Board Briefing on IT Governance

Introduction

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

In today's corporate governance environment, where the value and importance of information 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 information and IT. The IT organization's enterprise alignment is essential. A culture of opaqueness is out of line with today's expectation of pro-activity and governance transparency.

This paper identifies key issues and describes appropriate next steps.

IT Governance

IT governance is "a framework for the leadership, organisational structures and business processes, standards and compliance to these standards, which ensure that the organisation's IT supports and enables the achievement of its strategies and objectives."[1]

The five major drivers of IT governance are:

1. the governance requirements of the Combined Code, the Turnbull Guidance and, for US listed companies, Sarbanes-Oxley;
2. increasing information and privacy related legislation (regulatory compliance);
3. operational risk (cf. Basel2), risk management and the proliferation of threats (internal and external) to information and IT;
4. the search for competitive advantage through information and IT;
5. the need to align technology projects with strategic organisational goals, ensuring they deliver planned value ('project governance')

The Combined Code, the Turnbull Guidance and Sarbanes Oxley

The Combined Code on Corporate Governance[2] requires UK listed companies to annually review "*all material controls, including financial, operational and compliance controls and risk management systems.*[3]"

The Turnbull Guidance[4] on compliance with the Combined Code provision C.2.1 explicitly requires boards, on an ongoing basis, to identify, assess and deal with significant risks in all areas, including information and communications processes. There must be a structured approach to risk assessment, and a risk treatment

[1] *IT Governance: Guidelines for Directors*, by Alan Calder (IT Governance Publishing) 2005
[2] The current version was issued in June 2006
[3] Combined Code provision C.2.1
[4] Internal Control: Revised Guidance for Directors on the Combined Code, October 2005

plan (in which risks are accepted, controlled, eliminated or contracted out) that is appropriate in the context of the company's strategic objectives.

Sarbanes Oxley ('SOX') requires US listed companies[5] to have an internal control system like the COSO framework. Both the management and the auditors of US-listed corporations are required by SOX S404 to annually certify the organization's internal control framework. COSO and CoBIT are both deployed to help management meet these requirements; CoBIT, however, is an audit-driven internal control framework. It is not a complete IT governance solution.[6]

The Australian standard AS 8015:2005 is the first formal standard for IT governance that has emerged and which recognizes that the heart of IT governance is the recognition that the board is responsible and accountable for the effective governance of its information and IT assets.

AS8015 is also not completely adequate. Only the Calder-Moir Framework[7] today provides a comprehensive IT governance model.

Regulatory compliance[8]

Information is increasingly subject to regulation. Customers, staff, and suppliers, tribunals and law courts all expect organisations 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. The growing reach of US state-level statutes and breach laws (such as California's SB1386) means that all organizations have to take adequate steps to protect individual data. Copyright, computer misuse and electronic trading legislation add to the confusion[9].

Regulatory compliance should not, though, disable the organisation. IT has a key role to play in delivering compliance, but it can only do so if the board has first prioritised and resourced the compliance requirements.

Risk management: proliferation of threats to information and information security

Business continuity[10] and disaster recovery planning are central to any risk management strategy. Compliance with a Business Continuity standard such as BS25999 goes some way to demonstrating genuine intent to survive unexpected business disasters.

Threats to information security are at least as important. They are wide ranging and complex. More information security incidents originate inside the organization than outside. The indirect costs of these incidents usually far exceed their direct ones and the reputational impacts are often even greater.

The challenge for directors and managers, however, is to ensure that the organization's information security solutions are proportionate to the value at risk and in line with its strategic and operational goals. Information risk must be managed within the enterprise risk management framework (which, itself, might be constructed in line with an external ERM standard[11]).

Risk management decisions affect the organization as a whole and are, therefore, board decisions. They should not be left to the IT department alone. Ongoing

[5] The *Turnbull Guidance* has also been recognised as an acceptable internal control framework for SOX purposes.

[6] See chapter 9 of *IT Governance Today: a Practitioner's Handbook*, by Alan Calder (IT Governance Publishing) 2005

[7] See http://www.itgovernance.co.uk/calder_moir.aspx

[8] Read more about IT regulatory compliance: http://www.itgovernance.co.uk/compliance.aspx

[9] For more information on information regulation, read the IT Governance Triptych

[10] Read more about business continuity planning: http://www.itgovernance.co.uk/bc_dr.aspx

[11] Read more about enterprise risk management: http://www.itgovernance.co.uk/erm.aspx

management failure to deal effectively with information risk is increasingly leading regulators to consider the use of legislation to force improvements to enterprise information security.

The emergence of the *PCI Data Security Standard*[12] and the stringent, precise compliance requirements demonstrate the extent to which leading financial organizations will go in attempting to protect critical personal data.

Information security is a fundamental IT governance building block. The international standard for best practice in information security, ISO/IEC27001, provides a generic framework that can be used to provide a single, coherent and comprehensive information security infrastructure across the whole organization.

Competitiveness

IT is not a low-cost, low-impact technology. 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.

The only purpose of IT is to serve the business. Alignment of IT with organizational goals and the delivery of IT as a service and support to the business in its pursuit of competitive success require clear board leadership. *IT Service Management*[13] frameworks (such as ITIL) can play a significant role in helping organizations improve the effectiveness of IT delivery.

Increasingly, organizational valuations have a high intangible relevance (intangibles are often more valuable than all the tangible assets) and IT intensity (the ratio of IT investment to headcount) continues to grow. High-performing firms are characterized by their ability to leverage their intangible assets and their IT investment. *Knowledge Management*[14] is a cornerstone of success today. This, in the information age, is hardly surprising.

The board must ensure the organization's information strategy, IT systems and IT infrastructure are appropriate for its business model and strategic goals[15]. And, if IT has become a commodity, then the board has to ensure that it gets best value from probably its highest area of ongoing expenditure.

Project governance

Shareholders no longer accept that a high percentage of IT projects simply don't deliver their promised benefits, let alone come in on time or to budget.

IT investment decisions (for OR against) expose an organisation to significant risk, financial, operational and competitive. The pace of change is a significant. IT projects should only ever exist as ***business projects.*** Business commitment, buy-in and support are essential. Project risks must be assessed within the organisation's strategic planning and risk management framework for the right decision, one which enhances competitive advantage and delivers measurable value, to be made.

Effective IT project governance always involves independent, informed board oversight of the implementation of a project that is initiated only after a systematic strategic decision-making process. Professional project managers, and appropriate project management methodologies and disciplines (such as PMBOK, Prince2 and MSP), should always be deployed for any IT project.

[12] Read more about the PCI Data Security Standard: http://www.itgovernance.co.uk/pci_dss.aspx
[13] Read more about IT Service Management: http://www.itgovernance.co.uk/itsm.aspx
[14] Read more about Knowledge Management: http://www.itgovernance.co.uk/km.aspx
[15] See Governance of the Extended Enterprise: Bridging Business and IT Strategies

The growing range of software tools[16] that automate and support project management – particularly for organizations that have a large IT project portfolio to manage – are important. Deployment of such a tool is not the same, however, as the implementation of an IT governance framework and, while better project governance is essential, it's not a completely adequate response to the challenge. What *is* critical is board oversight of all IT projects.[17]

What should Boards do about IT governance?

Every board urgently needs to develop a coherent IT governance framework and strategy. The initial steps are:

1. Make one or more board members responsible for IT governance and adopt an appropriate IT governance framework, including an IT Committee, ensuring that it has appropriate technical expertise and works closely with the audit committee;
2. Create a management and review framework in which the IT Committee has oversight of all IT activity in the company, is responsible for approving and reviewing all information related projects, protecting all the organization's information assets and for ensuring the board receives regular reports on system performance, information ROI and security;
3. Ensure that the corporate risk management plan systematically includes information (which might require deployment of an ISO27001 information security management system) and IT project risk;
4. Task an executive team with developing an IT governance strategy appropriate for the organization's business model and competitive position.
5. Ensure that the organization adopts an effective method – such as the IT balanced scorecard - for measuring IT performance.

The benefits

Organizations that adopt an IT governance framework consistently perform better than those that don't. Recent research shows that organizations with above average IT governance perform 20% better than those following the same strategy without an IT governance framework. And that translates into greater strategic leverage, superior EVA and better share price performance.

FURTHER READING:

IT Governance Library

IT Governance Today: a Practitioner's Handbook
IT Governance: Guidelines for Directors

[16] Read about project management software: http://www.itgovernance.co.uk/prince2_software.aspx
[17] Read more about Project Governance: http://www.itgovernance.co.uk/project_governance.aspx