Good Governance

A risk-based management systems approach to internal control

David Smith and Robert Politowski, iMS Risk Solutions Ltd
Contents

Foreword ..................................................................................................................... iv
Acknowledgements ................................................................................................. vi

1. Introduction ........................................................................................................... 1
2. Scope and definitions .......................................................................................... 2
3. Risk management system .................................................................................... 3
4. Implementation of risk management system ..................................................... 4
5. Other management processes ............................................................................ 5
6. Self-assessment questionnaire ............................................................................. 6

Appendix A Summary of risk management tools .................................................... 7
Appendix B References and further reading............................................................ 8
Foreword

This is a guide to how organizations can identify and manage their risks for good governance. Since the publication of PD 6668:2000, *Managing Risk for Corporate Governance*, upon which this book is based, there is a greater appreciation of the importance of risk management in organizations and society at large. All organizations take risks. They also need to recognize and manage those risks which, if realized, could prejudice the sustainability of the organization. This applies to organizations worldwide, in the private or public sectors, NGOs, as well as not-for-profit organizations. This book outlines a management framework for identifying the risks and opportunities, determining the extent of the risks, implementing and maintaining control measures and reporting on the organization’s commitment to this process.

There have been a number of developments in the international and national management standards field since PD 6668 was published in 2000. These developments, including those on risk management (2008), occupational health and safety (2007), environmental management (2004) and sustainable development (2006), can help organizations with internal control for good governance. Although the principles in many of these documents are similar they do not use the same approach. This is unfortunate as there is an increasing demand for an integrated approach. An integrated approach that was developed in 2006 was PAS 99, *Specification of common management system requirements as a framework for integration*. The framework used in this book has elements in common with PAS 99 and helps support the holistic approach to risk management for internal control and good governance.
A risk-averse business culture is no business culture at all.

(Blair, 2005)
Acknowledgements

The authors would like to thank Chris Millidge for his help in drafting this document and Michael Faber for reviewing it for us and his helpful suggestions.
1. **Introduction**

This book provides guidance for organizations that wish to develop a framework for managing risk for good governance. Research by analysts demonstrates the positive link between good governance and organizational performance. In a recent study, the Association of British Insurers – major investors in public companies in the UK – found that ‘well-governed companies will produce better returns for shareholders over time’ (Association of British Insurers, 2008).

It is clear that well-managed organizations generally, whether in the public or private sector, are far more likely to satisfy stakeholders. The focus of this publication is about managing those risks for the sustainable operation of organizations using a management systems standard approach.

In this introductory chapter the background to governance and the organizations to which the approach is applicable are briefly reviewed. The chapter explains why the approach adopted is generally applicable and consistent with international management systems standards.

**Background**

The term ‘corporate governance’ came into general use following a number of major scandals and corporate failures in the late 1980s and early 1990s, and in the UK became enshrined in the report from the Committee on the Financial Aspects of Corporate Governance (the Cadbury Committee): ‘Corporate governance is the system by which companies are directed and controlled’ (Cadbury et al, 1992).

Such failures have occurred throughout the world and continue to occur. The impact of these worldwide corporate failures had the potential to be of such a magnitude that there was the danger that the whole structure of the means of financing corporations might become threatened. The essence of the limited liability company is that external investors are willing to become shareholders, in the confidence that their interests will be safeguarded. Shareholders accept that not all investments will prove rewarding, but they are entitled to assume that there will be no mismanagement on the part of the directors and managers who are in day-to-day control of the corporation. If they cannot be confident that this is the case they will be unwilling to invest, and the basis of modern commercial activity will be under threat. Whilst an individual shareholder might have been willing to accept the risk, major investors such as insurance companies or pension funds began to demand that to safeguard the interests of their clients, there should be greater regulation of the behaviour of joint stock companies.

In 1999 the Organisation for Economic Co-operation and Development (OECD) produced a definition of corporate governance and a set of principles. These principles were revised in 2004 and at a high level comprise the following requirements of a corporate governance framework (Organisation for Economic Co-operation and Development, 2004a). It should:

1. ‘...promote transparent and efficient markets, be consistent with the rule of law and clearly articulate the division of responsibilities among different supervisory, regulatory and enforcement authorities...’;
2. ‘...protect and facilitate the exercise of shareholders’ rights...’;
3. ‘...ensure the equitable treatment of all shareholders, including minority and foreign shareholders. All shareholders should have the opportunity to obtain effective redress for violation of their rights...’;
4. ‘...recognise the rights of stakeholders established by law or through mutual agreements and encourage active co-operation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises...’;

5. ‘...ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, ownership, and governance of the company...’;

6. ‘...ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders...’

There are a number of sub-clauses to each of the main principles that cover specific areas.

There have been further definitions of governance and legislative powers in many countries around the world. These range from the voluntary code of practice approach as seen in the UK to the more prescriptive Sarbanes-Oxley Act (United States of America, 2002) in the US – a response from legislators in the US to high-profile failures such as Enron and WorldCom.

Organization-wide risk management and internal control are important for the successful running of any business and should remain relevant over time in the continually evolving global business environment. The OECD principles specifically highlight board responsibility:

*Ensuring the integrity of the corporation’s accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.*

(OECD Principle VI.D.7)

This has led to the formal consideration of risk and the identification of it as a ‘separate’ aspect that can benefit from specific management arrangements. That is not to say that organizations have not previously recognized these risks, but simply that a formal and structured approach had not been a feature in many organizations.

The characteristics of many successful organizations tend to reflect an attitude and culture of identifying opportunities, recognizing the risks and managing them appropriately. There are upsides and downsides to the risks that come with every opportunity and it is necessary to select the right balance. Organizations that are risk averse are unlikely to thrive in the long term because of continual change in the marketplace and social expectations.

**Application of this approach**

All organizations need to display good governance, whether they are corporate bodies, private entities, public bodies or charities.

In an increasingly complex world where stakeholders play an ever more important role there is the expectation of good governance and transparency. There are a variety of characteristics of good governance including promoting values in the organization, focusing on the purpose of the organization, effective performance, engagement with stakeholders and, most significantly from the perspective of this book, the management of risk.
Many organizations need to manage a whole host of risks, for example:

— corporate organizations operate in an increasingly complex world with global impacts, international supply chains and informed public opinion expressing concern about social responsibility;
— public bodies have to determine the benefits of new technology against the risk of data loss;
— charitable bodies have to balance the risks of supporting international disasters against the risks faced by their workers and donors’ concerns about misuse of aid;
— public bodies have similar accountabilities to their ‘shareholders’ – often taxpayers;
— charitable concerns need to assure their ‘investors’ that their donations are being applied to the purpose for which they were intended.

The principles of good governance equally apply to public bodies, charities, voluntary bodies, etc. There is a need for good governance of public bodies to reflect the need to ensure value for money, transparent decision making and reporting, proper codes of conduct, accountability and so on.

Despite the difference between the public and private sectors it is essential that people know for what they are responsible, and for what they are accountable. Within public bodies this probably varies more than within private ones.

There is also a drive for the public sector to be more creative and be prepared to take more calculated business risks in order to deliver the best possible services to the public. The public and private sectors differ in this respect. The public sector needs good governance to enable it to take certain calculated risks, whilst the private sector needs good governance in order to manage the risks that are taken in everyday business.

Figure 1.1 is a diagram from BS 6079-3:2000 that shows one way of expressing the relationship between threat and opportunity when managing projects.

**Figure 1.1 — Relationship between threat and opportunity**

Public bodies need to direct and control their functions and nowhere can this be more clearly demonstrated than in local government. Local government bodies have a real need to relate to their communities in a similar manner to corporate bodies, and to demonstrate continuous improvement and value for money through outward-looking, accountable and responsive services.
Introduction

Risk management and internal control should be included in all dimensions of public bodies such as:

— making public statements to stakeholders on the risk management strategy, process and framework, demonstrating accountability;
— the capability and capacity within the organization;
— mechanisms for monitoring and reviewing effectiveness against agreed standards;
— robust systems for identifying, profiling, controlling and monitoring all significant strategic, programme, project and operational risks;
— providing openness by involving all those associated with planning and delivering services, including partners.

All the above issues are equally applicable to charities, clubs, societies and associations. Large charitable concerns rely heavily on public donations to support their activities internationally.

There is clear recognition amongst boards of directors and investors – mostly those in the professional investment market – that there is a link between good corporate governance and organizational performance that is valued by stakeholders. There are a number of international ratings organizations that focus research on the development of scoring systems for ranking governance performance. This research is often used by professional investors to assist in making informed decisions to formulate an overall investment strategy, as a screening tool for analysts and portfolio managers and to adjust for governance risk when assessing credit risk, etc.

Additionally, companies themselves are beginning to use similar ranking research to help in their decision making, to reduce the chance of being targeted for shareholder action, to increase market trust in reported earnings, as a support to seek lower borrowing costs, and in attracting highly qualified and experienced directors who can add value to the organization and achieve a higher market capitalization.

A management systems approach

Good risk management is an essential element of good governance and it is against this background that this publication focuses on a risk management framework to help organizations in applying the principles of risk management throughout the whole organization from the lowest operating levels to the board of directors.

It is clearly important that all aspects of corporate governance are managed in a holistic manner. This book focuses specifically on the important management of risk and the development of effective internal control mechanisms: Clause C.2 of The Combined Code on Corporate Governance (Financial Reporting Council, 2008) as expanded upon from Internal Control – Revised Guidance for Directors on the Combined Code (Financial Reporting Council, 2005).

Chapter 2 provides details of the scope and definitions used. A more detailed description of an approach to managing risks is given in Chapter 3, which lays out a framework of the issues that should be addressed and follows a Plan, Do, Check, Act (PDCA) approach that is consistent with international management systems standards. This approach is based on the model given in PAS 99:2006 (The requirements included in section 4 of the PAS can be used as a specification against which organizations can be assessed by changing the word ‘should’ to ‘shall’.)
Chapters 4 and 5 contain a practical guide to delivering business requirements with respect to risk management for good governance. Chapter 6 provides a questionnaire to enable organizations to carry out a self-assessment of their systems for governance.

A good management system will enable identification of risks, their management and help in any disclosure requirements for stakeholders. The aspect of disclosure is specifically highlighted in the OECD principles for governance, which additionally call for inclusion of material information on ‘Foreseeable risk factors’ (Principle V.A.6).

Figure 1.2 — Three key components for delivering effective corporate governance

Figure 1.2 shows a simple model of the interrelationship of the three main components of a risk management system for good governance. It is essential that the risks are identified and understood and decisions taken on how they will be managed.

A key feature of a management systems approach is identification of objectives and a programme for delivering the defined objectives. Many international management systems standards have differing approaches; PAS 99 provides a common approach for managing business risk requirements in an integrated manner. Many organizations already have management systems in place, meeting the requirements of these international standards and the approach builds upon these to ensure the benefits of existing systems can be utilized, eliminating redundancy and increasing efficiency.

However, good internal control and risk management systems will not succeed in delivering the organizational objectives unless the arrangements are embedded within the organization and individuals committed to delivering

---

**Failure to identify risk of data loss**

A government department was seeking to transfer personal data to another department in a short space of time. Effective procedures were in existence but the time and cost of removing the sensitive elements of the data was considered too great. As a result, when the data was lost in transit the personal details of many millions of people were lost.

The loss of this information has had many repercussions:

- loss of confidence by the public in government departments handling confidential personal information;
- individuals whose details have been compromised;
- a possibility for fraudulent activity through the use of this information remains for many years to come.

**Charity and aid**

Charity A was challenged by a government department that had made a grant for an aid project. The charity was asked to demonstrate that its governance procedures were effective in the delivery of aid as news media reports suggested that those supposedly receiving the aid had made claims that it was inappropriate for their needs and some had fallen into the wrong hands. This threatened to become a scandal and affect not only funding from government but also the many donations from members of the public who regularly made a significant contribution to overall funds. The need for an effective control framework and monitoring and auditing became obvious.
Introduction

Financial turmoil

The turmoil in the financial markets in 2007 was a good example of the consequences of failing to recognize and manage risks. The failure of ‘sub-prime’ home loans in America led to failures in local banks. What would have been a local problem became international because large numbers of these sub-prime loans had been packaged up and sold to institutions around the world. The realization by investors that they had misjudged the risk of US mortgage borrowers led to a conclusion that risk had been underestimated in all kinds of debt markets, and banks were left with large amounts of unsellable debt. In the UK, mortgage lenders who were used to being able to borrow money when needed suddenly found that banks were no longer willing to provide the loans. A regional mortgage lender had grown substantially using wholesale money market borrowing which it was able to secure on very advantageous rates. The change in international money markets led to exposure to a shortfall in funding. Assessment of the risk and control of growth together with contingency arrangements should have prevented the collapse of the bank.

their objectives – ‘there has to be something in the lifeblood of the organization that persuades its people to do extraordinary things for it as well as for themselves’ (Hillson, 2007).
2. **Scope and definitions**

**Scope**

The guidance given in this book outlines how an organization can implement effective arrangements for managing risk, to ensure that it meets its corporate governance needs. A PDCA framework is used, which is consistent with the approach in management systems standards produced by the International Organization for Standardization (ISO).

This guidance is applicable to any organization that wishes to:

- establish arrangements at top management level to identify, manage and mitigate risks;
- implement, maintain and continually improve its management of risks in a manner which is consistent with its policy;
- assure itself of conformance with this policy;
- make a self-determination and self-declaration of its performance on an annual basis.

There are a number of documents an organization may wish to refer to for further guidance within its particular country, sectors, etc; some are included in Appendix B.

**Definitions**

*acceptable risk* risk at a level that can be tolerated by the organization

*audit* systematic examination to determine whether activities and related results conform to planned arrangements, and whether these arrangements are implemented effectively and are suitable for achieving the organization’s policy and objectives

*management system* part of the overall management that includes organizational structure, planning activities, responsibilities, practices, procedures, processes and resources for developing, implementing, achieving, reviewing and maintaining the organization’s policy

*nonconformity* non-fulfilment of a requirement

Note: a nonconformity can be any deviation from relevant work standards, practices, procedures, legal requirements, etc. (see BS EN ISO 9000:2005, 3.6.2 and BS EN ISO 14001:2004, 3.15).

*organization* company, corporation, firm, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration

Note: for organizations with more than one operating unit, a single operating unit may be defined as an organization (see BS EN ISO 14001:2004, 3.16).

*risk* effect of uncertainty on objectives

Note 1: an effect is a deviation from the expected – positive and/or negative.

Note 2: objectives can have different aspects, such as financial, health and safety, and environmental goals, and can apply at different levels, such as strategic, programme, project and operational.
Scope and definitions

Note 3: risk is often characterized by reference to potential events, consequences or a combination of these and how they can affect the achievement of objectives.

Note 4: risk is often expressed in terms of a combination of the consequences of an event or a change in circumstances, and the associated likelihood of occurrence (see BS 31100 (DPC) (2008).

top management  person or group of people who directs and controls an organization at the highest level (see BS EN ISO 9000:2005, 3.2.7)

Table 4.3 — Cascade of risk management system

<table>
<thead>
<tr>
<th>Operational level</th>
<th>Responsibility</th>
<th>Top management</th>
<th>Middle management</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic/management</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Strategic/management/operational</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Management/operational</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Operational</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Source: PD 6668:2000