2006

Towards an abbreviated COBIT framework for use in an Australian State Public Sector

Lynne Gerke
University of Tasmania, lbgerke@utas.edu.au

Gail Ridley
University of Tasmania, Gail.Ridley@utas.edu.au

Towards an abbreviated COBIT framework for use in an Australian State Public Sector

Lynne Gerke
Gail Ridley

School of Accounting & Corporate Governance
Formerly of School of Information Systems
University of Tasmania
Hobart, Tasmania

Email: lbgerke@utas.edu.au
Email: Gail.Ridley@utas.edu.au

Abstract

This paper details research undertaken to evaluate the potential to use the Control Objectives for Information and Related Technologies (COBIT) framework as the basis for Information Technology (IT) audits in a state public sector audit office from Australia. The research outlined here used a survey methodology to determine the high level control objectives from COBIT considered to be the most important to a selection of public sector organisations from within that state and provides a comparison with studies by Guldentops, van Grembergen and de Haes (2002), Liu and Ridley (2005) and results from the European Organisation of Supreme Audit Institutions (EUROSAI) IT working group COBIT self-assessment. Seventeen high level control objectives were identified as being important to Tasmanian public service organisations. As eight of these were also identified by the other studies it appears possible to derive an abbreviated instrument from COBIT that would be both enduring and relevant across geographical and organisational contexts.

Keywords

COBIT, IT audit, public sector, Australia, Tasmania, IT governance

INTRODUCTION

Public sector organisations are largely funded by the taxpayer and are 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.

While there are some regulatory requirements for IT governance measures implemented in Australia arising from the Corporations Act 2001 and the Australian Accounting Standards (which now reflect the International Financial Reporting System) amongst others, a growing number of private companies also 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, IT audits are being conducted at both a national and state level.

The Control Objectives for Information and Related Technology (COBIT) framework (now issued as Version 4) is widely used throughout the world for examination of IT control and audit. The framework is massive, consisting of thirty-four high level control objectives grouped into four domains. Each high level control objective is associated with between three and thirty detailed control objectives, producing a comprehensive framework of some three hundred and eighteen detailed control objectives. Previous practitioner studies have examined which of the high level control objectives can be perceived as being the most important to a range of industry sectors and nations. One reason for wanting to identify the most important IT control objectives from COBIT is to help tailor the framework for IT audit in a particular context. COBIT is increasingly being used by IT auditors to guide audit procedures, sometimes in an abbreviated form.

There is an extensive 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. A great deal of the practitioner literature emanates from the Information Systems Audit and Control Association (ISACA) and the Information Technology Governance Institute (ITGI), which are the custodians of COBIT. However, there is a lack of scholarly research into the framework to evaluate its effectiveness for IT governance or IT audit. This study investigated which of the high level control objectives from the COBIT framework were considered by IT managers in Tasmanian public sector organisations to be the most important and whether these control objectives would be applicable

across other geographical and organisational contexts. This was done as a precursor to developing an abbreviated audit program based around COBIT.

BACKGROUND

IT-related frameworks including COBIT

The annual spending for the Australian IT industry was estimated to be $80 billion in 2002, while worldwide in the same year the figure was estimated to be $3 trillion (Lateline 2002). The Australian Federal Government's 2002–2003 operating expenditure for ICT was an estimated $3.11 billion with an additional ICT capital expenditure of $1.10 billion. This was an increase of approximately 52% on the 1999–2000 figures (ANAO 2005). With such a large expenditure it is essential that the public is assured that the expenditure is both prudent and beneficial.

The most commonly mentioned IT-related 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, while 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 that guide quality management systems.

Auditing is a process of methodical examination and review, whereby the practitioner seeks evidences to confirm claims made by an organisation. Information Technology Audit has been a part of financial statement audit for some decades, but there is a renewed focus on its scope to incorporate governance considerations and link business processes and objectives. The COBIT framework is potentially of great benefit since it has a focus on aligning the business with 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 such alignment between use of IT in organisations and the achievement of business goals is seen as desirable. 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.

The 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 framework consists of 34 high-level control objectives grouped into four broad areas called domains. The domains are *Planning and Organisation*, *Acquisition and Implementation*, *Delivery and Support* and *Monitoring*. Note that while the research reported in this paper used Version 3.0, Version 4.0 was released in December 2005. Some differences exist between the versions, including the name of one of the domains. For ease of reference, the high-level control objectives are each labelled with the initials of the domain in which they are grouped, a number and a brief descriptive title. An example of this nomenclature is DS5 Ensure Systems Security. This control objective, number 5 in the Delivery and Support domain, is concerned with ensuring the overall security of systems. Each of the high-level control objectives has associated with it between three and thirty detailed control objectives, giving a total of 318 detailed control objectives in the whole framework.

Previous COBIT studies

Much of the literature available about the COBIT framework has been produced by practitioners, for practitioners (Ridley *et al.* 2004). People closely linked with ISACA and ITGI are commonly found as authors of such material. It has been suggested by Ridley *et al.* (2004) that such a widely adopted framework should be the subject of rigorous academic research, particularly as it has been adopted widely in the private and public sectors throughout the world. Liu and Ridley (2005) asserted that the widespread international adoption of COBIT in both the public and private sectors is illustrative of its acceptance and credibility. Sallé (2004) went even further, suggesting that COBIT is becoming a de facto standard for IT governance.

One international practitioner study (Guldentops *et al.* 2002) examined the high level control objectives perceived by a panel of senior IT and audit experts as being most important. Then the organisations assessed their performance against these objectives by using a six-point maturity scale defined by the COBIT framework to assess their level of development. The 15 most important high level control objectives identified by the expert panel in the Guldentops *et al.* study are detailed in Table 1 below.

The same list of control objectives was used by Liu and 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 constructed for research published in 2002, making it more than three years old at the time the current research project was undertaken. Given the pace of change in the IT sector, such a list may well no longer be relevant. Furthermore, it is not known whether different public sectors within Australia would prioritise control objectives in the same way. Yet such differences may impact on the acceptance of an IT audit methodology, where it is derived from COBIT.

Table 1: 15 most important COBIT control objectives identified by Guldentops *et al* (2002)

COBIT Control Objective
PO1 Define a Strategic IT Plan
PO3 Determine Technological Direction
PO5 Manage the IT Investment
PO9 Assess Risks
PO10 Manage Projects
AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI 5 Install and Accredit Systems
AI6 Manage Changes
DS1 Define and Manage Service Levels
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS10 Manage Problems and Incidents
DS11 Manage Data
M1 Monitor the Processes

Table 2: The 8 most important CobiT control objectives identified by the EUROSAI IT working group workshops (Huissoud 2005)

	COBIT Control Objective
Most Important	PO1 Define a Strategic Plan
	AI3 Acquire and Maintain Technology Infrastructure
	AI6 Manage Changes
	DS4 Ensure Continuous Service
	DS5 Ensure System Security
	DS7 Educate and Train Users
	DS10Manage Problems and Incidents
	M1 Monitor the Processes
Also … important	PO2 Define the Information Architecture
	PO3Determine the Technological Direction
	PO10 Manage Projects
	AI1 Identify Automated Solutions
	AI2 Acquire and Maintain Application Software
	AI4 Develop and Maintain Procedures
	DS11 Manage Data
	PO9 Assess Risks

The European Organisation of Supreme Audit Institutions is the peak body comprising 45 "External Control Institutions" or Supreme Audit Institutions (SAIs), from the European continent (EUROSAI undated). The EUROSAI IT working group has undertaken an ongoing project to design a self-assessment tool for SAIs based on the COBIT framework. The EUROSAI project referred to key control objectives as business processes. Participants examined the IT aspects of their own organisation in a workshop environment to determine the 10-15 key control objectives 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. An experienced facilitator from the working group ran these workshops. The results for the assessments performed prior to February 2005 have been reported. The eight control objectives rated in these

workshops as being the "most important" (Huissoud 2005) are presented in the top section of Table 2. An additional eight control objectives "also considered to be important" (Huissoud 2005) are presented in the lower section of the table.

Study setting

The Tasmanian Audit Office (TAO) is the independent authority charged with upholding public integrity within Tasmania (TAO 2004), an Australian state. Audits performed by the TAO embrace three major areas, Financial, Performance and Compliance Audit. The IT Audit section falls under the management of Financial Audit Services, with the Electronic Data Processing (EDP) auditors also supporting and assisting the financial audit team when required. At the time this study was undertaken IT audits were performed using an audit program derived in-house. This program focused entirely on the IT function without considering the way in which it integrated with the overall business of the organisation being audited. However, use of COBIT would enable the linking of IT use to the achievement of organisational goals. Given the constraints of both time and resources within which the TAO is forced to operate, it is impossible to implement an IT audit framework the size of COBIT in its entirety. This is in spite of the fact that such audits are performed only on clientele selected following a TAO risk assessment model.

Identification of context-specific COBIT control objectives considered by IT managers in public sector organisations as being the most important would allow a more meaningful and targeted IT audit to be conducted. It would also address the problem of scope. The COBIT Audit Guidelines contain a comprehensive listing of the audit measures (individual elements to examine) required to fully audit the IT control of an organisation. Most high-level control objectives have associated with them in excess of one hundred audit measures. Previous studies by Guldentops *et al*. (2002) and Liu and Ridley (2005), have examined organisational performance against 15 control objectives. To complete a comprehensive audit of 15 control objectives an examination of more than 1500 individual audit measures would be needed. This would require many weeks of interviews and investigation for each organisation.

Research Aims

Given the substantial public sector investment in IT infrastructure and the potential benefits of using an established framework such as COBIT to govern IT, the aim of this study is to identify the most important high-level control objectives from the COBIT framework for the Tasmanian public sector. The achievement of this aims is likely to offer a range of benefits. Prioritising those control objectives as most important gives a means of reducing the number of IT audit measures. At the same time prioritising the control objectives, and therefore the IT audit measures, makes the audit more relevant to the issues routinely encountered by the audited organisations. Additionally, IT audit measures tailored for the sector are likely to be better accepted, and are more likely to expose relevant control risks. The benefits are likely to extend to both to the auditor and the audited organisation. The second research aim, to compare the observed results with those of previous studies conducted both internationally and within Australia and in a range of organisations, will give an indication of the applicability of these control objectives across different geographical and organisational contexts.

METHODOLOGY

Research design and data collection

This research was conducted using 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 for the results of the study to be accepted and relevant to those in the field, it was considered desirable to use a similar philosophy. The Tasmanian Audit Office (TAO) expressed an interest in exploring use of the COBIT framework as a basis for future IT audits in the public sector in Tasmania. As an organisation which routinely deals with financial data, the TAO practices under a predominantly objective, positivist philosophy. The development and use of an instrument that utilised the same philosophy was considered likely to enhance the credibility of the findings.

The research involved the development and administration of a survey instrument to the target participants. The survey scope encompassed 30 public sector organisations nominated by the TAO after use of a risk assessment model. All the Tasmanian public sector organisations were surveyed that were considered to be of highest risk, using the model. These organisations were also considered to have IT infrastructure of a sufficient size to examine governance of IT. All types of public sector organisations found within Tasmania were represented, from government business enterprises and departments, to local government authorities.

Brief details about organisational type, respondent's role title and a ranking of familiarity with both organisational and IT goals of their organisation on a five point Likert-type scale were sought in the questionnaire. The main section of the survey instrument asked participants to rate the 34 high-level control objectives from the COBIT framework (Version 3.0) according to their importance to the agency on a Likert-type scale. Examples of the instructions, scales and questions from the second section of the questionnaire are located in Appendix 1. This section used the same rating system as that used to elicit the perceived importance of the control objectives in the EUROSAI project. These ratings would then be analysed to produce a ranked list, similar to that produced in the study by Guldentops *et al.* (2002), in order to determine the control objectives that were considered most relevant to Tasmanian public sector organisations.

A pilot test of the questionnaire was administered to managers in five organisations within the Tasmanian public sector that were not a part of the target population. In the main survey the questionnaires were distributed to IT managers or senior business managers with IT responsibilities. Distribution and contact with participants at this stage was conducted through the TAO as a requirement of obtaining ethics approval. It was anticipated that the co-operation of the TAO would improve the response rate. However there was a single follow up with the organisations to encourage non-respondents to participate, again through the TAO.

Validity

Several issues of validity were identified for this study. Selection issues were addressed by selecting the entire population identified by application of the risk model. Using the entire population also addressed the issue of generalisability. Testing was not seen as a threat to validity as no organisation was repeatedly exposed to the questionnaire. The pilot test was administered in organisations external to the target population, that is, they were not identified as being in the highest risk category from the model. Organisations from outside the target population were used for the pilot test since the target population was small (30 organisations).

Analysis of data

Data collected in this study included a series of ratings on a Likert-type scale. Data from the questionnaires were entered into a Microsoft Excel spreadsheet as the responses were received. The ratings from the second section of the questionnaire were analysed to give a total, mean and standard deviation for each high-level control objective. The data were then sorted in descending order on the basis of the totals. Any control objectives with the same totals were subjected to a second sort on control objective code in simple alphabetical order.

The totals were then subjected to statistical testing. Beginning at the highest ranked control objective, the totals were analysed using the paired sample Student's t-test to find significant differences. 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. All tests were conducted at $p < 0.05$ and 24 degrees of freedom. Testing commenced from the top of the ranked list (DS4) and continued until a statistical difference was detected. Testing then re-commenced using the first element in the next grouping as the point of comparison, a process that was repeated until the list of 34 control objectives was exhausted and six groupings, or tiers, were obtained. A list of 17 high-level control objectives was derived by using the top three tiers.

RESULTS

From the original 30 questionnaires originally distributed, 25 responses were received giving a response rate of 83%. As only two late responses (8%) were received after the closing date, the issue of non-response bias was not considered to be important. One study has suggested that the response rate for top managers or representatives of organisations is usually around 36%, and for mid-level managers about 60% (Baruch 1999). The higher response rate in this study may be attributable to the facilitating role of the TAO, in both providing advance notice of the questionnaire and in distributing the questionnaire. Consequently the excellent response rate for the study suggests that it was seen by participants as both credible and relevant.

Response rates of over 70% are considered to be "very good" (Babbie 1990). Since this survey was distributed to the entire population of TAO clients in the category chosen using the risk assessment model, and the response rate was over 80%, it was considered unnecessary to test the responses to determine whether they were representative of the whole population.

The second section of the questionnaire asked participants to rate the importance to their organisation of the 34 high level control objectives from the COBIT framework on a Likert-type scale. The ratings were analysed to produce the ranked list as shown in Table 3. The results of the t-tests and the subsequent tiers are also shown in Table 3.

Table 3: Results of t-tests showing tiers

	Control Objective	Total	Mean	Std Dev	t stat	P
Tier 1	DS5 Ensure Systems Security	120	4.80	0.41		
Tier 2	DS4 Ensure Continuous Service	114	4.56	0.51	2.30	0.02
	PO1 Define a Strategic IT Plan	113	4.52	0.65	0.27	0.39
	DS11 Manage Data	112	4.48	0.59	0.53	0.30
	DS12 Manage Operations	110	4.40	0.58	1.07	0.15
	AI6 Manage Changes	109	4.36	0.49	1.54	0.07
	PO8 Ensure Compliance With External Requirements	109	4.36	0.70	1.41	0.09
Tier 3	PO5 Manage the IT Investment	108	4.32	0.56	2.01	0.03
	AI3 Acquire & Maintain Technology Infrastructure	107	4.28	0.61	0.37	1.71
	PO6 Communicate Management Aims & Direction	107	4.28	0.61	0.33	0.37
	DS10 Manage Problems & Incidents	106	4.24	0.44	0.70	0.25
	DS9 Manage the Configuration	106	4.24	0.52	0.70	0.25
	AI2 Acquire & Maintain Application Software	105	4.20	0.58	0.16	1.71
	AI5 Install & Accredit Systems	105	4.20	0.65	0.90	0.19
	PO9 Assess Risks	105	4.20	0.50	1.14	0.13
	DS8 Assist & Advise Customers	104	4.16	0.55	1.16	0.13
	PO4 Define the IT Organisation & Relationships	104	4.16	0.55	1.69	0.05
Tier 4	AI4 Develop & Maintain Procedures	103	4.12	0.44	2.00	0.03
	DS13 Manage Operations	103	4.12	0.53	0.00	0.50
	PO10 Manage Projects	103	4.12	1.05	0.00	0.50
	PO3 Determine Technological Direction	103	4.12	0.67	0.00	0.50
	PO7 Manage Human Resources	103	4.12	0.53	0.00	0.50
	PO11 Manage Quality	102	4.08	0.57	0.37	0.36
	DS3 Manage Performance & Capacity	101	4.04	0.61	0.46	0.29
	M2 Assess Internal Control Adequacy	101	4.04	0.61	0.49	0.31
	PO2 Define the information Architecture	101	4.04	0.61	0.62	0.27
	DS7 Educate & Train Users	100	4.00	0.41	1.14	0.13
	AI1 Identify Automated Solutions	98	3.92	0.49	1.55	0.07
	DS2 Manage Third Party Services	98	3.92	1.12	0.87	0.20
	M1 Monitor the Processes	95	3.80	0.96	1.44	0.08
	DS1 Define & Manage Service Levels	94	3.76	1.09	1.62	0.06
	DS6 Identify & Allocate Costs	94	3.76	0.72	1.98	0.03
Tier 5	M4 Provide for independent Audit	86	3.44	0.71	4.24	0.00
Tier 6	M3 Obtain Independent Assurance	77	3.08	0.95	1.98	0.03

As the statistical testing identified six tiers, and there were several points at which an abbreviated list could be formed, previous studies were consulted 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 and Ridley (2005) used the same list. As previously reported, the EUROSAI IT working group recommended forming a list of 10-15 control objectives (EUROSAI undated) and reported a combined list of 16 control objectives (Huissoud, 2005). These sources suggested the creation of an abbreviated list using the first three tiers of control objectives, giving a size of 17 control objectives. Furthermore, a list of 17 control objectives would be appropriate for comparison with the other studies. The abbreviated list is shown in Table 4.

Table 4: Abbreviated list of COBIT Control Objectives in Tasmanian Public Sector Organisations Ranked by Importance

COBIT Control Objective
DS5 Ensure Systems Security
DS4 Ensure Continuous Service
PO1 Define a Strategic IT Plan
DS11 Manage Data
DS12 Manage Operations
AI6 Manage Changes
PO8 Ensure Compliance With External Requirements
PO5 Manage the IT Investment
AI3 Acquire and Maintain Technology Infrastructure
PO6 Communicate Management Aims & Direction
DS10 Manage Problems & Incidents
DS9 Manage the Configuration
AI2 Acquire & Maintain Application Software
AI5 Install & Accredit Systems
PO9 Assess Risks
DS8 Assist & Advise Customers
PO4 Define the IT Organisation & Relationships

DISCUSSION

The control objectives in the abbreviated list were derived from three of the COBIT domains: *Planning and Organisation*, *Acquisition and Implementation* and *Delivery and Support*. No control objectives from the *Monitoring* domain were considered by the surveyed organisations to be of a high level of importance. While the rankings were important to determine the composition of the list, the exclusion of any control objectives from the *Monitoring* domain suggests that the value of control objectives in this domain may be under valued.

DS5 Ensure Systems Security

The rating of DS5 Ensure Systems Security as the most important control objective may be explained in part by a requirement of the Tasmanian Government Security Charter, administered by the Inter Agency Policy and Projects Unit of the Department of Premier and Cabinet (DPAC), that all government agencies develop and implement an appropriate Agency Information Security Plan that identifies the information assets of the agency (DPAC, 2003). Although under Tasmanian legislation the term "agency" means a "Government department or a State authority" (State Service Act 2000), it also includes other organisations specifically named in the legislation. The Charter requires the agencies to conduct regular information security risk assessments and monitor and review their security plan in order to minimise information security risks. It also covers issues such as outsourcing, the protection of ICT systems, and the need for staff to hold standards of integrity and honesty, as well as the use of resources in the home-based and mobile environments. While not all organisations that responded to the questionnaire were classified under legislation as agencies and consequently subject to the charter, the issue was topical in the public sector at the time the research was undertaken.

Comparisons with previous research

The results of this research can be compared with that of previous studies by Guldentops *et al.* (2002), Liu and Ridley (2005) and the self assessment project facilitated by the EUROSAI IT working group as reported by Huissoud (2005). The primary focus of Guldentops *et al.* (2002) and Liu and Ridley (2005) was for organisations to assess their own maturity against the COBIT maturity models for each of 15 pre-determined high level control objectives from the framework. These control objectives were determined in the former study by an international group of experts. The EUROSAI project used a rating system much the same as that employed in this study to determine the most important control objectives, before self assessing maturity against 10-15 of the top rated objectives, as determined by the individual organisations. Table 5 presents a list of control objectives common to the Tasmanian data and the studies by Guldentops *et al.* (2002) and Liu and Ridley (2005), as well as the EUROSAI results reported by Huissoud (2005). Table 5 then illustrates that eight of the 17 control objectives (or 47%) identified in this study have been previously identified by all three of the studies as being significant in their context. When all control objectives identified in Table 5 are taken into account, 11 (or 65%) of the most highly ranked Tasmanian control objectives were common to at least one previous study.

Consequently, analysis indicates that the majority of control objectives rated as important were not unique to the Tasmanian public sector.

Table 5: Comparison of control objectives between studies

Guldentops (2002) and Liu & Ridley (2005)	Tasmanian	Huissoud (2005)
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	
AI5	AI5	
	AI3	AI3

Unique results

Since 11 of the 17 most highly ranked control objectives identified in this study were common to those ranked highly in other studies, it can be seen that six (or 35%) can be considered to be unique to the Tasmanian public sector. These control objectives are presented in Table 6.

Table 6: Unique Control Objectives Identified

COBIT Control Objective
DS12 Manage Operations
DS8 Assist & Advise Customers
DS9 Manage the Configuration
PO4 Define the IT Organisation & Relationships
PO6 Communicate Management Aims & Direction
PO8 Ensure Compliance With External Requirements

With all of the control objectives in the abbreviated list of 17 being drawn from the domains of *Planning and Organisation* (6 of 17 control objectives), *Acquisition and Implementation* (4 of 17 control objectives) and *Delivery and Support* (7 of 17 control objectives) it could be implied that the level of maturity of Information Technology services in the participating Tasmanian public sector organisations is not well developed, since there is a focus on early cycle activities, rather than those concerned with monitoring. It may be expected that in an audit of organisations with such a focus, monitoring activities would be less important than those associated with planning and organising, as well as delivery and support activities, with less focus on acquisition and implementation activities.

Previous studies

The studies by Guldentops *et al.* (2002) and Liu and Ridley (2005) used the same listing of control objectives considered by the former authors to be important, while Huissoud (2005) also reported a list of control objectives considered to be important. Neither the two former studies, nor the latter project report, provided a list that ranked all control objectives by their perceived importance. As a result, comparisons are able to be drawn regarding common entries, but not common rankings.

When comparing results among individual studies it can be seen that ten control objectives (or 59%) were common to the current study as well as to both the Guldentops *et al.* (2002) and Liu and Ridley (2005) investigations. Commonalities between the current study and Liu and Ridley (2005) might be expected, since Liu and Ridley (2005) reported results from the Australian public sector. However, it must be remembered that the listing used by those authors was adopted, unchanged, from Guldentops *et al.* (2002), which reported on an international, cross-sector study. Given that the list was originally derived from research published in 2002 and consequently was at least three years old when the Tasmanian study was undertaken, it suggests that some processes can be considered to be important regardless of the context (international, national or state) and are of enduring interest.

Comparing the current study with the results reported by Huissoud (2005) from the EUROSAI self-assessment project, nine control objectives (or 53%) appeared in both listings. The EUROSAI project examined control objectives considered by public sector audit organisations in Europe. The participants in the EUROSAI project were audit practitioners. However, in the Tasmanian study, data were gathered from IT managers. Auditors are likely to place a greater emphasis on monitoring activities, with one monitoring control objective (M1 Monitor the Processes) appearing in the listing of important control objectives reported by Huissoud (2005), while the highest rated monitoring control objective in the Tasmanian results was ranked 25 of 34. M1 Monitor the Processes was ranked at 30 while the other two control objectives from this domain appeared at rankings 33 and 34. Given the commonalities also found between the Tasmanian results and those of Guldentops *et al.* (2002) and Liu and Ridley (2005) the consistencies between the Tasmanian results and those reported by Huissoud are not particularly surprising and support the suggestion that the importance of some control objectives is independent of geographical context. There appears to be some evidence that the importance of the control objectives is also independent of organisational type, given the difference in the organisational setting between the two studies.

This commonality suggests that it may be possible to derive an abbreviated instrument from the COBIT framework for use in IT audit in different contexts. One potential starting point for such an instrument would be the list of eight control objectives that were common to all the studies examined in this paper (Guldentops *et al* 2002; Liu and Ridley 2005; Huissoud 2005). These control objectives were common regardless of geographical and organisational context. While Liu and Ridley (2005) examined only Australian public sector organisations, Guldentops *et al.* (2002) examined a range of sectors and nationalities, so further studies could compare the maturities reported by these latter authors against other sectors and nations.

CONCLUSION

This research identified an abbreviated list of 17 high level control objectives from the COBIT framework that were considered to be important to Tasmanian public sector organisations. Eight of these processes were also identified by three other authors (Guldentops *et al* 2002; Liu and Ridley 2005; Huissoud 2005) as being important in other contexts. This suggests that it would be possible to derive an abbreviated instrument from the framework for IT audit that would be both enduring and relevant across geographical and organisational contexts. Future work could develop IT audit measures for the most important IT control objectives, and trial such measures in public and private sector organisations in Tasmania and elsewhere.

REFERENCES

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.

Babbie, E. R. (1990) Survey Research Methods, Wadsworth Publishing Company, Belmont, California.

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

DPAC (2003) Tasmanian Government Information Security Framework Accessed 4/8/2006 at: http://www.go.tas.gov.au/standards/information_security_framework/information_security_charter.htm.

EUROSAI (undated) EUROSAI Institutional Information webpage, accessed 12/7/2005 at http://www.eurosai.org/Ingles/info_inst.htm.

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.

Huissoud, M (2005) IT self-assessment project, current results and next steps, Presentation to EUROSAI IT working group, Cypress, 14 February, 2005.

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

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.

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.

Salle, M., (2004) IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing, accessed on 20/04/2005 at http://www.hpl.hp.com/techreports/2004/HPL-2004-98.pdf.

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.

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.

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

ACKNOWLEDGEMENTS

The assistance of the Tasmanian Audit Office, particularly Christina Buell and Kate Tamayo is gratefully acknowledged.

APPENDIX

Instructions:

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.

**Note: The instructions appeared at the beginning of the second section of the questionnaire.

The scale:

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

**Note: The scale appeared at the top of each page of the questionnaire

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
☐	☐	☐	☐	☐	☐

**Note: All control objectives were laid out in a similar manner with the abbreviated version in bold and the remainder of the text in plain font. The control objectives were grouped according to their domains.

COPYRIGHT