COBIT and its Utilization: A framework from the literature

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

Judy Young
University of Tasmania
Judy.Young@infosys.utas.edu.au

Peter Carroll
University of Tasmania
Peter.Carroll@utas.edu.au

1. Introduction

The Control Objectives for Information and Related Technology (COBIT) is a "trusted" open standard [15: p.33] that is being used increasingly by a diverse range of organizations throughout the world. COBIT is arguably the most appropriate control framework to help an organization ensure alignment between use of Information Technology (IT) and its business goals, as it places emphasis on the business need that is satisfied by each control objective [3]. This paper reports on the use of a simple classification of the published literature on COBIT, to highlight some of the features of that literature.

The appropriate alignment between use of IT and the business goals of an organization is fundamental to efficient and effective IT governance. IT governance "…is the structure of relationships and processes to develop, direct and control IS/IT resources in order to achieve the enterprise's goals" [12: p.9]. IT governance has been recognized as a critical success factor in the achievement of corporate success by deploying information through the application of technology [12]. The importance of IT governance can be appreciated in light of the Gartner Group's finding that large organizations spend over 50% of their capital investment on IT [11]. However, research has suggested that the contribution of IT governance varies in its effectiveness [12]. IT control frameworks are designed to promote effective IT governance.

Recent pressures, including the failure of organizations such as Enron, have led to an increased focus on corporate accountability. For example, the Sarbanes-Oxley Act of 2002 introduced legislation that imposed new governance requirements [4]. These and other changes have resulted in a new corporate governance model with an increased emphasis on IT governance, which goes beyond the traditional focus of corporate governance on financial aspects [18].

2. Mechanisms to Promote Effective IT Governance

In part as a response to new governance requirements, increasing emphasis has been placed on internal controls in organizations. Controls are activities that are undertaken either to eliminate risks or reduce them to a level that is considered acceptable [8]. The "rules, policies and procedures involved in managing an organization's risks *[are considered]* as the system of internal controls" [15: p.32], where internal control is designed to give "reasonable assurance" on the achievement of objectives relating to the "efficiency and effectiveness of operations", the "reliability of financial reporting" and compliance with relevant laws and regulations [20]. The development of frameworks of internal control objectives to allow for international standardization has arisen also from pressure by auditors. Without a framework it is difficult for auditors to be able to substantiate their view on internal control [16].

In recent years a range of documents has been issued that aimed to assist with the definition, assessment, reporting on and improvement of internal control in organizations [3]. These include COBIT, Committee of Sponsoring Organizations (COSO), the Institute of Internal Auditors Research Foundation's Systems Electronic Security Assurance and Control (eSAC) and the IT Infrastructure Library (ITIL). Although such documents have been developed to address different needs and audiences, many of them have built on the contribution of previous documents and consider much the same internal control concepts [3]. For example, amongst others, COBIT has drawn on both COSO and a predecessor of eSAC.

3. COBIT

While a range of frameworks, standards and documents related to the control of IT exist, the primary focus of COBIT is on aligning use of IT with the achievement of organizational goals. COBIT is a comprehensive framework of 34 control objectives that has been developed from "41 international source

documents" [13: p.20] and validated internationally to help balance IT risk against investment in IT controls. The control objectives have been organized into a hierarchy of processes and domains that are designed to help bring about the alignment of business and IT objectives, by identifying the requirements for IT resources and information associated with 318 detailed control objectives. IT processes are grouped into four domains: planning and organization, acquisition and implementation, delivery and support and monitoring. As the framework considers all aspects of information and its supporting IT, management can use COBIT to help provide an appropriate control system for IT.

COBIT has been implemented in many countries since its introduction in 1996 [6, 7]. One explanation for COBIT's popularity is that its extensive *Executive Summary*, *Framework*, *Control Objectives*, *Management Guidelines* and *Implementation Tool Set* are free of charge. Payment is required only for the Audit Guidelines.

Organizations where COBIT has been adopted include Daimler-Chrysler in Germany [13], New South Wales Department of Health in Australia [23], Royal Philips Electronics in the Netherlands [25], Curtin University of Technology in Australia [9], Blue Cross Blue Shield of Michigan in the USA [9] and Department of Defense, USA [9]. That COBIT seems to be becoming an influential framework for the control and governance of IT is attested to by the significance and diversity of the organizations in which it has been utilized. Furthermore, as COBIT is currently in its 3rd edition, and a version for Small to Medium Sized Enterprises called CobiT Quickstart is due to be released in mid–2003, such developments further indicate COBIT's influence.

Surprisingly, it appears that relatively little academic literature has been published that investigates the utilization of COBIT. This may be because the extensive electronic sources available on COBIT are primarily designed for IT and audit practitioners. These sources are produced by Information Systems Audit and Control Association (ISACA) and the IT Governance Institute and are not referred to by many academic authors. Few studies that benchmark the adoption or use of COBIT have been published [7, 5, 21]. Apart from the excellent case studies produced by the IT Governance Institute, there is little literature that considers the range and characteristics of organizations that have utilized COBIT and the outcomes of implementation. If it can be established that implementation of COBIT is related to more effective IT governance, as it is hoped, then analyses of cases of both successful and unsuccessful implementations will lead to a better understanding of current best practice. Moreover, analysis of the extent of implementation by organization and industry, and categorization by size, sector, geographic area and so on, will be valuable in helping to identify trends. In turn, the results of such analyses will help to identify organizations with the greatest and least need for public and private sector investment in IT governance in the future, and as a consequence, lead to more effective targeting of expenditure.

To date it appears that only limited examination of the published literature on COBIT has been reported. Because much of the literature that is available on COBIT appears to have a practitioner focus, and has been made available through a range of often non-academic fora, the literature is not as accessible as that available in areas that have been investigated intensively by academic researchers. Consequently, there is a need to synthesize and characterize the literature that does exist.

4. Development of a Framework for Research

A research framework is a way of organizing past and present research [14]. Research frameworks should display completeness, consistency, mutual exclusivity, conciseness and have the potential to impact on research behavior [1]. This paper develops a simple framework that characterizes the COBIT literature along a range of dimensions, including: the extent of theoretical or applied orientation, whether primarily of practitioner or academic orientation, the organizational sector under consideration, industry and size, geographic location and degree of utilization. The development of a framework will make it easier to examine both the literature that is currently available and that to be published, as well as to identify gaps in the literature so as to promote future research.

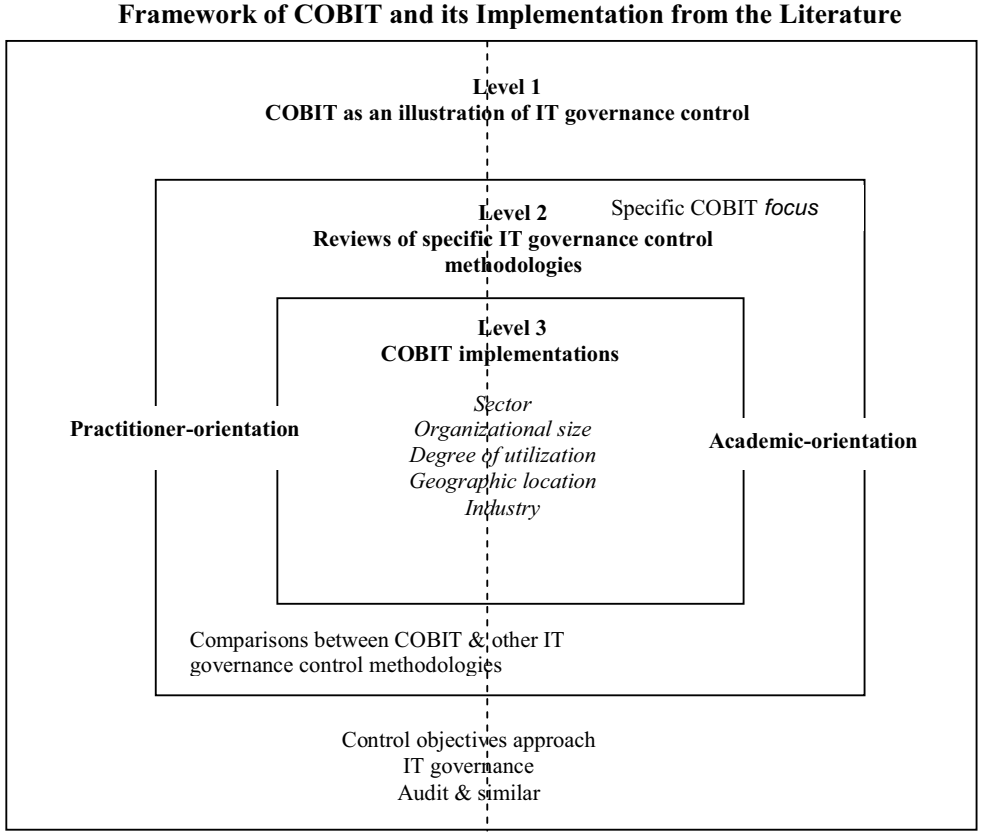

Figure 1 Framework of COBIT and its Implementation from the Literature

The conceptual framework, as indicated above in Figure 1, consists of three levels which display a decreasing theoretical, and increasing applied, orientation from the first level to the second and third. At all levels there is a differentiation between academically-oriented papers and practitioner-oriented papers. The basis for differentiating between the latter two groups is discussed in the methodology section of this paper.

4.1. Level 1 of framework

Level 1 literature that is "Illustrative of IT governance control document", typically includes one or more references to COBIT to illustrate some aspect of IT governance, the control objectives approach, audit procedures or similar. Discussion tends to be at a theoretical or conceptual level rather than at an applied or implementation level. There is only a minor emphasis upon COBIT in the literature at this level.

4.2. Level 2 of framework

Level 2 literature concerned with "Reviews of specific IT governance control methodologies" is also primarily theoretical, and may either focus entirely on COBIT, or may present a comparison between COBIT and one or more other IT governance control methodologies, such as COSO or eSAC. Surveys regarding COBIT, including those that present an overview of its implementation, would be classified at this level. Surveys of COBIT implementations are not classified as belonging to Level 3, as specific implementation criteria are needed to be able to classify an implementation at this level. Surveys are unlikely to provide sufficient detail on an individual implementation to be able to classify them at Level 3. There is more frequent reference to COBIT in Level 2 literature than in Level 1.

4.3. Level 3 of framework

Level 3, "COBIT implementations" has an applied orientation, with the literature typically considering the actual use of COBIT in individual organizations, including case studies. The publications focus on one or more of a range of dimensions, including organizational sector, organizational size, the degree of implementation of COBIT, the geographic location and industry**.**

At Level 3, the literature was classified using the dimension Sector, that is, whether the literature reported upon implementations of COBIT in organizations within the Public, Semi-public or private sector.

The category Organizational Size was included in Level 3 of the Framework, so that implementations of COBIT could be coded as either Large or Small to Medium Sized Enterprise (SME).

As COBIT contains a range of tools, including Audit Guidelines, Maturity Models, CobiTonline and Critical Success Factors, it is possible for organizations that adopt the methodology to use it as a reference only, to use some of its tools, or to use it in its entirety. For this reason Level 3 of the Framework included a category, Extent of Implementation, which could be recorded as High, Medium or Low.

It was anticipated that implementations of COBIT reported in the literature will come from a range of nations. For this reason the category Geographical Location was included in Level 3 of the Framework.

Finally, the Framework including a classification of organizations that implemented COBIT, using ten industry categories: *Energy, Materials, Industrials, Consumer-discretionary, Consumer-staples, Health Care, Financials, IT, Telecoms* and *Utilities*.

5. Methodology

An objective ontology and positivist epistemology were adopted for the investigation, which used a descriptive, quantitative approach and the content analysis method.

A search was made of the ProQuest electronic database and google.com in June 2003, to find refereed and non-refereed journal and conference proceedings, as well as practitioner-based publications that included the acronym COBIT. The ProQuest full collection database was used, rather than other databases or in conjunction with other databases, as it contains a high level of full-text papers in comparison with other electronic databases. It also contains abstracts for almost all papers, whereas many other electronic databases do not. ProQuest is not case sensitive for search terms. An extensive range of management, accounting and IT academic and non-academic publications are indexed by ProQuest. It is acknowledged that other papers that include the term COBIT may also have been published that would not be located in a search of these resources. However, this investigation did not seek to find all publications on COBIT, but instead sought an indication of the number and categories of publications that make reference to COBIT.

Book reviews were excluded from the analysis. The remaining publications were categorized on the basis of the full-text version, where available, or where they were not available, on the basis of the abstracts.

Both practitioner-oriented and academic-oriented papers were examined and included in the analysis, differentiating between the two groups at each level. Practitioner publications tended to be shorter, had few if any references, to be published in non-refereed publication outlets and were usually, although not always, written by authors from industry rather than academia. The academically-oriented publications usually had a more comprehensive list of references, tended to be longer, and usually, but not always, were published in refereed outlets and were usually written by authors from academia.

Publications were classified within each of the three levels of the developed framework. Theoretical publications that included one or more references to COBIT for illustrative purposes in a theoretical discussion of topics including IT governance, the control objectives approach and audit processes were placed in Level 1. For one such example of an academically-oriented paper refer to [17]. The primary focus of publications classified as belonging to Level 1 was not on COBIT or other IT control methodologies. Publications that were categorized at Level 2 of the framework included those that reviewed COBIT as a specific IT control methodology (for example, the practitioner-oriented paper, [13], or compared and contrasted two or more control frameworks where one was COBIT (for example, the academically-oriented paper [3]. Publications that were coded as belonging to Level 3 were individual implementations of COBIT in organizations. As noted in the earlier discussion on the Framework, the sector, organizational size, extent of utilization of COBIT, geographic location and industry of the organization were sought. Where these could not be identified, the code "unknown" was recorded.

Ten industry category sectors were used for classification purposes, following the first level of the Global Industry Classification Standard (GICS). These are *Energy, Materials, Industrials, Consumer discretionary, Consumer staples, Health care, Financials, Information technology, Telecommunication services and Utilities* [19]. The term "industry" was used by the authors instead of "sector" as the latter term was reserved in the Framework for the public or private enterprise characteristic. GICS was chosen as it provides a limited set of current, comprehensive and consistent industry categories that is appropriate for global use [19].

For organizational size, this study will use the US definition of SMEs, where they are organizations with less that 2500 employees [24]. For geographic location, COBIT implementations were recorded for the Americas, Asia/Oceania, Europe or Africa.

Frequencies for each of the categories were recorded and then presented in tabular form. As it was likely that a degree of subjectivity could affect the coding process, two researchers trained in Information Systems research methods classified the papers independently after becoming familiar with the framework, and a comparison was made between the codes of each to determine the level of intercoder reliability. An acceptable level of intercoder reliability was assumed to exist where the agreement was 70% or more. It is argued that substantial agreement between the coders is an indicator of the completeness, consistency and mutual exclusivity of the framework**.**

6. Results

Table 1 sets out the number of publications found in each level of the framework. The two researchers agreed as to classification for 62 of the 83 or 74.7% of the publications identified.

A total of 17, or 20.5% were classified at Level 1. Another 32 publications, or 38.6%, were classified as Level 2, of which the great majority focused on COBIT only, while a small minority compared COBIT with one or more control documents. A total of 34, or 41% of the publications was classified at Level 3.

Only 6, or approximately 7% of the publications were classified as having an academic orientation, while 77 or approximately 93% were classified as being practitioner-based.

A breakdown of the different categories at Level 3 is presented in Table 2.

From the 34 publications that reported on COBIT implementations, two separate publications reported on the same implementation, the New South Wales Health case [22, 23].

Of the 34 publications regarding implementations of COBIT classified at Level 3, seven or approximately 21% related to public organizations, two or approximately 6% were semi-public while 25 or approximately 74% were from the private sector.

For the category organizational size, 18 or approximately 53% of the publications were from large organizations, five or approximately 15% were found to be of SME size while in a further 11 cases, or approximately 32%, organizational size was unknown.

The next category, extent of implementation, was the most subjective of the classification categories as, in many of the case studies, the number of employees was implied in the description rather than made explicit. In nine or approximately 24% of the publications, COBIT had been implemented to a high degree in the organization, while in 7 publications or approximately 21%, the extent of implementation was regarded as medium. The extent of implementation was regarded as low in 17 publications, which represented 50% of the total, while in one publication the extent of implementation was classified as unknown.

A total of 15 publications, or approximately 44%, reported implementation of COBIT in the Americas geographical region, while seven or approximately 21% of the case studies reported on organizations in Asia/Oceania. Publications reporting on implementations in Europe totaled seven, while three or approximately 9% were from Africa and two, or approximately 6% were located in an unknown geographical location.

One publication (approximately 3%) was recorded for each of the following industries: Energy, Materials, Consumer-discretionary, Consumer-staples and Utilities, while no publications were found that reported on implementations in the Telecom industry. In three publications (approximately 9%) the industry was unknown while four publications (approximately 12%) reported on implementations in the IT industry. Five publications (or approximately 15%) were noted for both the Industrials and Health care. The largest number of publications reported on implementations in the Financial industry, at 12 or approximately 35% of the total. Of the financial group, eleven publications reported on COBIT implementations in the private sector. From the financial group, 6 publications or approximately 18% reported a high extent of implementation.

Table 1 Number of Papers in Each Level of the Framework

	Orientation		**Totals**
Level 1 Illustrative of IT controls or similar *	Academic 4	Practitioner 13	17
Level 2 Reviews of IT control methodologies etc.			
Sole focus on COBIT **	1	27	28
Comparison with COBIT	1	3	4
Level 3 COBIT implementations		34	34
Totals	**6**	**77**	**83**

Note that papers marked either with * or ** that also appeared in the references for this paper have been marked in the same way in the list of references as examples of papers in their category.

Table 2 Number of Papers in Each Dimension from Level 3 of the Framework

	Sector			**Organization Size**			**Extent of Implementation**				**Geographical Location**				
Industry	**Public**	**Semi-public**	**Priv**	**Large**	**SME**	**Unknown**	**High**	**Med**	**Low**	**Unknown**	**Americas**	**Asia/ Oceania**	**Europe**	**Africa**	**Unknown**
Energy			1		1				1		1				
Materials			1	1					1		1				
Industrials	2	2	1	4		1	1	2	2		4	1			
Consumer-discretionary			1	1			1						1		
Consumer-staples			1	1			1							1	
Health Care	3		2	5					4	1	1	3		1	
Financials	1		11	3	3	6	6	4	2		5	2	4	1	
IT			4	1	1	2			4		1		2		1
Telecoms															
Utilities			1			1		1			1				
Unknown	1		2	2		1			3		1	1			1
Totals	**7**	**2**	**25**	**18**	**5**	**11**	**9**	**7**	**17**	**1**	**15**	**7**	**7**	**3**	**2**

0-7695-2056-1/04 $17.00 (C) 2004 IEEE

7. Conclusions

The results of the preliminary analysis of the COBIT literature found that the majority of the publications examined focused on the private sector. Further empirically-based study would have to be undertaken to see if this was the case in practice.

The difficulty in determining the size of organizations from the material provided in the case studies made it hard or impossible to classify them by this dimension. If the COBIT-implementing organizations of unknown size are allocated to the large and SME category in a similar proportion to those that could be categorized, then the data suggest that large organizations are more likely to implement COBIT. While this is speculation, if it proves to be the case then it is not surprising, given that IT governance is more complex in large organizations and so it is likely that there will be more interest in IT control from these organizations.

A low extent of COBIT implementation within organizations was found to be the most common. However, classification of organizations on the basis of this criterion was difficult due to the often limited detail available in the publications examined. The highest proportion of publications reporting implementation of COBIT came from the Americas, which was not surprising when it is considered that the body that developed COBIT originated in the USA. It was heartening to see a reasonable proportion of implementations were reported in both Europe and Asia/Oceania, suggesting that COBIT has support beyond the USA.

Financial organizations appeared more likely to implement COBIT. This finding was not unexpected when it is remembered that many of the drivers to monitor IT governance have been derived from corporate governance, and the latter area has traditionally focused on financial issues.

Although the results of the analysis of the publications are of interest, readers need to be cautious in their interpretation. Not all publications referring to COBIT have been identified. It is likely that a wider range of academic and practitioner conference publications and other practitioner publications that have considered COBIT are available. Consequently it is difficult to know how representative the identified publications are of the total publications available that make reference to COBIT. However, given the status and size of the resources searched, the specificity of the term, and the number of publications found, it is likely that the results will act as a reasonable indicator of the characteristics of publications that refer to COBIT. The results of this investigation are at least sufficient to warrant a more detailed literature review that is capable of drawing firmer conclusions. Moreover, as this paper may be the first to examine the COBIT literature, it is appropriate that it was exploratory and descriptive in nature.

Application of the framework to the literature that referred to COBIT confirmed that the great majority of the publications identified were practitioner-oriented, with very few academically-oriented publications. Of the limited number of academic publications found, only two focused on COBIT, and none reported on COBIT implementations. This suggests both a need for rigorous research in the area and considerable potential for future work. The practitioner publications revealed an interest in COBIT, as did the number and characteristics of the implementations reported.

The simple framework developed for the current investigation could be used to classify all 83 of the publications found which made reference to COBIT, with an acceptable degree of inter-coder reliability. However, some of the Level 3 characteristics regarding implementation needed to be recorded as unknown for case studies that lacked detail. These findings suggest that the framework is at least reasonably robust. As the number of COBIT publications increases over time, further testing of the framework will determine whether it can be regarded as complete, consistent, mutually exclusive and concise, with the potential to impact on research behavior.

8. References

[1] M. Bariff and M. Ginzberg, "MIS and the Behavioral Sciences: Research patterns and prescription", *Data Base*, 1982, Vol. 14, No. 1, pp. 19–26.

[2] P.Campbell, Survivability via Control Objectives, *3rd IEEE Information Survivability Workshop* (ISW-2000), 2000, pp. 1–4.

[3] J.Colbert, and P.Bowen, "A Comparison of Internal Controls: COBIT, SAC, COSO and SAS 55/78", *IS Audit & Control Journal*, 1996, Vol. 4, pp. 26–35.

[4] G. Coppin, "The Tentacles of the US Law", *Accountancy SA*, 2003, Jan., pp.14–17.

[5] J.Fedorowicz, and J. Ulric, "Adoption and Usage Patterns of COBIT: Results from a survey of COBIT purchasers", *Information Systems Audit & Control Journal*, 1998, Vol. 6, pp. 45–51.

[6] E. Guldentops, and S. De Haes, "COBIT 3rd Edition Usage Survey: Growing Acceptance of COBIT", *Information Systems Control Journal*, 2002, Vol. 6, pp. 25–31.

[7] E Guldentops, W. Van Grembergen, and S. De Haes, "Control and Governance Maturity Survey: Establishing a Reference Benchmark and a Self-Assessment Tool",

Information Systems Control Journal, 2002, Vol. 6, pp. 32–35.

[8] A. Hollander, E. Denna, and J. Cherrington, *Accounting Information Technology and Business Solutions*, 2nd Edn., Irwin McGraw-Hill, Boston, USA, 2000.

[9] Information Systems Audit and Control Association COBIT Case Studies, Available: http://www.isaca.org/ct_case.htm, 2003, Accessed: 17th January, 2003.

[10] IT Governance Institute COBIT 3rd Edition Executive Summary, Available: http://www.isaca.org/execsum.pdf, 2000, Accessed: 28th January, 2003.

[11] C. Koch, "The Powers That Should Be: IT decisions have to reflect the goals of the business and engage the attention of the business, often without the participation or even the interest of the business", *CIO*, 2002, Vol. 15, No. 23, pp. 48–54.

[12] N. Korac-Kakabadse, and A. Kakabadse, "IS/IT Governance: Need for an Integrated Model", *Corporate Governance*, 2001, Vol. 1, No. 4, pp. 9–11.

[13] J. Lainhart, "An IT Assurance Framework for the Future", *Ohio CPA Journal*, 2001, Jan–Mar, pp. 191–193.

[14] K. Lyytinen, "Different Perspectives on Information Systems: Problems and solutions", *ACM Computing Surveys*, 1987, Vol. 19, No. 1, pp. 5–46.

[15] J. Pathak, "Internal Audit and E-Commerce Controls", *Internal Auditing*, 2003, Vol. 18, No. 2, pp. 30–34.

[16] N. Payne, "IT Governance and Audit", *Accountancy SA*, 2003, Jan, p. 35.

[17] J. Rodero, J. Toval and M. Piattini, "The Audit of the Data Warehouse Framework", *Proceedings of the International Workshop on Design and Management of Data Warehouses*, Heidelberg, Germany, 1999, June 14–15, pp. 14–1:14–12.

[18] R. Roussey, "The New Corporate Governance Model: A focus on independence, the audit committee and the accounting profession", Available: www.ebusinessgovernance.org/rsr-governance.doc, 2003, Accessed: May 23, 2003.

[19] Standard and Poor's Global Industry Classification Standard, Available: http://www.sptopix.com/icp_e/industry/peers/gics_e.html, 2003, Accessed May 28, 2003.

[20] The Committee of Sponsoring Organizations of the Treadway Commission, Internal Control-Integrated Framework: Executive Summary, Available: http://www.coso.org, 1992, Accessed: May 15, 2003.

[21] J. Tongren, and S. Warigon, "A Preliminary Survey of COBIT Use", *EDP Audit, Control and Security Newsletter*, 1997, Vol. 25, No. 3, pp. 17–19.

[22] R. Tyler, "Implementing COBIT in New South Wales Health", *EDP Audit, Control and Security Newsletter*, 1999, Vol. 27, No. 1, pp. 1–6.

[23] R. Tyler, "Implementing COBIT in New South Wales Health", *Information Systems Control Journal*, 2000, Vol. 3, pp. 30–32.

[24] US Census Bureau Statistics, About Business Size (Including Small Business) from the US Census Bureau, Available: http://www.census.gov/epcd/www/smallbus.html, 2002, Accessed: June 24, 2003.

[25] A. Van Gils, "Implementation of the COBIT-3 Maturity Model in Royal Philips Electronics", in Gertz M., Guldentops, E. and Strous, L. (eds.) *Integrity, Internal Control and Security in Information Systems: Connecting Governance and Technology, IFIP TC11/WG11.5 Fourth Working Conference on Integrity, Internal Control and Security in Information Systems*, 2001, Nov. 15–16, 2001, Brussels, Belgium, pp. 161–174.