Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2010 Proceedings | Australasian (ACIS)

2010

Selecting IT Control Objectives and Measuring IT Control Capital

Harminder Singh
Auckland University of Technology, hsingh@aut.ac.nz

Selecting IT Control Objectives and Measuring IT Control Capital

Harminder Singh
Faculty of Business & Law
Auckland University of Technology
Auckland, New Zealand
Email: harminder.singh@aut.ac.nz

Abstract

COBIT is a well-known framework for IT governance, and provides an extensive list of control objectives for IT managers. However, anecdotal evidence shows that many organizations that use COBIT do not implement the entire framework. Instead, they focus their efforts on only some of COBIT's control objectives. We argue that this could be due to the bounded rationality of IT managers, which affects their ability to assess the outcomes of control, and the diminishing returns from implementing controls, because of enforcement costs incurred to control shirking. Managers would thus find it useful if the various control objectives could be ranked, so that they could prioritize their efforts. We use network analysis to identify the most central control objectives in COBIT. We also discuss the development of a measure of "control capital" to capture the level of control an organization achieves after implementing a particular set of controls. Future research will test the empirical validity of this measure.

Keywords

governance, control, capital, network analysis

INTRODUCTION

As the use of information technology (IT) in organizations has expanded, both IT and functional managers have become increasingly concerned about IT governance. This is driven by the greater risks of using IT: modern information systems are more integrated and heterogeneous, and can be accessed by a wide range of organizational members (Markus, 2000). These risks, which include poorly-integrated infrastructure, unstandardized data and workarounds (Sherer & Alter, 2004; Westerman, 2006) are aggravated by the uncertain benefits and irreversible costs of IT adoption decisions (Fichman, 2004).

While earlier research on IT governance examined the different governance structures organizations use and the contingencies that influenced their choice (Brown & Magill, 1994; Brown, 1999; Brown & Grant, 2005; Weill, Soh & Sia, 2007; Sambamurthy & Zmud, 2000; Agarwal and Sambamurthy, 2002; Schwarz & Hirschheim, 2003), recent research has focused on the use of codified frameworks, such as COBIT (Control Objectives for IT)[1] and ITIL (IT Infrastructure Library), and their impacts. This shift is motivated by the widespread use of these frameworks by IT practitioners. However, the proliferation of such guidelines, their complexity, and the uncertainty over how they should be modified to fit the specific circumstances of each organization highlights the importance of identifying the key practices within these frameworks- that is, those that offer the most "bang for the buck". This question is further complicated by the relationships that exist between the IT processes in these frameworks. For example, some processes provide inputs for others, or use the outputs of other processes as their inputs. Some studies in this field have examined this question by surveying practitioners (e.g. Debreceny & Gray, 2009; Kim, Phelps & Milne, 2006). This paper attempts a different approach to answering it. Focusing on the pattern of relationships within COBIT, I use network analysis to identify the most central control objectives within it.

A second question addressed in this paper is how the level of IT governance in an organization can be assessed after it has deployed a control framework. Currently, it is difficult to quantify the impacts of implementing IT governance controls. They are often perceivable only in the negative: that is, when no IT-related "problems", such as delayed projects, budget over-runs, conflicts with vendors, security breaches, loss of data, or dissatisfied users, take place. Building on the concepts of social capital, which refers to the level of resources that can be accessed by individuals (Lin, 1999), and process capital, which estimates the value of organizational processes

[1] COBIT is a framework that lists best practices on the types of controls required for managing a firm's IT assets. It was developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI).

(Johnson, 1999), I define "control capital" as a measure of the level of control in an organization's IT portfolio, in terms of how extensively it uses COBIT. This approach builds on the knowledge embedded within COBIT, which is the basis on which the various control objectives have been structured into a framework. In short, since the control processes with the highest centrality in COBIT contribute the most to increasing the level of IT governance in an organization, an organization's control capital can be assessed by looking at the specific control processes it has deployed.

I begin by discussing some recent research on the practice and consequences of IT governance, and propose some reasons why IT managers adopt these frameworks at different levels of comprehensiveness. Next, I show how network analysis can be used to help these managers decide which control objectives they should focus their efforts on. I then illustrate my concept of "control capital" by comparing it to process capital and social capital. Finally, I discuss the limitations of this study and offer some future directions for research.

USE OF IT GOVERNANCE FRAMEWORKS

Broadly defined as an organization's IT-relevant decision-making structure, IT governance has been found to be significantly positively correlated with firm performance (Weill, 2004), and to affect the returns firms receive from their IT investments (Gu, Xue, & Ray, 2008). Prior literature on IT governance has discussed the variety of structures organizations can use to manage their IT resources (e.g. Warkentin & Johnson, 2006; Weill & Broadbent, 1998), and the contingencies that influence the choice of governance structures (Brown & Grant, 2005), such as economies of scope and absorptive capacity (Sambamurthy & Zmud, 1999), firm culture and vision (Brown & Magill, 1994), and the level of globalization (Weill, Soh & Sia, 2007).

More recently, some researchers (e.g. Milne & Bowles, 2009; De Haes & Van Grembergen, 2008; Debreceny. 2006; Kim, Phelps & Milne, 2006; Guldentops, Grembergen & De Haes, 2002; Liu & Ridley 2005; Nicho & Cusack, 2007) have studied the use of externally-developed and rigorously-codified frameworks for IT governance, such as COBIT and ITIL. These are auditable lists of requirements that organizations are recommended to adopt, so that their IT systems remain usable and useful, as well as aligned with their business[2]. The use of these frameworks increased (see Table 1 below) as concern grew in the early 2000s over the lack of internal controls in publicly-traded firms in the US. This anxiety led to the passage in the United States of the Public Company Accounting Reform and Investor Protection Act of 2002[3], whose Section 404 requires public firms to evaluate and report the viability of their system of internal controls in their regulatory submissions. The Act's emphasis on enhancing internal control spurred the use of COBIT and other similar frameworks to enhance the overall level of control of work processes, especially those related to financial and accounting information.

Table 1. Use of Different IT Control and Performance Frameworks

	2006	2005	2004
Balanced Scorecard	63.81%	59.60%	59.16%
Capability Maturity Model Integration	30.00%	29.40%	18.85%
Capability Maturity Model for Software	25.00%	25.00%	18.32%
Malcolm Baldrige Quality System	9.29%	11.20%	6.54%
People Capability Maturity Model	7.62%	8.40%	3.40%
Six Sigma	41.19%	38.20%	35.86%
Lean Six Sigma	29.76%	19.80%	-
QPR Scorecard (Corporate Performance Management)	14.29%	14.60%	7.33%
Business Activity Monitoring	22.14%	20.20%	8.90%
IT Infrastructure Library (ITIL)	50.71%	38.40%	6.02%
ISO 9000x	40.95%	43.80%	35.60%

[2] Some, such as ITIL, focus on the day-to-day operational aspects of providing IT services, so as to enhance their quality. They cover procedures such as providing a help-desk, rolling out software updates and managing IT security. Others, such as COBIT, take a different approach. Developed by auditing professionals, these guidelines emphasize balancing the risks and returns of IT use by putting in place a set of internal controls.
[3] The Act is commonly known as "SOX", after its legislative sponsors, Senator Paul Sarbanes and Representative Michael Oxley.

COBIT	5.48%	2.60%	1.31%
Other*	6.19%	8.00%	24.35%
None	23.10%	18.00%	12.30%
European Foundation for Quality Management	-	-	2.09%
Software Acquisition Capability Maturity Model	-	-	3.14%
System Engineering Capability Maturity Model	-	-	5.24%

**: "Other" includes COBIT (2004, 2005 & 2006 surveys) and ITIL (2004 survey). The data is from Information Week's annual survey of IT executives. Data from the 2007 and 2008 surveys is in the process of being procured.*

Despite the extensive and detailed guidance in governance frameworks, a recent survey found that half of the organizations that use such frameworks use them as a reference source, with only about a third applying them strictly (Information Technology Governance Institute, 2008). Similarly, Debreceny & Gray (2009) found that only about 16% of the firms they surveyed were intensive users of COBIT. One reason for this could be that a subset of COBIT's control processes provided most of the desired governance benefits. Kim and his colleagues (Kim et al., 2006; Kim et al., 2007) found that the organizations that saw themselves as high-performers in terms of IT used only a few controls. These "foundational controls" focused on change management, access management, and error management procedures.

A behavioural theory perspective (March & Simon, 1958; Cyert & March, 1963) provides alternative explanations as to why these frameworks are not adopted exhaustively. First, because IT managers are boundedly rational, they could decide to "satisfice", not maximize, the extent to which their IT portfolios are governed. Instead of aiming to control all aspects of their portfolio rigorously, they could target a "good enough" level of governance by putting in place only some controls. Second, there could be diminishing returns from deploying controls, if the costs of enforcing them (such as preventing individuals from shirking) are greater than their benefits. There may thus be an "inverted-U"-shaped relationship between the intensity of controls applied and the actual level of control achieved. As more and more controls are put in place, the level of control achieved increases at first but after reaching a peak, begins to decline. This would encourage IT managers to deploy the sub-set of controls indicated by the peak of the inverted U-shape. Third, bounded rationality leads to IT managers making imperfect assessments of the outcomes of control. They may overestimate the benefits that accrue from implementing IT controls and/or underestimate the costs of implementing and maintaining them. Alternatively, they may initially deploy all the controls in a framework, and then reduce the number of controls as they learn more about their respective costs and benefits.

Control Capital

The preceding paragraph discussed a variety of reasons why IT practitioners will select only a subset of the controls recommended by IT governance frameworks. It will thus be useful for IT managers to find some way of deciding which controls they should choose. This study proposes one way of doing so: it applies network analysis techniques on the COBIT control framework, and identifies the control objectives that are highly central in COBIT as the core control objectives.

From a theoretical perspective, this exercise will help researchers develop a way of assessing an organization's level of IT governance. Currently, the effectiveness of IT-related controls is only obvious post-hoc and in the negative (i.e. no IT-related "problems", e.g. delayed projects, budget over-runs, conflicts with vendors, or dissatisfied users, take place). This makes is difficult to evaluate how well an organization is governing its IT investments. Counting the number of controls deployed for this purpose is inadequate, because each control's impact depends on which other controls are deployed. While some corporate governance researchers have used counts to evaluate the level of corporate governance (Bebchuk, Cohen & Ferrell, 2008; Gompers Ishii & Metrick, 2003), others have argued that such measures are prone to measurement error and have developed indices using principal components analysis (Larcker, Richardson & Tuna, 2007).

This study adopts an alternative perspective by developing the concept of "control capital" and measuring it with network analysis. The concept of control capital draws from the literature on process capital, which refers to the tacit knowledge embedded in an organization's corporate practices, procedures and trade (Johnson, 1999), and social capital, which can be defined as the resources embedded in a social structure which are accessed and/or mobilized in purposive actions (Lin, 1999).

These two forms of capital are relevant here because, over and above formal policies and practices, IT governance is built upon personal relationships within an organization (Agarwal & Sambamurthy, 2002; IT Governance Institute, 2003; Yu & Wu, 2008). Assessing the quality of a organization's IT governance by examining how many formal checks it has put in place may be convenient but it ignores the role of those in charge of carrying out these checks and how well they interact with each other.

One way of understanding the quality of the relationships in an organization is to examine the level of social capital, which is embedded in these. Its three aspects – structural, relational and cognitive – can be combined to create intellectual capital (Nahapiet & Ghoshal, 1998). The structure of an organization is key to understanding the notion of social capital, as it determines who has access to the valuable resources embedded in that structure (Lin, 1999) and who has the opportunity, motivation and ability to develop social capital (Adler and Kwon, 2002).

At the same time, it is also important to study how well the processes recommended by IT governance frameworks are being carried out. Process capita attempts to place a value on organizational processes, so that organizations can be compared based on their efficiency and effectiveness. The underlying idea is that processes are beneficial because they enable organizations to carry out their tasks, such as producing and delivering goods to their customers, and represents tacit, embedded knowledge (Johnson, 1999; Joia 2000; Kannan & Aulbur, 2004; Bontis 2004; Skandia, 1996). Process capital is thus considered part of an organization's intellectual capital and is part of its intangible assets (Edvisson & Malone, 1997).

Social and process capital are both forms of intangible capital. They are valuable to organizations because they can help them uncover their tacit attributes, which they can deploy to improve their performance, but are also difficult to measure. IT control is in the same category, as an insufficient amount of it would make it difficult for organizations to obtain value from their IT investments. Like social and process capital, IT control has various aspects – policies, individuals, and procedures – and managing their inter-relationships is crucial to achieving a high level of each form of capital. Each of these components also represents valuable embedded organizational knowledge that has been developed over time, as managers have learned from their experiences. Finally, all three are similar in that they can be measured in many different ways, with each being an incomplete snapshot.

Researchers have proposed various measures of process capital, For example, Johnson (1999) used a mixture of quantitative and qualitative indicators, such as throughput efficiency, while de Pablos (2002) suggested counting the number of ISO 9000 certifications. Skandia, a Swedish financial firm, has developed a tool, called the Skandia Navigator, to divide process capital into different types of capital, such as intellectual capital (Edvisson & Malone, 1997). Social capital has been measured with network analysis by examining dimensions such as the types and strength of ties in an organization and the ability of nodes to act as bridges to resources for other nodes. Other ways of measuring it include estimating the value of the resources in the network and the intensity of other dimensions, such as the relational and cognitive aspects.

Since network analysis is one of the tools used to measure social capital, we propose to do the same with control capital, so that a value can be placed on an organization's IT control environment. One possibility for improving our understanding of control capital would be to examine different ways of assessing IT control capital by drawing on prior studies in the other two domains. Here, we make a start at doing so by using network analysis. The next section presents the data and methods that were used to determine the most central objectives in COBIT. The following section discusses the results and presents our future plans in this area.

DATA AND METHODOLOGY

Network analysis is used to reveal patterns in relationships between entities, or to understand properties of entire networks, such as their density, sparseness or level of clustering. Some contexts in which it has been used include research networks (Reagans and McEvily, 2003), communication networks (Monge and Contractor, 2003) and influence networks (Meyer, 1994). It is an appropriate methodology in this context because the various control objectives in COBIT are related to each other: each of them is an input to or output from another objective. Thus, the objectives vary in terms of how many and which objectives they are linked to.

Analysing the position of each objective vis-à-vis all other objectives will reveal which COBIT objectives are the most central. That is, across all objectives, which objectives have the highest number of links with other objectives? Our contention is that these objectives are the core objectives in the COBIT framework. Compared to previous research that mainly looks at frequency counts of the individual COBIT objectives or self-assessments of COBIT use, network analysis allows us to use more of the information embedded within the framework to reveal its underlying architecture.

The entities that are linked together are called "nodes" in network analysis, while the relationships between the nodes are "ties" or "links". In the context of this paper, the links are directional, because COBIT objectives can be either inputs to or outputs from other objectives. In other contexts, such as studies of collaboration networks, links can be non-directional. While network analysis can be used to conduct a wide range of tasks, our focus here is on identifying the most central nodes. These central nodes are very well-integrated into the network. Other uses of network analysis include: identifying clusters or sub-communities within networks, locating nodes that have the same pattern of relationships (i.e. they are structurally equivalent), or uncovering unused connections.

The data for the network analysis comes from the COBIT version 4.1 framework (ITGI, 2007). It lists how each objective is related to the other objectives. For example, page 35 of the framework states that the outputs of Objective PO2 ("define the information architecture"), such as the data dictionary and the optimized business systems plan, are used as inputs for various objectives, including AI2 ("acquire and maintain application software") and PO3 ("determine technological direction"). In the same way, the outputs of other objectives are used as inputs for PO2; one example is AI7's post-implementation review.

This information was used to construct a square matrix, with the rows and columns containing all of the control objectives. The cells in the matrix were filled with 1 if there was a link between each pair of control objectives. Separate matrices were created for the "input" and "output" information. Although it was assumed that they would be mirror images of each other, this was not to be. A selection of the "output" matrix for the ME objectives is shown below (Table 2). The "1" in the intersection of the ME3 row and the ME4 column indicates that an output from the ME3 objective is used in the ME4 objective.

Table 2 "Output" Relationship Matrix for ME Objectives

	ME1	**ME2**	**ME3**	**ME4**
ME1	0	1	0	0
ME2	1	0	0	1
ME3	1	0	0	1
ME4	1	0	0	0

These matrices were then used as inputs into UCINet (Borgatti, Everett, and Freeman. 2002) and NetDraw (Borgatti, n.d.) UCINet is used to create networks based on the data matrices and analyse them, while NetDraw is used to visualize the networks as graphs. Figures 1 and 2 below depict the networks that were revealed by the analysis of the COBIT framework. These networks represent the links between the nodes as lines with arrows, indicating the directionality of the relationship between the objectives. For example, Figure 1 shows that outputs from node DS10 are used as inputs in DS 13, DS9 and DS8. At the same time, DS10 uses as its inputs the output from AI6 and ME1. The different colours of the nodes (red, blue, black and grey) represent the four COBIT domains: PO, AI, DS and ME.

It can be observed that:

a) the two networks differ in the denseness of the links between the nodes;

b) some nodes, such as DS1 and PO10, have relatively more links (i.e. are more "central" in the language of network analysis) to other nodes; and

c) only some nodes are central in both networks.

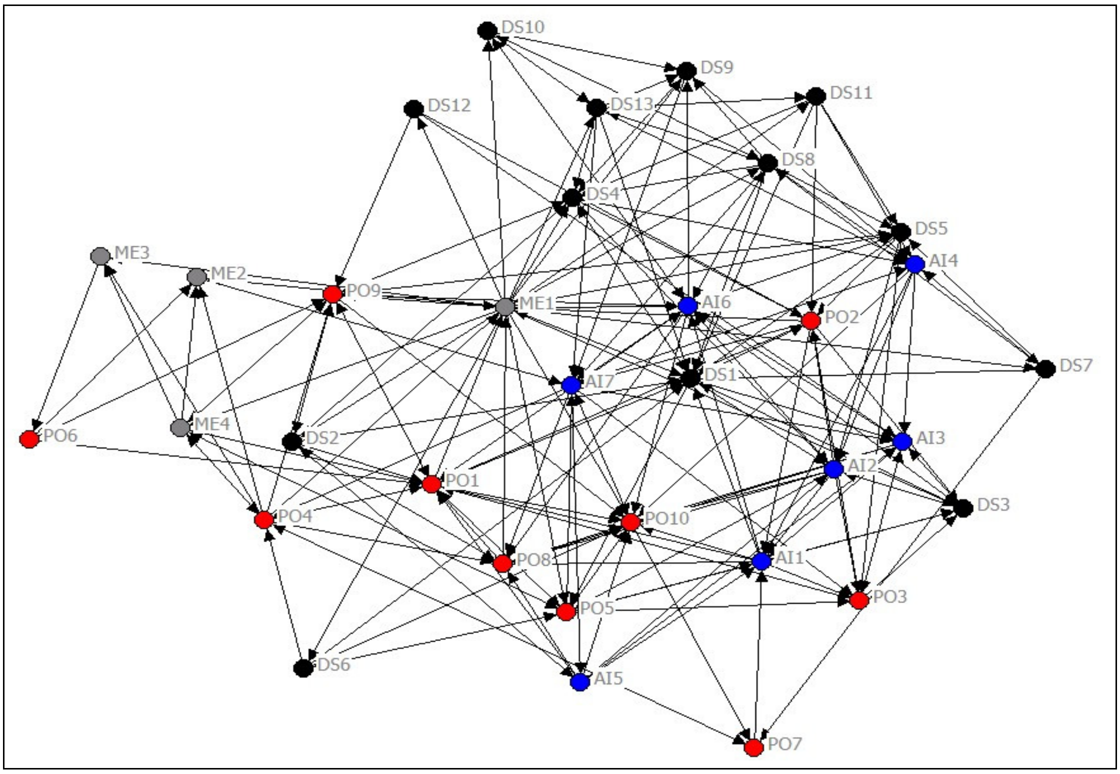

Figure 1 "Input" Network Diagram of COBIT Objectives

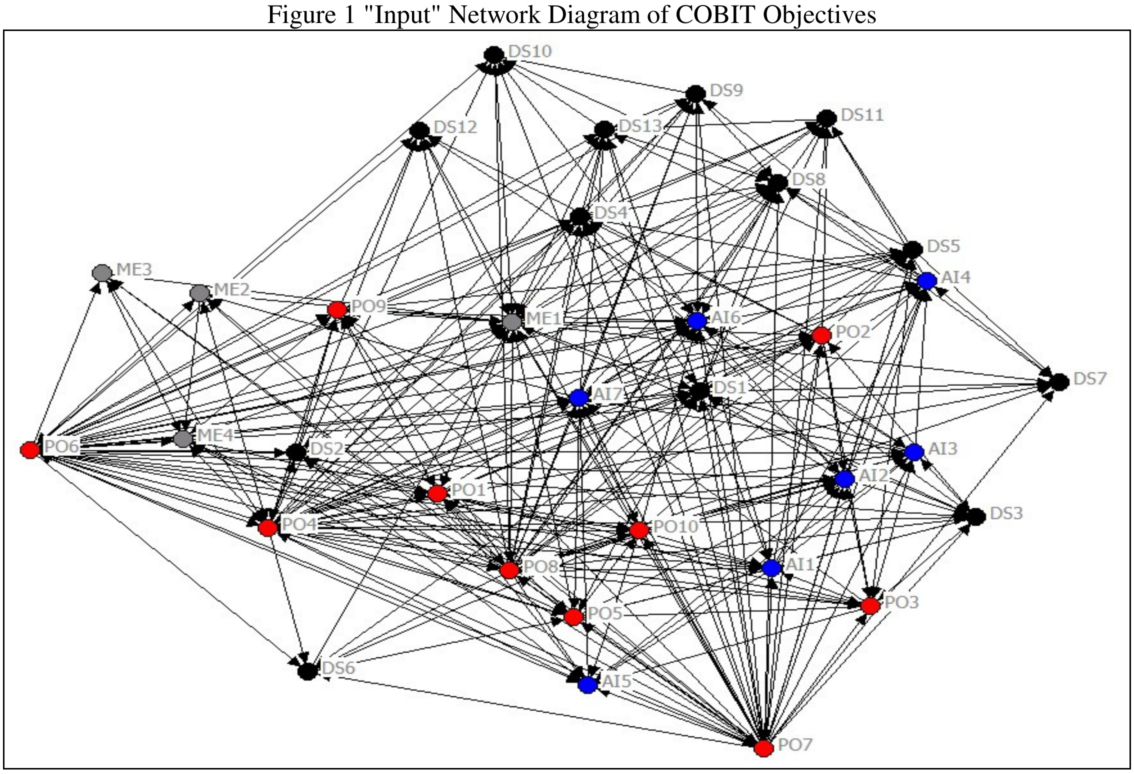

Figure 2 "Output" Network Diagram of COBIT Objectives

UCInet can be used to calculate multiple measures of centrality and the Freeman Betweenness Centrality measure was used for the purposes of this paper. Betweeness refers to the number of times that a node lies along the shortest path between two other nodes. The table below (Table 3) lists the betweenness scores for all of the nodes in both networks. The scores are correlated at 0.890, and the numbers in bold are the highest scores in each network. Among these high-scoring COBIT objectives, the four that are common to both networks are:

- ME1 Monitor and evaluate IT performance
- DS1 Define and manage service levels

- AI7 Install and accredit solutions and changes
- PO9 Assess and manage IT risks

Table 3 Betweenness Scores for COBIT Objectives

	Betweenness Scores	
COBIT ID	"Input" Network	"Output" Network
AI1	2.69	2.28
AI2	2.772	1.602
AI3	2.423	1.411
AI4	3.377	2.227
AI5	0.891	0.647
AI6	6.095	3.845
AI7	**9.888**	**5.528**
DS1	**9.99**	**5.813**
DS10	0.176	0.145
DS11	0.268	0.288
DS12	0.173	0.177
DS13	0.876	0.641
DS2	1.123	0.993
DS3	1.329	1.315
DS4	3.008	2.147
DS5	1.944	1.583
DS6	0.205	0.038
DS7	1.001	0.487
DS8	1.958	1.528
DS9	0.699	0.559
ME1	**27.992**	**24.979**
ME2	2.052	1.255
ME3	3.03	0
ME4	2.654	0.379
PO1	9.074	4.319
PO2	4.814	2.783
PO3	1.002	1.039
PO4	5.57	13.685
PO5	4.739	3.111
PO6	3.03	3.305
PO7	0.795	1.851
PO8	3.508	7.437
PO9	**8.374**	**5.528**
PO10	5.53	2.19

DISCUSSION AND CONCLUSION

This study's objectives were to determine the most central control objectives in the COBIT IT governance framework, so as to evaluate the quality of IT governance in an organization. Control capital was conceived as a broader measure of the latter, as it incorporates the value of the relationships within an organization as well as the quality at which the processes were being carried out, unlike prior measures that essentially counted which components of governance frameworks had been put in place.

Moving beyond the formal aspects of governance, control capital encompasses social capital and process capital. Both of these can be measured in a number of different ways, but network analysis is especially useful in the case of social capital, as it directly reflects the relationships within an organization. Thus, it was adopted as a methodology in this study. However, the findings here provide only a limited perspective, as they are based only on the links between the control objectives, and not the relationships between those involved in the governance process, which would be a measure of social capital. The findings also do not measure the quality with which governance processes are being carried out, which would indicate the level of process capital. Thus, they reflect only part of the overall IT governance structure of an organization.

Nevertheless, the results of the network analysis are supportive of the actions of the IT managers reported in the ITGI's surveys. Not all COBIT objectives are "born equal", and some are more important than others. The reasons for this behaviour may be satisficing, learning, or a cost-benefit analysis, and it is difficult to argue either way without actual data from IT managers. One avenue of further research would be to examine whether the objectives that were found to be the most central in our analysis are the ones that are being put in place early on in IT control enhancement projects. Another issue would be to explore why the "input" and "output" networks differ from each other.

The next step in this research project will be to explore the different ways in which "capital" has been measured as a property of an entire network. Although initial searches of the literature have yielded little information, it may be that a combination of various properties of a network, in addition to node centrality, may help to differentiate the level of control capital. Ultimately, once the measure has been developed, it will be tested in various organizational contexts to determine its usefulness and validity by, for example, comparing it to qualitative measures and other quantitative indicators, such as the length of server down-time or the number of projects completed on schedule. It would be especially useful to follow the development of an organization's IT controls longitudinally so as to understand how IT control frameworks evolve over time.

In conclusion, this paper provides one avenue for researchers in IT governance to improve their understanding of organizational IT governance. As IT becomes pervasive, IT governance is increasingly important and more sophisticated approaches need to be developed to assess how well IT controls and practices are fulfilling their objectives.

REFERENCES

Agarwal, R. and Sambamurthy, V. (2002). "Principles and Models for Organizing the IT Function", MIS Quarterly Executive, (1:1), pp. 1-16.

Adler, P.S. and Kwon, S-W. (2002). "Social Capital: Prospects for a New Concept", *Academy of Management Review*, (27:1), pp. 17-40.

Bebchuk, L., Cohen, A. and Ferrell, A. (2009). "What Matters in Corporate Governance?", *The Review of Financial Studies*, (22:2), pp. 783-827.

Bontis, N. (2004) "National Intellectual Capital Index: Intellectual Capital Development in the Arab Region", *Report produced by the Institute for Intellectual Capital Research for the United Nations Development Program.*

Borgatti, S. P., M. G. Everett, L. C. Freeman. (2002). *UCInet for windows: Software for social network analysis*. Analytic Technologies, Harvard, MA.

Borgatti, S. P. (not dated). *NetDraw*. Analytic Technologies, Harvard, MA.

Brown, C. V. (1999). "Horizontal Mechanisms under Differing IS Organization Contexts," MIS Quarterly (23:3), pp. 421-454.

Brown, C. V., and Magill, S. L. (1994). "Alignment of the IS Functions with the Enterprise - Toward a Model of Antecedents," *MIS Quarterly* (18:4), pp. 371-403.

Brown, A.E. and Grant, G.G. (2005) "Framing the Frameworks: A Review of IT Governance Research," *Communications of the Association for Information Systems*, (15), pp. 696-712.

Bueno, E. (1998). "El capital intangible como clave estratégica de la competencia actual" *Boletín de Estudios Económicos*, (LIII:164), pp.207-229

Cyert, R.M., & March, J.G. (1963). *A Behavioral Theory of the Firm*. Englewood Cliffs, NJ: Prentice-Hall.

de Haes, S. and van Grembergen, W. (2008). "Analyzing the Relationship between IT Governance and Business/IT Alignment Maturity", *Proceedings of the 41st Annual Hawaii International Conference on System Sciences* (HICSS'08), pp. 1-10.

de Pablos, P.O. (2002) "Evidence of intellectual capital measurement from Asia, Europe and the Middle East", *Journal of Intellectual Capital*, (3:3), pp. 287 - 302

Debreceny, R. S. 2006. "Re-Engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls", *Proceedings of the 39th Annual Hawaii International Conference on System Sciences* (HICSS'06) Track 8, pp.196c.

Debreceny, R.S. and Gray, G. (2009). "IT Governance and Process Maturity", *ISACA Journal*, (1)

Edvinsson, L. and Malone, M. (1997) *Intellectual Capital*. New York: Harper Business

Fichman, R. 2004, "Real Options and IT Platform Adoption: Implications for Theory and Practice", *Information Systems Research* (15:2), pp. 132–154.

Gompers, P., Ishii, J. and Metrick, A. (2003). "Corporate Governance and Equity Prices," *The Quarterly Journal of Economics*, (118:1), pp. 107-155.

Gu, B., Xue, L. and Ray, G. (2008). "IT Governance and IT Investment Performance: An Empirical Analysis," Downloaded from the *Social Science Research Network,* http://ssrn.com/abstract=1145102. (Last accessed on October 6, 2008)

Guldentops, E., Grembergen, W. V. and de Haes, S. (2002). "Control and Governance Maturity Survey: Establishing a Reference Benchmark and a Self-assessment Tool", *Information Systems Control Journal*, (6), pp. 32–35.

IT Governance Institute. (2007). *COBIT 4.1 Framework*, Rolling Meadows, IL: IT Governance Institute.

ITGI (IT Governance Institute) (2008*) IT Governance Global Status Report*, Report published by ITGI and PriceWaterhouseCoopers, from www.itgi.org

Kannan, G. and Aulbur, W. G. (2004) "Intellectual capital: Measurement Effectiveness", *Journal of Intellectual Capital*, (5:3), pp. 389 – 413

Kim, G., Phelps, K. and Milne, D. (2006). "Prioritizing IT Controls for Effective, Measurable Security", *IT Process Institute Research Study*.

Larcker, D. F., Richardson, S. A. and Tuna, A. I. (2007). "Corporate Governance, Accounting Outcomes, and Organizational Performance", *Accounting Review*. Available at SSRN: http://ssrn.com/abstract=976566

Lin, N. (1999). "Building a Network Theory of Social Capital", *Connections,* (22:1), pp. 28-51.

Liu, Q and Ridley, G. (2005). "IT Control In the Australian Public Sector: An International Comparison," *Proceedings of the 13th European Conference on Information Systems*, 26-28 May 2005, Regensburg, Germany.

March, J.G., & Simon, H.A. (1958). *Organizations*. New York: Blackwell.

Markus, M. L. 2000. "Conceptual Challenges in Contemporary Information Systems Research," *Communications of the AIS*, (3:1), Article No. 4.

Meyer, G.W. (1994). "Social information processing and social networks: A test of social influence mechanisms", *Human Relations, 47,* 1013-1048.

Milne, K. and Bowles, A. (2009). "Three tier maturity model of recommended IT governance practices, *IT Process Institute Research Study*.

Monge, P. R. & Contractor, N. S. (2003). *Theories of Communication Networks*. New York: Oxford University Press.

Nahapiet, J. and Ghoshal, S. (1998) Social capital, intellectual capital, and the organizational advantage, *Academy of Management Review* (23:2), pp. 242-266.

Nicho, M. and Cusack, B. 2007. A Metrics Generation Model for Measuring the Control Objectives of Information Systems Audit, *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'06)*, pp.235c

Reagans, R. and B. McEvily (2003). “Network Structure and Knowledge Transfer: The Effects of Cohesion and Range”, *Administrative Science Quarterly 48(2),* 240-267.

Sambamurthy, V. and Zmud, R. W. (1999). “Arrangements for Information Technology Governance: A Theory of Multiple Contingencies,” *MIS Quarterly*, (23:2), pp. 261–290.

Schwarz, A. and Hirschheim, R. (2003). “An Extended Platform Logic Perspective Of IT Governance: Managing Perceptions And Activities Of IT,” *Journal of Strategic Information Systems*, (12:2), pp. 129-166.

Sherer, Susan A. and Alter, Steven (2004) "Information Systems Risks and Risk Factors: Are They Mostly About Information Systems?," *Communications of the Association for Information Systems,* (14:2), pp. 29-64.

Sveiby, K.E. (1997) *The New Organizational Wealth: Managing and Measuring Knowledge- based Assets*. San Francisco: Barrett-Kohler.

Warkentin, M and Johnston, A. (2006). “IT Security Governance and Centralized Security Controls,” Chapter II, pp. 16-24 in Warkentin, Merrill and Rayford Vaughn (Eds.), *Enterprise Information Assurance and System Security: Managerial and Technical Issues*, Hershey, PA: Idea Group Publishing.

Weill, P. (2004). “Don’t Just Lead, Govern: How Top-Performing Firms Govern IT”, *MIS Quarterly Executive*, (3:1), pp. 1-17.

Weill, P. and Broadbent, M. (1998). *Leveraging the New Infrastructure: How Market Leaders Capitalize On Information Technology*, Harvard Business School Press, Boston, MA.

Weill, P., Soh, C. and Sia, S.K. (2007). “Governance of Global Shared Solutions at Proctor & Gamble,” *CISR-MIT Research Briefing*, (7:3A).

Westerman, G. (2006) “The IT Risk Pyramid”, *MIT CISR Research Briefing*, (5:1D).

ACKNOWLEDGEMENTS

I would like to thank Professor Brian Pentland of Michigan State University for his guidance, comments and suggestions.

COPYRIGHT