December 2004

Corporate Governance and IT Governance: exploring the board's perspective

Ernest Jordan
Macquarie Graduate School of Management, Sydney

David Musson
Macquarie Graduate School of Management, Sydney

Corporate Governance and IT Governance: exploring the board's perspective

Professor Ernest Jordan
David Musson
Macquarie Graduate School of Management

Macquarie Graduate School of Management
Sydney, New South Wales
Email: Ernest.jordan@mgsm.edu.au
Email: Davidmusson@optusenet.com.au

Abstract

Information technology (IT) exceeds half the capital spending of large organisations (US Commerce 2003) and should thus be a major concern of boards. How corporate governance extends into the domain of IT, becoming IT governance, is not widely researched. Concerns of board members on IT features little in the literature and board members' views are rarely obtained by academic researchers, partly due to the difficulty of obtaining access. We aim here to add to that literature. We describe an Australian study that explores IT governance issues from the board's perspective, a grounded theory approach, and examine some propositions drawn from the literature that does exist. The study used the topical issue of the risks of electronic commerce to stimulate the respondents. A questionnaire instrument was then developed and piloted. Methodological challenges are then discussed.

Keywords

Corporate governance, IT governance, risk, e-commerce

INTRODUCTION

For many organisations very significant investments are made in IT. The US Dept of Commerce (2003) reports that large organisations are dedicating more than half of their capital expenditure on IT. The issue of dealing with all the investments of the organisation, and the risks, is the domain of corporate governance (Hilmer 1993, p. 33). This is the name used by a wide range of literature on the top-level management of companies (eg Cadbury 1992, Demb and Neubauer 1992, Tricker 1997). Whilst there is no one accepted definition of corporate governance, Tricker (1984) noted that:

"*The governance role is not concerned with running the business per se, but with giving overall direction to the enterprise…*" (p6).

In a similar vein, one of the key UK corporate governance documents, the Cadbury Report (Cadbury 1992) defined corporate governance as: *"…. the system by which companies are directed and controlled"* (para 2.5).

The literature on corporate governance (eg ASX 2003a, FRC 2003) covers three main subjects, namely

- The way the board works (its composition, size, remuneration and stakeholder relations).
- The leadership role (initiating strategies, overseeing management, making key decisions), and,
- The management of risk (establishing and overseeing the system of risk oversight and internal control).

In most developed countries, governments have become greatly concerned with the control of corporate governance, usually after a major corporate collapse[1]. The concerns with corporate governance have usually led to the introduction of legislation (such as the Sarbanes-Oxley Act (SOX 2002) in the US) or to rules enforced by the Stock Exchange and by company audits, as in the cases of the UK and Australia.

[1] For example, in the US (Treadway 1997), following the Savings and Loan collapse; in the UK after the failure of Polly Peck, Barlow Clowes and Maxwell (ICAEW 1999); in Germany after the failure of Metallgesellschaft, Schnieder, Knoeckner-Humboldt-Deutz and Philip Holtzmann (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) the Control and Transparency in Companies Law, 1998).

The result of this level of legislative and regulatory attention is that the corporate governance obligations of a director of a listed company are clearly defined. In the UK, the Common Code (FRC 2003) sets out the requirements for UK listed companies, together with statements of best practice and guidance for board members. In Australia, the Australian Stock Exchange has published its guidelines for corporate governance (ASX 2003a), setting out 10 principles of corporate governance, derived from the Organisation for Economic Cooperation and Development's core principles of good corporate governance (OECD 1999). A series of "best practice" recommendations and specific guidance on disclosure are provided for each principle. These recommendations apply to a listed company's first financial after January 1st 2003, but are not mandatory. ASX Listing Rule 4.10.3 (ASX 2003b) was amended in January 2003 requiring each Australian listed company, in its Annual Report, to state the extent to which it had followed the ASX corporate governance guidelines. The Rule notes that if the entity has not followed all of the requirements, it must identify the recommendations that have not been followed and give the reasons for not following them. The recommendations are thus effectively annexed to the Listing Rules

The Australian guidelines go further than the requirements of the Sarbanes-Oxley Act (SOX 2002) in the US and the UK requirements set out by Smith (2003) and Higgs (2003), in that they require the CEO and the CFO of an organisation to say in writing (essentially to the ASX) that:

- The accounts are "true and fair" and accord with the relevant accounting regulations,
- They base this statement on a sound system of internal control and risk management, and,
- The organisations internal control, risk management and compliance systems are operating effectively and efficiently (ASX 2003a, section 7.2).

The term "efficiently" clearly suggests some form of benchmark, although no control framework is specified by the ASX. The Group of 100 (an Australian association of CFOs) has proposed that the 1992 COSO model (COSO 1992) is used (G100 2003). There is no requirement in the ASX document for the CEO/CFO statement to be audited.

GOVERNANCE OF IT

The term governance is also applied to Information Technology (IT), but with much less clarity and focus than with corporate governance. There is an extensive literature on IT governance, most of which is theoretical in nature. There is little in the literature on the actual processes involved with IT governance, and it is clear that a gap exists between theoretical frameworks and contemporary practice (Ribbers et al. 2002). In general, the literature sees IT governance as either a structure or a process.

IT governance as structure

The largest body of literature on IT governance is concerned with the locus of the IT decision-making authority within an organisation (Brown 1997, Sambamurthy and Zmud 1999). In this view, IT governance is concerned with three issues (Weill and Broadbent 1998, Sambamurthy and Zmud 1999)

- IT infrastructure management, which refers to decisions relating to the types of hardware and software platforms, network and data architectures used within the organisation and the corporate standards for procurement and deployment of its IT assets,
- IT use management, which refers to decisions relating to IT planning and priorities and to the routine provision of IT services, and
- IT project management, which requires both infrastructure and system skills to be used to develop and implement new systems.

The literature identifies three modes of IT governance (Sambamurthy and Zmud 1999, Brown and McGill 1994, Davenport et al. 1992). These are:

- Centralised, where corporate management have the cross-organisational IT decision-making authority.
- Decentralised, where divisional management have IT decision-making authority for their systems, and,
- Hybrid or Federal, where corporate management have IT infrastructure decision-making authority for the entire organisation, and divisional management has authority for their applications and system development.

The literature suggests that the hybrid mode is dominant (Hodgkinson 1996, Sambamurthy and Zmud 1999, Weill and Broadbent 2003).

This view of IT governance is strikingly similar to the earlier debates on the organisational structure of the IT function (see for example Olsen and Chervany 1980, King 1983, Tavakolian 1989 and Brown and Magill 1994). Part of this debate concerns whether the IT function should be centralised, controlling organisation-wide IT services from a single unit, or decentralised, with each business unit having its own IT function (Dearden 1987). Neither choice is applicable in every case (Boynton et al. 1992).

This view has the unfortunate effect of decoupling IT governance from corporate governance. The emphases on leadership from the top and the accountability of the board for risk is here diminished by what appears to be a lower level focus on operational issues.

IT governance as process

This view sees IT governance as corporate governance applied to Information Technology. As Hogg (2002) noted: “It is poor corporate governance to push ICT[2] governance down to the ICT manager level. ICT is an integral part of their business and ICT governance is an integral part of corporate governance.” This view, perhaps surprisingly, is largely taken only by the practitioner literature.

It is this view of IT governance that is adopted in the following sections of this paper. IT governance is seen as a process, implemented as part of the corporate governance of an organisation. This view is pressed in the literature by a number of auditing bodies, most notably by two US-based organisations, ISACA, (Information Systems Audit & Control Association) and the IT Governance Institute, who jointly developed a proprietary approach to implementing and evaluating controls in the IT environment. This approach is called CobiT (Control Objectives for Information and Related Technology) (ITGI 2002). The basis of the approach is that accountability of the IT systems is achieved by the use of a set of audit control processes. The CobiT framework is built on the COSO framework mentioned above.

THE MANAGEMENT OF IT

The link between the managers responsible for managing an IT function and the board of their organisation, according to the literature, is two-fold. Firstly, the actions of IT management are guided by a stable, formal, agreed business strategy (Hirschheim et al. 1995, Lederer and Sethi 1996) and corporate objectives (O’Connor 1993). The development of business strategy and the oversight of its implementation, as earlier noted, are board responsibilities.

Secondly, IT carries risks. Given the centrality of IT to the operation of most companies and the companies’ heavy capital investments in IT, the risk of, for example, failure, underperformance or overspend on IT needs to be understood and managed at board level. The 2003 Chaos report of IT project failure (Standish 2003) shows that, based on data from 13,522 cases, only 34% of IT projects were considered successful. 15% of projects were complete failures and the balance of 51% was what is referred to as challenged. Challenged means a project overran on time and/or cost (Standish 2003). Data from the projects surveyed showed that 52% of the specified features and functions of an IT project appear in the final released version (Standish 2003).

This paper concentrates on the key IT governance issue of the management of IT-related risk by the board. The risks that can arise with IT include both operational risk and strategic risk. Whereas the management of operational risk is assisted by a number of frameworks such as the risk processes set out in AS/NZS 4360:1999, Risk Management Standard, (AS/NZS 1999) strategic risks have potentially long latency periods and are difficult to detect. There is little literature on the detection and management of strategic risk. Detection and correction of IT-related risks is generally an intensely technical operation, so the governance activity will require close co-operation between the board and IT management

IT GOVERNANCE EXAMINED

Studies of governance practice are hard to carry out, because of the difficulty of obtaining interviews with directors of major companies. The literature contains very little that specifically deals with the perspectives of board members in dealing with IT, so a ‘grounded theory’ (Glaser and Strauss 1967) approach was appropriate. This aimed to understand the world of the board members and how the boards on which they served dealt with IT. Since

[2] ICT is Information and Communications Technologies

it has been observed that the perceived risks of electronic commerce are major impediments to the adoption of electronic commerce systems (Brynjolfsson and Smith 2000, Ernst and Young 2000), it was decided to use this as a focus. The level of interest in electronic commerce in the business community generally added interest to the potential research subjects. This paper details this study and the subsequent design of a questionnaire. The questionnaire was then pilot tested.

Two propositions were developed from the literature:

1. Published standards, such as those for risk management and information security management, would be useful to board members (ASX 2003a, p. 44). Given that board members have a duty of care (s232(4) of the Corporations Act 2001, (Australia 2001)), ensuring that applicable standards were being met or exceeded would give them greater confidence that they were doing their jobs effectively. While standards relating to workplace conditions and hazardous environments are expected to be met, management standards are less rigid in their adoption.

2. Boards of Directors receive information and advice about IT, as well as proposals for expenditure. In general, they could not be expected to be IT 'experts' and hence would need to either rely on this advice or seek expert advice (such as from consultants). Following the literature, we proposed that board members would be proactive in ensuring that the information that they received would be sufficient to carry out their duties of risk monitoring and governance (ASX 2003a, p. 48).

The literature was not particularly helpful to our work, because of the sparsity of references to IT, as noted earlier. The models that informed the work were the Australian Standard on risk management (AS/NZS 4360:1999) and the Pricewaterhouse Coopers (1999) document on risk management. These are, however, very general with no specific references to IT. Operational risks are covered in the Information Security Management standard (AS 4444) but this standard is aimed substantially at existing systems; accordingly, development and implementation issues are not covered[3]. These documents also give no suggestions of appropriate performance measures that might be reported to boards.

There is very little published research on the subject of board level risk management and even fewer papers on board attitudes to specific e-commerce risks. The Australian Accounting Research Foundation has published AGS 1056 "Electronic Commerce: Audit Risk Assessments and Control Considerations" (AARF 2000), but this is specifically aimed at auditors. Accordingly, the study was intended to produce an account of the theory-in-use of board level risk management. It examined what processes are used; it did not examine the processes themselves.

METHODOLOGY

The overall study was carried out in three phases. Firstly, interviews were held with 13 board members with positions on a total of sixty boards, examining their perceptions of board and management actions concerning electronic commerce projects. From the results of these interviews, a questionnaire was produced and tested on two further directors. The tested questionnaire was then sent to a sample of company chairmen. This paper deals mainly with the first phase of the research.

A random sample of companies was selected from the The Business Who's Who of Australia (D+B 2003). This was restricted to companies ranked in the Business Review Weekly (BRW) top 1000 organisations in Australia (BRW 1999). From the randomly selected companies, each director was reviewed. Those with two or more such directorships were included into the mailing list. The random sample was such that a mailing list of 50 individuals was created. Personalised letters were sent to these individuals requesting their participation in the study. Given that a grounded theory, theory-building approach was taken (Glaser and Strauss 1967), a short semi-structured interview framework was constructed (shown in the Appendix). Table 1 below shows the interview framework question and the territory that it was intended to explore.

Question	Purpose
What boards are you a member of?	The selection of targets was chosen with the intention of finding individuals with roles on multiple boards. This would tap into the wider circles of all the participants by reaching out to many more organisations. A smaller sample would thus gain a wider relevance.

[3] ISO/IEC 15288, Systems Engineering: System Life-cycle processes (ISO 2002) does cover risk management in the section on project processes

What is your role in these boards?	It was expected that the different formal roles, such as chairman, CEO, executive director, non-executive director, audit committee member, etc, would have some impact on the perspective of the subject. Furthermore the professional background of the subject may be a basis for their board membership, especially lawyers and accountants. We also wanted to hear the subject's views on their role relative to management, shareholders and other parties.
How much do you know about electronic commerce?	It was to be anticipated that board members who regarded themselves as knowledgeable or well-informed would be more involved in electronic commerce and would be able to answer the other questions differently. A definition was prepared in advance to guide the remaining interview, in case the subject expressed confusion or ignorance. It was important to establish the subject's baseline knowledge for the subsequent questions.
What do you see as its risks and rewards, its threats and opportunities?	The 'risk-reward' trade-off and the threats-opportunities dilemma are generic across business decision making and thus represented standard approach mechanisms for the subjects to articulate their knowledge and experience. We saw both of these models as representing important aspects of the role of board members in any organisation, the twin challenges of strategy and risk.
Have you had any involvement in electronic commerce projects, as a board member or otherwise?	This question complemented that on their knowledge. It is commonly held that board members are appointed to 'bring their experience' to the board, hence their experience of electronic commerce projects would be expected to colour their understanding and to lead to different views.
What were your experiences?	IT has more than its share of negative experiences and it was expected that, if the subjects had had them, their attitudes to the control of risks, in particular, would be more carefully thought out. Similarly if they had had positive experiences, it was anticipated that their views on strategic opportunities would be more developed.
How are electronic commerce ventures reviewed in your boards?	Here we expected the subjects to draw from the range of experiences across multiple organisations and highlight contrasts. It was also expected that each board would have a single review process, that might have changed over time. By asking about the review mechanisms or processes, rather than specific projects, we could also avoid confidential matters.
Do the boards have risk assessment routines for these ventures?	We wanted to see how close the formal standards for risk management, for example, impacted on the ways in which boards carried out their duties. It was conceivable that risk assessment would be demanded by the board as a whole, by the audit committee, or simply as an extension of any proposal from management.

Table 1 Semi-structured interview questions and their justification

S

An initial target of eight such directors was extended as the range of issues raised in the early interviews was wider than had been anticipated. Eventually 13 directors took part in the study with collective representation on more than sixty boards. In most of the interviews, two researchers were present, each with extensive experience of IT. The interviews lasted from one hour to two and a half hours as the subjects were highly engaged in the topic and appeared to find the interview to be interesting. With each director participating in an average of more than four boards, there were many comparisons to be made and many differences to be highlighted. This had been an objective in the question design and it proved to be effective in general. The proceedings were tape recorded and transcribed later. Content analysis was performed using categories raised by the subjects.

DISCUSSION

Table 2 below draws from the interviews and indicates the nature of the responses that were given. The subjects were originally established as a random sample, and selected in any way that they could be deemed to be broadly representative, however the number of respondents is not sufficient to give quantitative indicators.

Question	**Responses**
What boards are you a member of?	Between two and twelve organisations, included listed and private companies. Statutory authorities were also included in some of the responsibilities. Some of the boards had featured in the media as ‘fractious’ or stressed.
What is your role in these boards?	All of the anticipated roles were found with the greatest number being non-executives. Professional backgrounds were commonly professional with finance and law dominating. Engineering and manufacturing backgrounds were also found. Very strong expression of their duties to shareholders were articulated. An unanticipated finding was that the presence of dominant shareholders with effectively controlling interests led to differences in the board members’ roles, as these board members were unable to be completely independent of such dominant shareholders.
How much do you know about electronic commerce?	The general level of knowledge was very poor, with most directors expressing at best only survival skills in IT. The exceptions were quite distinct, with comprehensive and thoroughly up-to-date knowledge. This led to a supplementary line of questioning: as IT-capable board members were a rarity, did their other board members rely on them or put other expectations on them? In general this was not the case.
What do you see as its risks and rewards, its threats and opportunities?	For many the strategic risks were a dilemma: e-commerce was risky to get into and it was risky to stay out. There was a significant challenge in timing e-commerce initiatives. Rewards were generally seen as unlikely. The subjects did view e-commerce as high risk, and their duty of care would ensure great caution. While most thought that they had no opportunity to gain ‘first mover advantage’ for example, they were apprehensive that others might. There was also significant concern at the undermining of existing business models through such forces as disintermediation.
Have you had any involvement in electronic commerce projects, as a board member or otherwise?	Experience was limited with most initiatives being extensions of pre-existing business processes into web-based interaction, with no change in the flow of goods or services. Two subjects (both CEOs) were leading strategic initiatives that were central to the strategic positioning of their organisations.
What were your experiences?	Apart from the two CEOs mentioned above, the experiences had been routine, not challenging their existing business models or business understanding.
How are electronic commerce ventures reviewed in your boards?	This question was most effective in revealing a diversity of approaches and methods. In some organisations consultants were used heavily both to articulate proposals and to review them or to implement them. Audit committees had limited roles for the review of new ventures, with generally the full board being involved. The relationship between management and the board also varied, with some boards interacting, almost in a collegial sense, with business and IT management on the challenges of a specific proposal.
Do the boards have risk assessment routines for these ventures?	Risk assessment was generally not a stand-alone process. Whatever risk assessment was done, it was usually incorporated into the more general review (e.g. costs and benefits). Occasionally consultants were engaged for risk assessment.

Table 2 Semi-structured interview questions and response overview S

From the analysis, a pilot questionnaire was devised. This was not an easy task, as a director is likely to be unwilling to take part in such research and so the instrument has to engage the respondent. There was also the challenge of the legal responsibilities of directors: close identification of any question with a legal duty would not lead to informative responses. Also, given the diversity of responses on some of the interview questions, any questionnaire needed to exploit these to draw contrasts.

The design of the instrument

The instrument has 27 questions, divided into three sections (refer to authors' website[4] for a pdf. of the questionnaire):

- Eight general questions about the respondent and his/her board
- Five questions about risk management processes in use by the company.
- Fourteen questions about e-commerce, its risk, benefits and its effects on the company's industry.

These sections reflected the individual's position in the organisation, the risk management processes that were in place for all business activity, and how the specific issues of e-commerce were dealt with as these three dimensions had emerged as clearly distinguishable and potentially independent. The relationships between the three dimensions were valuable to explore. Additional literature was sought, drawing from the terms introduced by the interview subjects. For example, it was commonplace that subjects used language from Michael Porter's competitive strategy, especially the 'five forces model' (Porter, 1980) so this model was included in the survey instrument as a way of expressing the attractiveness or otherwise of the industry, and how this was changing.

The general questions are unexceptional except for question 6, which asks whether the board has a member with a controlling share. During the interviews we came to believe that, in such a case, the opinions and attitude of the responding director may not be able to influence the board. Question 5, about whether the company is listed reflects the extra obligations of corporate governance placed on listed companies by the ASX. Question 8 concerning membership of the audit committee relates to the role of the audit committee in managing risk.

Questions 9, 10 and 11 in the risk management questions reflect the responses made during the interviews. Question 9 asks, inter alia, whether the evaluation of an e-commerce proposal (a highly technical issue) would be dealt with by the board in a different manner to more usual proposals. Question 13 asks how the organisation's risk management system would detect a risk caused by an employee operating within his/her area of delegated authority, a potential area for fraud with e-commerce.

The third set of questions starts with a working definition of e-commerce. This is to counter the confusion shown by the interviewees on the subject, whose views of e-commerce included buying something in a shop by credit card (which is electronically processed), or buying something over the telephone or by fax. These questions seek to discover the view of e-commerce risk of both the respondent and his company, how quickly they responded to this risk, and the nature of that response. The last question asks the effect of e-commerce on the respondent's industry. Rather than asking a number of further questions, it was decided, after some debate, to use the classic Porter five force diagram of the influences on an industry (Porter 1980). Each box has a plus sign, a minus sign and the word "no". For each box, respondents were asked to consider whether e-commerce had changed the level of activity in the box, circling the plus sign if the level had gone up, the minus sign if it had gone down and the word "no" if it was unchanged.

The pilot questionnaire was tested for how understandable it was, its usability and to test responses. This was done with interviews with two further directors, and only minor amendments made to take account of their comments. A report on the use of the questionnaire has appeared elsewhere (reference to be supplied after reviewing), however it is the methodological implications that we discuss.

IMPLICATIONS FOR RESEARCHERS

The challenge of the methodology lies in the delivery of the instrument to board members and in gaining an adequate response to it. The approach reported elsewhere involved sending batches of questionnaires to the chairmen of boards for distribution to board members. This appeared to be satisfactory for small boards, especially those for small private companies where most of the board members were executive directors. However, for boards

[4] http://www.gsm.mq.edu.au/facultyhome/ernest.jordan/

that are more formally organised, with meetings at monthly intervals – or less often, this imposed several problems. Firstly the chairman invariably regarded the survey as a matter to be brought to the board, or to be summarily dismissed. If it went to the board, it would hardly be a priority item and so may not be dealt with for quite some time. Secondly, it is normal that board deliberations are confidential and PAs and secretaries are assiduous in safeguarding this confidentiality. Thus it was extremely difficult to gain information as to what was happening to the survey, whether it had been considered or would be. The third major problem in this approach was that, if the survey was to be undertaken, one or two 'volunteers' or interested parties would be conscripted. The selection of these respondents would be far from random and militate against survey representativeness. It also became difficult to determine the true response rate. These problems seemed to grow with intensity and frequency as the organisations became larger and held larger public profiles.

One of the problems in dealing with organisations as the unit of analysis is that the organisation will have established procedures for dealing with outside requests and the most cherished research instrument can end up on the refuse pile of procedure. However, it is the organisation that is the valid unit of analysis. The board is an organ of the organisation and deals with the organisation's issues. It is the whole of the board that needs to be studied, in the context of the whole organisation.

A second approach would seek to secure the commitment of the organisation before sending out questionnaires. This approach also makes it easier to adhere to privacy legislation and the concerns of university ethics committees. This approach would be time consuming and would require substantial effort in building a set of participant organisations.

A third approach would involve sending questionnaires by mail to the home addresses of a random sample of directors. These are available on mailing lists, from public sources in some cases, and in directories. Given that some directors are on many boards, a sample could be weighted to reflect their activity. This would ensure that all organisations have similar chances of being represented, but would a director, receiving a questionnaire, answer it with respect to the company that you intended to cover in your research? However, even here the mathematics gets difficult. Company A has 8 board members, who are on fifty boards between them, some of them in common with B. If you want to survey A, you may find it impossible to also survey B as the board members may receive multiple questionnaires.

An alternative approach may be to echo the original interview discussed above and to take the instrument to the board members individually. The use of the draft instrument in the two validation interviews showed that the approach and content interested the interviewees and produced fruitful interviews. There was a high rate of agreement to participate in the original interviews and this would be improved if a short questionnaire was to be used. However, this method is unlikely to be successful for junior researchers or for research assistants. An approach from a senior academic directly, or through a mutual reference, has a higher chance of success.

An earlier version of this paper was presented at a corporate governance conference. This version addresses the information systems community. The authors would like to acknowledge the kind sponsorship of Gadens Lawyers, who were also able to facilitate the access to the interviewees.

REFERENCES

AARF (2000). "AGS 1056 Electronic Commerce: Audit Risk Assessments and Control Considerations", Melbourne: Australian Accounting Research Foundation.

AS/NZS (1999), "AS/NZS 4360: 1999, Risk Management", Sydney: Standards Australia.

ASX (2003a), "Principles of Good Corporate Governance and Best Practice Recommendations", Sydney: ASX Corporate Governance Council. http://www.shareholder.com/visitors/dynamicdoc/document.cfm?documentid=364&companyid=ASX , accessed February 2004.

ASX (2003b), "ASX Listing Rules", Sydney: Australian Stock Exchange. http://www.asx.com.au/ListingRules/LRChps.shtm, accessed January 2004.

Australia (2001). Corporations Act, Act no. 50, as amended. Canberra, Attorney-General, http://scaleplus.law.gov.au/cgi-bin/download.pl?/scale/data/pasteact/3/3448 , accessed July 2004

Boynton, A.C., G.C. Jacobs, and R.W. Zmud (1992), "Whose responsibility is IT management?" Sloan Management Review, 33 (4), 32 - 38.

Brown, C. (1997), "Examining the emergence of hybrid governance solutions: Evidence from a single case site," Information Systems Research, 8 (1), 69 - 94.

Brown, C.V. and S.L. McGill (1994), "Alignment of the IS function with the enterprise: Toward a model of antecedents", MIS Quarterly, 18 (4), 371 - 403.

BRW (1999). "Top 1000 Australian Companies", BRW 21 (44), November 12.

Brynjolfsson, E. and M. Smith (2000). "Frictionless Commerce? A Comparison of Internet and Conventional Retailers", Management Science, 46 (4), 563 - 585

Cadbury, A. (1992), "Report of the Committee on the Financial Aspects of Corporate Governance", London: Gee and Company Ltd. http://www.blindtiger.co.uk/IIA/uploads/2c9103-ea9f7e9fbe--7e3a/Cadbury.pdf, accessed April 2003.

COSO (1992), "Internal Control - Integrated Framework", New York: Committee of Sponsoring Organisations of the Treadway Commission.

D+B (2003). The Business Who's Who of Australia. Sydney, Dun and Bradstreet (Australia).

Davenport, T., R. Eccles, and L. Prusak (1992), "Information Politics", Sloan Management Review, 34 (1, Fall), 53 - 62.

Dearden, J. (1987), "The withering away of the IS organisation", Sloan Management Review, 28 (4), 87 - 91.

Demb, A. and F.-F. Neubauer (1992). The corporate board: confronting the paradoxes. Oxford, Oxford University Press.

Ernst&Young (2000), "An Australian View of Risk Management", Sydney: Ernst & Young Australia.

FRC (2003), "The Combined Code", London: Financial Reporting Council. http://www.frc.org.uk/publications/content/CombinedCodeFinal.pdf, accessed January 2004.

G100 (2003), "Guide to compliance with ASX Principle 7: Recognise and Manage Risk", Melbourne: The Group of 100. http://www.group100.com.au/policies/guide-asx-principle-7.pdf , accessed February 2004.

Glaser, B. and A. Strauss (1967), "The Discovery of Grounded Theory", Chicago: Aldine.

Higgs, D. (2003), "Review of the role and effectiveness of non-executive directors", London: Department of Trade and Industry. http://www.dti.gov.uk/cld/non_exec_review/pdfs/higgsreport.pdf, accessed January 2004.

Hilmer, F. (1993). "Strictly Boardroom: Improving Governance to Enhance Company Performance", Melbourne:The Business Library.

Hirschheim, R., H. K. Klein, and K. Lyytinen (1995), Information Systems Development and Data Modelling – Conceptual and Philosophical Foundations, Cambridge: Cambridge University Press.

Hodgkinson, S. T. (1996), "The Role of the Corporate IT Function in the Federal IT Organization", in Information Management: The Organizational Dimension, M.J. Earl, Ed. Oxford: Oxford University Press.

Hogg, R. (2002), "Keynote address," in CIO 2002. Sydney: Australian Computer Society. http://www.acs.org.au/news/050302.htm, accessed September 2003.

ICAEW (1999). Implementing Turnbull: A Boardroom Briefing. London: Institute of Chartered Accountants in England and Wales.

ISO (2002), "ISO/IEC 15288: Systems Engineering-System life-cycle processes." Geneva: International Standards Organisation.

ITGI (2002), "CoBIT: Control Objectives for Information and related Technology, 3rd Edition", Rolling Meadow, IL: IT Governance Institute.

King, J.L. (1983), "Centralised versus decentralised computing:Organisational considerations and management options," Computing Surveys, 15 (4), 320 - 49.

KonTraG (1998), Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (Control and Transparency Act). Germany. BGBl I 1998, S. 786

Lederer, A.L. and V. Sethi (1996), "Key Prescriptions for Strategic Information Systems Planning," Journal of Management Information Systems, 13 (1), 35 - 62.

O'Connor, A.D. (1993), "Successful strategic information systems planning.," Journal of Information Systems Management, 3 (2), 71 - 84.

OECD (1999), "OECD Principles of Corporate Governance." Paris: OECD.

Olsen, M.H. and N.L. Chervany (1980), "The relationship between organisational characteristics and the structure of the Information Services function," MIS Quarterly, 4 (2), 57 - 68.

Porter, M. (1980). "Competitive Strategy", New York: Free Press.

Pricewaterhouse Coopers (1999) *Enhancing Shareholder Wealth by Better Managing Business Risk*, IFAC Study 9. New York : International Federation of Accountants.

Ribbers, P.M.A., R.R. Peterson, and M.M. Parker (2002), "Designing Information Technology Governance Processes: Diagnosing Contemporary Practices and Competing Theories," in Proceedings of the 35th Hawaii International Conference on System Sciences - 2002. Hawaii: IEEE Computer Society.

Sambamurthy, V. and R. W. Zmud (1999), "Arrangements for Information Technology Governance: A Theory of Multiple Contingencies," MIS Quarterly, 23 (2), 261 – 90.

SOX (2002), "Sarbanes-Oxley," in The US Congress Vol. HR 3763. http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf, accessed March 2004.

Standish (2003), "CHAOS Chronicles v3.0." West Yarmouth, MA: The Standish Group International Inc.

Smith, R (2003), "Audit Committees Combined Code Guidance." London: Financial Reporting Council. http://www.frc.org.uk/publications/content/ACReport.pdf, accessed January 2004.

Tavakolian, H (1989), "Linking the information technology structure with organisational competitive strategy: a survey," MIS Quarterly, 13 (3), 309 - 17.

Treadway (1987). Report of the National Commission on Fraudulent Financial Reporting. Washington D.C., National Commission on Fraudulent Financial Reporting (TheTreadway Commission).

Tricker, R. I. (1984), Corporate Governance: Practices, procedures and powers in British companies and their boards of directors. Aldershot: Gower.

Tricker, R. I. (1997). "All corporate entities need to be governed." Corporate Governance, an International Review 5(1), 1 - 2

US Commerce (2003) "Digital Economy 2003", US Dept of Commerce, Washington

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

Weill, P. and M. Broadbent (2003), "Creating Effective IT Governance, a Gartner EXP Premier Research Report." Stamford, CT: Gartner.

APPENDIX: INTERVIEW FRAMEWORK

a. Board membership.

What boards are you a member of? What are your roles and responsibilities on these boards? (Prompt to obtain the distribution of time spent on each of the boards).

b. Electronic commerce.

How much do you know about electronic commerce? (Have definition of e-commerce ready if requested)

As a director, what do you see as:

- Its risks and rewards? (prompt for reasons and/or examples)
- Its opportunities and threats? (prompt for reasons and/or examples)

- What sorts of e-commerce ventures might be useful for one or more of your companies? (prompt for source of ideas)
- Do you personally know any directors whose companies have implemented such ventures?

c. Electronic commerce projects.

Do any of your companies currently have, or have they had, e-commerce projects? (prompt for details)

How do your boards (or would your boards) review electronic commerce projects?

Do the boards have:

- policies on e-commerce?
- risk assessment and management processes to apply to these ventures?

Have you had any involvement in these or other electronic commerce projects, as a board member or otherwise?

What were your experiences?

Hypothetical question for interviewees with no e-commerce experience

If one of your boards received a project proposal to integrate the company's IT systems more closely with those of your (customers or suppliers), how would you evaluate the proposal?

Would you require any new processes to be put in place to assess and manage the potential risks entailed in enacting such a proposal?