensure Compliance with External Requirements

Audit Measure	Conclusion
<p>External requirements reviews are:</p> <ul style="list-style-type: none"> ✧ current, complete and comprehensive with respect to legal, government and regulatory issues. ✧ result in prompt corrective action. 	
<p>Reviews of safety and health are undertaken within the IT function to ensure compliance with external requirements</p> <ul style="list-style-type: none"> ✧ Problem areas which do not comply with the safety and health standards are rectified. 	
<p>IT compliance with the documented privacy and security policies and procedures.</p>	
<p>Existing contracts with electronic commerce trading partners adequately address the requirements specified in organisational policies and procedures.</p>	
<p>Existing insurance contracts adequately address the requirements specified in organisational policies and procedures.</p>	
<p>Actual EDI processes being deployed by the organisation ensure compliance with organisational policies and procedures, and compliance with the individual electronic commerce trading partner contracts (and the EDI vendor contract if applicable).</p>	

A16 Manage Changes

Audit Measure	Conclusion
<p>For a sample of changes, the following have been approved by management:</p> <ul style="list-style-type: none"> ✧ request for change ✧ specification of change ✧ access to source programme ✧ programmer completion of change ✧ request to move source into test environment ✧ completion of acceptance testing ✧ request for compilation and move into production ✧ overall and specific security impact has been determined and accepted ✧ distribution process has been developed. 	
<p>Review of change control documentation for inclusion of:</p> <ul style="list-style-type: none"> ✧ date of requested change ✧ person(s) requesting ✧ approved for change request ✧ approval of change made — IT function ✧ approval of change made — users ✧ documentation update date ✧ move date into production ✧ quality assurance sign-off of change ✧ acceptance by operations. 	
<p>Analyse types of changes made to system for identification of trends.</p>	
<p>Evaluate adequacy of IT libraries and determine the existence of base line code levels to prevent error regression.</p>	
<p>Code check-in and check-out procedures for changes exist.</p>	

Audit Measure	Conclusion
Change control log ensures all changes on log were resolved to user satisfaction and that there were no changes made not on log.	
Users are aware and understand need for formal change control procedures	

Appendix K – Collated Audit Responses

Audit Measure	1	2	3	4	5	6	7	8	9
<p>Does the agency have a password policy that incorporates the following:</p> <ul style="list-style-type: none"> ❖ Minimum and maximum length; ❖ Special restrictions in the setting of passwords (ie at least one numeric character); ❖ System forced change ❖ History preventing/limiting reuse; ❖ Lockout after number of unsuccessful attempts; ❖ System timeouts. 	No strong passwords. Endorsed policy on length, system forced change, history preventing/limiting reuse, lockout, time out	All incorporated, policy is part of security policy	All incorporated, policy accepted September, implementation in progress	All incorporated - timeout to password locked screensavers	Policy, looking into pass phrases, limit reuse of last password, all others incorporated	No restrictions on characters, system times out to password locked screen saver, all other aspects included	Technically have policy, time out to password locked screensaver, all other aspects included	Time out to locked screen saver, FIMIS does not force change but scheduled as a task, all other aspects included	No special restriction on non-alpha characters, other aspects included in network passwords
Review system configuration and confirm that password policy has been set and this is consistent with Security policy and procedures	Consistent	Part of security policy	No security policy	Will be consistent	Security policy references pw policy	Consistent	Security policy does not cover, training issue	Consistent	No security policy
Identify whether multiple layers of passwords are required for sensitive functions application	In some systems	Handled by systems admin	Yes	No	Tied to active directory	To access HR and Finance	Yes, multiple entry of passwords	No	Yes
Are there network access logs?	Yes	Yes	On server	Yes	Yes	External access only	Yes	Yes	Yes embedded in OS security event logs enabled
Are these logs regularly reviewed by appropriate staff?	Alerting reviewed as needed	Individual users, HR, IT security	Not really viewed for security	Three reviews per year	Only on detection of problem	Daily	Through help desk, duties rotate	Yes	Reviewed on alert
An audit trail of access/activity is reviewed daily or weekly.	Review on incident	Individual users, HR, IT security	No	Only network logs reviewed	Only on detection of problem Rely on trust	Access logs, reviewed on detection of problem	Log monitoring system, review on exception	Yes	No
<p>Are there formal policies in regard to:</p> <ul style="list-style-type: none"> ❖ Internet use ❖ Email use ❖ File Sharing <p>How are these disseminated amongst staff, particularly new users?</p> <p>Do staff members have to agree with these policies?</p>	Acceptable use - covers internet, e-mail. No P2P file share server access controlled thru HR. Given out on induction, formal sign off.	No file sharing, policies disseminated at induction, formal sign off required.	Yes, file sharing on server, no P2P. Circulated to all staff on induction, no formal sign off	Formal policies. Communicated through intranet and inductions, sign contract but not on these	Internet & e-mail policies, file share server managed thru active directory. Discussed with new users, no formal sign off	Formal policies on all, hard copies issued, formally sign off on starting	Formal policies in security policy, issued at induction, also in centralised repository, splash screen on login, formal sign off	Acceptable use of IT - internet and e-mail, file sharing on servers only. Sign off on security policy on first day & any changes	Formal policies, communicated at corporate induction, and more if appropriate, no formal sign off

DS4 Ensure Continuous Support

Audit Measure	1	2	3	4	5	6	7	8	9
Verify the existence of a current and endorsed IT continuity plan. Determine if the key business stakeholders have provided input to the continuity plan	BCP for some systems; DRP in place; input of stakeholders	Yes, all can attend meetings at which plan is reviewed	BCP to be drawn up - external contractor. DRP in place.	DRP, continuity plan currently being changed	BCP & DRP, in review, no input but can review	Continuity plan, key stakeholder input	BCP & DRP, no stakeholder input to DRP	Continuity plan, key business stakeholder input	No BCP, no DRP, meeting 21/03/05 to consider these
Review publication policy, eg management required to approve all Internet content.	External to IT function	Handled by Corporate Marketing Unit	No internal policy, follow government policy, done thru single point in org.	Have legal opinion & directors opinion, only 2 people can publish to Internet	Content management system, replacing policy	Externally hosted, managed thru Corporate Affairs	Policy exists, 2 people only can publish	Policy exists	Covered by procedure not an IT role
Evaluate how the agency ensures the backup/archiving has completed correctly (eg. Are tapes readable?)	Use of commercial product	Covered by policy, run back, daily rotation of operators	Recover on some tapes, ad hoc	Physical checking	Clean and re-tension tapes six monthly, run back tapes	Log checks, monthly random restores	Logs checked daily, 3 month random restore, 6 month test of DRP	Tested in 6 month test, intermittent restore	Tested, run back tapes
Does the agency periodically check data maintained to ensure integrity and correctness?	Run back	Routine	Integrity checks on databases	Yes - running monthly reports	Most are not primary systems, responsibility of business owners	Log checks, monthly random restores	Line of Business apps good practice, others, auth, system	Yes	Not accuracy, done at system level
Review and evaluate standard backup and archiving procedures	Determined by system, currently nightly full	As per policy	Varies across systems	Data backed up, Domain controller to disc & tape; archiving ongoing	As per policy	Included in Information Security policy	As per policy	As per policy	As per policy
For each system, what types of backups are performed (Consider frequency, cycle and rotation)? Are these backups performed in accordance with the predetermined backup schedule? Are the backups/archives stored in appropriately secure, on-site and off-site, locations?	DIMQA off site /ip safe to bank vault	As per policy, stored offsite.	DIM on some, DWM on some, on schedule, secure storage	Backup as per schedule, appropriate storage	DWM stored, according to schedule, tapes offsite, in /ip safes	DWMQ, according to schedule, on & off site locations	DWM, as per schedule, on-site up to 1 week, then to Reserve Bank	Oracle server 10am, 12 & 5pm, overnight and weekend	DWM, exceptions for shared network files, stored appropriately
Determine if media at off-site location are matched to appropriate media management system	Yes	Yes	Yes	Fireproof safe	Yes	Yes	Yes	Yes	Yes

DS11 Manage Data

Audit Measure	1	2	3	4	5	6	7	8	9
For a selected sample of source documents consistency is evident with respect to stated procedures relating to authorisation, approval, accuracy, completeness and receipt by data entry and data entry is timely.	Segregation of duties, ministerial system requires approval	Managed at business unit level	Yes, IT has no access to finance system	Segregation of duties	Not considered applicable - no FMS	Segregation of duties	Segregation of duties	Segregation of duties in critical system	Segregation of duties within practical constraints
Audit trails are provided to facilitate the tracing of transaction processing and the reconciliation of disrupted data.	Logging in database systems.	Audit trails, review by Sys Admins.	Yes	In two applications	Not considered applicable	Yes	Yes	Yes	Done at an application level but not by IT
Error handling procedures and actions comply with established policies and controls.	Handled on system basis	Systems Admin level	For the FMS	Complies	Yes	Yes in FMS	Handled by Lines of Bus.	Yes	Yes
Output reports are secured awaiting distribution, as well as those already distributed to users in compliance with established procedures and controls.	Under local Sys Admin control	Systems Admin level	Physical on need basis, limited syst. access	Controls exist	Not considered applicable	Yes	Yes	Yes	Responsibility of users
Disposed sensitive information procedures and actions comply with established policies and controls.	Under local Sys Admin control	Systems Admin level	Yes	Shred or archive, remove hard drives	Not considered applicable	Yes	Yes	Yes	No
Media storage sites are physically secure and inventory current.	Under local Sys Admin control	Off site, secure	Yes in sales.	24 hour security, hard & soft copy invent.	In locked cabinet, inventory current	Yes	Yes	Yes	Yes
Adequate protections ensure integrity, confidentiality and non-repudiation of sensitive messages transmitted over the Internet or any other public network.	Encryption when necessary SSL to internal sites no e-mail filtering	Part of e-mail policy	Not done in organisation	E-mail policy required no sensitive data sent.	Provide advice not to do this	Unsure	As much as possible	Yes	No
The risk of misaddressing messages (by letter, fax or e-mail) is mitigated by appropriate procedures.	Global address book, system tells sender if not delivered	Not specifically addressed	No, use global address book for outgoing where possible	Use of global directory where possible	Use global address book in Outlook and GDS	Internal only	Use global address book	Use global address book	No
Controls that are normally applied to a specific transaction or process, such as faxing or automatic telephone message answering, also apply to computer systems that support transaction or process (e.g., fax software on a personal computer).	A fax gateway is provided by IAB. Managed & monitored by business units	Not through IT department	Yes	Faxing thru single point, copied to director, checks every 15 minutes	Not considered applicable	Tighter controls on system performance of these tasks	Yes	Yes	Not considered applicable

Audit Measure	1	2	3	4	5	6	7	8	9
Obtain a copy of backup and archiving policy and procedures.	Backup only	Done	Done	Done	Sighted	Done	Done	Done	Done
Determine what training has been provided to operations staff with regard to backup/archiving and restore procedures?	All IT staff trained either formally or peer	Training provided	Documented, Inducted, walked thru multiple times	Training provided	Training provided	On the job training	Training, rotating duty	Training provided	Training provided
Determine if the backup and restore procedures been documented sufficiently to allow someone other than the primary IT resource to perform the necessary tasks.	Yes	All staff trained	Yes - but need IT exp.	Yes	Yes	Yes	Yes	Yes	Yes
Is test data protected and controlled: <ul style="list-style-type: none"> minimise use of personal information for test purposes if used the data should be depersonalised before use 	Use live data to test. Vendors using sign off on confidentiality	Load testing, use live data	Not used much, use live data	Use test server - use full data for test - no depersonalising	May use live data, no personal information	Unknown, done in HR and finance, not IT	Not considered applicable	Not used	Replicate production data for test
Strict controls in place over access to a programs source library.	Outsourced s with vendor in house SourceSafe	Strict access control - use open source code	Not much source code, built getting program	Yes	Yes	Yes	Yes	Yes	No development - no code kept
Data security function: <ul style="list-style-type: none"> The function is staffed with sufficient personnel of appropriate expertise and experience. User and group profiles should be defined to reflect CIS and user department organisation ensuring that appropriate segregation of duties is maintained. Profile attributes and special authorities should reflect users' business functions. 	Through management and empower system	No outsourcing, well trained staff, most have 1 st class honours degrees	Yes	Yes - constantly reinforced	Staff experienced and academically qualified	Yes	Yes	Yes	Yes
Access to on-line editors which have capabilities to replace/modify file contents, internal storage areas or programs is limited through access control software or security profiles to system administrator or other authorised personnel.	Including content mnt	Not considered applicable	Limited - sys admin function	Online editing done by 2 people only	Not considered applicable	Access limited to IT personnel	Not considered applicable	Yes	Yes - covered by policy
Audit trail of all changes is kept.	For datasets, not file shares	Yes	Yes	Yes	Version roll back, datasets, database, criticality	On programs and data	Change control for key syst. Help desk	Yes	Yes - covered by policy
Direct editing is approved and fully documented.	For datasets, not file shares	Not done	Addition rather than edit	Approval by Dr. Versions kept	Not considered applicable	Yes	Not considered applicable	Yes	Yes - covered by policy
Audit trails of changes to transaction files and master files are kept.	If important (finance & HR)	No. All databases are in Oracle, can wind back.	Yes	Yes	Not considered applicable	Yes	Yes for high & at risk systems. Q. systems. O. vague	Yes	Yes - covered by policy

DS12 Manage Facilities

Audit Measure	1	2	3	4	5	6	7	8	9
The building is locked down overnight (outside of business hours).	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Building visitors are monitored by reception and security.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Restriction beyond the reception area is restricted via locks (i.e. proxy cards).	Yes	In progress	Not during the day	Yes	Yes	Yes	Yes	Yes	Yes
Access outside of business hours requires appropriate privileges upon proxy cards.	Role & dongle coding annual review	Yes	Yes - thru key	Yes	Yes - but access from home encouraged	Yes - exec area access in b hours only	Yes - reviewed every 3 months	Yes - security card	Yes
Video/sensor monitors in place throughout the building	Yes	Yes	No - manned 24/7	Sensors - video being added	Yes	No, video on street access only	In public areas only	Yes	Sensors, video in some locations
Adequate procedures are in place for providing and terminating staff members' physical access.	Through HR for electronic & reception for physical	Through HR system	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<p>The server room is physically locked (i.e. proxy cards).</p> <p>Access to the room is restricted to relevant staff (i.e. IT Staff Only).</p> <p>Adequate procedures are in place for providing and terminating staff members' physical access</p> <p>Video camera's monitor the entry points to the server room.</p> <p>The room is within sight of IT staff.</p> <p>No other access risks (windows etc).</p>	Server room locked, access through role approved by RE, procedures for provision & termination, video monitoring of access & internal, situated in sight of IT staff, no access risks	Server room locked, access restricted to IT staff, procedures for provision & termination of access, video monitoring of entry points, in sight of IT staff, no access risks	Server room locked, access restricted to relevant staff, procedures for provision & termination of access, no video monitoring, not in sight of IT staff, window - looks over road of site, locked	Server room locked, access restricted, procedures for provision & termination of access, no video monitoring yet, room in sight of IT staff, no other access risks	Server room locked, access restricted, procedures for provision & termination of access, no video monitoring, in sight of organisation secretary, no access risks	Server room locked, access restricted, procedures for provision & termination of access, no video monitoring, motion detector inside active after hours, in sight of IT staff, no access risks	Server room locked, access restricted, procedures for provision & termination of access, no video monitoring on access, in sight of IT staff, no other access risks	Server room locked, access restricted, procedures for provision & termination of access, no video monitoring on access, in sight of IT staff, no other access risks	Server room locked, access restricted, procedures for provision & termination of access, no video monitoring on access, motion detectors, in sight of IT staff, has windows with security grille
Is there a signing in procedure for visitors entering the computer facilities?	Yes & server room	No - must be acc.	No	No	No, acc. or pass. only	No	Building yes, facilities no	Building yes, facilities no	No
Are reviews conducted of the visitor registration log book?	Both logs	By security only	Front entry - unsure	Not applic.	Not applic.	Not applic.	Not applic.	No	No

Audit Measure		1	2	3	4	5	6	7	8	9
Is there a long term plan for the facilities required to support the agency's computing environment?		Yes, review this year	Yes - about to be expanded	No	Yes	Not beyond 5 years	In the BCP	No	Yes	Yes as part of other planning documents
Are periodic review of access privileges and profiles conducted?		Yes	yes	Yes	Ongoing	Yes	No	Every 3 months	Yes	At network access level
Adequate fire devices in place: <ul style="list-style-type: none"> ✧ Air Conditioning Unit ✧ Humidity/Temperature monitors ✧ Fire/Smoke Alarms/Sensors ✧ Fire Extinguishers 		Air con, humidity/temp alarm, fire/smoke alarms, no fire extinguishing facility	Air con, humidity/temp monitors, fire/smoke alarms/sensors, fire extinguishers	Air con, temperature monitors, vesda system, fire extinguishers	Air con, humidity/temp monitors, fire/smoke alarms/sensors, fire extinguishers	Air con, humidity/temperature monitoring, heat sensors, sprinkler system	Air con x2, no humidity/temp monitors, fire/smoke alarms/sensors, fire extinguishers	Air con x2, vesda system, multi zone alarms/sensors, fire extinguishers at all entry/exit points	Air con, humidity/temp monitors, fire/smoke alarms/sensors, fire extinguishers	Air con, humidity/temp monitors, vesda system, fire extinguishers
Temperature and humidity is controlled and monitored (i.e. air conditioner unit, vesda system).		Yes - vesda system with alarm	Yes with SMS to mobile on incident	Vesda system	Yes	Yes with air con, remote checking of processor heat	Yes	Yes	Yes	Yes
Is the server room adequately located? Consider: <ul style="list-style-type: none"> ✧ Other business operations nearby ✧ Areas prone to natural disaster ✧ The type of business conducted, that may pose risk of terrorism ✧ Nearby water risks (i.e. running water pipes etc) 		Shared building, other businesses not risk, not disaster prone, no water risk, nearby terrorism risk	Shared building, other govt organisations, not disaster prone, no water risk, not terrorism target	No other businesses, not prone to disaster, business may be terrorist target, unfootable	No other businesses, not prone to disaster, no terrorism risk, no water risks	Shared building, other govt orgs, not prone to disaster, may be terrorist target, no nearby water risk	No other businesses, not prone to disaster, not terrorism target, no nearby water risk	Shared building, no public access, not prone to disaster, no terrorism risk, no nearby water risk	Shared building, not prone to natural disaster, not terrorism risk, no nearby water risk	No other businesses, not prone to disaster, not terrorism target, no nearby water risk
Appropriate floors - anti static.		Raised floor, anti static matting	Use rubber matting.	No special consideration - on upper floor	No special consideration - on upper floor	Rubber matting, static not considered a risk	Yes	Yes	Yes	Considered appropriate - no matting, on upper floor
Boxes are all racked and raised.		Racked & raised	Racked & raised	Racked & raised	Racked & raised	Racked & raised	Racked & raised	Racked & raised	Racked & raised	Racked & raised
All components of the communication network under the organization control are physically secured.		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Appropriate back-up or alternative routing for key elements in communications networks exists.		Out to tender for IMB, WAN single link thru Networking Tas	Redundant laser link, triangulating with another building	Yes	Yes	Yes	Have a plan	Locally yes, wide area, no	Yes	Yes

Audit Measure		
Access to terminals which may have network master terminal status is restricted.		
All boxes feature UPS. UPS are regularly tested. Appropriate shutdown & battery time.		
All production boxes have UPS, ongoing monitoring & alerting, shutdown & restart schedule	Physical access to location, & by password	1
UPS on critical machines, not considered necessary.	Not considered applicable	2
UPS on all boxes, regularly tested. Shutdown & battery time not relevant - generator	Sun server console, in computer room, password req.	3
UPS on all boxes, regular testing, appropriate shutdown & battery	Restricted	4
UPS on all boxes, management ongoing, appropriate shutdown & battery	No - require systems admin privilege to access	5
UPS on all boxes, regularly tested, have appropriate shutdown & battery	Restricted to those who can access server room	6
UPS on all boxes, tested 3 monthly, ongoing monitoring, 12 hours battery time	Restricted to those who can access server room	7
UPS on all boxes, regularly tested, have appropriate shutdown & battery	Restricted to those who can access server room	8
UPS on all boxes, regularly tested, monitor ongoing, have appropriate shutdown & battery, generator	Restricted	9

PO1 Define a Strategic Information Technology Plan

Audit Measure	1	2	3	4	5	6	7	8	9
Minutes from IT planning/steering committee meetings reflect the planning process.	IMB managers & director meeting minutes	Info. Mgmt Steering Committee - minutes	Yes	Yes	Yes	IS Steering Comm. Meet 6 weekly, minutes	IT planning committee, minutes	Committee meets, minutes	No
Relevant IT initiatives are included in the IT long- and short- range plans (i.e., hardware changes, capacity planning, information architecture, new system development or procurement, disaster recovery planning, installation of new processing platforms, etc.).	As needed by appl. Determined at acct. or dev.	Branch business plan run 6 monthly	"Sort of" - not formally done, documented thru request for funds	Yes - most recent 2003/4	Yes - IT strategic plan 3 years.	Yes	Yes	Yes	Yes
IT initiatives support the long- and short-range plans and consider requirements for research, training, staffing, facilities, hardware and software.	Project based development	Branch business plan run 6 monthly	Yes	Closely linked to business	Yes	Yes	Yes	Yes	Within budget constraints
Consideration has been given to optimising current and future IT investments.	Yes	Branch business plan run 6 monthly	Yes	Yes - considering open source	Yes - going to 4 year turnover	Absolutely	Only to 3 years, info & KM 3-5 years, IT not cons. possible	Strategic plan 3 years	In the nature of what is done
IT long- and short-range plans are consistent with the organisation's long- and short-range plans and organisation requirements.	Departmental initiative gives direction	Aligned	Yes	IT plan part of organisational plan	Yes	Very aligned with the business	Yes	Yes	Yes
Plans have been changed to reflect changing conditions.	Yes	Yes - secretary dictated focus this year	Yes	Yes	Yes	Yes	Yes and no	Manual review annually	Yes
IT long-range plans are periodically translated into short-range plans.	Yes! Plans, projects, initiatives system.	Yes	Thru request for funds	Yes	Yes	Yes	Annual review	Yes	Yes
Tasks exist to implement the plans.	Yes. Initiatives.	As projects	Yes	As projects	Mostly projects	Yes	Yes	Yes	Yes

PO8 Ensure Compliance with External Requirements

Audit Measure	1	2	3	4	5	6	7	8	9
<p>External requirements reviews are:</p> <ul style="list-style-type: none"> ◇ current, complete and comprehensive with respect to legal, government and regulatory issues ◇ result in prompt corrective action. 	Not a function of IMIS. Concern: information security. Have legal advisor.	Conducted, consider regulation.	Yes	Yes	Yes, example SPAM review	ISO compliant, internal and external audit	Yes - certified by KPMG in last internal audit	Yes, corrective action when required	No
<p>Reviews of safety and health are undertaken within the IT function to ensure compliance with external requirements</p> <ul style="list-style-type: none"> ◇ Problem areas which do not comply with the safety and health standards are rectified. 	OHS committee meet 3-4 times a year, prompt correction of problem areas.	OHS - spot audits, corrective action if needed	Yes	Yes - corrective action if needed	Yes, corrective action if needed	Yes, corrective action if needed	Yes, corrective action if needed	Yes, corrective action if needed	Ongoing within OHS, corrective action if needed
IT compliance with the documented privacy and security policies and procedures.	Yes.	Yes	Privacy through legislation, have org policies on privacy.	Yes	Yes	Yes	Yes	Yes	Yes
Existing contracts with electronic commerce trading partners adequately address the requirements specified in organisational policies and procedures.	Yes - identified bank - encryption of pay file, confirm send/receive	Yes	Not considered applicable	Yes	Yes - identified bank	Bank & major client	Yes, B2B only	Not considered applicable	Yes identified bank
Existing insurance contracts adequately address the requirements specified in organisational policies and procedures.	Yes	Not considered applicable	Not considered applicable	Yes	Not much insurance	Not considered applicable	Yes	Not considered applicable	Yes
Actual EDI processes being deployed by the organisation ensure compliance with organisational policies and procedures, and compliance with the individual electronic commerce trading partner contracts (and the EDI vendor contract if applicable).	Yes - Identified e-commerce partner, considered question to be vague.	Not considered applicable - use of e-mail instead	Not considered applicable	Not considered applicable	Not considered applicable	E-commerce system of information exchange with clients	Internal only within single line of business applications	Not considered applicable	Not considered applicable

A16 Manage Changes

Audit Measure		1	2	3	4	5	6	7	8	9
For a sample of changes, the following have been approved by management: ❖ request for change ❖ specification of change ❖ access to source programme ❖ programmer completion of change ❖ request to move source into test environment ❖ completion of acceptance testing ❖ request for compilation and move into production ❖ overall and specific security impact has been determined and accepted ❖ distribution process has been developed.		Implementing ITIL to manage this. Procedures currently not consistent.	Runs 6 month business program for IT forward plan, on Feb - Aug cycle. Individual changes run as projects, each documented prior to submission to IT department.	Don't code. Do have customisation done, request for change and specifications well documented.	Change infrequent but well documented	Documented processes, purchase where possible and outsource builds	Formal methodology, well documented	Linked to lines of business, risk based, IT has request for change, for high risk, must go through risk committee, project documentation, CRM is only whole of business application other than lines of business	Well documented processes	Limited documentation only, no development, corporate applications through a 3 rd party provider, interfaces between corporate applications provided by IT
Review of change control documentation for inclusion of: ❖ date of requested change ❖ person(s) requesting ❖ approved for change request ❖ approval of change made — IT function ❖ approval of change made — users ❖ documentation update date ❖ move date into production ❖ quality assurance sign-off of change ❖ acceptance by operations.										
Analyse types of changes made to system for identification of trends.		Server rotation, systems upgrades	No trends identified	No trends identified	Upgrades	Upgrades	Bugs & enhancements	Change of technology	Upgrades	Mainly version upgrades
Evaluate adequacy of IT libraries and determine the existence of base line code levels to prevent error regression.		Minimal – reliant on vendors & testing	Electronic libraries, re-use code	Not considered applicable	Adequate	No code library	Adequate	Not yet, development only just restarting	Adequate	Not considered applicable
Code check-in and check-out procedures for changes exist.		Through another IMB group	Yes	Not considered applicable	Yes	Done through providers	Yes	Source control system	Yes	Under control of developer

Audit Measure	1	2	3	4	5	6	7	8	9
Change control log ensures all changes on log were resolved to user satisfaction and that there were no changes made not on log.	Change control log on each server, compliant	Not considered applicable	No change control log	Yes	Through technical services manager	Managed through methodology	Through help desk system	Yes	Yes
Users are aware and understand need for formal change control procedures	Users aware of need & for test plans in SLAs	Not considered applicable	No	Yes	Clients don't get to do changes, can put in change request	Yes	Not generally	Yes	Yes

Appendix L – Frequency Tables for Assigned Maturity Levels

DS5 Ensure Systems Security***Frequency against Audit Measure***

Measure	Maturity Level					
	0	1	2	3	4	5
1	1	1	1	0	6	0
2	0	0	1	3	5	0
3	0	0	0	3	6	0
4	0	0	3	3	3	0
5	0	0	0	1	8	0
6	0	0	1	0	8	0
7	2	0	1	3	3	0
8	2	0	2	1	4	0
9	0	0	2	0	7	0
10	1	0	1	0	7	0
11	2	4	0	0	3	0
12	0	0	0	0	9	0
Totals	8	5	12	14	69	0

Frequency against Organisation Number

Maturity Level	Organisation								
	1	2	3	4	5	6	7	8	9
0	0	0	4	1	0	0	0	1	2
1	1	0	0	2	1	1	0	0	0
2	1	0	3	0	1	3	2	0	2
3	1	1	1	1	1	1	2	4	2
4	9	11	4	8	9	7	8	7	6
5	0	0	0	0	0	0	0	0	0

DS4 Ensure Continuous Support***Frequency against Audit Measure***

Measure	Maturity Level					
	0	1	2	3	4	5
1	1	0	0	3	5	0
2	0	0	0	1	7	1
3	0	0	0	5	4	0
4	0	0	2	3	4	0
5	0	0	0	1	8	0
6	0	0	0	0	9	0
7	0	0	0	9	0	0
Total	1	0	2	22	37	1

Frequency against Organisation Number

Maturity Level	Organisation								
	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	1	0	0	0	1
3	3	3	4	2	2	1	1	3	3
4	4	4	2	5	4	6	6	4	2
5	0	0	1	0	0	0	0	0	0

PO1 Define a Strategic Information Technology Plan***Frequency against Audit Measure***

Measure	Maturity Level					
	0	1	2	3	4	5
1	1	0	0	8	0	0
2	0	1	5	3	0	0
3	0	0	2	7	0	0
4	0	1	1	7	0	0
5	0	0	1	7	1	0
6	0	0	1	8	0	0
7	0	0	1	8	0	0
8	0	0	0	9	0	0
Totals	1	2	11	57	1	0

Frequency against Organisation Number

Maturity Level	Organisation								
	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	1
1	1	0	0	0	0	0	0	0	1
2	0	3	2	0	0	1	2	1	2
3	7	5	6	7	8	7	6	7	4
4	0	0	0	1	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0

DS11 Manage Data***Frequency against Audit Measure***

Measure	Maturity Level					
	0	1	2	3	4	5
1	1	2	0	5	1	0
2	1	1	0	5	2	0
3	0	5	0	4	0	0
4	2	3	0	4	0	0
5	2	2	0	5	0	0
6	0	1	0	7	1	0
7	4	1	2	1	1	0
8	1	7	1	0	0	0
9	3	0	0	4	2	0
10	0	0	0	0	9	0
11	0	0	0	9	0	0
12	2	1	0	6	0	0
13	1	0	0	6	2	0
14	0	0	0	5	4	0
15	3	1	0	5	0	0
16	0	2	1	5	1	0
17	3	1	0	4	1	0
18	1	2	0	5	1	0
Totals	24	29	4	80	25	0

Frequency against Organisation Number

Maturity Level	Organisation								
	1	2	3	4	5	6	7	8	9
0	0	3	1	1	8	1	3	1	6
1	7	5	5	1	3	2	3	2	1
2	0	0	0	0	0	2	1	1	0
3	5	5	11	11	5	11	9	13	10
4	6	5	1	5	2	2	2	1	1
5	0	0	0	0	0	0	0	0	0

DS12 Manage Facilities

Frequency against Audit Measure

Measure	Maturity Level					
	0	1	2	3	4	5
1	0	0	0	0	0	9
2	0	0	0	0	0	9
3	0	1	0	1	0	7
4	0	0	0	0	9	0
5	0	2	0	0	4	3
6	0	0	0	7	2	0
7	0	0	0	4	3	2
8	0	0	0	8	1	0
9	6	0	2	0	1	0
10	2	2	0	5	0	0
11	1	1	0	5	2	0
12	0	0	0	2	7	0
13	0	0	0	5	4	0
14	0	0	0	3	6	0
15	0	0	2	5	2	0
16	0	0	0	0	9	0
17	0	0	0	9	0	0
18	0	0	0	7	1	1
19	1	1	0	5	2	0
20	0	1	0	4	4	0
Totals	10	8	4	70	57	31

Frequency against Organisation Number

Maturity Level	Organisation								
	1	2	3	4	5	6	7	8	9
0	0	1	1	1	1	2	2	1	1
1	0	1	1	0	1	2	1	0	2
2	0	1	2	1	0	0	0	0	0
3	5	6	8	9	9	9	6	10	8
4	10	6	6	6	5	4	8	6	6
5	5	5	2	3	4	3	3	3	3

AI6 Manage Changes

Frequency against Audit Measure

Measure	Maturity Level					
	0	1	2	3	4	5
1	0	1	1	5	2	0
2	0	1	1	5	2	0
3	3	2	3	0	1	0
4	1	2	0	4	2	0
5	2	0	0	5	2	0
6	2	2	0	5	0	0
Totals	8	8	5	24	9	0

Frequency against Organisation Number

Maturity Level	Organisation								
	1	2	3	4	5	6	7	8	9
0	0	2	4	0	1	0	0	0	1
1	1	0	2	0	2	0	2	0	1
2	0	0	0	1	0	1	0	1	2
3	4	2	0	5	3	3	0	5	2
4	1	2	0	0	0	2	4	0	0
5	0	0	0	0	0	0	0	0	0

PO8 Ensure Compliance with External Requirements

Frequency against Audit Measure

Measure	Maturity Level					
	0	1	2	3	4	5
1	1	0	1	5	2	0
2	0	0	0	0	9	0
3	0	0	1	8	0	0
4	2	0	0	5	2	0
Totals	3	0	2	18	13	0

Frequency against Organisation Number

Maturity Level	Organisation								
	1	2	3	4	5	6	7	8	9
0	0	0	1	0	0	0	0	1	1
1	0	0	0	0	0	0	0	0	0
2	1	0	1	0	0	0	0	0	0
3	1	3	1	3	3	1	2	2	2
4	2	1	1	1	1	3	2	1	1
5	0	0	0	0	0	0	0	0	0