December 2005

An Integrated IT Risk Model

Ernest Jordan
Macquarie University, Sydney

An Integrated IT Risk Model

Ernest Jordan
Macquarie Graduate School of Management
Macquarie University, Sydney, Australia
Ernest.Jordan@mgsm.edu.au

Abstract

The worldwide concern with corporate governance concerns itself, inter alia, with the risks that an organisation faces; for many, IT is significant among those risks. This paper examines the audit approach, and others, to dealing with risks in IT-based systems. This paper summarises the findings of research in IT-related areas of risk and then draws together a charter for IT governance that meets the wider needs of corporate governance. IT risks are collated in the form of a portfolio so that risk is dealt with in a positive, systematic manner. The portfolio sets out to be exhaustive so that all risk can be brought together under a single managerial role. The IT governance model balances risks with strategic goals and the specific benefits that are intended through the implementation of IT. A case study illustrates the application of the model.

Keywords: IT governance, IT risk portfolio, information assets

1. Introduction

Investments in information technology are challenging to many organisations – they are large and have greater uncertainty about them than other investments. For example, the US Dept of Commerce (2003) reports that large organisations are dedicating more than half of their capital expenditure on IT. Making decisions about the investments of the organisation, and the risks faced by the organisation, is the domain of corporate governance. This is consistent with perspectives such as Tricker (1984):

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

Moreover, the Cadbury Report (Cadbury 1992) – a key contribution in the pursuit of corporate governance, defined it as: "…. the system by which companies are directed and controlled" (para 2.5). This view of corporate governance as a system enhances the concern with IT, which is often used to implement systems within organisations. Many IT applications will be concerned with the 'systems of control' of the organisation – that are themselves some of the instruments of governance.

The literature on corporate governance (eg ASX 2003, 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. The concerns with corporate governance have usually led to the introduction of legislation (such as the Sarbanes-Oxley Act

in the US) or to rules enforced by the Stock Exchange and by company audits, as in the cases of the UK and Australia.
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 2003), 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 2004) 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.

The term "efficiently" clearly suggests some form of benchmark, although no control framework is specified by the ASX. The Group of 100 (G100, an Australian association of CFOs) has proposed that the 1992 COSO model (COSO 1992) is used (G100 2003). Yet, there is no requirement in the ASX document for the CEO/CFO statement to be audited.
The Australian context thus is a suitable example for wider discussion and enables us to articulate IT governance practices that could be adequate for today's heightened corporate governance standards.
This paper first sets the scene by summarising from the literature the wide range of risks that IT may present to the organisation. These are then classified into an 'IT risk portfolio'. The IT risk portfolio is then used to generate requirements for IT governance that would be reflecting high standards of corporate governance. The paper concludes with an illustrative case study.

2. IT risks

IT risks are widely seen – from the failure of major projects to the threat from hackers and viruses. The level of threat can be such that the organization could be financially destroyed, yet systematic and comprehensive approaches to dealing with these threats are seldom undertaken. Because the language of risk is commonly confused – with threat, risk, vulnerability and hazard being used interchangeably by some commentators – we adopt a definition of IT risk as:

> *"An IT risk is something that can go wrong with IT and cause a negative impact on the business"* (Jordan and Silcock 2005, p.48)

This definition is drawn from the Australian Standard for Risk Management (AS4360) and is comparable to that of Markus (2000) and others (Pfleeger 2000; Keil et al. 2000). It emphasises the causative role of IT in unanticipated and /or undesirable outcomes. The negative outcomes may be located in any part of the organization, not just the IT function. The literature and

popular press alike are full of examples of outcomes that are unwelcome. Some examples are shown in Table 1. It is important to point out that the 'risk' is the causative element and the 'business impact' is the result. Thus terms like 'reputation risk' are unacceptable – 'damage to the organisation's reputation' is a consequence and some risk (e.g. inadequate confidentiality for information assets) is the cause. In this case, the risk is an 'information asset confidentiality' risk.

Impact	**IT risk cause and examples**
Financial	*IT project failure* Sydney Water spent A$60 million on a Customer Information and Billing System project that was cancelled in late 2002 (NSW Auditor-General 2003). *Outsourcing failure* UK magistrates court Libra contract costs have nearly doubled (*IntoIT* 2003). *Criminal intent* Kidder Peabody suffered significant loss with the illicit activities of a trader who fabricated profits of approximately US$339 million (Dhillon and Moores 2001).
Reputational	*Service outage* SQL Slammer worm caused extensive ATM outages for Bank of America in January 2003 through corruption of database servers (Trickey 2004). *Customer data misuse* Leakage of 4.5 million customer records reported by Softbank in Japan with attempted extortion (Softbank 2004).
Regulatory or legal	*Information integrity breach* AT&T incorrect billing resulting in successful legal action by the State of Florida in 2004. *Compliance failure* After 14 yrs of legislative requirement for US Coast Guard to develop a vessel identification system, no such system exists (GAO 2002)
Customer	*Customer service shortfall* After Cigna HealthCare's $1 billion IT overhaul and CRM initiative went live they lost 6% of its customers (Bass 2003) *Closed to customers* Early in 2004 the SCO Group was the target of a massive denial of service attack ad its site was closed for business until a new internet address was adopted (Lebihan 2004). *Not meeting customer needs* UK eUniversity flopped after having attracted only 900 students (*The Times* 2004).
Competition	*No longer the best mousetrap* Standard & Poor's survey revealed that more than six out of ten Google users would switch search engines if a better service came along (Standard & Poor's 2004).

Table 1 Business impact examples with IT risk causes (Jordan and Silcock, 2005, p.58)

These examples suggest a wider range of potential consequences for organizations. For some, IT service delivery is at the core of business processes and IT is needed to function. Delivery of IT services is necessary for the business to operate continuously. Other organizations have critical business assets that are stored digitally. Yet more use IT as the key enabler for organizational development. Such change is produced with major IT projects that are risky as demonstrated by sorry track records. IT governance is an appropriate way of thinking for dealing with such a range and for placing into the organization's wider context (Jordan and Musson 2001). In the end, the board has to take authority for the organization's use of IT although many board members are themselves apprehensive of IT (Jordan and Musson 2003).
IT governance is more than managing risks. Boards direct investment and need to know that the organization is able to achieve business benefits from its use of IT. In its simplest form, the board needs to be able to be confident of the organization's IT capability. IT governance should identify capabilities and inadequacies, and then be able to establish remedies. It is particularly

important to use a governance framework so that all risks and inadequacies are gathered together rather than each being dealt with by a separate set of processes, as Markus so clearly puts it:

> *"The business world is beginning to see the value of an integrated approach to identifying and managing business risk; the time is right for the IS field to begin developing an integrated approach to identifying and managing IT-related risk. Not only will such an approach be useful to businesses in their attempts to obtain maximum value from their IT investments, it will also help bring together a large part of the IS literature under a common conceptual umbrella. By viewing system development and maintenance along with package acquisition and outsourcing as part of the business's IT investment process, risk management becomes the centre of attention. By viewing system development failure, security breaches and competitive threats as different types of the unitary phenomenon of IT-related risk, it becomes possible to make intelligent end-to-end tradeoff decisions throughout the lifecycles of systems in organizations."* (Markus 2000, p 176)

It is also important that IT risk is dealt with urgently; IT is increasingly seen as part of national critical infrastructure.

> *"There is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being … The Secretary shall coordinate protection activities for each of the following critical infrastructure sectors: information technology; telecommunications…"* (Bush 2003)

This view is also echoed by the OECD, which recognises that IT has significant economic impacts:

> *"As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security."* (OECD 2002)

We now examine current approaches to IT risk management.

3. IT risk management

Organizations' responses to the risks of IT are uneven – some high risk areas will be well-covered and other areas neglected. For example, standard backup procedures are done routinely by most organizations but IT projects may have no risk management after the initial assessment at the project definition stage. Yet a project may be very expensive with critical business deliverables, while not all the data that is backed up is valuable. Risks in project selection are challenging – boards and senior management may be out of their depth and relying on advice that they cannot or do not test.

When discussing IT risk, many organizations see this as a role for technical specialists only, such as project managers and network engineers. Thus risk communications in most organizations come from the bottom up, but they should be flowing in many directions:

- board members should be able to give advice on strategic imperatives;
- business unit managers should be aware of risks that affect their business operation;
- service delivery staff may be aware of failings in an outsourced service contract.

Risks can thus be perceived around an organization but there is a need for centralised priority determination and management. Using an integrated IT risk portfolio in a single IT governance framework saves on duplicated and redundant processes that deal in only one type of risk.

Historically IT has been seen to offer business opportunities with a continuing trend towards control of costs. The fundamental approach has been costs versus benefits. Risks seldom got serious assessment. There are several discernable failings in IT risk management, shown in Table 2.

When assembled in such a form, it becomes clear that IT risk management is too important to be left to technical staff and becomes an important dimension of corporate governance. There is however an approach that will enable this to be dealt with. Firstly establish a framework for IT risk governance, then integrate the risks into a portfolio so that a single management approach can be used and finally reduce the complexity in the portfolio by tackling all of the risk categories.

4. The IT risk portfolio

Bringing together all of the IT risks into a single portfolio reduces the chance of some area of risk being overlooked. It also ensures that the multiple impacts of any threat or change can be worked out collectively. Furthermore, the portfolio approach enhances the likelihood that a full assessment of all the risks will be carried out. Thus we should achieve completeness, connectedness and significance in our assessment of IT risks.

A portfolio approach should reveal that continuous monitoring is needed, as the rate of change is high. By having a complete set of indicators for IT risk, we reduce the chance of missing anything and we enhance the likelihood that the diverse impacts of a problem will be identified. It is also likely that the overwhelming level of risk that is revealed will raise the priority within the organization for dealing with the risks.

Outcome	Driving factors
Piecemeal approach	Organizations do not take a holistic approach to IT risk, where risks are determined throughout the organization and then assembled into a corporate score sheet. Each risk component such as projects, service provider, etc., has its own management approach, if anything.
Commun-ication failure	Technical risks discovered by the network manager or a project manager may well be incomprehensible to the Board, where decisions must be made and accountability ultimately resides. The challenge of communicating an issue from technologist to IT manager or business manager and then to a director will be similar to the challenge when the concern is travelling in the other direction.
Reactivity	Things do go wrong! Hardware breaks down, software bugs get discovered, staff and customers engage in fraud, telecommunications and electricity stop from time to time, projects get stuck, critical staff leave, and even regulators and lawmakers tighten legislation. All predictable – admittedly very difficult to predict, but predictable nevertheless. When something goes wrong, the standard approach is one of reacting to the event and finding someone to blame.
Playing catch-up	The nature of IT risks continues to evolve and offer up new challenges. Every day new defects are found in technologies and upgrades appear. Each change means that risks are changed, and until the potential consequences have been worked out, the level of uncertainty is heightened.
Creeping goals	Corporate governance and risk management standards are being raised on a regular basis. Expectations of other stakeholders are also increasing – such as supply chain partners, customers and stockholders. IT risk management needs to be continually improved upon.
Competitive underper-formance	IT failure saps the business's potential to compete, undermining other endeavours; more, it can lead to reputation loss and detrimental effects on the brand of the organization.

Table 2 Persistent failings in IT risk management (Jordan and Silcock, 2005, p.5-6)

Much of the literature dealing with IT risks uses confused definitions so that we find terms such as 'fraud risk' (an impact), 'virus risk' (a threat) and 'communications risk' (an event). We adopt seven classes of IT risk (Jordan and Silcock, 2005), where something goes wrong with IT and the business consequences are negative:

- Projects – failing to deliver;
- IT service continuity – business operations are reduced or stop;
- Information assets – are not protected and preserved;
- Service providers and vendors – do not deliver;
- Applications – systems fail the business;
- Infrastructure – foundations are inadequate; and
- Strategic and emergent – IT impacts on strategy.

4.1Projects

Projects are the fundamental unit of change in the IT environment as they are the way in which new business applications are developed, existing processes are improved or the underlying infrastructure is modified. Any failure of a project means that the business benefits are not obtained or they are deferred. There are opportunity costs – other things could have been done – as well as direct costs. Consequences can affect the business strategy. Typical failings are in scope, time and delivered quality. Managing project risk requires capability in project management, software engineering, and IT acquisition and implementation.

4.2 IT service continuity

This concerns IT service outages and unreliability that cause some form of disruption. Operational and production systems need to keep going so that users are able to work and in turn deliver their services to customers. Managing service continuity risk requires, *inter alia*, capability business continuity management and disaster recovery.

4.3 Information assets

Damage, loss or (negative) exploitation of information assets represents a growing risk for many organisations. Increasingly organizations hold their information assets in their IT systems, however they are seldom formally recognized. Managing information asset risk requires capability in security management and information management.

4.4 Service providers and vendors

Increasingly organizations source their IT skills from outside the organization, this is especially the case for large scale software, such as ERP systems. When such a service provider fails, either completely or simply to deliver according to contract, the consequences can be very significant. It can be particularly severe if a vendor decides to phase out a key application. Managing service provider and vendor risk involves vendor management, outsourcing and contract management.

4.5 Applications

Almost all IT applications have bugs and the significance ranges from negligible to catastrophic. But today most business applications are composed of a collection of technologies that work together, that were purchased or developed separately. Each component can be modified with unanticipated consequences. Managing application risk builds on the software engineering capabilities of maintenance, enhancement, integration, testing and release management, configuration management, system administration, monitoring and problem management.

4.6 Infrastructure

The underlying technology on which the applications operate is termed the infrastructure – which seldom provides direct business benefits in its own right. It needs to be developed, maintained and enhanced over long time periods. Selection is particularly difficult as future trends may not be discernable. Managing infrastructure risk requires configuration

management, system administration and capacity management abilities as well as long-range planning and architecture skills.

4.7 Strategic and emergent

This should be of particular concern to board members as the organization's ability to work towards its strategy is put at risk. Competitors will be introducing IT changes and the challenge is that the leading edge can often be very high risk. New technologies can also emerge that make excellent applications obsolete in a very short time – whatever the cost. Managing IT strategic and emergent risk exercises skills in strategy, architecture and planning.

5. IT governance requirements

IT governance is concerned with building, monitoring and reviewing the organization's IT capability. We argue that the capabilities need to be in the areas of strategy, benefits and risks. Overall, the board must be confident that the organization is able to identify its needs and opportunities to exploit IT, and is then able to satisfy them (suggested by Edwards et al. 1993).
We continue our above emphasis on risk with four requirements proposed in Jordan and Silcock (2005).

- Requirement 1: The board needs to know how much IT risk the organization is taking.

The board has overall responsibility for the risks that the organization is undertaking which can extend to a personal responsibility. This is not to suggest that organizations become risk averse, merely that they become risk aware. This can be a demand of regulators. Clearly the board should trust that the assessments of risk that it receives are both accurate and complete. For each of the risks revealed, the board would want to be assured that it was verifiable by audit and that appropriate measures were in place to deal with it.

- Requirement 2: The board needs to be able to respond to an IT risk assessment with requirements for the risk to be moderated.

This is as much a statement of the board's capability as the organization's. The board should be able to make decisions – it needs that capability. If the organization faces a significant risk and the board cannot make the decision, it is derelict. However it requires that the technical expertise should exist within the organization that presents the IT risk decisions in a form and format the that board can deal with.

- Requirement 3: The board needs to be confident that the organization is able to make the requested changes, without bringing other risks into existence.

Having been required to make a decision, the board should be confident that the organization can achieve what has been proposed. Requiring that fixing one problem does not create another, demands a capacity for understanding risk across the whole portfolio. This suggests that IT risk governance should be a process that is well-behaved, auditable and capable of delivering consistent and reliable results.

- Requirement 4: A shared language is developed between technologists, business unit heads and senior management for dealing with IT risk.

A shared language for understanding IT strategic potential has been developing over the last twenty years however language for risk is lagging severely. We anticipate that particular benefits will be achieved by encouraging the development of shared language and shared understanding.
The overall concept of IT capability is at the heart of IT governance. It is a matter of being able to determine requirements and then achieve them – the essence of capability. This is not to suggest that the board itself has to do this, simply be assured that the organization does.

5.1 Different approaches to governance

IT governance has been adopted it in various forms (Schwarz and Hirschheim, 2003), however, in some cases there are few differences from the IT management practices that went before. Legalistic and regulatory approaches to governance tend to dominate the debate, but there are alternative viewpoints that enhance the understanding. These enable an organization to find the approach or blend of approaches that are most suitable. Within the literature we find seven dominant perspectives on governance, as shown in Table 3.

Perspective	**View**	**Proponent**
Corporate governance	Accountability	Director
Investment	Funding	Investor
Compliance	Rules	Compliance manager
Enterprise wide risk	Risk	Risk manager
Audit and control	Control processes	Auditor
Engineering and systems	Effective systems	Systems analyst
Life sciences, biology and ecology	Holistic	User

Table 3 Governance perspectives, views and proponents

Each of these perspectives has something to contribute (see wider discussion in Jordan and Silcock, 2005) but the integration of them into a coherent framework is to be seen as a valid goal of IT governance. Table 3 shows that, dramatically different perspectives on IT governance can be held simultaneously within the organization. Given that auditors have received particular attention for their responsibilities, we discuss in some detail the strengths and weaknesses of their perspective.

5.1 The audit and control perspective

Auditors approach risk management by examining organizational processes, especially those used for financial reporting. Similarly, processes that deal with physical goods or valuable resources will be tested for their reliability, integrity and efficiency. This tends to make the audit process itself reactive, so that it deals effectively only with existing processes and procedures. If processes are missing, their absence may be discovered, but it is less likely.

Although auditors have much more power than risk managers, they are similarly circumscribed in their scope. Their practice focuses on how processes operate rather than why they exist. Auditors usually have an accountancy background which colours their approach and management control concepts dominate. This approach suggests that inherent risks will exist in any system or initiative but these are mitigated by the correct design and application of management controls. The quality of these management controls can be tested by the application of standard review techniques (Pacini et al. 2001). Then the resultant residual risk is examined against pre-existing scales to see if it is material (Moulton and Coles (2003) define an *Enterprise Pain Threshold*).

A tightening of management controls to reduce the likelihood or severity of a risk will be the response to those items that warrant attention. The determinations of the auditor will frequently seen as compliance requirements and may not sit well in the organisational context. The audit and control perspective has a tendency to be look back over what has taken place, with a focus on monetary / materiality outcomes. Another issue is the 'checklist' view of some by auditors, who will be scanning for precise conformity to all items in a list, without screening them for relevance. Also audit findings that are not material may be discarded whether they are valuable or not.

It is however the unremitting thoroughness of the auditor that reveals the detailed blow-by-blow of the many IT failures in public corporations and government agencies. The most significant literature is not academic research but the professional practice of, especially, government auditors, such as the US General Accounting Office (GAO), the United Kingdom National Audit Office (NAO), Australian National Audit Office (ANAO) and the Australian state-based New South Wales and Victorian Auditors-General, who have exposed many IT disasters and much incompetence.

5.3 An integrated perspective

There is a unique contribution to be obtained from each of the seven perspectives, shown in Table 4, and by combining these we can overcome or minimise their limitations. Furthermore, we would argue that all of the positive contributions are beneficial so that they should not be discarded – in other words, it is necessary to include elements of all perspectives.

Perspective	**Contribution**
Corporate governance	Ensure that shareholders' and legal needs are met
Investor	Ensure an optimum balance of risk and return from IT investments
Compliance	Ensure the right rules are defined and applied
Enterprise wide risk	Ensure that impacts from IT on any part of the organization are surfaced
Audit and control	Ensure that controls are in place to cover likely faults
Engineering and systems	Ensure that the systems and processes are functioning effectively
Life sciences, biology and ecology	Ensure that the organization is adaptive, agile and responsive to its environment

Table 4 Contribution of the governance perspectives (Jordan and Silcock, 2005, p.34)

Generally, individuals will be more 'at home' in one of these perspectives, but the others will be held by other members of the organization. We argue that collectively these views enhance the organization's overall risk governance stance. Furthermore, in some situations one particular perspective may be more critical – that is, we do not regard all of them as equally important. Interestingly, although these perspectives have been developed by studying the approach to risk, in the end the perspectives operate effectively in dealing with the benefits of IT and the development of an IT strategy.

5.4 Balancing risks and rewards

We return to the issue of "IT-capability". While an upper bound has little meaning, there is a sense of a minimum requirement (Peppard and Ward 2004). Namely: the costs of IT should be exceeded by the delivered benefits, and both should be known accurately. On the risk-reward scale, IT investments should also come out ahead. Third, and most importantly, when business strategy demands IT support or enablement, this should be provided. For many organisations, scoring three out of three here would be sufficient to claim 'capability' – however some industries have more exacting requirements. In particular, the IT industry itself has higher requirements as it must develop 'IT solutions' for use by other organisations that will be successful in a business sense. For them, IT is the core business activity and hence higher standards are needed.

In the sections above we have expanded the capability statement to give details about the IT risk dimension. Similarly we would need to develop statements about IT benefits – and here the work of Ward at Cranfield Management School is exemplary (Ward and Peppard 2003).
The third dimension – an IT strategy capability – is one that has been extensively researched. Beyond meeting requirements and achieving benefits, IT strategy needs to be articulated. The alignment of IT with strategy has been the subject of much debate and research but hard results are scant. Organizations develop strategic applications that are critical to the business, but an enduring advantage is rare. However the arguments of Carr (2003) suggest that the days of competitive advantage from IT are now gone, and risk is a much more important dimension of IT management.
The IT Governance Institute also brings together these themes in their all-embracing definition of IT Governance: "A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes." (ISACA 2000, p. 3). Both this succinct definition and our three dimensions underscore two-way communication between the board, business leaders and IT management.

6. Case study

6.1 Methodology

A series of interviews were conducted with the IT management team (7 people) in a medium-sized public corporation (ServCorp) that was composed of several semi-autonomous business units, each with some IT capability, but largely supported by a centralised IT office (ITO). ITO developed and maintained a substantial body of infrastructural services as well as head office functionality.
The interview framework prompted responses for each of the seven IT risk areas: projects, IT service continuity, information assets, service providers & vendors, applications, infrastructure, and strategic & emergent. Interviewees were asked:

- How important is this risk area?
- What are your current practices to contain risk here?
- How well do you perform (in risk containment)?

When the seven areas were completed, interviewees were asked to identify any omitted areas of risk as a test of the completeness of the model.
The interviewees were also asked the extent to which the seven governance perspectives were operative. This enabled an analysis of the effectiveness of the current IT governance arrangements for dealing with the current IT risk portfolio.

6.2 Results

There was a high level of consensus between the interviewees. It is anticipated that other stakeholders – business unit heads, risk managers, auditors, board members – would have different perceptions and current investigations are including these subjects. As the dominant concern of ITO is to build, maintain and operate the organisation's IT infrastructure, it is not surprising that 'infrastructure risk' was rated high, however it was unanticipated that the highest would turn out to be 'information assets' and 'IT services'. With infrastructure as a critical responsibility, governance processes were such that the risk was reduced, similarly for the information assets. However a critical gap in governance was identified for 'IT services' where there was evidence of problems and clear room for improvement.
With business unit heads having prime responsibility for IT-based business projects, ITO rated 'project risk' as low. The IT risk portfolio is summarised in Table 5.

Portfolio	Important to	Room for	Evidence of

component	business	improvement	problems
Projects	No	Yes+	Yes
IT services	Yes+	Yes+	Yes
Information assets	Yes+	Yes	No
Service providers	Yes	No	No
Applications	Yes	Yes	Yes
Infrastructure	Yes	Yes	No
Strategic and emergent	No	Yes+	Yes

Table 5 The IT Risk Portfolio for ServCorp

The only additional area of risk that the IT management team faced concerned their staffing: there were issues concerned with attracting and retaining appropriate staff, ensuring that staff followed security, control and authorisation processes, as well as maintaining skill levels and their currency. In general we would argue that these are not 'things that go wrong with IT,' hence they are not IT risks. The IT risk portfolio does not attempt to be an enterprise-wide risk framework. It must integrate into other dimensions of an organisation's risk management, control and governance procedures.

6.3 Discussion

The response from the interviewees was that the framework, its components and the assessment mechanisms were able to contribute to their on-going responsibilities. Additional case studies are in progress, attempting to develop a standardised instrument for IT risk portfolio assessment. The most up-to-date results will be presented at the conference.

This paper has presented a unifying model for integrating IT risks that organisations face together with an IT governance framework that will balance risks against rewards, in the context of IT strategy. An exploratory case study demonstrated that the portfolio and the governance framework have the potential to make a significant contribution to the area. Much research lies ahead.

References

ASX. *Principles of Good Corporate Governance and Best Practice Recommendations*, Australian Stock Exchange Corporate Governance Council, Sydney, 2003.

ASX. *ASX Listing Rules*, Australian Stock Exchange, Sydney, 2004.

Cadbury, A. *Report of the Committee on the Financial Aspects of Corporate Governance*, Gee and Company Ltd, London, 1992.

Carr, N.G. "IT Doesn't Matter," *Harvard Business Review*, May 2003.

Bass, A. "Cigna's Self-Inflicted Wounds," *CIO*, 15 March 2003.

Bush, G. W. *Presidential Directive Critical Infrastructure Identification and Protection,* US Homeland Security Agency, December 17, 2003.

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

Dhillon, G. and Moores, S. "Computer crimes: theorizing about the enemy within," *Computers & Security* (20:8), 2001, pp. 715-723.

Edwards, C., Ward, J. and Bytheway, A. *The Essence of Information Systems, 2nd ed.*, Prentice Hall, Hemel Hempstead, 1995.

FRC. *The Combined Code*, Financial Reporting Council, London, 2003.

G100. *Guide to compliance with ASX Principle 7: Recognise and Manage Risk*, The Group of 100, Melbourne, 2003.

GAO. *Coast Guard's Vessel Identification System GAO-02-477*, General Accounting Office, Washington, 2002.

Higgs, D. *Review of the role and effectiveness of non-executive directors,* Department of Trade and Industry, London, 2003.

IntoIT. "Courts Libra System", *IntoIT Journal*, No. 18, National Audit Office, London, August 2003.

ISACA. *COBIT ® Executive Summary 3rd ed.*, Information Systems Audit and Control Foundation (ISACA), New York, 2000.

Jordan, E. "Performance Measures in Business Continuity". *Proceedings of the Australasian Conference on Information Systems*, Perth, 2003.

Jordan, E. and Musson, D. "Public and private sectors: contrasts in IT risk governance" in Fischer-Hubner, Simone and Olejar, Daniel and Rannenberg, Kai (Eds), *Security & Control of IT in Society – II Proceedings of the IFIP WG 9.6/11.7 Working Conference*, Bratislava, Slovakia, 15-16 June 2001.

Jordan, E., and Musson, D. "The board view of electronic business risk," *Proceedings of 16th Bled eCommerce Conference*, Bled, Slovenia, June 9-11 2003.

Jordan, E. and Silcock, L. *Beating IT Risks*, Wiley, Chichester, 2005.

Keil, M., Wallace, L., Turk, D., Dixon-Randall, G. and Nulden, U. "An investigation of risk perception and risk propensity on the decision to continue a software development project," *Journal of Systems and Software* (53), 2000, 145-157.

Lebihan, R. "SCO rides out the Mydoom storm," *Australian Financial Review*, 4 February 2004.

Markus, M.L. "Toward an Integrative Theory of Risk Control" in *Organizational and Social Perspectives on Information Technology,* R. Baskerville, J. Stage, and J.I. DeGross (eds.), Kluywer Academic Publishers, Boston, MA, 2000, pp.167-178.

Moulton, R. and Coles, R. "Operationalizing IT risk management," *Computers & Security,* (22:6), 2003, pp. 487-493.

NSW Auditor-General. *Review of Sydney Water's Customer Information and Billing System*, New South Wales Auditor-General, Sydney, 2003.

OECD. *OECD Principles of Corporate Governance,* Organisation for Economic Cooperation and Development, Paris, 1999.

OECD. *Guidelines for the security of Information Systems and networks: Towards a culture of security*, OECD Council, Paris, 2002.

Pacini, C., Hillison, W., and Andrews, C. "The international legal environment for information systems reliability assurance services: the CPA/CA SysTrust," *Commercial Law Journal*, (105:4), 2001, pp. 351-398.

Peppard, J. and Ward, J. "Beyond strategic information systems: towards an IS capability," *Journal of Strategic Information Systems*, (13:2), 2004, pp. 167-194.

Pfleeger, S. "Risky business: what we have yet to learn about risk management," *Journal of Systems and Software*, (53), 2000, pp. 265-273.

Schwarz, A. and Hirschheim, R. "An extended platform logic perspective of IT governance: managing perceptions and activities of IT," *Journal of Strategic Information Systems*, (12), 2003, pp. 129-166.

Smith, R. *Audit Committees Combined Code Guidance*, Financial Reporting Council, London, 2003.

SOX. "Sarbanes-Oxley Act" *The US Congress Vol. HR 3763*, Washington, 2002.

Standard & Poor's. "Google faces challenges as it expands beyond core search engine competency, says S&P research services in Google pre-IPO report," *Press release*, Standard & Poor's, New York, June 7, 2004.

The Times. "E-university shutdown joins list of IT failures" in "Information Technology Issue of the Week," *The Times*, London, 4 May 2004.

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

Trickey, F. "Are you prepared?" *Infosecurity*, January 2004.