Best Management Practice
For Portfolio, Programme, Project, Risk and Service Management

OGC

Corporate Governance and Management of Risk (M_o_R®)

John Fisher, UnconfuseU

UnconfuseU

White Paper
April 2010

Contents

Introduction

Ever since organizations first sought finance to fund their activities, there has been a need for accountability to protect the interests of those providing the funding.

The call for increased accountability grows louder every time there is a crisis in public confidence. Whether this is the stock market crash of 1929, for example, or the more recent high-profile collapses of a number of large firms such as Barings Bank, Enron Corporation, WorldCom, MG Rover and Northern Rock, the resulting uncertainty has led to renewed interest in corporate governance practices.

This accountability comes at a price however. In the US, additional regulation costs on large businesses have resulted in an average increase of $2.4 million in auditing fees for each company. Firms with revenue of less than $100 million per annum now pay out more than 2.5% of turnover in compliance. Risk management across an organization, including insurance costs, accounts for a large part of these compliance costs.

Therefore, one of the key questions facing today's managers is: 'How do we provide a set of corporate governance controls that protect the organization's interests without disadvantaging the organization in a competitive market?'

The question that this paper attempts to answer is: 'How can the OGC's guidance on Management of Risk help managers implement a balanced set of risk-related corporate governance controls?'

What is corporate governance?

Before addressing the question of whether Management of Risk (M_o_R) can help with corporate governance, let's first define what is meant by both 'governance' and 'corporate governance'.

To govern means to 'control the actions or behaviour of'. In organizations, governance (or the act of governing) is becoming a widespread term. Programmes and projects are now 'governed' by a programme or project board, or by a steering committee. Governance is provided by internal audit, and operational governance ensures that policies and procedures for the day-to-day activities of the organization are implemented and followed.

Corporate governance can be defined as the set of processes, customs, policies, laws and institutions affecting the way a company is directed, administered or controlled.

Although corporate governance is designed for the protection of its external funders, it also applies to government, not-for-profit and other membership organizations. In this context, the 'external funders' become stakeholders who could, for example, be members of the public, or special interest groups to whom the body is accountable.

Types of corporate governance

Across the world, there are several different models of corporate governance in use. This is firstly a reflection of the way organizations are funded, and secondly reveals the control imposed by legislation or an external regulator.

Corporate governance enables governments and wider stakeholders to ensure organizations working in the same market space all behave in a similar way. In organizations with legislative or regulatory control, the internal controls are a reflection of the imposed external controls.

Taking a worldwide view, governments have created many different approaches to regulate companies and corporations in order to protect assets, earning capacity and the reputation of the organization. The main types of governance are:

- **Anglo-American** Anglo-American corporate governance is based on the corporate objectives set by the owners of the organization. The shareholders are the primary stakeholders to whom the organization is accountable and the internal performance and external accountability is geared towards the achievement of these objectives.
- **Franco-German** Franco-German corporate governance views a firm as a collective entity that has responsibilities and duties towards key stakeholders, with shareholders perceived to be only one group of such stakeholders.
- **Japanese** Japanese industrial structure is based on a network of supplier and buyer companies ('keiretsu'). Keiretsu are known for their extensive cross-shareholding among members and their main banks. Organizations have long-term and stable relationships among firms and the banks that finance them.

With increased foreign ownership and global competition, there is a slow trend towards the adoption of the Anglo-American governance approach.

UK responses to corporate governance

The UK has been at the forefront of the debate on corporate governance with the publication of several major reports. The Cadbury Report (1992) examined the financial aspects of corporate governance; while the Greenbury Report (1995) studied directors' remuneration. Hampel (1998) reviewed various aspects of the recommendations on corporate governance made by the two earlier reports and came up with a revised code.

In total, 18 reports, codes or guides on corporate governance were published in the UK between 1992 and 2005.

The UK Stock Exchange controls publicly listed companies through the Combined Code on Corporate Governance. These rules require UK companies listed on the main market of the London Stock Exchange to describe their corporate governance performance in their annual reports and accounts, including details on how they adhere to the Code's principles and provisions.

In the US, a more radical approach was taken resulting in new legislation in the form of the Public Company Accounting Reform and Investor Protection Act of 2002 (also known as 'Sarbanes–Oxley' or 'SOX'). The main thrust of the Act is to influence the behaviour and conduct of public companies to ensure that they issue informative and accurate financial statements.

For many countries, applying rules similar to those in the US has been seen as the way forward. In Japan they have applied the 'J-SOX' regulatory system, while in Germany they operate the German Corporate Governance Code. France operates its Financial Security Law of France ('Loi sur la Sécurité Financiere'), and in Australia they have the ASX Corporate Governance Council.

Corporate governance and risk management

To achieve internal corporate governance, organizations will often implement controls to protect the assets of the organization. This explains why the more usable definition of corporate governance is "a sound system of internal controls".

Those of us working in an organization will be familiar with internal controls: claiming for expenses incurred during the execution of business away from the office, procuring equipment and services, booking annual leave, and even (in some organizations) taking stationery out of the stationery cupboard!

In the same way that internal control is one aspect of corporate governance, risk management is one aspect of internal control. This is because a company's objectives, internal organization and the environment in which it operates, are continually evolving, and as a result the risks it faces are continually changing.

Since profits in an organization are in part the reward for successful risk-taking, the purpose of internal control is to protect the organization's assets so they can be used to generate profits. A sound system of control therefore depends on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed. The evaluation helps manage and control risks rather than eliminate them.

In order to achieve effective protection of assets, risk evaluation needs to take place across the organization. This, in turn, means that risk management needs to be implemented across the whole organization. The OGC's guidance on management of risk (M_o_R) is one approach to help achieve this.

What is M_o_R?

M_o_R provides guidance in helping organizations put in place an effective framework for taking informed decisions about the risks that affect their performance objectives across all activities. This means that setting the strategic direction, managing change through programmes and projects, or running the day-to-day operations, can all be covered by one approach.

The first edition of the M_o_R guide was published in 2002 in response to the Turnbull Report's recommendation to provide a generic framework for risk management across all parts of an organization. The second edition, published in 2007, reflected the further developments in the world of risk management. Examples included:

- In the UK public sector, HM Treasury had revised its Orange Book, which outlines the principles and concepts of risk management.
- In the global private sector, change had been instigated by new regulatory environments such as the Combined Code on Corporate Governance 2006 (UK), Basel II Accord 2004 (Europe), and Sarbanes–Oxley 2002 (US).

This common approach, which M_o_R recommends should be applied across the organization, includes a route map for performing risk management. This provides a way of tuning the guidance to ensure the correct approach is adopted, as well as providing sources of advice on risk management techniques and specialisms. The route map, together with the processes described in M_o_R, creates the basis for a joined-up approach to risk management.

How does M_o_R fit with other OGC methods and guidance?

The OGC has developed a range of best-practice products for dealing with change across the organization. All of these products rely on sound risk management as one of their core elements.

The OGC best management practice guidance *Managing Successful Programmes* (ISBN 9780113310401) provides a framework to enable the achievement of high-quality change outcomes and benefits that fundamentally affect the way that organizations work.

A key theme is managing risks to enable the achievement of a programme's objectives.

PRINCE2 is a structured method to help effective project management. One of the themes of PRINCE® is risk, in recognition that 'project management must control and contain risk if a project is to stand a chance of being successful.

A recent addition to the OGC family of publications is *Portfolio, Programme and Project Offices* (ISBN 9780113311248), which brings together a set of principles, processes and techniques to facilitate effective portfolio, programme and project management through enablement, challenge and support structures.

The OGC's ITIL® series of publications has applications to technology-oriented operational environments, offering internationally recognized guidance for IT service management and providing a very powerful base for understanding the business-as-usual processes and services at risk.

How does M_o_R support corporate governance?

M_o_R is based on a set of principles that are essential for the development of good risk management practice. These are all derived from proven corporate governance principles in the recognition that risk management is a subset of any organization's internal controls. The 12 principles are given in Figure 1.

Figure 1 The 12 principles of M_o_R

Principle:	Corporate Governance Principle	M_o_R Principle
Organizational context	A company's system of internal control will reflect its control environment and should be capable of responding quickly to evolving risks to the business arising from factors within the company and to changes in the business environment.	The starting point for risk management is to understand the context of the organization or activity under examination and hence avoid blind spots. Context includes the political, economic, social, technological, legal and environmental backdrop.
Stakeholder involvement	The board as a whole has responsibility for ensuring that a satisfactory dialogue with shareholders takes place. The annual report and accounts should include such meaningful, high-level information as the board considers necessary to assist shareholders' understanding of the main features of the company's risk management processes and system of internal control, and should not give a misleading impression.	Risk management should engage with all primary stakeholders to ensure that the objectives of the organization or activity under examination are established and agreed.
Organizational objectives	A company's objectives, its internal organization and the environment in which it operates are continually evolving and as a result, the risks it faces are continually changing. A sound system of internal control therefore depends on a thorough and regular evaluation of the nature and extent of the risks which the company is exposed.	As the purpose of risk management is to strive to understand and manage the threats and opportunities arising from the objectives of the organization or activity, risk management can only commence when it is clear what these objectives are.
M_o_R approach	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 the system is functioning effectively.	Organizations should develop an approach to the management of risk that reflects their unique objectives. It is common for organizations to describe their approach through their policies, processes, strategies and plans.

Figure 1 ***continued***

Principle:	Corporate Governance Principle	M_o_R Principle
Reporting	The reports from management to the board should, in relation to the areas covered by them, provide a balanced assessment of the significant risks and the effectiveness of the system of internal control in managing those risks. Any significant control failings or weaknesses identified should be discussed in the reports, including the impact that they have had, or may have, on the company and the actions being taken to rectify them.	The governing body of the organization should receive, review and act on risk management reports. As a result, a fundamental aspect of risk management is the timely communication of risk information to the management team to enable it to make informed decisions.
Roles and responsibilities	All employees have some responsibility for internal control as part of their accountability for achieving objectives. They, collectively, should have the necessary knowledge, skills, information, and authority to establish, operate and monitor the system of internal control.	Organizations should establish clear roles and responsibilities for the management of risk in terms of leadership, direction, control, ongoing risk management, reporting and reviewing.
Support structure	People in the company (and in its providers of outsourced services) have the knowledge, skills and tools to support the achievement of the company's objectives and to manage effectively risks to their achievement.	A risk management team is required to ensure that the policies are adhered to, the process is followed, appropriate techniques are adopted, reports are issued to meet senor management and board requirements, the regulators' guidelines are adhered to and best practice is followed – all at the appropriate time.
Early warning indicators	A sound system of internal control therefore depends on a thorough and regular evaluation of the nature and extent of the risks which the company is exposed.	Organizations should establish early warning indicators for critical business activities to provide information on the potential sources of risk. These will enable risk management to be proactive and to anticipate potential problems.
Review cycle	The directors should, at least annually, conduct a review of the effectiveness of the group's system of internal control 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'.	As with an organization's objectives, its internal organization and environment within which it operates are continually evolving. A sound and effective risk process is contingent on regular reviews of the risks faced and the policies, processes and strategies it is adopting to manage them.
Overcoming barriers to M_o_R	The company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control system.	There needs to be recognition that even though an organization has risk management policies, processes and strategies in place, this will not automatically lead to robust, effective and efficient risk management practices. There are a number of barriers to the implementation of risk management that need to be addressed.
Supportive culture	Senior management should demonstrate, through its actions as well as its policies, the necessary commitment to competence, integrity and fostering a climate of trust within the company.	Organizations should establish the right culture to support management of risk throughout the organization. A supportive culture will be one that embeds risk management into day-to-day operations and recognises the benefits of risk management.
Continual improvement	The board's annual review of the effectiveness of the group's system of internal controls should cover all material controls, including financial, operational and compliance controls and risk management systems.	Organizations that are interested in continual improvement should develop strategies to improve their risk maturity to enable them to plan and implement step changes in their risk management practices

Whilst these principles are not intended to be prescriptive, they do provide supportive guidance to enable organizations to develop their own policies, processes and plans to meet their specific needs.

Implementing M_o_R

Implementing M_o_R will usually start with the development of a risk management policy – an organization-wide communication on how risk management will be implemented throughout the organization in order to support the achievement of its strategic objectives.

The policy is the key document that forms the foundation of risk management across the organization. From this starting point the organization can develop individual strategies for implementing risk in each area of the business. This enables specialist risk management approaches required for different parts of the organization to be brought together. This might include business continuity planning in an operational area or the setting of a new business strategy in another area.

Why is M_o_R better than other approaches?

In many ways, M_o_R has similarity with other risk approaches, including defined roles and responsibilities, and other common tools such as risk registers and defined risk management processes.

Very few methods, however, offer such a complete support package as M_o_R. This support package includes, obviously, the guidance. This is a flexible approach to the implementation of risk, based on experience and lessons learned across many organizations.

Implementing risk management relies on all staff having an understanding of risk, supported by others with skills and experience in risk management. Staff in an organization have the opportunity to demonstrate their understanding of M_o_R by acquiring recognized Association for Project Management (APM) Group's foundation and practitioner qualifications.

M_o_R is also supported through a best practice management support group. This has been in existence for over 15 years, supporting its members in their understanding of the OGC programme, project and risk management products.

As well has having a web presence, the Best Practice User Group (known as BPUG) supports its community through newsletters, workshops and an annual members' conference.

M_o_R is also supported by a range of titles and formats published by TSO.

Summary

Whilst organizations will always be controlled by national guidelines, which may vary from country to country, the one constant is the need for organizational risk management.

M_o_R provides organizations with the appropriate level of guidance to enable them to adopt the latest best-practice approach to their organization and embed the approach through an established support network. This encourages openness and discussion of real business issues when implementing risk management.

About the author

John Fisher is the APM Group Chief Examiner for the M_o_R qualification. He works with the Institute of Risk Management (IRM) as an examiner for the IRM certificate in risk management.

John is an independent management consultant and has for many years worked in a variety of public and private sector organizations. He is currently working as a consultant and trainer in the fields of consultancy, risk management, project management, and project and programme support as an interim resource.

As a trainer, he is accredited to deliver Information Systems Examining Board (ISEB) courses in consultancy skills, project management, project support and software testing. John is also accredited by the APM Group as a PRINCE2 and M_o_R trainer. He has been responsible for delivering training to some of the UK's leading companies, including airlines, major financial institutions and mobile telecommunications companies.

John Fisher, UnconfuseU, www.unconfuseu.com

Further information

To learn more about Management of Risk: Guidance for Practitioners, visit: www.best-management-practice.tvwww.mor-officialsite.com.

Acknowledgements

Sourced by TSO and published on www.best-management-practice.com

Trademarks and statements