COMPUTERS & LAW

Journal for the Australian and New Zealand Societies for Computers and the Law

Editors: Claire Elix and Laura Seeto

ISSN 08117225

Number: 61

September 2005

ICT Governance - new buzz, same issues?

Bill Leonida, Counsel, Westpac Banking Corporation and

Peter Mulligan, Henry Davis York

Bill Leonida is Counsel at the Technology & Intellectual Property Group, Westpac Banking Corporation and Peter Mulligan is a Senior Associate at Henry Davis York.

ICT governance is a buzz phrase we have been hearing progressively more about this year. Standards Australia has released a new standard on the governance of information and communications technology and some of the more established international standards are beginning to be adopted by Australian companies.

Also this year, a study conducted by ACA Research of companies with more than 500 employees and an annual turnover of greater than $250 million found that 83% of those companies had some sort of formalised ICT governance framework and 45% per cent had fully implemented their ICT governance framework.[1] The results confirm that ICT compliance is seen as an important issue among Australian and New Zealand companies.

Why the sudden flurry of activity - when surely the concept of ICT governance has been around for a long time - and what are the obstacles to implementing an ICT governance framework?

ICT governance defined

ICT governance is an integral part of corporate governance. Both have

Continues page 3

In this issue:

Continued from page 1

gained greater prominence from recent well-publicised corporate failures. The collapses of HIH and One.Tel in Australia, as well as Enron, WorldCom and Tyco in the United States, have revealed failures in the governance of these once-reputable companies. The spotlight is now firmly on corporate accountability.

Corporate governance is the system by which companies are directed and controlled.[2] At its core is the proper management of companies through rules and procedures that ensure fairness and transparency. It is concerned with the formulation of policies and procedures, requires meticulous documentation and establishes a plan for constant improvement.

ICT governance is the application of these general principles to the information and communications technology (**ICT**) function of a company. Its focus is on setting up processes to ensure that a company's ICT supports and is aligned to the business function, whilst mitigating risks and delivering value.

The inherent problem - a question of profile and goals?

In the days of enterprise applications, e-business and Y2K, the ICT function was expected to think fast and respond quickly. This often led to 'moving goalposts', budget blowouts, missing deadlines and intervention by boards of directors. Whilst we may not have called the process ICT governance, policies and procedures were developed to address these issues and to set out high-quality, well-defined and repeatable processes for successful outcomes.

The Y2K issue did much to lift the profile of the CIO. It drew the attention of those at the top to the importance of ICT contingency plans and had companies at least talking to their vendors and suppliers about disaster scenarios. Arguably, Y2K turned out to be a non-event because of the good work that went into fixing systems. In some companies, however, the success of these efforts has led to complacency among senior executives. A general decline in the number of high profile ICT projects has also meant that the CIO's profile has recently fallen.

Many CIOs tend to engage in techno-speak, which can result in the CIO being misunderstood and marginalised. This is often the result of the differences in goals, styles and attitudes of the executive team. Generally speaking, the CEO is customer-focussed; the CFO is concerned with balancing cost and risk whilst the CIO is concerned with the introduction and management of new technology. The fact that most CIOs report to the CFO rather than the CEO is not helpful.

The profile of the IT department and the alignment of business and ICT goals are hurdles that many companies are yet to overcome. They are also two of the factors that may potentially inhibit the attainment of value from ICT investment.

The rise and rise of ICT governance

During the last few years, leading industry researchers such as Gartner and the Standish Group have pointed to the high percentage of IT projects that fail outright or deliver below expectations.[3] The rate of performance failure of IT projects is a matter for concern.

However, performance failure is not the only risk that must be accounted for: ubiquitous threats to Internet security by global hackers, theft of information, disaster recovery and the increase in terrorism also present significant risks. Coupled with this, the CIO must balance the need to improve return on ICT investment, increase service levels and manage a tight budget.

There is a greater awareness in Australia that effective management of ICT is critical to the productivity and performance of companies today. Companies are starting to recognise that ICT is able to transform their business, provide competitive advantage and enhance earnings and shareholder value. A recent Federal Government study[4] found that ICT can provide key benefits including:

- *informational benefits* such as an increase in the quality, quantity and availability of business and other information;
- *strategic benefits* such as creating competitive advantage;
- *transactional benefits* leading to efficiencies and cost savings; and
- *transformational benefits* associated with positive organisational change.[5]

The study found that improved performance can be obtained through good practices in ICT regardless of the size of an organisation or the industry in which it operates.

What are good ICT practices and how can organisations achieve them while balancing risk and return? By being aware of the benefits that technology can yield and changing how the IT department is run by implementing effective ICT governance.

Let's consider the legal obligations attached to ICT governance, some practical suggestions and best practice tools.

Corporate governance obligations under statute and the implications for ICT governance

ICT governance is simply a subset of overall corporate governance. As a result, to understand ICT governance it is necessary to understand the law relating to corporate governance.

In Australia, obligations relating to corporate governance arise out of legislation such as the *Corporations Act* 2001 (Cth) (**Corporations Act**), common law duties imposed on directors and officers and guidelines developed by the Australian Stock Exchange (**ASX**).

By its very nature, one of the central concerns of the Corporations Act is the governance of corporations. Governance obligations are dispersed throughout the Corporations Act. This includes duties upon directors and officers to act with reasonable care and diligence, in the interests of the company and for a proper purpose. Directors are also subject to common law duties that may be imposed by the

express or implied terms of a director's contract of service, by way of an equitable obligation or by the law of negligence.

Statutory duty to exercise due care and diligence

Section 180(1) of the Corporations Act provides that a director or other officer must exercise their powers and discharge their duties with the degree of care and diligence that a reasonable person would exercise if they:

(a) were a director or officer of the corporation in the corporation's circumstances; and

(b) occupied the office held by, and had the same responsibilities within the corporation as, the director or officer.

The standards imposed under section 180(1) are essentially the same as those imposed upon directors at common law.[6]

A director or officer who makes a business judgement will be taken to have met the requirements of the duty of care and diligence in section 180(1) (and those duties under the common law) if they:

(a) make the judgment in good faith and for a proper purpose;

(b) do not have a material personal interest in the matter;

(c) inform themselves about the matter to the extent they reasonably believe to be appropriate; and

(d) rationally believe the judgement to be in the best interests of the corporation.[7]

Australian courts are generally reluctant to interfere with directors' judgements on business decisions. In *Harlowe's Nominees* it was stated that the judgement of directors "if exercised in good faith and not for irrelevant purposes, is not open to review in the courts".[8] Similarly, in *Howard Smith v Ampol* it was noted that "it would be wrong for the court to substitute its opinion for that of the management, or indeed to question the correctness of the management's decision, on such a question, if bona fide arrived at."[9]

Statutory duty to exercise good faith and act for a proper purpose

In addition to the duty of care and diligence, there is a duty to act in good faith and for proper purposes in section 181(1). This provides that a director or officer must exercise their powers and discharge their duties:

(a) in good faith in the best interests of the corporation; and

(b) for a proper purpose.

Other duties are contained in sections 182 and 183 of the Corporations Act. They include a prohibition on a director, secretary, other officer or employee from improperly using their position or information to gain an advantage or cause detriment to the corporation.

Delegation and reliance on information provided by others

Section 198D of the Corporations Act provides that the directors may, unless the company's constitution provides otherwise, delegate any of their powers to:

(a) a committee of directors;

(b) a director;

(c) an employee of the company; or

(d) any other person.

Further, under section 189, a director is entitled to rely on the information and advice provided by others. This provides a "safe harbour" for directors so long as the reliance was made in good faith after making an independent assessment of the information or advice. This is a provision that is highly relevant to the ICT function of companies. The specialised nature of ICT means that the directors will often need to rely on expert ICT advice provided by others.

The power to delegate and the ability to rely on the information and advice of others is explicit recognition that directors, in discharging their duties, are not expected to undertake a detailed inspection of the day-to-day activities of their companies. However, they are still required to make proper enquiries if the circumstances indicate the need to do so. A director cannot choose to remain ignorant and must have at least a rudimentary understanding of the business of a company. This includes a requirement to become familiar with the fundamentals of the business in which it is engaged.[10]

The degree of knowledge required by a director will depend on the importance of ICT to the company. Where a company is heavily reliant on ICT or is a key player in the ICT industry, it is common sense that its directors should take a keen interest in ICT investment, strategy and risk. In the authors' opinion, the duties upon directors of these companies in relation to the ICT function will generally be greater.[11] Equally, a director that is skilled in relation to a particular matter will be subject to a higher duty.[12]

Corporate and ICT governance obligations of listed entities

The Corporate Governance Council of the ASX has developed its *Principles of Good Corporate Governance and Best Practice Recommendations* (**ASX Principles**).[13] The ASX Principles were developed to provide best practice guidelines for listed entities in corporate governance.

The ASX Principles consist of 10 core principles, which the ASX believes underlie good corporate governance. Each principle is explained in detail, with guidance for implementation in the form of best practice recommendations.

Under ASX Listing Rule 4.10.3, listed entities are required to provide a statement in their annual report disclosing the extent to which they have followed the ASX Principles in the reporting period. Where an entity has not followed the ASX Principles, it must identify what has not been followed and give reasons for the non-compliance.[14] This is known as the "if not, why not?" approach.

The ASX Principles were not designed to be one-size fits all. The principles that are adopted, and the extent to

which they are adopted, will depend on the size, complexity and operations of an entity.

While each of the ASX Principles contains some implications for the ICT function of listed entities, the ones that are most relevant are ASX Principles 1, 2 and 7.

ASX Principle 1 - Lay solid foundations for management oversight

Principle 1 requires that a listed entity recognise and publish the respective roles and responsibilities of the board and management.[15] In terms of ICT, this may mean that the listed entity identifies whom, on the board and at a management level, is responsible for the ICT function and includes a formal statement of their responsibilities.

ASX Principle 2 - Structure the board to add value

Principle 2 requires that a listed entity have a board of an effective composition, size and commitment to adequately discharge its responsibilities and duties.[16] In relation to its ICT operations, this may lead the entity to appoint a director with a deep understanding of ICT. Ultimately, however, this will depend on the industry in which the entity operates and whether or not it is a significant consumer of ICT.

ASX Principle 7 - Recognise and manage risk

Principle 7 requires that a listed entity establish a sound system of risk oversight and management and internal control.[17] It includes a recommendation that the CEO and CFO state to the board in writing that:

(a) their certification of the financial statements is founded on a sound system of risk management and internal compliance and control which implements the policies adopted by the board; and

(b) the entity's risk management and internal compliance and control system is operating efficiently and effectively in all material respects.

The impact of ASX Principle 7 on the ICT function is obvious. A company's IT systems will often play a crucial role in processing the underlying transactions on which the financial statements are based and generating the reports used to prepare them. The CEO and CFO will have to rely on the CIO to provide the necessary assurances that the company's IT systems are sufficiently robust to support their certification of the financial statements.

More generally, to comply with ASX Principle 7 a listed entity may decide to set up an ICT committee responsible for the management and oversight of ICT investment, operations and risk. It may also favour the creation and implementation of policies and procedures that deal with ICT risk. In any event, it would seem that a line of responsibility and reporting should be established between management and the board to identify, evaluate and report on ICT risk.

Lessons for the Board

In the past, boards have tended to adopt a reactive approach to ICT governance. They only sought to intervene when IT problems jeopardised the viability or reputation of the business. The study by ACA Research shows that executives are well aware of the importance of ICT governance to a successful governance strategy.[18] With this increased recognition, it is anticipated that boards will begin adopting a more robust oversight role to ensure that ICT delivers value, properly accounts for risk and is aligned with business objectives.

In the authors' opinion, it is poor corporate governance to push ICT governance down to the functional level. ICT is an integral part of most companies and ICT governance is an essential part of corporate governance.[19] The supervision of the management of ICT, like any other critical business function, must come from the top.

To improve the ICT governance of a company, some of the things that boards of directors and CEOs may consider doing include:

- being actively involved in guiding and monitoring the management of ICT;
- providing the structures that support the implementation of the ICT strategy;
- articulating and conveying to all relevant stakeholders the business' objectives for ICT;
- ensuring that ICT plans are aligned with strategic plans;
- making ICT a regular agenda item for the board;
- having a board member to whom the CIO reports having relevant ICT business skills;
- in highly ICT dependant entities, having the CIO on the board and/ or report to the CEO not the CFO;
- asking the right questions and understand what is happening with major ICT investment from a risk and return perspective;
- assisting and supporting the CIO in communicating with the business;
- in highly ICT dependant entities, setting up an ICT governance committee to deal with matters such as the integration of ICT with business strategy, value delivery, risk management and performance management;
- ensuring the ICT governance committee comprises a number of independent board members and key executives and, where appropriate, seconding ICT experts to the committee;
- ensuring ICT related business education of the board and management; and
- researching and implementing the ICT governance tools available to help achieve value from the use of ICT.

Additionally, the CIO and any ICT governance committee should ensure that they:

- are business-orientated and work towards bridging the gap between ICT and the business;

- work with the board and CEO in managing all aspects of ICT risk, not just security or disaster recovery;
- provide accurate reporting of ICT risk to the board;
- do not wait to be asked the right questions by the CEO or the board;
- scrutinise each ICT project for value and alignment with business objectives;
- implement a process which requires formal project requests for ICT projects and appropriate approvals;
- ensure that managing risk is not just about risk transference to suppliers and that ICT contracts have flexibility to adapt to changing circumstances; and
- research and implement the ICT governance tools available to help achieve value from the use of ICT.

Best practice ICT governance tools

There are a number of products and standards that may be used to formalise the ICT management process. The adoption of a best-practice ICT framework will go some way to discharging the legal duties upon companies and their directors with respect to the governance of ICT.

In Australia, three of the more prominent standards are the *Control Objectives for Information and related Technology* (**CobiT**), the *Information Technology Infrastructure Library* (**ITIL**) and Australian Standard 8015-2005 *Corporate Governance of Information and Communication Technology* (**AS 8015-2005**). There are also others, such as Basel II in the financial services industry, ISO 17799 for IT security and Six Sigma as a broader best-practice framework.

Control Objectives for Information and related Technology

The *Control Objectives for Information and related Technology* (**CobiT**) were developed by the IT Governance Institute in the United States. CobiT was first released in 1996 and is now in its third edition. Its main objective is to provide organisations with a framework of generally applicable and accepted IT governance and control practices.

CobiT has been developed for application to organisation-wide information systems. It looks at the fiduciary, quality and security needs of organisations and provides seven information criteria that can be used to define generically what a business requires from IT. The criteria are effectiveness, efficiency, availability, integrity, confidentiality, reliability and compliance.[20]

The CobiT framework divides IT into 34 processes to assess and measure an organisation's IT capability. For each of the 34 IT processes, a high-level control objective is defined:

(a) identifying which information criteria are the most important;

(b) listing which resources will usually be leveraged; and

(c) providing considerations on what is important for controlling that IT process.

By structuring IT governance in this way, a company can ensure that an adequate control system is provided for the IT environment that is both pervasive and intrinsic across all levels.

CobiT has been adopted in both the public and private sector in the United States and its influence is growing in Europe and across the world. In Australia, some of the early adopters include the Australian National Audit Office, the Federal Attorney General's Department, the Federal Department of Transport and Regional Services and Curtin University.

CobiT publications are available at www.isaca.org/cobit.

Information Technology Infrastructure Library

The *Information Technology Infrastructure Library* (**ITIL**) was developed by the Office of Government Commerce in the United Kingdom more than 15 years ago and has been refined and refreshed many times since. Worldwide, ITIL is the most widely used best practice tool for IT service management. Its adoption is highest in North America and Europe.

The purpose of ITIL is to assist organisations to develop a framework for IT service management. It provides a tool that facilitates the in-depth consideration of the components of IT service provision, at a level aligned to the value of IT to the organisation. The ultimate goal is to make IT service support and delivery cost effective, predictable, repeatable and accountable.

CobiT's bottom line is to ensure that IT funds are spent on business outcomes and is designed to expose flaws in IT investment and execution. As a result, it is favoured by accountants and auditors. ITIL, on the other hand, looks at whether technology delivers the services that it promises and is more popular with IT managers.

The ITIL documentation defines the organisational structure and skill requirements of the IT department and documents a set of procedures to facilitate the management of IT operations and infrastructure. It is intended to be a top-down approach that addresses the strategic business value generated by IT and the need to deliver a high quality IT service.

As the name implies, ITIL consists of a series of books that provide guidance on IT service management. The documents that make up ITIL are the core titles:

(a) Service Support;

(b) Service Delivery;

(c) Planning To Implement Service Management;

(d) Applications Management;

(e) ICT Infrastructure Management;

(f) Security Management;

(g) Software Asset Management; and

(h) The Business Perspective.

The 2 most commonly used titles are Service Support and Service Delivery.

ITIL is becoming more and more popular as organisations take a greater interest in the importance of managing

IT as a service. Compared to Europe, the take up of ITIL in Australia has been slower. In the public sector, an early adopter was the Department of Employment and Workplace Relations. In the private sector, organisations such as Tabcorp, Telstra and Microsoft have implemented aspects of ITIL.

Copies of the ITIL books can be obtained from the UK Office of Government Commerce at *www.ogc.gov.uk.*

AS 8015-2005: Corporate Governance of Information and Communication Technology

Earlier this year Standards Australia released Australian Standard 8015-2005 *Corporate Governance of Information and Communication Technology*. AS 8015-2005 purports to apply to all organisations, including public and private companies, government entities and not-for-profit organisations.

The aim of AS 8015-2005 is to provide guiding principles for directors of organisations, rather than to set down strict rules. It applies to the governance of resources, computer-based or otherwise, used to provide information and communication services.

The standard sets out six principles for good corporate governance of ICT:

Principle 1 - Establish clearly understood responsibilities for ICT

This requires that individuals and groups within the organisation understand and accept their responsibilities for ICT.

Principle 2 - Plan ICT to best support the organisation

This requires that ICT plans fit the current and ongoing needs of the organisation and that the ICT plans support the corporate plans.

Principle 3 - Acquire ICT validly

ICT acquisitions should be made for approved reasons in the approved way, on the basis of appropriate and ongoing analysis. An organisation must ensure that there is an appropriate balancing of costs, risk and long-term and short-term benefits.

Principle 4 - Ensure that ICT performs well, whenever required

An organisation should ensure that its ICT is fit for its purpose, is kept responsive to changing business requirements, and provides support to the business when required.

Principle 5 - Ensure ICT conforms with formal rules

This means that an organisation should ensure that ICT conforms to all external regulations and complies with all internal policies and practices.

Principle 6 - Ensure ICT respects human factors

An organisation should ensure that ICT meets the current and evolving needs of all the 'people in the process'.

The standard proposes that directors should govern ICT through three main tasks:

(a) evaluating the use of ICT;

(b) directing preparation and implementation of plans and policies; and

(c) monitoring conformity with the organisation's policies, and performance against the plans.

The standard provides a governance framework by which these three activities of evaluation, direction and monitoring are applied to each of the six stated principles. It also provides guidance to those advising, informing or assisting directors. This includes senior managers, members of groups monitoring the resources within an organisation, external business or technical specialists, vendors of ICT products and services, internal or external service providers and ICT auditors.

It is noteworthy that AS 8015-2005 is directed to the boards of organisations and not just to those who have a specific responsibility for ICT. This focus endorses the view that ICT governance is first and foremost a board issue. The standard, of course, is not binding but sets a benchmark for good practice in this area.

AS 8015-2005 is the first in a series of standards and publications being developed by Standards Australia to provide guidelines for directors on the effective, efficient and acceptable use of ICT within their organisation. Copies of AS 8015-2005 are available from Standards Australia at *www.standards.com.au.*

Conclusion

Corporate objectives around gaining competitive advantage, enhancing shareholder value, complying with regulatory requirements and keeping up with increasing security requirements have combined to breathe new life into ICT governance.

The management of ICT risk is crucial to the successful operation of most organisations today. In the current regulatory and business environment, a prudent company will look to properly document its risk minimisation and compliance strategies. For most companies, this should involve a formalised ICT governance framework. Many directors will consider that this is the only rational approach to ensure that they properly discharge their duties under the Corporations Act and at common law.

CobiT, ITIL and AS 8015-2005 are all useful tools to assist in the design and implementation of an ICT governance framework. They each have their individual strengths and focuses. Ultimately, however, the framework that is adopted will depend on the particular needs of the organisation and which standard provides the best fit.

---

1 see ACA Research, *"Corporate and IT Governance Research- Executive Summary June 2005"* (2005).

2 see Cadbury, *"The Financial Aspects of Corporate Governance"* (1992) at para 2.5.

3 see, for example, www1.standishgroup.com/sample_research/index.php and www.gartner.com/Init and www.it-cortex.com/Stat_Failure_Rate.htm

4 Gregor, Fernandez, Holtham, Martin, Stern, Vitale & Pratt, *"Achieving Value from ICT: key management strategies- Department of Communications, Information Technology and the Arts, ICT Research Study"* (2005).

5 see Gregor, Fernandez, Holtham, Martin, Stern, Vitale & Pratt, *"Achieving Value from ICT: key management strategies - Department of Communications, Information Technology and the Arts, ICT Research Study"* (2005) at 11.

6 see, for example, *ASIC v Adler* (2002) 41 ACSR 72, *Adler v ASIC* (2003) 46 ACSR 504 and *Daniels v Anderson* (1995) 37 NSWLR 438.

7 see section 180(2) *Corporations Act* 2001 (Cth).

8 *Harlowe's Nominees Pty Ltd v Woodside (Lakes Entrance) Oil Co NL* (1968) 121 CLR 483 at 492.

9 *Howard Smith Ltd v Ampol Petroleum Ltd* [1974] AC 821 at 832.

10 see generally *Daniels v Anderson* (1995) 37 NSWLR 438.

11 see generally Sir Douglas Menzies, *"Company Directors"* (1959) 33 ALJ 156 at 164 and *Commonwealth Bank of Australia v Friedrich* (1991) 5 ACSR 115 at 126, although cf Romer J in *Re City Equitable Fire Insurance Co Ltd* [1925] Ch 407.

12 see generally *Re Brazilian Rubber Plantations and Estates Ltd* [1911] 1 Ch 425, *Daniels v Anderson* (1995) 37 NSWLR 438 and *ASIC v Vines* [2003] NSWSC 1116.

13 Australian Stock Exchange, *"Principles of Good Corporate Governance and Best Practice Recommendations"* (2003).

14 Australian Stock Exchange, *"Principles of Good Corporate Governance and Best Practice Recommendations"* (2003) at 5.

15 see Australian Stock Exchange, *"Principles of Good Corporate Governance and Best Practice Recommendations"* (2003) at 15-17.

16 see Australian Stock Exchange, *"Principles of Good Corporate Governance and Best Practice Recommendations"* (2003) at 19-24.

17 see Australian Stock Exchange, *"Principles of Good Corporate Governance and Best Practice Recommendations"* (2003) at 43-45.

18 ACA Research, *"Corporate and IT Governance Research- Executive Summary June 2005"* (2005) at 2.

19 see Musson and Jordan, *"The Broken Link: Corporate Governance and Information Technology"* at www.une.edu.au/febl/Business/Conference/CorpGov/Papers/

20 IT Governance Institute, *"Board Briefing on IT Governance"* (2003) at 62.