PREFACE

This book was written with two objectives. The first was to provide a detailed companion to *IT Governance: Guidelines for Directors* – that book was aimed squarely at non-executive and executive directors, as well as their professional advisers, and its intent was the provision of common sense guidelines for the development and implementation of an effective IT governance framework. That book concentrated on some of the prime areas that concern boards: governance, strategy, policy, compliance and risk management. The detailed guidance that might aid the execution of such a framework was committed to this companion in the hope that the Guidelines would thereby remain clear and succinct, and that boards would find them easy to access, useful and informative.

This book's second purpose was, of course, to stand alone in its own right, as a guide for IT governance practitioners to a number of the detailed areas that are important in thinking through and creating and IT governance framework that will have the characteristics described in the Guidelines. Inevitably, therefore, some material has been repeated in this Handbook; readers of both will, from time to time, have a sense of *déjà vu.* But this handbook did develop a determined life of its own and there will inevitably be some areas in which it diverges from the Guidelines. Recognizing this, and recognizing that there will inevitably be a second edition of both, I would like to invite anyone who spots discrepancies to e-mail me (alan@itgovernance.co.uk) with details of them and, in return, I will ensure that you get a complimentary copy of the new edition when it comes out.

This book argues that – apart from the Australian AS 8015-2005 standard - there are no meaningful, comprehensive IT governance frameworks available today and suggests two different models drawn from our practical experience with clients. This book is very much the first outing for these models; I am certain that there will be

a range of responses to them and I invite you to share yours with me. I will gladly encourage you to do so by extending our offer of a complimentary copy of the next edition of this book to everyone who does so – irrespective of whether your comments are positive or not!

Finally, the IT Governance website will, by July 2005, have a subscribers' area that will contain a range of further information on IT governance; you might like to take a look at it later this year.

markets or see their competitive position eroded and ultimately destroyed.

IT on its own and of itself is not, however, necessarily a source of competitive advantage. The *way it is used* by an organization may be a source of competitive advantage but, in many sectors, IT is already commoditized and organizations have to ensure that their systems and processes are as good as (or no worse than) those of their competitors, if they're to ensure they don't fall behind in key performance areas.

Governance convergence

The OECD Principles of Corporate Governance were published in 1999, but it wasn't until after the Enron and WorldCom debacles, and the US Sarbanes Oxley response in 2002, that most other OECD countries made a determined effort to adopt their own codes of corporate governance. With the exception of the US though, individual OECD countries have all adopted corporate governance codes that work on the 'comply or explain' principle. The Sarbanes Oxley act ('SOX') works on the basis of 'comply or be punished.' One of the knock-on impacts of SOX is that those companies subject to it are requiring the partners and suppliers on whom they depend to also certify conformance to SOX because that gives them greater certainty of ongoing compliance themselves.

The most recent UK legislation (the 2004 Companies Act) and the current revision to the EU's 8th Directive on company law also point to greater compulsion – from governments, regulators and justice departments - in governance requirements becoming the norm across the OECD.

At the same time, convergence in accounting and auditing standards across the OECD, and particularly between the US and EU, which contain the vast bulk of the world's capital markets, is driving institutional shareholders to a common framework of governance requirements. Internationally, banks also operate within a common

Benefits of an IT governance framework

If good governance makes sense, good IT governance makes even more sense: 'top-performing firms succeed where others fail by implementing effective IT governance to support their strategies. Firms with above-average IT governance following a specific strategy…had more than 20 percent higher profits than firms with poor governance following the same strategy.'[13] Research by Weill and Ross also indicates that 'top-performing enterprises generate returns on their investments up to 40 percent greater than their competitors.'[14]

An IT governance framework is an integral and essential component of the value-focused 21st Century organization's overall governance approach. The key benefit of an effective, integrated IT governance framework is the leap forward in competitiveness that is achieved through the complete integration of IT into the strategic and operational management approach of the organization. Survival in the information economy is hard without integrating IT into the total business operation; long term success is impossible.

IT governance today

As boards begin to focus on their IT governance responsibilities, as they start applying themselves to de-mystifying IT within their organizations and ensuring that their substantial IT investments generate the type of strategic return that is required for long term survival, the IT governance practitioner has the great responsibility of helping the board implement a real, working IT governance framework. The IT governance starting point is with board leadership and the application of common sense, rather than the immediate implementation of a complex formal framework or the purchase of a software 'solution'. This means that IT governance

[13] IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Weill and Ross, HBS Press, 2004
[14] IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Weill and Ross, HBS Press 2004

information security failure (in financial terms) and the (fully absorbed) cost of meeting the compliance and security objectives? What is the total actual (direct and indirect) cost of all the compliance and information security incidents in your organization in the last twelve months?

5. What is the real, financial value to your organization of its information and intellectual capital and how are you leveraging it?
6. How are you driving up the intellectual capital/headcount ratio? What's the relationship between this ratio and the IT intensity (IT investment to headcount) ratio?
7. Do all your IT projects come in on time, to budget and to specification?
8. How does your D&O insurance deal with the personal consequences for directors of IT failures arising from inadequate board oversight of core business processes and significant financial transactions?

Two or three of these questions are likely to have a specific and immediate resonance within any organization that doesn't already have an established IT governance framework. They will resonate because the organization has a history of poor IT project delivery, because applications are not felt to be fit for purpose, the organization is being out-competed by a one or more rivals who are making better use of technology, or there have been significant information security or compliance issues either inside the company or in other companies in the sector.

The IT governance guerrilla will therefore identify and target these two or three key corporate issues and ensure that the broader questions are asked determinedly – preferably with some reference to how things appear to be done differently elsewhere, with different (better) results. Like any good bridgehead, these questions enable one to move to explore other areas, until the underlying need for an IT governance framework is laid bare. Some organizations may choose to bring in outside consultants to do this but, apart from the usual benefit of getting a third party to tell your people what you

risk management processes, Pillar 3 explicitly sets out to enhance transparency in banks' public reporting in order to 'leverage the ability of market discipline to motivate prudent management'.

While not all financial institutions are enthusiastic about embracing operational risk management methodologies (because, while the impact of operational risk is not always clear, the actual day-to-day cost of implementing an operational risk management approach tends to be very clear, and there's not always equal clarity about the real business value of the implementation), it can only be effective if it is driven by the board and management, integrated into the internal control structure and made part of the overall corporate governance framework.

The board must assign management accountability to someone (the Chief Risk Officer, for instance) who will be adequately resourced to drive the program forward, and the business line managers need to be 'bought-in' to the value of the initiative. They will only be 'bought-in', though, if the business objectives of the operational risk management initiative clearly include driving down costs (including the cost of economic capital), reducing the burden of regulatory compliance, improving operational efficiency and customer service. One immediate benefit that ought to be available to business-line managers is a reduction in both market risk and credit risk as a result of the reduction in those operational risks that have an immediate impact on the other two categories (such as, for instance, the market loss that arises from unauthorized trading of specific products, or incorrect market positions arising from incorrect data entry).

A key component of an operational risk framework is a set of business-line 'loss databases' that include three years worth of data relating to 'loss events' in each of the various categories of operational risk. In theory, these databases should enable financial institutions to make statistically meaningful estimates of the likelihood and impact of losses arising from operational risk. Not all financial institutions have historic data that is sufficiently granular to make such estimates. Operational risk management tools are also

there should be a standard method of risk assessment for every project, that fits within the enterprise risk management framework (*see* chapter four), for allocating risk factors. Risk, like return, is an estimate, not an absolute number and this should be borne in mind: it is more useful to have a range of likely outcomes projected for a project that take into account a range of critical factors. Traditionally, this is called a sensitivity analysis, and it focuses on the issues most likely to impact the outcome and attempts to predict the outcome in each of a number of scenarios in which the variables are higher or lower than expected.

Projects should, whatever project management methodology they use, whatever their long term objectives, aim to deliver ROI gains in relatively short time frames – like 90 days. This keeps the project team focused on delivering business value and provides an early indicator of whether or not the project is really on track in terms of what matters to shareholders: the return on their investment.

Transition

Any organization that is implementing an IT and project governance framework will have to deal with a mixture of current and future projects. Most of them will be projects that were started prior to implementation of the new project governance framework, and which were assessed, prioritized and resourced in line with the previous management criteria. There will also be an increasing number of new projects, overtly driven by the (newly articulated) business and information strategies.

What happens in most organization is that the transition from the old to the new way of doing things is phased over a period of time. Current live projects are continued through until completion. The reasons advanced for sticking with them are all some version of 'I've started so I should be allowed to finish;' they include: 'the business really needs this, and we're too far advanced to go back through a new approval process now'; 'we're so far advanced/got so much to do that we can't allocate the resources to doing the