



governance

Guidelines for Directors

Alan Calder

IT GOVERNANCE

GUIDELINES FOR DIRECTORS

ALAN CALDER

Publisher's Note

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and the author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

First published in the United Kingdom in 2005 by IT Governance Publishing

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form, or by any means, with the prior permission in writing of the publisher, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers at the under-mentioned address.

IT Governance Publishing
IT Governance Ltd
66 Silver Street
Ely
Cambs CB7 4JB
United Kingdom

www.itgovernance.co.uk

© Alan Calder 2005

Version 1.2

ISBN 978-1-905356-02-7

About the author

Alan Calder is the founder director of IT Governance Ltd (www.itgovernance.co.uk), a information, advice and consultancy firm that helps company boards tackles governance, risk management, compliance and information security issues. He has many years of senior management experience in the private and public sectors.

The company's website also provides access to a range of unique books, tools and other publication on governance, risk management, compliance and information security.

Other books by Alan Calder:

[IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799](#), 3rd edition, with Steve Watkins (Kogan Page, June 2005)

[IT Governance Today: a Practitioner's Handbook](#) (IT Governance Publishing, May 2005)

[The Case for 7799](#) (IT Governance Publishing, May 2005)

[Nine Steps to 7799 Success](#) (IT Governance Publishing, June 2005)

For homeowners and home-based businesses:

[The NON-Geek Guide™ to Wireless Security](#) (IT Governance Publishing, 2005)

[The Internet Highway Code](#) (IT Governance Publishing, 2005)

Other books by Alan Calder are planned for publication during 2005 and 2006; see the website for details.

CONTENTS

INTRODUCTION	9
Symptoms of inadequate IT governance	9
Competitiveness	10
Shareholder accountability	12
Compliance	13
Directors' personal liability	14
Conclusion	18
CHAPTER 1: WHY IT GOVERNANCE MATTERS	19
Governance background	19
Information economy, intellectual capital	21
Competitiveness	23
Governance convergence	25
Strategic and operational risk management	26
Regulatory compliance	28
Information risk	29
Strategic system deployment and project governance	30
Benefits of an IT governance framework	31
CHAPTER 2: GOVERNANCE AND RISK MANAGEMENT	33
Fiduciary duties	34
Governance frameworks	35
<i>OECD Principles of Corporate Governance</i>	35
<i>BIS and Basel 2</i>	36
<i>Operational risk</i>	37
Capital markets and financial reporting convergence	38
Converging audit requirements	39
<i>UK Companies Act 2004</i>	40
<i>EU 8th Company Law Directive</i>	41
Corporate Governance in Europe	42
Combined Code and the Turnbull Guidance	43
<i>The Turnbull Report</i>	44
<i>Revised Combined Code</i>	44
Sarbanes Oxley	48

<i>Internal controls and audit</i>	49
Risk management framework	51
<i>Risk Assessment</i>	52
Controls	53
<i>Risk management</i>	53
Conclusions	54
CHAPTER 3: INTELLECTUAL CAPITAL	56
Knowledge assets	57
Tangible relevance	58
Structure of intellectual capital	59
The role of IT governance	61
Beyond knowledge management	62
Protecting intellectual assets	64
<i>Copyright</i>	66
<i>Design</i>	66
<i>Patent</i>	66
<i>Trademark</i>	67
Third party intellectual property rights (IPR)	68
<i>Software copyright</i>	68
Conclusion	70
CHAPTER 4: COMPLIANCE	72
Privacy and Data Protection	72
<i>OECD Guidelines</i>	73
<i>Tomorrow</i>	74
National regulation	75
<i>EU Regulation</i>	76
<i>UK Regulation</i>	76
<i>US Regulation</i>	78
<i>APEC regulation</i>	81
Anti-spam legislation	81
Freedom of Information legislation	84
Computer misuse legislation	85
Human Rights	87
Other legislation	89
Record retention and destruction	89
Conclusion	91

CHAPTER 5: INFORMATION RISK	92
Overview of threats and impacts	92
<i>Threats</i>	<i>92</i>
<i>Impacts</i>	<i>94</i>
Information security governance	95
<i>Governance failure</i>	<i>97</i>
Complexity and larger organizations	98
<i>Threats to larger organizations</i>	<i>98</i>
<i>Vulnerabilities in larger organizations</i>	<i>99</i>
<i>Impacts on larger organizations</i>	<i>100</i>
‘Traditional’ external threats	101
‘Traditional’ insider threats	102
Organized crime	104
Terrorism	106
Emerging trends	107
Information security best practice	108
The need for metrics	109
CHAPTER 6: SYSTEM DEPLOYMENT AND PROJECT RISK	111
Project failure	112
Project governance objectives	113
Execution risk	115
Executive level project governance	116
Board level project governance	117
Conclusions	119
CHAPTER 7: DESIGNING AN IT GOVERNANCE FRAMEWORK	120
Business context and culture	120
IT governance framework	123
Business, information and ICT strategies	125
IT steering and executive committees	127
<i>Board steering committee</i>	<i>129</i>
<i>Executive committee</i>	<i>132</i>
<i>Enterprise IT architecture committee</i>	<i>133</i>
<i>Technology committee</i>	<i>134</i>
Hierarchy of IT decisions	135

<i>Key implementation principles</i>	135
<i>Follow the money</i>	136
<i>Mind the gap</i>	137
Reporting and monitoring framework	137
<i>IT audit</i>	138
External systems and standards	139
Metrics	141
CHAPTER 8: IT GOVERNANCE IN ACTION	142
‘Operationalization’ of strategy	142
Responsibility and accountability	144
IT goals, functional organization and communication	146
<i>Communication</i>	148
Information Strategy	149
ICT Strategy	150
<i>Application strategy</i>	152
<i>Enterprise IT architecture</i>	153
Project governance	154
<i>Portfolio management</i>	155
<i>Risk management</i>	157
<i>Change Management</i>	158
Information security and compliance	158
<i>Information risk assessment</i>	159
<i>Compliance risks</i>	159
IT performance optimisation	160
CHAPTER 9: ISSUES FOR THE PUBLIC SECTOR AND NOT-FOR-PROFIT ORGANIZATIONS	162
Public sector organizations	162
Voluntary sector organizations	168
CHAPTER 10: IT’S ALL ABOUT LEADERSHIP	170
Board leadership	171
CEO’s role	172
CIO leadership	174
IT users	175
FURTHER READING	177
USEFUL WEBSITES	179

INTRODUCTION

‘Can IT align with the business?’¹

Your immediate response to this question gives a sense of the adequacy or otherwise of your IT governance arrangements. If you think it’s a good question, one worth pursuing, then you’ve just identified the first, and most critical, symptom of inadequate IT governance: a disjunct between your most important business enabler and the business itself.

If you find the question incomprehensible – because, to you, it’s axiomatic that IT aligns with the business – you may not need this book. However, before putting it aside, consider this: a late-2004 global study² of North American and European businesses found that only one-quarter of the respondents considered their business and IT strategies to be ‘fully integrated and developed simultaneously’ – which is a backward step from the findings of the same study in 2002, in which one-third of respondents considered these processes to be fully aligned.

Symptoms of inadequate IT governance

1. How does your board assess (measure) the real contribution made by any of your IT systems to improving the organization’s competitiveness?
2. What divergence is there between the views that your sales/operational management has of the benefits of IT systems and projects and those of the IT management? Who is right and how do you find out? Are you getting maximum value (maximum business benefit for minimum actual total cost) for each of your IT investments? How would you know? How

¹ *Computer Business Review*, March 2005

² ‘Why Today’s IT Organization Won’t Work Tomorrow,’ AT Kearney, 2005

Introduction

would you know if your IT spending is putting your company at a cost disadvantage?

3. What is your board's process for comparing the (fully costed) ROI on your technology projects to those of any other strategic options, including acquisitions, and how does this affect strategic planning?
4. What is your board's view on the relationship, in your organization, between the potential impact of a compliance or 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?

If your organization has a clear, widely understood set of answers to these questions, complete with meaningful metrics, then you probably have an effective IT governance framework in place. The fact is, very few organizations do. There are a number of reasons for this.

Competitiveness

The first is that IT and IT governance simply don't feature on the CEO's top 10 list of challenges. Tighter cost control makes it in at number seven; transferring knowledge/ideas/practices within the

Introduction

company (which could, arguably, be linked to using IT as an enabler), makes it on to the list at number 10.

What are the top three challenges?

Not surprisingly, they are all related to competitiveness as measured by revenue growth. The Conference Board's annual survey for 2004³ listed the top three challenges identified by CEOs worldwide:

1. Sustained and steady top-line growth
2. Speed, flexibility, adaptability to change
3. Customer loyalty, retention

This focus on top-line revenue growth is as much a challenge in the public, voluntary and not-for-profit sectors as it is the private one. Information technology is, surprisingly, only a subsidiary issue in responding to this challenge, as is evidenced by the IT Governance Institute's 'IT Governance Global Status Report 2004'⁴, which found that:

1. 93 percent of business leaders recognize that IT is important for delivering the organization's strategy, yet
2. 93 percent of respondents experienced IT problems in the previous year; 40 percent of respondents identified operational failures, incidents and an 'inadequate view on how IT is performing';
3. 75 percent of the IT community recognize that IT has problems that need resolving;
4. More than 80 percent of the IT community thinks that IT governance has some part to play in resolving these issues.

In the AT Kearney survey⁵, only 28 percent of IT leaders ranked IT as a top 10 percent issue; only 37 percent of ALL the executives surveyed ranked IT as being this important.

³ 'Conference Board CEO Challenge 2004', Executive Summary

⁴ 'IT Governance Global Status Report, Executive Overview', IT Governance Institute, 2004

⁵ 'Why Today's IT Organization Won't Work Tomorrow', AT Kearney, 2005

Introduction

Historically, therefore, the CEO community has not rated the importance of IT governance nearly as highly as does the IT community. However, while shareholder and regulatory pressures have been driving IT governance up the board agenda, the over-arching reason for IT to become a key board room issue in the 21st Century is the extent to which information and information technology is now driving and shaping the competitive environment.

Shareholder accountability

Institutional investors carry part of the blame for the fact that IT has not historically been on the CEO's agenda. 'One of the key problems with IT is that the City just doesn't get it. When analysts sit down with CEOs and finance directors, attention is focused on the financial performance of the business and its strategy moving forward. As a key driver of the competitive profile of the business, IT systems and plans should be rigorously studied. But very few analysts know the right questions to ask to assess how IT will support the business goals.'⁶

Institutional shareholders are becoming more muscular. Technology is as significant a component of the organization's cost base as its headcount, but usually consumes substantially more capital. Driven, in part, by the changing corporate governance climate and, in equal part, by the poor record of IT projects, stakeholders and institutional shareholders increasingly seek transparency around IT. This is hardly surprising, when you consider the extent of project disaster made possible by the historic culture of opaqueness around IT governance.

For instance, the Standish Group's research on IT project failure⁷ found that:

- 16.2 percent of software projects completed on time and on budget;
- 31 percent of projects were cancelled before completion; and

⁶ Justin Urquhart-Stewart, HP IT Governance Roundtable, November 2002

⁷ 'The Chaos Report', the Standish Group, 1995

Introduction

- 53 percent of projects would cost over 189 percent of their original estimates.

There hasn't been a significant improvement since then. A Conference Board survey in 2001 found that:

- 40 percent of projects failed to achieve their business case within one year of 'live';
- Where benefits came through, it was six months later than expected;
- Implementation costs were, on average, 125 percent of budget;
- Support costs were, on average, 120 percent of budget.

But it's not only about project failure. 80 percent of corporate assets today are digital⁸ and, as shareholders and boards focus on the extent to which information and intellectual capital are fundamental to their competitive position and long term survival, so they recognize the fiduciary nature of their responsibility to shareholders in respect of the organization's information assets and IT.

Compliance

Regulatory compliance and risk management appear to go hand in hand. The best companies have always addressed strategic risk from the boardroom; Basel 2 and today's corporate governance regimes increasingly expect risk management to be pervasive throughout the culture of all organizations.

Across the world, a proliferation of sometimes competing data protection, privacy and computer misuse legislation, little of which has clear implementation guidance or established case law, creates new challenges for corporate boards. Governance regimes – particularly Sarbanes Oxley - have substantial IT compliance components. Securing information against organized crime and cyber terrorism ought to be high on corporate agendas, but isn't: just 20 percent of the respondents in a global survey strongly agreed that

⁸ Testimony of Jody R Westby, PwC Managing Director, to the House of Congress Committee on Government Reform, September 2004

Introduction

their organizations perceived information security as a CEO level priority.⁹

Is it therefore surprising that authorities are increasingly looking to regulation to force the issue up the agenda? ‘The road to information security goes through corporate governance. America cannot solve its cyber security challenges by delegating them to government officials or CIOs. The best way to strengthen US information security is to treat it as a corporate governance issue that requires the attention of boards and CEOs.’¹⁰

Directors’ personal liability

Historically, the outside, or non-executive, directors of companies have been personally immune – financially, if not in terms of reputation – from the legal consequences of failure of the companies on whose boards they sit. A Stanford University study, for instance, found only four US cases, by 2003, where individual defendants had been forced to contribute personally to the settlement securities class actions.

However, in 2004, an ex-Chairman of Global Crossing made a substantial (US\$30 million) personal contribution to settling a class action.

In January 2005, substantially all of the outside directors of both WorldCom and Enron agreed to settle class actions by contributing personal funds to the settlements. Ten Enron directors agreed to contribute an aggregate US\$13 million; ten WorldCom directors agreed to contribute an aggregate US\$18 million, which reportedly represented approximately 20 percent of their wealth. These personal contributions were in excess of the amounts provided by Directors and Officers insurance, which was exhausted by the cases.

While these settlements don’t constitute an admission of liability or of wrongdoing by any of the settling directors (the cases are still, at

⁹ Ernst & Young, ‘Global Information Security Survey 2004’

¹⁰ ‘Information Security Governance: a Call to Action’, US National Cyber Security Summit Task Force, April 2004

Introduction

the point of finalising this book, subject to court approval, with the WorldCom agreement in serious jeopardy), they point to significant changes in the personal exposure of outside directors. There is an argument that the WorldCom and Enron settlements are aberrations and that, once the dust has settled, courts will return to the ‘norm’.

In the UK, Equitable Life is suing its former auditors, Ernst & Young, and its previous directors, both executive and non-executive, for professional negligence in relation to its near collapse in 2000. While hearing the £2.6 billion claim started in April 2005, the UK’s Commercial Court had already ruled in 2003 that the company could proceed with a claim that its non-executive directors were negligent over implementing a strategy which later proved to be unlawful.

The Disney case, in which the company is taking action against its directors in respect of the hiring – and later firing – of Michael Ovitz, provoked the comment that the alleged facts in the case: ‘suggest that the defendant directors consciously and intentionally disregarded their responsibilities, adopting a “we don’t care about the risks” attitude concerning a material corporate decision. Knowing or deliberate indifference by a director to his or her duty to act faithfully and with appropriate care is conduct, in my opinion, that may not have been taken honestly and in good faith to advance the best interests of the company.’¹¹

In a similar vein, the former Chief Justice of Delaware commented, in March 2005: ‘Directors are expected to act—indeed are presumed to act, unless the presumption is rebutted—“on an informed basis, in good faith, and in the honest belief that the action taken was in the best interests of the corporation.” This means that when making a business decision directors are expected to inform themselves with all material information reasonably available.’ In other words, the reasons for action against outside directors are not limited to fraudulent activity; negligence or breach of fiduciary duty is the main thrust of any such action.

¹¹ Chancellor Chandler, in the US Court of Chancery

Introduction

‘There are seven normal expectations that a stockholder should have of a board of directors. Although there may be others in some situations, the stockholders expect that:

1. The stockholders will have a right to vote for the members of the board of directors and have a right to vote on fundamental structural changes, such as mergers;
2. The board of directors will actually direct the management of the company, including strategic business plans and fundamental structural changes;
3. The board will see to the hiring of competent and honest business managers;
4. The board *will understand the business of the firm* and develop and monitor a business plan;
5. The board will *monitor the managers as they carry out the business plan and the operations* of the company;
6. When making a business decision, the board will develop a *thorough understanding of the transaction* and act in good faith, on an informed basis, and with a rational business purpose;
7. The board will operate with basic honesty, care, and loyalty; and
8. The board will take good-faith steps to make sure the company complies with the law.’

He went on to advise outside directors that they should:

- ‘Embrace best practices in governance practices;
- Pay special attention to the board agenda—is the board focused on the right issues and is the board involved in making that determination?
- Make sure you have a *reasonably complete understanding of the company’s business, competitive environment*, financial controls, and financial disclosures. The same is true of the need to have a *thorough understanding* of a particular transaction being considered for board action.’¹²

¹² ‘A Perspective on Liability Risks to Directors’ (emphasis added by the present writer), E. Norman Veasey, former Chief Justice of Delaware and now a senior partner at Weil, Gotshal and Manges LLP, March 2005

Introduction

While the law itself hasn't changed, the 'norm' may be in the process of doing so:

- These various settlements and actions raise expectations for future settlements;
- Plaintiffs' legal firms (who are competitive and fee-orientated) will use these cases as benchmarks in future cases;
- Legal actions for breach of fiduciary duty can be expected, over the years ahead, to include failures in areas other than simply keeping the CEO and the executives in check: failures of large IT projects, for instance, through inadequate project governance, or of significant corporate losses through inadequate information security, might each be at the heart of a future action against directors personally;
- The corporate governance and information security climate is changing with increasing scrutiny of governance practices and information security arrangements and, therefore, the likelihood of new scandals emerging.

The costs involved in legally defending directors are substantial, as are the personal penalties that can be incurred. Directors and Officers' (D&O) insurance has developed to transfer this risk to the insurance market and D&O covers have gradually broadened over the years. It usually (in the UK, certainly) includes protection in respect of any claim or claims first made against the directors 'jointly or severally by reason of any wrongful act' committed – or alleged to have been committed - by them in their capacity as a director or officer of the company. But a combination of rising claim numbers, a doubling of average settlement cost per claim, and increased shareholder activism has radically changed the insurance market. Not only are premiums increasing, but layers of cover are being stripped away, leaving many directors unknowingly exposed to greater personal risk than ever before.

There is 'an increasing trend to impose personal liability on directors and other officers for the shortcomings of companies. In considering the practical consequences of this liability regime, it cannot be assumed that all those exposed to personal liability are able to obtain

Introduction

protection through insurance. The availability of insurance cover reflects the market's appreciation of relevant risks.’¹³ The market for D&O insurance is tightening as the willingness to take on these risks has decreased. Policies have increasing limitations and fees have increased, with the result that smaller companies and high risk enterprises may have difficulty securing cover. This trend may be exacerbated as more insurers understand the potential for IT-related disaster and realize that boards with inadequate IT governance frameworks may have significant legal exposures.

‘The future of how D&O policies will be handled by the courts is an open question as bankruptcies mount and laws and regulations change to meet the challenge. There is an absence of case law determining how courts will rule on certain policy language and no guarantee that they will uphold policy provisions.’¹⁴

Conclusion

The pressures on boards – in both the public and private sectors – to implement an effective IT governance framework are becoming inexorable. The straightforward guidance provided in this book recognizes that, while there is no one-size-fits-all solution, IT governance, to be of value, has to simultaneously deliver improved competitiveness, better compliance and greater shareholder transparency – while enabling directors to clearly and properly discharge their fiduciary duties in a way that helps them avoid the risks of litigation that exposes them to personal, financial ruin.

¹³ Australian Corporations and Markets Advisory Committee Report on Directors and Officers Insurance 2004

¹⁴ www.aon.com/uk

CHAPTER 1: WHY IT GOVERNANCE MATTERS

In the 21st Century, IT governance is, within the broader corporate governance context, critical for all organizations. Those without an IT governance strategy face significant risks; those with one perform measurably better.

Governance background

The ‘greed is good’ business philosophy of the 1980s and 1990s seemed to give way, at the end of the 20th Century, to a ‘looting is good’ approach. Catastrophic financial failure is, of course, a characteristic of the business cycle. Looting has happened before: BICC and Maxwell Communications are good examples. Corporate collapse, originating in a failure of internal control, has happened before: Baring is an instance. The spate of collapses and financial failures at the end of the Internet bubble, though, suggested a systemic weakness, and one whose increasingly worldwide implications have a significant, negative knock-on effect on already problematic pension funds and pensioner assets. Enron, Worldcon, Marconi, Parmalat and many other corporate disasters are the storm damage of unbridled executive authority; shareholders are no longer enthusiastic about losses on this scale.

Governments, already grappling with the challenge of funding the pensions of an inexorably graying population bulge, cannot afford further wanton asset destruction and have started applying themselves to rooting out corporate misbehavior. They are doing this through a combination of overt regulatory action and slightly more covert pressure on institutional investors to stand up for their rights as shareholders and more determinedly exercise their *de facto* responsibility to insist on proper governance from those organizations in which they are invested.

The concept of governance is a simple one: ‘corporate governance is the system by which business corporations are directed and

1: Why IT governance matters

controlled.’¹⁵ The ‘holy trinity’ of good corporate governance has long been seen as shareholder rights, transparency and board accountability. While corporate governance is overtly concerned with board structure, executive compensation and shareholder reporting, the underlying assumption is that it is the board that is responsible for managing the business and controlling the risks to its assets and trading future.

In today’s corporate governance environment, where the value and importance of intellectual assets are significant, boards must be seen to extend the core governance principles - setting strategic aims, providing strategic leadership, overseeing and monitoring the performance of executive management and reporting to shareholders on their stewardship of the organization – to the organization’s intellectual capital, information and IT. A culture of opaqueness is out of line with today’s expectation of pro-activity and governance transparency. Boards that treat IT as merely a functional or operational issue simply don’t ‘get it’; directors who are not proactive in understanding the strategic importance of, and operational risks in, intellectual capital, information and communications technology, are – at best – a drag on the effectiveness of their boards. As younger companies, controlled and managed by people who have grown up with IT and its possibilities, transform the business landscape, so those boards that fail to respond can expect their businesses to be destroyed – and whether the destruction is piece by piece or wholesale is, in the long run, irrelevant.

IT governance is a framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensure that the organization’s IT supports and enables the achievement of its strategies and objectives. In the future, IT governance will be even more important than corporate governance is today: information and IT are absolutely fundamental to business survival, and organizations that fail to ‘direct and

¹⁵ *OECD Principles of Corporate Governance*, 1999

1: Why IT governance matters

control' their IT to best competitive advantage will be left as roadkill on the information superhighway.

The five major drivers of IT governance are:

1. The search for competitive advantage – in the dynamically changing information economy - through intellectual assets, information and IT;
2. Rapidly evolving governance requirements across the OECD, underpinned by capital market and regulatory convergence;
3. Increasing information and privacy related legislation (compliance);
4. The proliferation of threats to intellectual assets, information and IT;
5. The need to align technology projects with strategic organizational goals, ensuring they deliver planned value ('project governance')

Guideline for Directors: *there is no simple technology IT governance solution for this need, whatever vendors say. IT governance, like corporate governance, is about board accountability for the management of the organization.*

Information economy, intellectual capital

The new information, or knowledge, economy is (as we all know) fundamentally different from the old manufacturing economy. The globalization of markets, products and resourcing has lead to increasingly similar shopping streets selling increasingly similar products throughout the developed world. In the less developed world, counterfeit versions of western products usually sell just as well. Over 70 percent of workers in developed economies are now knowledge, rather than manual, workers – including those factory and farm workers whose work depends on understanding and using information technology. Information networking and telecommunications connectivity make this 'global village' possible – and bring numerous other threats and challenges at the same time.

1: Why IT governance matters

The key characteristics of the global information economy, in contrast to those of the older manufacturing one, are:

- Information and knowledge are not depleting resources to be protected; on the contrary, sharing knowledge drives innovation;
- Effects of location and time are diminished – virtual organizations now operate round the clock in virtual marketplaces, and organizations based on east coast America manufacture in China, handle customer support from India, and sell globally through a single web site;
- Laws and taxes are difficult to apply effectively on a national basis as knowledge quickly shifts to low tax, low regulation environments;
- Knowledge enhanced products command price premiums;
- Captured knowledge has a greater intrinsic value than ‘knowledge on the hoof’.

In a very real sense, knowledge grows as it is shared; more knowledge leads to more innovation, which drives more competition which in turn drives more globalization, and so on.

In the manufacturing economy, an organization’s key asset was its productive capability: its machinery, logistical support and distribution equipment, and its stocks of raw materials and finished goods. In the information age, an organization’s key asset is its intellectual capital: its human resources, retained knowledge, structural capital and intangible assets. Every organization with a long term desire to survive and succeed in its chosen market has to focus on preserving, protecting, developing, and applying its intellectual capital for the benefit of its shareholders.

Intellectual capital depends, for its productive existence, on information and communication technology: proper IT governance is, therefore, fundamental to both the proper governance and the long term survival of any 21st century organization.

1: Why IT governance matters

Competitiveness

In 2005, Singapore displaced the United States as the top economy in information technology competitiveness, according to the World Economic Forum's Global Information Technology Report¹⁶. Iceland, Finland and Denmark followed Singapore, knocking the US down to fifth place after three years at the top. ICT (Information and Communications Technologies), observed the report, is 'increasingly playing the catalytic role in pushing the development process forward.'

The same is true for business. IT is neither low-cost nor low-impact. It is investment-intensive. Innovation is common; speed of innovation and deployment can be critical in developing and maintaining competitive advantage. Organizations must respond pro-actively to change within their markets or see their competitive position eroded and ultimately destroyed. Schumpeter called the process 'Creative Destruction': the 'process of Creative Destruction is the essential fact about capitalism...every business strategy acquires its true significance only against the background of that process and with the situation created by it. It must be seen in its role in the perennial gale of creative destruction; it cannot be understood irrespective of it or, in fact, on the hypothesis that there is a perennial lull...'¹⁷

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 source of competitive advantage but, in many situations, 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, in order to ensure they don't fall behind in key performance areas.

In the post Internet-bubble era, we no longer believe that the Internet changes everything *immediately*. IT WILL TAKE A LITTLE

¹⁶ www.weforum.org/gitr has the full report and the comparative 2004 and 2003 rankings.

¹⁷ *Capitalism, Socialism and Democracy*, Joseph A Schumpeter, 1975

1: Why IT governance matters

LONGER. Not much longer though: ICT makes revolutionary business models¹⁸ possible and dramatically transforms the business environment. The fact that online security is an issue only slows down the speed with which online banking, financial services and other e-commerce applications develop, but the final outcome is not in doubt. The Internet does enable small businesses everywhere to compete with larger ones, globally; digital communication speeds up outsourcing, customer awareness and reputation destruction. Instant messaging, voice over IP, spyware and sequential auto-responders are technologies as disruptive as CRM (Customer Response Management), HRM (Human Resource Management) and ERP (Enterprise Resource Planning) systems were in their day. Of course, the Internet doesn't replace the need for a real business strategy, or for generating real economic returns for shareholders; it just transforms the environment within which the board has to create and execute strategy.

Guideline for Directors: *The board must ensure the organization's information strategy, IT systems and IT infrastructure are appropriate for its business model and strategic goals. A board which is not aware of how technology is transforming its business space, and which is not actively investigating how it can use technology to transform its own business (cannibalizing existing activities if appropriate) is a business for which some other organization is already creating a silver bullet.*¹⁹

¹⁸ '[The term 'business model'] seems to refer to a loose conception of how a company does business and generates revenue. Yet simply having a business model is an exceedingly low bar to set for building a company. Generating revenue is a far cry from creating economic value, and no business model can be evaluated independently of industry structure. The business model approach to management becomes an invitation for faulty thinking and self-delusion.' Michael E Porter, 'Strategy and the Internet,' HBR, March 2001

¹⁹ See *Leading the Revolution*, Gary Hamel, 2000

1: Why IT governance matters

Governance convergence

The modern corporate governance movement arguably started with the Cadbury and Greenbury reports in the UK in the 1990s. They were merged into the Combined Code in December 1998 and, in 1999, the Turnbull Report provided directors with additional guidance on how to tackle internal control.

The OECD Principles of Corporate Governance were also 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 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 impacts of SOX is that companies that are directly affected by it are requiring their partners and suppliers to certify conformance to SOX because that gives them greater certainty of ongoing compliance themselves.

And that's the way the OECD is beginning to move. Eliot Spitzer, the New York Attorney General, expressed a not uncommon view when he said: 'the honour code amongst CEOs didn't work. Board oversight didn't work. Self-regulation was a complete failure.'²⁰ Executives are fighting back, but the most recent UK legislation (the 2004 Companies Act) and the current revision to the European Union's 8th Directive on company law 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

²⁰ Eliot Spitzer interviewed in Wall Street Journal, 8 April 2005

1: Why IT governance matters

governance and risk management framework defined by BIS (the Bank of International Settlements) and Basel 2²¹

The requirement for all organizations to adopt best corporate governance practices, irrespective of their nationality or location, is – in spite of the resistance of many executives in many jurisdictions – growing stronger. The ‘entry price’ for access to western capital markets is, increasingly, acceptance of western accounting and corporate governance norms. These requirements cannot be met without an effective IT governance framework.

Strategic and operational risk management

Risk management has always been a key governance issue. The board’s job is strategy and, therefore, strategic risk has always been a board responsibility. The modern corporation’s fundamental goal is to continuously create and add value to its business. That means that strategic management is about finding an appropriate balance between profit maximization and risk reduction.

Strategic risk is the enterprise level risk of a negative impact on earnings or capital arising from an organization’s future business plans and strategies, improper implementation of decisions, or lack of responsiveness to industry changes. It includes risks associated with plans for entering new businesses, expanding existing services, mergers, acquisitions and divestments, and enhancing the infrastructure. As discussed above, information and the technology on which it is stored and with which it is manipulated and communicated is at the heart of 21st century business strategy.

Two key strategic risks related to information and communications technology are:

1. Interruptions to business processes and customer services, and
2. Overspending on IT, placing the company at a cost-disadvantage to its competitors.

²¹ ‘International Convergence of Capital Measurement and Capital Standards: a Revised Framework’, was published by the Basel Committee on Banking Supervision in June 2004.

1: Why IT governance matters

Both these risks should be dealt with as part of the strategic risk management process.

In the last few years, the parallel importance of operational risk ('the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events'²²) has been recognized. The UK's Combined Code requires listed companies to annually review 'all material controls, including financial, operational and compliance controls, and risk management systems.'²³ The Turnbull Guidance explicitly requires boards, on an *ongoing basis*, to identify, assess and deal with significant risks in all areas, including in *information and communications processes*.²⁴ Sarbanes Oxley requires US listed companies (and, increasingly, there is a knock through effect on their major suppliers) to annually assess the effectiveness of their internal controls, and places a number of other significant governance burdens on executive officers, including the section 409 requirement that companies notify the SEC 'on a rapid and current basis such additional information concerning material changes in the financial condition or *operations* of the issuer.'

Risk assessment has, over the last few years, become a pervasive and invasive concept: a risk assessment must be structured and formal, and nowadays one is expected in almost every context – from a school outing through to a major corporate acquisition. It is certainly a cornerstone of today's corporate governance regimes. In the context of both strategic and operational risk, a risk assessment is the first step that a board can take to controlling the risk; the most important step is the development of a risk treatment plan (in which risks are accepted, controlled, eliminated or contracted out) that is appropriate in the context of the company's strategic objectives.

²² 'Operational Risk', a consultative document from the Basel Committee on Banking Supervision in January 2001

²³ *Combined Code on Corporate Governance*, Section C.2.1, July 2003

²⁴ 'Turnbull Guidance', paragraph 21

1: Why IT governance matters

Guideline for Directors: *risk management at both the strategic and operational levels is a board responsibility and is impossible without effective IT governance.*

Regulatory compliance

Information is increasingly subject to legislation. Customers, staff, and suppliers, tribunals and law courts all expect organizations to proactively comply with it. There is international, foreign and industry specific legislation and regulation. All OECD countries have some form of Data Protection and Privacy legislation and national regulations often overlap, are sometimes contradictory and almost all lack implementation guidance or adequate precision. Copyright, digital rights, computer misuse and electronic trading legislation are changing rapidly, and money laundering, proceeds of crime, human rights and freedom of information legislation all add to the confusion.

Complex organizations, with diversified or (partially) virtual business models, operating in and across a number of legal jurisdictions, have an even more complex task. While any one regulation (and its related compliance failure) might apply only to a subsidiary national entity, it is the global parent whose reputation is damaged, and the more failures, the more damage.

While fines and the personal liability of directors and officers can appear as significant risks in relation to some – but not all – of this legislation, few of the regulatory bodies have the resources and capability to pro-actively investigate and pursue possible transgressors. That will change, and soon.

The need for regulatory compliance should not be allowed to disable the organization; nor should it be ignored. Shareholders don't expect their companies to be in breach of national or international regulations.

Guideline for Directors: *there are no technology 'silver bullets' for regulatory compliance – whatever the vendors may say. IT does have a key role to play in delivering compliance, but it can only do so if the board has first identified, risk-assessed, prioritized and*

1: Why IT governance matters

resourced a compliance plan across all the jurisdictions in which the organization has exposures.

Information risk

Organizational information is an asset and therefore, by definition, someone outside the organization wants it. If no-one else wanted it, it wouldn't be an asset. Information, to be useful to an organization, must be available (to those who need to use it), confidential (so that competitors can't steal a march) and its integrity must be guaranteed (so that it can be relied upon). Information risk arises from the threats – originating both externally and internally - to the availability, confidentiality and integrity of the organization's information assets.

Headline figures dramatically illustrate the cost of security failures: the UK's National High Tech Crime Unit (NHTCU) reported²⁵ that 89 percent of firms interviewed had suffered some form of computer crime in the previous 12 months (up from 83 percent in the previous year), at a cost of at least £2.4 billion.

Threats to information security are wide ranging, complex and costly. External threats include casual criminals (virus writers, hackers), organized crime (virus writers, hackers, spammers, fraudsters, espionage, ex-employees) and terrorists (including anarchists). More information security incidents (involving members of staff, contractors and consultants acting either maliciously or carelessly) originate inside the organization than outside it. Baring, Enron, WorldCom and Arthur Andersen were all bought down by insiders. The indirect costs of these incidents usually far exceed their direct ones and the reputational impacts are usually even greater.

Guideline for Directors: *the organization's information security solutions must be proportionate to the value at risk and in line with its strategic and operational goals. These are board decisions, and should not be left to the IT department alone.*

²⁵ 'Hi-Tech Crime: the Impact on UK Business 2005', survey conducted by NOP for the UK's NHTCU

1: Why IT governance matters

Strategic system deployment and project governance

Clearly, in today's ICT-enabled business world, organizations are continuously upgrading their existing systems or deploying new systems to improve customer service, reduce cost, improve product or service quality, deliver new products, services and business models. These system deployments often involve strategic risk for the organization; they always involve operational risk. Risk management is a board responsibility and, therefore, project governance – from inception through to deployment – must also be a board responsibility.

But IT projects are not always delivered successfully. Authoritative research shows that the majority of projects fail to deliver the benefits that justified commencing the project and that, of those that do, the majority come in late and/or over budget. Organizations whose IT project failed all deployed recognizable project management methodologies; the reasons for failure were invariably to do with failures of project governance rather than simply of operational management.

Increasingly, shareholders are concerned about project failure. In the pasts, investment analysts were reluctant to assess IT. As they recognize the impact that technology has on business performance (and, consequently, on shareholder value), so they look increasingly for a framework which ensures that IT projects are aligned with commercial objectives and which enables companies to quantify and report in a consistent manner on IT investments.²⁶

IT investment decisions (for OR against) expose an organization to significant risk, strategic, financial, operational and competitive. The pace of change is a significant. Project risks must be assessed within the organization's strategic planning and risk management framework for the right decision, one which enhances competitive advantage and delivers measurable value, to be made. Critically, projects need continual oversight; the assumptions on which they were predicated need continual re-assessment and the expected

²⁶ HP IT Governance Roundtable, 24 October 2002

1: Why IT governance matters

benefits need regular re-appraisal. A paranoid, pro-active expectation of project failure is the only healthy way of giving it half a chance of success.

Guideline for Directors: *effective IT project governance, therefore, always involves independent, informed, critical board oversight of the implementation of a project that is initiated only after a systematic strategic decision-making process.*

Benefits of an IT governance framework

Good governance only makes sense if it makes sense. In 1996, McKinsey and Company found that two-thirds of the companies in a survey would pay an 11 percent premium for the stock of a company with good governance practices.²⁷ More than that, ‘companies whose boards engage in one or more of [the] three governance practices that signal board independence from management outperform their peers and produce higher returns for their shareholders,’²⁸ as measured by economic value added (EVA – earnings (post-tax) in excess of the cost of the capital required to generate them).

And 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.’²⁹ Research by Weill and Ross also indicates that ‘top-performing enterprises generate

²⁷ Ned Regan in ‘Entrepreneurial Companies, Strong Boards and Shareholder Value’, *Corporate Board Member Magazine*, August 2002

²⁸ ‘The Active Board of Directors and Improved Performance of the Large Publicly Traded Corporation’, Millstein and MacAvoy

²⁹ *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Weill and Ross, HBS Press, 2004

1: Why IT governance matters

returns on their investments up to 40 percent greater than their competitors.³⁰

An IT governance framework is an integral and essential component of the value-focused 21st Century organization's overall governance approach. The development, deployment and integration into its total governance structure of such a framework, though, does far more than simply ensure that the board is complying with both the spirit and the letter of current and emerging national and international corporate governance requirements. It does more than give boards and directors a reliable defence, in commercial or regulatory legal actions, that they took reasonable steps to deploy identified best practice for protecting and enhancing corporate information and intellectual assets, managing risk, controlling IT investment and for complying with information and computer related regulation.

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 governance into the overall corporate governance structure; long term success is impossible.

Guideline for Directors: *at the very least, you need to have thought through and articulated your board's response to the suggestions in this book. No organization that is unpersuaded by these arguments of the need to implement an IT governance framework will survive – nor will its directors.*

³⁰ *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Weill and Ross, HBS Press 2004

CHAPTER 2: GOVERNANCE AND RISK MANAGEMENT

Chapter one observed that corporate governance is overtly concerned with board structure, executive compensation and shareholder reporting, but the underlying assumption is that the *board* is responsible for managing the business and controlling the risks to its assets and trading future. Governance matters, and not just to the press: 20 out of the 30 largest European asset managers now factor governance into their investment assessments; institutional shareholders (particularly in the US and UK) are increasingly militant, with big pension funds under government pressure to exercise their votes in favour of effective corporate governance; and the regulatory objectives of governments across the OECD are converging – as this chapter will show - around a common understanding of corporate governance.

There are still substantial practical differences between corporate governance frameworks in different jurisdictions: separation of the roles of CEO and Chairman is uncommon in the US, as is the right of shareholders to call an EGM, whereas the converse is true in the UK and in UK-related economies. Two tier boards are more likely in continental Europe than in either the UK or the US. The US corporate governance framework has a far higher degree of compulsion about it than does the UK's 'comply or explain' regime; continental European regimes are still in their infancy. This book is not, however, about corporate governance per se. It is about extending best practice in corporate governance to the governance of information and IT in the modern enterprise.

And effective corporate governance is transparent, protects the rights of shareholders, includes both strategic and operational risk management, is as interested in long term earning potential as it is in actual short term earnings, holds directors accountable for their

2: Governance and risk management

stewardship of the business, and ensures that directors exercise their fiduciary duties responsibly.

Fiduciary duties

Corporate governance could be thought of as the framework within which boards of directors exercise their fiduciary duties to the organizations that appoint them. Most people know what is meant by ‘fiduciary duties’ and the summary here is simply designed to provide the context for the rest of this chapter.

‘Fiduciary duties were first elaborated by common law judges, operating without any guidance from the formal written law. Indeed, the company laws of the United States, and many other common law jurisdictions, contain no statement at all of the core fiduciary duties of care and loyalty. The fiduciary duties of directors are continuing to evolve, again without formal written law. The classic statement...is that directors owe to shareholders, or perhaps to the corporation, two basic fiduciary duties: the duty of loyalty and the duty of care.’³¹

Professor Black, of the Stanford Law School, says that the duty of loyalty is the most important: directors should act in the interests of their organization, not of themselves. They must avoid conflicts of interest. A standard method of doing this, in possible conflict-of-interest situations, is to seek transaction approval from independent, non-interested directors.

The duty of disclosure expects directors to provide full disclosure to shareholders of all matters that might affect the outcome of a vote on an issue on which shareholders are entitled to vote, and on all conflict-of-interest transactions.

The third duty is the duty of care: the duty to pay attention and to try and make good decisions. The decisions do not actually have to be good ones; the directors are simply required to *try* and make good decisions. The United States has the ‘business judgement rule’, also

³¹ Professor Bernard S Black, Stanford Law School, Presentation at Third Asian Roundtable on Corporate Governance, April 2001.

2: Governance and risk management

known as the ‘doctrine of non-interference.’ This allows directors to take business risks, even extreme ones, without fear of legal penalty for failure.

However, as was described in the introduction, directors are starting to discover that their personal liabilities in respect of corporate failures may lead to personal financial losses; the duty of care is being re-defined in a number of court cases and, in the current governance climate, it might be expected that a much tougher definition will emerge.

Governance frameworks

The cost of failure is, however, born by shareholders, by employees, suppliers and other stakeholders in the organization. The UK, in the Cadbury, Greenbury and Turnbull Reports of the late 1990s, led the way in defining how the directors’ duty of care – in respect of executive compensation and board management - should be exercised. Progress, particularly in the aftermath of the post-Internet Bubble scandals, has continued. The UK’s revised Combined Code is now explicit in saying that all directors are required to “provide entrepreneurial leadership of the company within a framework of prudent and effective controls which enable risk to be assessed and managed”³². This recognises the need for a risk management framework and leaves rather less room for ‘wild’ risk taking than Professor Black described in 2001. By 2002, the US Sarbanes Oxley Act had mandated the adoption, by US listed companies, of an appropriate system of internal control and, in parallel, had required directors to start monitoring and reporting operational risk.

OECD Principles of Corporate Governance

The OECD Principles of Corporate Governance were originally issued in 1999 and quickly became an international benchmark for corporate governance developments across the world, including into the non-OECD countries. Within the OECD, 30 voluntary codes of

³² ‘UK Revised Combined Code, Higgs Suggestions for Good Practice’, January 2003

2: Governance and risk management

corporate governance have been adopted, mostly since 2002. These include Australia (2003), Austria (2002), Canada (2002), France (2002), Germany (*Kodex* – 2003), Italy (2002), Japan (2001), Netherlands (*Tabaksblatt*, 2003), and Switzerland (2002). These codes are all very recent, are all on a ‘comply or explain basis’ and, within a varied legal and cultural climate for compliance, there are widely varying levels of compliance.

The OECD principles were revised, following extensive consultation, and re-issued in April 2004. They identified six key areas in which a corporate governance framework should operate, including the protection of shareholders’ rights, the timely and accurate disclosure of all material matters regarding the corporation, and that the board should be accountable to the company and the shareholders for providing strategic guidance and effective monitoring of management. The board should ‘focus on long-term issues, such as assessing corporate strategy, and activities that might involve a change in the nature and direction of the company’.³³

Guideline for Directors: *the board cannot meet this obligation without extending its corporate governance responsibilities to explicitly include information and IT.*

BIS and Basel 2

Banking failure can be more catastrophic than any other failure. Banking organizations need, for that reason, to go further in risk management terms than other commercial entities. In the banking world, an international accounting and risk management framework, driven by the Bank of International Settlements (BIS) has already emerged. BIS is the central banks’ central bank. It exclusively serves central banks and other international organizations and its declared aim is to ‘foster cooperation among central banks and other agencies in pursuit of monetary and financial stability’. In June 2004, the Bank’s Basel Committee on Banking Supervision published its ‘International Convergence of Capital Measurement and Capital Standards: a Revised Framework’, which has become known as

³³ ‘The OECD Principles of Corporate Governance’; policy brief, April 2004

2: Governance and risk management

Basel 2. (Basel 1, the Basel Capital Accord of 1988, set out the first internationally accepted definition of, and measurement for, bank capital. It is thought to have been adopted in more than 100 countries.) The Basel 2 framework detailed ‘more risk-sensitive requirements’ for banking organizations in assessing their capital adequacy, and ‘seeks to strengthen market discipline by enhancing transparency in banks’ financial reporting.’³⁴ While the Chairman of the Basel Committee on Banking Supervision has admitted that ‘implementing the Basel 2 rules governing international banks’ capital will be as difficult and important as drawing up the rules, which took five years’, there can be no doubt about BIS’s determination to complete implementation, the start date for which is 2007. While practical difficulties may lead to a deferral in the actual start date, the implementation of these rules is now inescapable.

Operational risk

Basel 2 seeks to achieve its goal of strengthening the international financial system through three pillars. Pillar 1 aims to align a bank’s minimum capital requirements more closely to its actual risk of economic loss, aiming to establish an explicit capital charge for a ‘bank’s exposures to the risk of losses caused by failures in systems, processes, or staff or that are caused by external events,’³⁵ Those banks whose approaches to measuring, managing and controlling their operational risk exposures are appropriate to the risk area will have lower capital requirements. While Pillar 2 allows for supervisory review of banks’ 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’.

These governance frameworks all require the collection and storage of commercially sensitive data in order to satisfy their reporting obligations. These requirements are contained in general legislation

³⁴ BIS Press Release, 26 June 2004

³⁵ BIS Press Release, 26 June 2004

2: Governance and risk management

such as the US Sarbanes Oxley Act, the UK Companies (Audit, Investigations and Community Enterprise) Act 2004 as well as in sector specific regulation enforced by bodies such as the Financial Services Authority and the Securities and Exchange Commission.

Guideline for Directors: *in order to comply, directors will need to satisfy themselves that their IT system themselves do not pose any operational risks to the company, and that their automated controls are all adequate.*

Capital markets and financial reporting convergence

The governance and financial reporting requirements of the UK, US and the rest of the world are converging. This is inevitable, given the sheer size of the western capital markets, and the freedom (and speed) with which financial capital moves around the world: 81 percent of international debt issuance takes place in the EU and US; nearly 90 percent of derivative trading (both OTC and exchange traded) takes place in the EU and US; at the end of 2003, the EU and US represented US\$22bn out of the world's US\$31bn in stock market capitalization. The UK represents the lion's share within the EU.

The simple truth is that any organization wanting to access the world's largest pool of liquid, available financial capital can only turn to the west. And governance requirements, just like financial reporting requirements, are converging as financial institutions and regulatory bodies drive for increased transparency and ease of comparison across multiple jurisdictions.

Recently, the major accounting standards were US GAAP (Generally Accepted Accounting Practice), used by the US and Canada, UK GAAP, used in the UK in UK related economies, and the IAS (International Accounting Standards) used almost everywhere else; different accounting treatments made it difficult for investors – even where corporations reconciled accounts drawn up in accordance with two (or more) standards - to compare corporate performance both within and across sectors.

2: Governance and risk management

The UK's ICAEW (Institute of Chartered Accountants of England and Wales) said: 'the globalization of the business world and the attendant structures and regulation which support it, as well as the development of e-commerce have all had a profound effect on business. Deregulation and increased competition are also bringing paradigm changes to the way in which the profession operates.

As markets converge and geographical borders no longer present the same trade barriers increasingly there is a need for globally accepted accounting standards. Business needs them, investors are demanding them and accountants are under an obligation to ensure delivery.' And that is what is happening.

IAS – renamed IFRS (International Financial Reporting Standards) is being adopted (by EU directive) for all EU listed companies with effect from 2005 and the US FASB (Financial Standards Accounting Board) and the IASB are now working toward convergence of accounting standards. This initiative is expected to finalise a single set of international accounting standards by 2007. The IASB is also working with the Bank of International Settlements (BIS), IOSCO (the International Organization of Securities Commissions) and the Japanese accounting body to drive IFRS into all non-US markets, having already endorsed the use of IFRS (in May 2000) for cross-border reporting.

Converging audit requirements

Inevitably, with one set of accounting standards, applied by companies accessing a single corporate pool of capital, there is also a drive toward a convergence in auditing requirements. While the Corporate and Auditing Accountability, Responsibility, and Transparency Act of 2002, named the Sarbanes Oxley Act after its sponsors, was a response to a specific set of post-asset bubble circumstances, it did raise the bar for audit standards world wide, as it mandated board and auditor independence, and required management to report (with an audit opinion) on the quality of its internal control over financial reporting.

2: Governance and risk management

UK Companies Act 2004

The UK's Companies (Audit, Investigations and Community Enterprise) Act of 2004 placed a statutory duty on officers and employees (including ex-employees) to provide auditors with information (other than legally privileged information) and explanations in respect of any issue related to their audit of the company's accounts. The directors are required to make a statement that they have disclosed (having taken appropriate steps to ascertain it) all relevant information to the auditors and making a false statement will be a criminal offence. The UK's Financial Reporting Review Panel (the FRRP), which was originally set up in 1990 to look into instances of corporate accounting non-compliance with UK GAAP, gained new powers to require companies, directors and auditors to provide documents, information and explanations if there might be an accounts non-compliance with relevant reporting requirements.

With the exception of small and medium enterprises, UK companies will be required to make detailed disclosure of non-audit services supplied by their auditors.

For financial years beginning 1 April 2005, UK quoted companies (which includes UK registered companies that are officially listed in an EU state, on either the NYSE or Nasdaq, but not on AIM or OFEX) will be required to publish an Operating and Financial Review (OFR). Under the Companies Act 1985 (Operating and Financial Review and Directors' Report etc) Regulations 2005, companies are required to include a fair review of their business in the directors' report and publish an auditor's opinion on the consistency of the OFR and the accounts; a criminal and administrative enforcement regime is also created. Previously a voluntary report, the OFR must reflect the directors' view of the business, with the objective of assisting investors to assess the strategies adopted and the potential for those strategies to succeed. DTI guidance is that the OFR must 'include a description of the

2: Governance and risk management

resources available to the company, [and] of the principal risks and uncertainties facing the company'.³⁶

The FRRP, the FSA (the UK's Financial Services Authority) and the UK Inland Revenue are also in the process of coordinating their investigative activities so as to comply with standards set by the Committee of European Securities Regulators. The FSA retains the power to decide on corrective or punitive action and it has a range of sanctions available to it.

EU 8th Company Law Directive

Clearly driven as much by SOX as by its own home grown corporate disasters, the EU issued a 'Directive on Statutory Audit' in 2004. This directive (sometimes called 'Europe's SOX', or 'SOX-lite') will, when it is adopted, replace the existing EU 8th Company Law Directive of 1984. It 'clarifies the duties of statutory auditors, provides for their independence and ethical standards, introduces a requirement for external quality assurance, and provides for the public oversight of the audit profession and improved cooperation between oversight bodies in the EU'.³⁷ The directive, seen as a 'minimum harmonisation' proposal for statutory audits within the EU, also provides a basis for international co-operation between EU regulators and those in third countries. 'The Commission believes that the [PCAOB (the US Public Corporate Accounting Oversight Board)] is particularly important because of the global nature of modern capital markets.'

Negotiations between the EU, the SEC (the US Securities and Exchange Commission) and the PCAOB have been taking place to try and avoid EU auditors having to register with the PCAOB. In the UK, the FRC (Financial Reporting Council)'s remit was extended to include independent oversight (through its newly set up Professional Oversight Board for Accountancy (POBA)) of the

³⁶ 'Guidance on the OFR and changes to the directors' report', January 2005 by the UK's DTI.

³⁷ 'Proposal by the European Commission for a Directive on Statutory Audit of Annual and Consolidated Accounts', September 2004 by the UK's DTI.

2: Governance and risk management

accounting profession. EU and US audit rules are now 'quite convergent', following the principles of independent public oversight, audit quality assurance, more frequent auditor rotation and avoiding conflicts of interest.

The adoption of IFRS and the regulatory convergence opens up the opportunity for the widespread formal adoption of the International Standards on Auditing (ISA). ISAs are published by the IAASB (the International Auditing and Assurance Standards Board) and are already incorporated into the national auditing standards in a number of countries.

Corporate Governance in Europe

There are two main corporate governance models in the EU. The first is the traditional, continental European model, in which companies are largely controlled by 'block holders', an individual, group of individuals or an organization that controls most of the votes at the company's annual general meetings. The second is the UK (or 'Anglo-Saxon') model, in which shares in a company are widely owned and there is a broad equity base. While there has been some convergence toward the UK model in respect of protection of minority shareholders and the regulation of takeover bids, there is still considerable difference across Europe in the legal substance of national corporate governance frameworks.

The European Corporate Governance Forum was set up, in early 2005, by the European Commission, to pursue the objective of EU-wide coordination of corporate governance developments across the EU as a whole. 'The Commission does not want to enact a European Code of Corporate Governance,' said European Commissioner Charlie McCreevy, 'we see no need for this at present and the adoption of such a code, if it were even possible, would be an inevitable and possibly messy political compromise, which would be unlikely to achieve full information for investors about the key corporate governance rules.'³⁸ McCreevy described the Forum's

³⁸ Charlie McCreevy, European Commissioner for Internal Market and Services, 20 January 2005

2: Governance and risk management

priorities: ‘a first area of work is to examine the existing national codes of corporate governance in order to determine whether there is convergence - if yes to which extent and if not, to determine whether, and, if so, how convergence could be reached.’

A conclusion of the EU’s Barcelona summit in 2002 was that economic efficiency has its basis in solid corporate governance. The drive to achieve it will not abate in the foreseeable future. The Anglo-Saxon model is already well advanced.

Combined Code and the Turnbull Guidance

The first version of the UK’s Combined Code, issued in 1998, replaced, combined and refined the earlier requirements of the Cadbury and Greenbury reports on corporate governance and directors’ remuneration. It came into force for all listed companies for year-ends after December 1998. In the UK, corporate governance is on a ‘comply or explain’ basis; in other words, listed companies are expected to comply but are not statutorily required to do so. They can, if they have good reason, choose not to comply with a particular clause of the Combined Code as long as they explain, in their annual report, why that decision was taken. The market will tend to punish companies that choose not to comply, unless the given reasons are cogent.

The Combined Code requirements were broadly similar to those of the earlier reports, but in one important respect – reporting on controls – there was a major and significant development in 1999, prior to the most recent (2003) revision of the code. Whilst the Cadbury report had envisaged companies reporting on controls generally, the guidance which was issued at that time to clarify those requirements permitted, and indeed encouraged, companies to restrict their review of controls, and the disclosures relating to that review, to *financial* controls. This meant that potentially more important issues relating to *operational* control were left outside the reporting framework.

2: Governance and risk management

The Turnbull Report

The Turnbull Report – Internal Control: Guidance for Directors on the Combined Code, published by the Internal Control Working Party of the Institute of Chartered Accountants in England and Wales – provided further guidance in 1999 as to how directors of listed companies should tackle this issue.

Paragraph 20 of the Turnbull Report stated that a company's 'internal control system encompasses the policies, processes, tasks, behaviors and other aspects of a company that, taken together:

- Facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use and from loss or fraud, and ensuring that liabilities are identified and managed.
- Help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organization.
- Help ensure compliance with applicable laws and regulations.'

Paragraph 21 recognized that 'a company's system of internal control... will include... *information and communications processes*'. Paragraph 28 was clear that 'internal controls... should include all types of controls including those of an operational and compliance nature, as well as internal financial controls'.

Guideline for Directors: *the Turnbull Report for the first time made it clear to the directors of UK public companies that their internal control systems had to address all forms of information as well as the systems on which it resided.*

Revised Combined Code

Following the work of the Smith and Higgs committees, the Combined Code was revised and re-issued in July 2003. The Turnbull Report was renamed the Turnbull Guidance and included into the revised Combined Code.

2: Governance and risk management

In Section 1, the revised Combined Code states that the ‘board’s role is to provide entrepreneurial leadership of the company within a framework of prudent and effective controls which enables risk to be assessed and managed.’ Risk management, in other words, is a key responsibility of the board. The non-executive directors are required to ‘satisfy themselves on the integrity of financial information and that financial controls and *systems of risk management are robust and defensible.*’

Principle C.2 of the revised Combined Code deals with Internal Control. The Board is required to maintain a sound system of internal control to safeguard shareholders’ investments and the assets of the company. In practice, directors are required ‘at least annually, to conduct a review of the the effectiveness of the group’s system of internal controls and should report to shareholders that they have done so. The review should cover all material controls, including financial, *operational and compliance controls and risk management systems.*’ The Code then refers the reader to the Turnbull Guidance for details on how to apply this provision.

Paragraphs 17,18 and 19 of the Turnbull Guidance provide an admirably brief and clear description of the principles of a risk treatment plan, of the board’s responsibility to set the policy around risk treatment, the executive’s to implement it, and that of all staff to comply with the system of internal control.

While listed companies are not legally required to comply with the provisions of the revised Combined Code, the Financial Services Authority’s Listing Rules (paragraph 12.43A) require any UK listed company to include the following items in its annual report and accounts:

- a) a narrative statement of how it has applied the principles set out in Section 1 of the Combined Code, providing explanation which enables its shareholders to evaluate how the principles have been applied;
- b) a statement as to whether or not it has complied throughout the accounting period with the Code provisions set out in Section 1 of the Combined Code. A company that has not complied with

2: Governance and risk management

the Code provisions, or complied with only some of the Code provisions or (in the case of provisions whose requirements are of a continuing nature) complied for only part of an accounting period, must specify the Code provisions with which it has not complied and (where relevant) for what part of the period such non-compliance continued, and give reasons for any non-compliance.

The company's auditors must verify the statement made by the directors in respect of the board's compliance with the Code provisions. This is a clear example of how corporate governance regimes provide a framework within which directors are forced to appropriately exercise their fiduciary duty.

The UK government has adopted the principles of internal control set out by Turnbull and published its own 'Orange Book', in which it adapts Turnbull's recommendations to the public sector. All non-governmental organizations (NGOs) and non-departmental public bodies (NDPBs) are expected to conform to these requirements and all UK government and government-controlled bodies were expected to ensure implementation and integration of the processes by the end of 2003.

The key questions that directors of listed companies and 'Orange Book' public sector organizations seek to answer (and which are not meant to be exhaustive) are set out in Appendix 1 to the Turnbull Guidance and are quoted below. Key questions include:

- Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis? (Significant risks may, for example, include those related to market, credit, liquidity, technological, legal, health, safety and environmental, reputation, and business probity issues.)
- Does the board have clear strategies for dealing with the significant risks that have been identified? Is there a policy on how to manage these risks?

2: Governance and risk management

- Are information needs and related information systems reassessed as objectives and related risks change or as reporting deficiencies are identified?
- Are there specific arrangements for management monitoring and reporting to the board on risk and control matters of particular importance? These could include actual or suspected fraud and other illegal or irregular acts, or matters that could adversely affect the company's reputation or financial position.

The Turnbull Guidance does not specify which risks should be included in the scope of the report and what can be left out. The report simply says, in paragraph 16, that 'the board of directors is responsible for the company's system of internal control. It should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy itself that the system is functioning effectively'. In paragraph 17, it goes on to say that, in determining its policies, the board should consider 'the extent and categories of risk which it regards as acceptable for the company to bear, [and] the likelihood of the risks concerned materialising'.

Given the absence of definitive guidance on what risks to include or exclude, and the evident information and IT-related risks faced by every organization, IT governance is fundamental component of effective risk management.

It is clear that systems designed to meet the requirements of Turnbull should be integrated into the organization. This means that the necessary internal control systems should form part of the organizational culture and be part of the day-to-day management of the organization. They certainly should not be a separate structure designed solely for the purpose of complying with the code, nor should they be introduced from outside the organization without there being real ownership within – and from the top of - the organization. Implementation does require the entire organization to embrace the principles of the Code; this can only happen if the process is taken sufficiently seriously for it to be embraced at board level and to be owned by the chairman, chief executive and the whole board.

2: Governance and risk management

Sarbanes Oxley

The Sarbanes-Oxley Act of 2002 (SOX), introduced in the United States of America in the aftermath of Enron, has important IT governance implications for listed American companies, their foreign subsidiaries and foreign companies that have US listings. It applies to all Securities and Exchange Commission (SEC) registered organizations, irrespective of where their trading activities are geographically based. SOX is fundamentally different from the Combined Code, and from codes of corporate governance adopted elsewhere in the OECD, in that compliance is mandatory, rather than 'comply or explain'. This aspect, combined with significant potential sanctions for individual directors, is driving SOX compliance requirements through the supply chain.

While the Act lays down detailed requirements for the governance of organizations, the three highest profile and most critical sections – which were implemented in phases - are 302, 404 and 409.

Key sections of Sarbanes Oxley Act

	302	404	409
Required:	• Quarterly certification of financial reports • Disclosure of all known control deficiencies • Disclose acts of fraud	• Management annually certify internal controls • Independent accountant must attest report • Quarterly change reviews	• Monitor operational risks • Material event reporting • 'Real-time' implications – 4 business days for report to be filed
Responsible	• CEO • CFO	• Management • Independent auditor	• Management • Independent auditor

2: Governance and risk management

The SEC, which is responsible for implementation of SOX, has relevant information available at www.sec.gov/spotlight/sarbanes-oxley.htm, and the Sarbanes-Oxley web site itself is at www.sarbanes-oxley.com.

Internal controls and audit

Under SOX, management is required to certify the company's financial reports and both management and an independent accountant are required to certify the organization's internal controls. In almost every organization, financial reporting depends on the IT infrastructure, whether it is for the rendering of an invoice, the effective operation of an ERP system, or an integrated, organization-wide management information and control system. Unless appropriate internal controls are built into this infrastructure, management will not be able to make the required certification.

The SEC has mandated US companies to use a recognized internal control framework that has been established by an organization that developed the framework through a due process, including inviting public comment. One widely used framework is known as the COSO framework or, to give it its own title, the 'Internal Control – Integrated Framework', which contains the recommendations of the Committee of Sponsoring Organizations of Treadway Commission (www.coso.org). The sponsoring organizations included the AICPA, the Institute of Internal Auditors, the Institute of Management Accountants and the American Accounting Association. The PCAOB (Public Company Accounting Oversight Board, at www.pcaobus.org, created under SOX to oversee the activity of the auditors of public companies in the United States) expects the majority of public companies to adopt the COSO framework and its Auditing Standard No 2, dealing with audit of internal control over financial reporting, assumes that the COSO framework (or one substantially like it) will have been adopted..

Auditing Standard No 2 contains, at paragraph 15, a statement that demonstrates close alignment with the Turnbull guidance in the UK:

2: Governance and risk management

‘Not all controls relevant to financial reporting are accounting controls. Accordingly, all controls that could materially affect financial reporting, including controls that focus primarily on the effectiveness and efficiency of operations or compliance with laws and regulations and also have a material effect on the reliability of financial reporting, are a part of internal control over financial reporting.’

COSO identifies two broad groups of IT systems control activities: general controls and application controls. General controls are those controls which ensure that the financial information from a company’s application systems can be relied upon. General controls exist most commonly as part of an Information Security Management System (such as that identified in BS7799/ISO17799). Application controls are embedded in the software to detect or prevent unauthorized transactions. Such controls can be used to ensure the completeness, accuracy, validity and authorization of transactions.

Paragraph 50 of Auditing Standard No 2 identifies the need for what we call an IT governance framework in maintaining the internal control environment: ‘information technology general controls over program development, program changes, computer operations, and access to programs and data help ensure that specific controls over the processing of transactions are operating effectively.’

Auditing Standard No 2 goes on, at paragraph 52, to evaluate the effectiveness of company-level controls at the outset of the audit engagement, on the basis that it is the company-level controls that have such a ‘pervasive impact on controls at the process, transaction or application level.’ These company level controls include consistent policies and procedure and codes of conduct – all of which are at the heart of ISO17799. The auditing standard specifically cross-references the existing *Consideration of Internal Control in a Financial Statement Audit*, issued by the AICPA in 1990, because it sets out clearly the effect of information technology on internal control over financial reporting.