The KPMG Review

Internal Control:
A Practical Guide

This book has been prepared to assist clients and others in understanding the implications of the ICAEW publication *Internal Control: Guidance for Directors on the Combined Code*. Whilst every care has been taken in its preparation, reference to the guidance should be made, and specific advice sought where necessary. No responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication can be accepted by KPMG.

KPMG is registered to carry on audit work and authorised to carry on investment business by the Institute of Chartered Accountants in England and Wales.

Designed and produced by Service Point (UK) Limited

Printed by Service Point (UK) Limited

Foreword

From discussions with many Board directors over the years since the Cadbury and the Rutteman guidelines were issued, there has been much criticism of regulators and consultants alike that organisations are being driven to create bureaucratic processes - divorced from managing the business - with the sole purpose of complying with regulations. The spirit of Cadbury was right, the enactment was flawed. By taking the easy option of reporting on internal financial control companies created an annual review process disconnected from managing the business.

The Combined Code and Turnbull guidance recognise that this was neither beneficial for organisations, nor provided the comfort sought that governance was being enhanced. There has always been an opportunity to enhance business performance through better management of risk. With Turnbull, the connection between managing the business and managing risk is now explicit.

This guide has been written with this objective in mind and recognises that whilst one size does not fit all, the principles and practical issues are common. It has relevance to the Board member and line manager alike.

I owe my thanks to those who have provided me with the challenge over the years to provide practical solutions. I believe this book meets those challenges by providing genuinely practical guidance which, in my view, is as much about enabling performance as it is about embedding risk and control. My thanks in particular to Timothy Copnell and Christopher Wicks, without whose efforts this book could not have been produced.

Mark Stock

Head of Corporate Governance Services

KPMG

Contents

Executive summary 1

1 Introduction 10
1.1 Background 10
1.2 Objectives. 11
1.3 Groups 12
1.4 Effective date 13

2 The importance of internal control and risk management 14

3 Maintaining a sound system of internal control 18
3.1 Responsibility for the system of internal control. 18
3.2 The system of internal control 19
3.3 Understanding the nature and context of control 22

4 Reviewing the effectiveness of internal control. 27
4.1 Responsibility for reviewing the effectiveness of internal control 27
4.2 The process for reviewing effectiveness 30
4.3 Business objectives 31
4.4 Risk identification and assessment 33
4.5 Identification of appropriate controls 38
4.6 Monitoring of controls 40

5 Disclosure 49
5.1 The new requirements 49
5.2 Implementation 54
5.3 Specimen statements on internal control 54

6 Internal audit 56
6.1 Background 56
6.2 The revised requirements. 57
6.3 The role of internal audit 58
6.4 Other assurance providers 60

7 The KPMG methodology 61

Appendices

I Recommended immediate actions and decisions 65
II Specimen statements 69
III Internal control benchmarking 74
IV Board timetable 77
V Criteria for reviewing the effectiveness of internal control 80
VI Questions to ask when assessing the effectiveness of internal control 84
VII KPMG offices in the UK 87

Executive summary

Despite speculation in the financial press that the final guidance on internal control would be essentially similar to April's consultative document, the final guidance was significantly tightened by the removal of the option for a single annual review. This should act to discourage bureaucratic procedures that provide neither the depth nor quality of information provided by the now required regular review process. At KPMG we are particularly pleased to see that the final guidance reflects many of the recommendations made in our response to the consultative document.

On 27 September, the ICAEW published *Internal Control: Guidance for Directors on the Combined Code* (the Turnbull guidance). The guidance aims to provide assistance to directors of listed companies in applying principle D.2 of the Combined Code on Corporate Governance; and determining the extent of their compliance with code provisions D.2.1 and D.2.2. The document seeks to reflect sound business practice that can be adapted to the particular circumstances of individual companies.

Implementation

Full compliance with the guidance is expected in respect of accounting periods ending on or after 23 December 2000. However, to allow companies to take the necessary steps to adopt the new guidance, transitional provisions apply for accounting periods ending on or after 23 December 1999 and up to 22 December 2000. These are:

- as a minimum, state in the annual report and accounts that procedures necessary to implement the guidance have been established or an explanation of when such procedures are expected to be in place; and

- report on internal financial controls pursuant to *Internal Control and Financial Reporting - Guidance for directors of listed companies registered in the UK (the Rutteman guidance)*.

A company which adopts this transitional approach should indicate within its governance disclosures that it has done so.

KPMG recommends that the onus should be on developing and implementing an embedded process. This may mean not being in a position to comply fully in year one; nevertheless, we believe this to be preferable to developing a 'make do' solution.

Responsibilities

The responsibilities of both directors and management are well defined in the guidance. Reviewing the effectiveness of internal control is an essential part of the Board's responsibilities while management is accountable to the Board for developing, operating and monitoring the system of internal control and for providing assurance to the Board that it has done so.

Aspects of the review work may be delegated to the Audit Committee and other appropriate Board committees such as a Risk Committee or Health and Safety Committee. However, the Board as a whole should form its own view on the adequacy of the review after due and careful enquiry by it or its committees.

The directors' responsibilities in respect of maintaining a sound system of internal control are discussed in Chapter 3. The directors' responsibilities for reviewing the effectiveness of such a system are dealt with in Chapter 4.

KPMG recommends that for most organisations the formulation of a Risk Committee would be beneficial and appropriate. It is important that Audit Committees do not become overburdened and deflected from their already significant obligations.

Reviewing the effectiveness of internal control

At the heart of the guidance is the premise that sound internal control is best achieved by a process firmly embedded within a company's operations. However, the guidance asserts that the Board cannot rely solely on such an embedded process, but should regularly receive and review reports on internal control from management. A single annual assessment in isolation is not acceptable.

When reviewing reports during the year, the Board should:

- consider what are the significant risks and assess how they have been identified, evaluated and managed;
- assess the effectiveness of the related system of internal control in managing the significant risks, having regard, in particular, to any significant failings or weaknesses that have been reported;
- consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and
- consider whether the findings indicate a need for more extensive monitoring of the system of internal control.

Turnbull paragraph 31

In addition to the regular review process, the Board is required to undertake a specific annual assessment for the purpose of making its public statement on internal control. The assessment should consider issues dealt with in reports reviewed by it during the year together with any additional information necessary to ensure that the Board has taken account of all significant aspects of internal control. This assessment should cover not only the accounting period, but also the period up to the date of approval of the annual report and accounts.

The Board's annual assessment should, in particular, consider:

- changes since the last review in the nature and extent of significant risks and the company's ability to respond effectively to changes in its business and external environment;
- the scope and quality of management's ongoing monitoring of risks and the system of internal control, and, where applicable, the work of its internal audit function and other providers of assurance;
- the extent and frequency of the communication of the results of the monitoring to the Board - or Board committees - which enables it to build up a cumulative assessment of the state of control in the company and the effectiveness with which risk is being managed;
- the incidence of significant control failings or weaknesses that have been identified at any time during the period and the extent to which they have resulted in unforeseen outcomes or contingencies that have had, could have had, or may in the future have, a material impact on the company's financial performance or condition; and
- the effectiveness of the company's public reporting process.

Turnbull paragraph 33

The directors review of the effectiveness of the system of internal control is discussed in more detail in Chapter 4.

KPMG recommends that the organisation adopt/devise a control framework as a standard against which to assess the effectiveness of its system of internal controls. Various control models exist, two of which we have outlined in Appendix V. As a minimum, we believe for any control model to work effectively and be relevant to the performance of the business, it must contain the following key components.

- ***Philosophy and policy** - The Board should make its risk management expectations explicit. Managers must be clear as to both what is expected of them and what is not.*

Executive Summary

- ***Roles and responsibilities*** *- The roles and responsibilities of all key constituencies in an organisation - in respect of the identification, evaluation, monitoring and reporting on risk - should be made explicit. In particular, the Board should determine their own role, together with that of any Board committees, responsible officers, management heads and internal audit.*
- ***Converting strategy to business objectives*** *- Risks, which include those which directly impact on the strategic objectives together with those which threaten the achievement of business objectives, should not be defined too narrowly. By making strategic and business objectives explicit, the likelihood of overlooking significant risks will be reduced. The link between strategy and business planning is therefore a critical risk management process which is often overlooked.*
- ***Risk to delivering performance*** *- The Board should formally identify the significant business risks (or review and endorse the process by which they have been identified) and be able to demonstrate that they are aware of such risks. Without a clear focus on the significant risks to strategic objectives, the review of internal controls will be compromised.*
- ***Performance appetite*** *- For each identified risk, the Board should consider the probability of the risk occurring and the impact its crystallisation would have on the business. Controls identified and implemented should be appropriate to maintain the key business risks within the Board's defined risk tolerance levels. Cost/benefit considerations apply here.*
- ***Demonstration of performance and risk effectiveness*** *- The Board should be periodically provided with an assessment of the effectiveness of control. However, a balance must be struck between direct involvement by the directors and a high level review in which some areas of responsibility are delegated. Performance should be monitored against the targets and indicators identified in the organisation's objectives and plans. This process has a degree of circularity as monitoring may signal a need to re-evaluate the company's objectives or control.*
- ***Behaviour*** *- Shared ethical values, including integrity, should be established, communicated and practiced throughout the organisation. Authority, responsibility and accountability should be clearly defined and support the flow of information between people and their effective performance toward achieving the company's objectives.*

Taken together, elements, are indicative of an embedded system of internal control. These concepts are illustrated further in Chapters 3 and 4.

Disclosure

The required disclosures include:

- that there is an on-going process for identifying, evaluating and managing the significant risks faced by the group, that has been in place for the year under review and up to the date of approval of the annual report and accounts, and that is regularly reviewed by the Board in accordance with the guidance;
- a summary of the process the Board has applied in reviewing the effectiveness of the system of internal control; and
- the process the Board has applied to deal with material internal control aspects of any significant problems disclosed in the annual report and accounts.

Where the Board is unable to make such disclosures, it should state this fact and explain what it is doing to rectify the situation.

The Board should also disclose that it is responsible for the company's system of internal control and for reviewing its effectiveness.

Additional information to assist understanding of the company's risk management processes and system of internal control is encouraged.

Chapter 5 deals with disclosure issues in more detail and, for illustrative purposes only, Appendix II contains specimen statements on internal control. These are not 'standard wordings' and should be tailored to a company's particular circumstances.

KPMG recommend that all directors, including the non-executive directors, ensure that they are satisfied that the Board's statement on internal control provides meaningful high-level information that enables shareholders to evaluate how the principles of good governance have been applied.

Internal audit

The Combined Code recommends that groups which do not have an internal audit function should, from time to time, review the need for one - but does not specify what is meant by 'from time to time'. Turnbull suggests that this review should be conducted annually. Furthermore, where a group does have an internal audit function, the Board should annually review its scope of work, authority and resources.

The role of internal audit is discussed more fully in chapter 6.

KPMG recommend that the Board ensure that internal audit is in a position to provide the Board with much of the assurance it requires regarding the effectiveness of the system of internal control. It should not only assess the 'parts', but also the 'corporate glue' holding the parts together.

Implementing Turnbull

The Turnbull guidance will impact all UK incorporated listed companies. Boards should already have started considering where they wish to be on the scale between Sunday morning jogger and Olympic champion. Even those Boards not at the vanguard of corporate governance should take steps to ensure that they have in place a risk review process across all elements of the business together with a control assurance process to mitigate such risk.

Executive Summary

KPMG recommend that organisations should first assess how they currently manage risk, before embarking on a programme of change. It is important that existing practices are captured and codified so as not to 'throw the baby out with the bath water'. In assessing compliance with the substance of Turnbull, and not just the form, we recommend that directors should consider the following steps in implementing an embedded risk management and control system:

- *'The case for change' - Why should we do anything? The case for change will need to be generated from within the Board and must, from the outset, articulate the benefits to performance that embedding risk management and control will bring. The CEO will, as the appointed sponsor, demonstrate the commitment to the process and a nominated Board member (the implementer) should drive the process forward.*
- *'As- is' - Where are we now? The implementer will need to appoint a responsible officer as the champion for the process. The officer will document, understand and assess the current process and environment - the 'as-is'.*
- *'To-be' - Where do we want to be? It is necessary to develop a vision of what one expects to see, this will act as framework or standard against which one can compare the actual results. The responsible officer will develop outline options for the process with the management team and assurance functions. The implementer will present the process to the CEO and the Board.*
- *Design - What needs to change? The design of the new or the adaptation of the existing process will be undertaken by management with input from, assurance functions. The Risk Committee will challenge the process before it is submitted to the Board for approval.*
- *Mobilise - How do we get there? The responsible officer will work with the management team to identify the barriers and enablers to implementing the proposed process. The Risk Committee will approve the resource level and the CEO will be required to sanction the commitment of the resources.*
- *Implement - What needs to get done? The management team will implement the process under the leadership of the implementer. The Risk Committee will review the implementation and provide independent reports to the Board.*

- *Monitor - What should we keep doing? The management team will provide regular reports to the Risk Committee who will report to the Board. The assurance functions will support the Risk Committee by providing resource to follow up key findings and to provide an independent view of the process to the Audit Committee who will report to the Board.*
- *Enhance - How can we improve? The Board will annually review the effectiveness of the internal control process. The implementer will lead the response to the annual review and management will action that response.*

Conclusion

The expectations of the Turnbull Committee are explicit and clear. A UK incorporated listed company should have a system of internal control in which the monitoring of risk and control is embedded into the fabric of the company. However, it is up to those companies at the cutting edge of compliance to disclose meaningful information that assists in understanding their risk management process and system of internal control. If the standard is set at a high level by those companies, peer pressure will encourage others to follow suit.

The guidance rightly addresses both cultural and behavioural issues and the link to the achievement of business objectives is plain. This should put risk and control firmly on every CEO's agenda. 'Good risk management is not just about avoiding value destruction - it is also about facilitating value creation.'

This book sets out practical guidance and illustrates our recommendations in a worked example.

Turnbull if embraced in the right spirit and with the right backing, will be a genuinely a good step forward for corporate governance. It's healthy for business and healthy for those investing in business.

"Risk management is about taking risk knowingly, not unwittingly."

1 Introduction

- Guidance on the implementation of the internal control recommendations set out in the Combined Code
- Effective, at least in part, for accounting periods ending on or after 23 December 1999

1.1 Background

Following the work of the Committee on Corporate Governance, in June 1998 the London Stock Exchange published a new Listing Rule together with related Principles of Good Governance and Code of Best Practice ('the Combined Code'). The Combined Code is exactly what it says it is - a code combining the recommendations of the so called Cadbury, Greenbury and Hampel committees on corporate governance.

Though it sits alongside the listing requirements of the London Stock Exchange, the Combined Code is, in itself, essentially toothless. However, the Listing Rules add a little bite.

Listed companies incorporated in the United Kingdom are required to include in their annual report and accounts:

- A statement of how they have applied the principles set out in Section 1 of the Combined Code, providing sufficient explanation to enable its shareholders to evaluate properly how the principles have been applied.
- A statement as to whether or not they have 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 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.

Listing Rule 12.43A(a) and (b)

Amongst the changes from the earlier corporate governance codes, perhaps the greatest was the extension of the requirement to report on the review of internal controls beyond financial controls. Strictly, this was the requirement of the

Cadbury Code, but the Cadbury Committee subsequently confirmed that it would be sufficient to deal only with internal financial controls and the Rutteman Working Group produced guidance to assist directors in carrying out their reviews and making their reports[1].

When the Combined Code was issued, no formal guidance was available in relation to the wider aspects of internal control, though the ICAEW - with the support of the London Stock Exchange - established a working party (the Turnbull Committee) to consider whether its earlier guidance required revision.

Pending the publication of this guidance, the Exchange granted listed companies a temporary dispensation from applying the full rigour of the Listing Rules in relation to the directors' statement on internal control, providing the directors reported on internal financial control pursuant to the guidance for directors published by the Rutteman Working Group.

1.2 Objectives

The objective of the Turnbull report, published by the ICAEW in September 1999 was to provide guidance, for directors of listed companies incorporated in the United Kingdom, on the implementation of the internal control recommendations set out in the Combined Code. In particular, the report seeks to provide guidance which can be adopted when applying principle D.2 of the Code and determining the extent of compliance with the Code provisions D.2.1 and D.2.2.

Principle D.2	The Board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets.
Provision D.2.1	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 controls, including financial, operational, and compliance controls and risk management.

[1] *Internal Control and Financial Reporting: Guidance for directors of listed companies registered in the UK* issued by the Rutteman Working Group on internal controls in 1994.

Provision D.2.2 Companies which do not have an internal audit function should from time to time review the need for one.

The guidance explains that the reference to all controls in provision D.2.1 should not be taken to mean that directors should review the effectiveness of controls designed to manage immaterial risks. Rather it means that the Board should consider all types of control including those of an operational or compliance nature as well as internal financial controls.

The Combined Code and the underlying Hampel recommendations were the catalysts for preparing the guidance. Nevertheless, the system of internal control has an essential role to play in ensuring that a business is well run and its strategic objectives achieved.

While the detailed provisions set out in the guidance have been drafted with listed companies in mind, the principles are indicative of good practice and apply equally to the public sector, unlisted companies and other organisations.

1.3 Groups

Throughout this booklet, reference is made to 'company'. However, where applicable, reference to company should be taken as referring to the group of which the listed holding company is the parent company. For groups of companies, the review of effectiveness of internal control and the report to the shareholders should be from the perspective of the group as a whole.

Where material joint ventures and associates are not dealt with as part of the group for the purposes of applying the Turnbull guidance, this fact should be disclosed.

KPMG recommend that material joint ventures and associates should, as far as possible, be dealt with as part of the group for the purposes of applying the Turnbull guidance.

1.4 Effective date

In a letter from the London Stock Exchange to finance directors and company secretaries of all UK listed companies, the exchange set out transitional provisions to allow companies to take the necessary steps to adopt the guidance.

Accounting periods ending on or after 23 December 1999 and up to 22 December 2000

Any company not complying in full with paragraphs 12.43A(a) and (b) of the Listing Rules (see section 1.1 above) will be required to:

- as a minimum, state in the annual report and accounts that procedures necessary to implement the guidance have been established or provide an explanation of when such procedures are expected to be in place; and
- report on internal financial controls pursuant to *Internal Control and Financial Reporting - Guidance for directors of listed companies registered in the UK* (the Rutteman guidance).

A company which adopts this transitional approach should indicate within its governance disclosures that it has done so.

Accounting periods ending on or after 23 December 2000

For accounting periods ending on or after 23 December 2000, full compliance with paragraphs 12.43A(a) and (b) of the Listing Rules will be required (see section 1.1 above).

KPMG recommend that companies do not rush into 'early compliance'. In our view this will be unrealistic for many companies. We are aware that even some of the largest groups have recognised that even though they may believe they have all the necessary controls in place, they are not in a position to state so with certainty, or that all components that contribute to the system of internal control are adequately codified. We commend those companies that are mature enough to recognise that more needs to be done before stating compliance.

2 The importance of internal control and risk management

- Sound internal control and risk management supplement entrepreneurship, they do not replace it
- The role of internal control is to manage risk rather than to eliminate it

It is important that risk management and control are not seen as a burden on business, rather the means by which business opportunities are maximised and potential losses associated with unwanted events reduced.

Risk, derived from the early Italian *risicare* or *to dare*, is an ever present aspect of the business world. Companies set themselves strategic and business objectives, then manage risks that threaten the achievement of those objectives. Internal control and risk management should supplement entrepreneurship, but not replace it. Increased shareholder value is the reward for successful risk-taking and the role of internal control is to manage risk appropriately rather than to eliminate it.

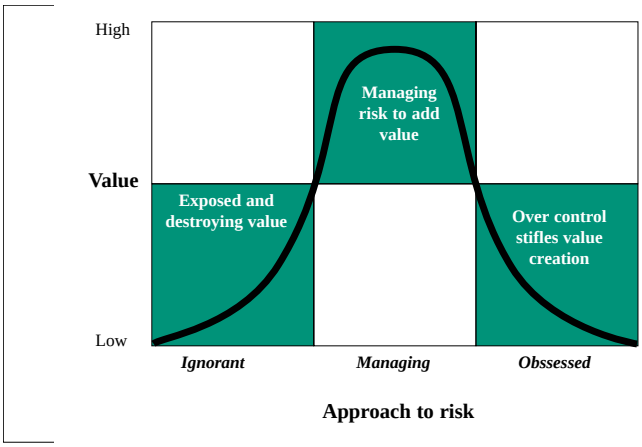
Risks manifest themselves in a range of ways and the effect of risks crystallising may have a positive as well as a negative outcome for the company. It is vital that those responsible for the stewardship and management of a company be aware of the best methods for identifying, and subsequently managing such risks.

Risk can be defined as real or potential events which reduce the likelihood of achieving business objectives. Or, put another way, uncertainty as to the benefits. The term includes both the potential for gain and exposure to loss.

2 The importance of internal control and risk management

Internal control is one of the principal means by which risk is managed. Other devices used to manage risk include the transfer of risk to third parties, sharing risks, contingency planning and the withdrawal from unacceptably risky activities. Of course, as discussed above, companies can accept risk too. Getting the balance right is the essence of successful business - to knowingly take risk, rather than be unwittingly exposed to it.

"Other devices used to manage risk include the transfer of risk to third parties, sharing risks, contingency planning and the withdrawal from unacceptably risky activities."



Despite the increased focus on risk management in recent years, controlling risks to maximise business objectives is not a new issue - as the following illustration demonstrates.

2 The importance of internal control and risk management

*The business **objective** of a nineteenth century coal miner was to maximise coal output. More tonnage meant more money. Unfortunately, there was always the danger that the mine workings would collapse, delaying output and injuring, if not killing, the collier. This is the risk which threatened the achievement of the miner's objective. Fortunately, the miner could use pit props to **control** or manage the risk of collapse.*

*For our miner, the secret of successful **risk management** was to maximise his time at the coal face by utilising the right number of controls. Too many props (over-controlled) would leave little time to dig coal. Too few props (under-controlled) would result in disaster.*

In the modern business world, corporate objectives and the environment in which companies operate are constantly evolving. As a result, the risks facing companies are continually changing too. A successful system of internal control must therefore be responsive to such changes - enabling adaptation quicker than its competitors. Effective risk management and internal control is therefore reliant on a regular evaluation of the nature and extent of risks. Compliance with the spirit of the Turnbull guidance, rather than treating it as an additional layer of bureaucracy, will go a long way to realising the benefits of effective risk management and internal control.

"A successful system of internal control must be responsive to change."

2 The importance of internal control and risk management

The advantages of embracing Turnbull may include:

- Exploitation of business opportunities earlier
- Increased likelihood of achieving business objectives
- Increased market capitalisation
- More effective use of management time
- Lower cost of capital
- Fewer unforecast threats to the business
- More effective management of change
- Clearer strategy setting

"For there to be a real advantage in embedding risk management, it should not only make the risks being managed more visible, but the resultant attention those risks receive must result in managing risks more effectively."

In summary, successful risk management - as envisaged in Turnbull's guidance - is the process that achieves the most efficient combination of controls necessary to provide reasonable assurance that business objectives can be achieved reliably.

KPMG recommends that the Board demand a business case centred on the proposition that the enhancement of business performance is dependent on embedding risk management.

3 Maintaining a sound system of internal control

- Control comprises those elements of an organisation that, taken together, support people in the achievement of the organisation's objectives
- Controls are effective to the extent that they provide reasonable assurance that the organisation will achieve its business objectives reliably

3.1 Responsibility for the system of internal control

The Board is ultimately responsible for the system of internal control. Boards will normally delegate to management the task of establishing, operating and monitoring the system, **but they cannot delegate their responsibility for it**.

The Board should set appropriate policies on internal control and regularly assure itself that appropriate processes are functioning effectively to monitor the risks to which the company is exposed and that the system of internal control is effective in reducing those risks to an acceptable level. It is essential that the right tone is set at the top of the company - the Board should send out a clear message that control responsibilities must be taken seriously.

"To improve performance, you have to understand how to better manage risk."

In determining its policies with regard to internal control, and thereby assessing what constitutes a sound system of internal control in the particular circumstances of the company, the Board's deliberations should include consideration of the following factors:

- the nature and extent of the risks facing the company;
- the extent and categories of risk which it regards as acceptable for the company to bear;
- the likelihood of the risks concerned materialising;
- the company's ability to reduce the incidence and impact on the business of risks that do materialise; and
- the costs of operating particular controls relative to the benefit thereby obtained in managing the related risks.

Turnbull paragraph 17

The Board, however, does not have sole responsibility for a company's system of internal control. Ultimately responsibility for the internal control system rests with the Board, but all employees have some accountability towards implementing the Board's policies on risk and control. This reflects the 'top-down, bottom-up' nature of a sound system of internal control.

While the 'tone at the top' is set by the Board, it is the role of management to implement the policies adopted by the Board. In fulfilling its responsibilities, management should identify and evaluate the risks faced by the group - for consideration by the Board - and design, operate and monitor an appropriate system of internal control.

"The Board should send out a clear message that control responsibilities must be taken seriously."

The operation and monitoring of the system of internal control should be undertaken by individuals who collectively possess the necessary skills, technical knowledge, objectivity, and understanding of the company and the industries and markets in which it operates.

3.2 The system of internal control

An internal control system encompasses the policies, processes, tasks, behaviours 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 or from loss and 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 organisation;
- help ensure compliance with *applicable laws* and *regulations*, and also internal policies with respect to the conduct of business.

Turnbull paragraph 20

3 Maintaining a sound system of internal control

A company's system of internal control commonly comprises:

- control environment;
  The control environment sets the tone of an organisation, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organises and develops its people; and the attention and direction provided by the Board of directors. [2]

- identification and evaluation of risks and control objectives;
  Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of objectives, forming a basis for determining how the risks should be managed.

  Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change. [2]

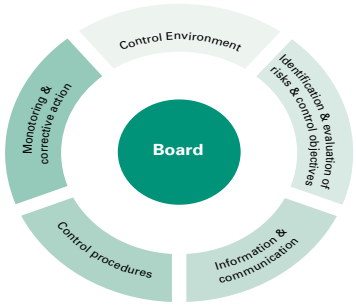
- control activities;
  Control activities are the policies and procedures that help ensure that management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organisation, at all levels and in all functions. They include a range of activities as diverse as approvals, authorisations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties. [2]

[2] *Internal control - integrated framework* published in the USA by the Committee of Sponsoring Organisations of the Treadway Commission ('COSO') in 1992.

- information and communication processes; and
  Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting Effective communication must also occur in a broader sense, flowing down, across and up the organisation. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders. [2]

- processes for monitoring the effectiveness of the system of internal control.
  Internal control systems need to be monitored - a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. On going monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the Board. [2]

The five common components of control



Delivering common components of internal control is, in itself, not enough. The nature and context of control must also be understood.

3.3 Understanding the nature and context of control

The following concepts are important in understanding the nature and context of control.

- Control 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.

  Risks include not only those related to the achievement of a specific objective but also those fundamental to the viability and success of the company such as failure to maintain the company's resilience or capacity to identify and exploit opportunities. Resilience refers to the company's capacity to respond and adapt to unexpected risks and opportunities, and to make decisions on the basis of telltale indicators in the absence of definitive information. Control needs to be 'close' to the associated risks - the shorter the chain, the quicker the reaction.

  Illustration 1 - Getting the control as close to the risk as possible

  A ship's captain is given absolute responsibility for their vessel whilst it is at sea, so they can take appropriate and timely action to remedy any problems that may arise during the course of the voyage.

.3 Understanding the nature and context of control

- The costs of control must be balanced against the benefits, including the risks it is designed to manage.

  Design decisions involve the acceptance of some degree of risk. The cost of control must always be balanced against the benefit of controlling the risk. It is possible to reach a position where the incremental cost of additional control is greater than the benefit derived from controlling the risk.

  Illustration 2 - Improving performance can mean greater tolerance of risk

  When Sony were designing the Walkman which required a significant advance in manufacturing technology, the CEO stated that in order to achieve the 50% reduction in the size of cassette player components, he would be willing to accept a higher level of failure in research and development projects and he had to visibly demonstrate this acceptance.

- The system of control must include procedures for reporting immediately to appropriate levels of management any significant control failings or weaknesses that are identified together with details of corrective action being undertaken.

  It should not be assumed, without making appropriate enquiries, that breakdowns in internal control are isolated occurrences. The key is continual learning rather than attribution of blame. This philosophy should come down from the top of the company. A blame culture encourages the concealment of breakdowns in control.

  Often major disasters are the result of the accumulation of a number of smaller, seemingly insignificant events, which if analysed collectively would provide the necessary warnings to enable preventative action.

3 Maintaining a sound system of internal control

- Control can help minimise the occurrence of errors and breakdowns but cannot provide absolute assurance that they will not occur.

  Human fallibility and the risk of unforeseeable occurrences are inherent limitations in any system of internal control. A control system cannot be designed to provide protection with certainty against: a company failing to meet its business objectives; or all material errors, losses, frauds or breaches of laws or regulations.

- The system of control should be embedded in the operations of the company and form part of its culture.

  Control is effected by people throughout the company, including the Board of directors, management and all other staff. People who are accountable, as individuals or teams, for achieving objectives should also be accountable for the effectiveness of control that supports the achievement of those objectives. It is important that criteria are in place by which the effectiveness of the system of control can be judged. By making individuals accountable, the likelihood that controls are operated properly is increased.

Illustration 3 - Getting the right management behaviour at the coal face

A photocopy salesman was offered a significant bonus for achieving demanding annual sales targets. The copiers were normally sold on a standard three year hire purchase contract. The salesman could not influence the contract but he was in a position to provide the purchaser with extended warranty cover beyond the contract term. This gave him an advantage over and above his competitors and enabled him to consistently meet his sales targets. The company was unaware that anything was wrong until year four when significant warranty claims began to be received on machinery which was no longer generating an income.

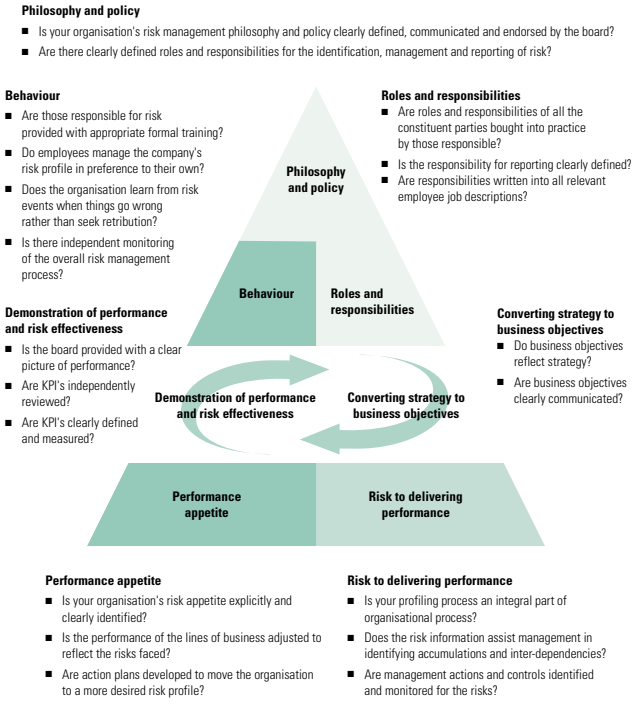
In this case the individual had replaced the corporate risk profile with his own individual risk profile - a behaviour which should have been known to be unacceptable.

.3 Understanding the nature and context of control

How do the common components of control, and the nature and context of control, fit together?

KPMG recommend companies adopt or adapt a framework which can articulate how all the components fit together. Companies should then challenge themselves as to whether the standard is met.

Using KPMG's Risk Management Diagnostic an organisation is able to challenge whether all the necessary components of a system of internal control exist. Furthermore the existence of all components enables risk management to be embedded into the organisation.



3 Maintaining a sound system of internal control

The most common weaknesses we see in organisations are:

- *Philosophy - understood but not written, open to misinterpretation;*
- *Roles and responsibilities - responsibilities are not explicit throughout the organisation;*
- *Converting strategy to business objectives - strategic objectives do not directly translate into business objectives;*
- *Risk to delivering performance - some form of risk profiling, but often divorced from the practical reality of doing business;*
- *Performance appetite - lack of understanding of the organisation's appetite for risk taking;*
- *Summary of performance and risk effectiveness - Boards do not receive the right information, either too little (underinformed) or too much (information overload);*
- *Behaviour - disincentives exist which lead employees to behave in a dysfunctional manner.*

Embedding risk management into the company is essentially a planning, doing, monitoring and learning process.

It cannot be underestimated how important it is for the company to adopt a framework for its system of internal control. This enables management to clearly articulate how the component parts of control fit together and the context in which those controls operate.

"Ultimately, a company's approach to control will depend on the Board's appetite for risk, its attitude and the corporate philosophy."

4 Reviewing the effectiveness of internal control

- Responsibility of the whole Board
- Defined process for the Board's review
- As part of an embedded process, the Board should receive and review ongoing reports on internal control
- The Board should carry out a specific annual exercise for the purpose of making its statement in the annual report

Throughout this chapter, the procedures involved in establishing sound internal control and the process for reviewing its effectiveness are illustrated by reference to a case study taken from KPMG's *Risk Scenes*, its risk scenario training and knowledge transfer toolkit.

Case study - Background

VIP Plc is based on the outskirts of Wolverhampton and manufactures valves, instruments and pipes. It is a FTSE 350 company which operates in fifteen countries the majority of which are in Central Europe and Scandinavia although for historical reasons it also has two operations in Africa. In the last twenty-four months it has started to expand into China and Chile.

Five years ago the company was the subject of a successful management buyout and was subsequently floated on the Stock Exchange. The company is well organised and has a strong culture and open management style.

4.1 Responsibility for reviewing the effectiveness of internal control

The responsibilities of both directors and management are well defined in the guidance. Reviewing the effectiveness of internal control is an essential part of the Board's responsibilities while management is accountable to the Board for developing, operating and monitoring the system of internal control and for providing assurance to the Board that it has done so.

4 Reviewing the effectiveness of internal control

Aspects of the review work may be delegated to the Audit Committee, and other appropriate committees such as a Risk Committee or Health and Safety Committee. These committees may be sub-committees of the Board, alternatively they may include representatives from throughout the company eg, a Risk Committee may include representatives from management, internal audit and other assurance functions. The Board as a whole, however, should form its own view on the adequacy of the review after due and careful enquiry.

In order to properly assess the adequacy of the review with a view to approving the directors' statement on the company's system of internal control, the Board will need to establish:

- the terms of reference of the Audit Committee, or other relevant committees, and their ability to contribute to such a review;
- how key business risks are identified, evaluated and managed;
- the rigour and comprehensiveness of the review process;
- what evidence the Board has gathered to support the statement; and
- whether the entire Board can satisfy itself that the proposed statement is factually correct.

The Board's knowledge must be detailed enough to allow it to concur with what is said in the proposed statement on internal control in the annual report and accounts.

The role of the Audit Committee, or other relevant committees, in the review process is for the Board to decide and will depend upon factors such as the size, style and composition of the Board and the nature of the company's principal risks. The Audit Committee will normally consider financial controls; however,

"The Board should consider the most appropriate forum for undertaking the detailed review."

.1 Responsibility for reviewing the effectivness of internal control

the Board may also request that the committee be used to provide a single focal point for some or all of the wider review of internal control and the proposed statement for inclusion in the annual report prior to approval by the Board. In this event, it may be necessary for the Audit Committee to draw together the results of the work of the Risk Committee and/or other Board committees in reviewing specific risks (e.g. safety and environmental issues).

The Audit Committee's role is, however, a non-executive one. In enquiring into these matters it is not seeking to take on an executive function that properly belongs to management. Instead, its aim is to satisfy itself that management has properly fulfilled its responsibilities.

KPMG recommends that the Board consider the most appropriate forum for undertaking the detailed review. This may, or may not, be the Audit Committee. Indeed a number of groups have set up risk management councils to undertake aspects of the Board's review. KPMG supports this approach where it enables sufficient resource and appropriate skills to be brought to bear.

Case study - philosophy and policy

VIP Plc issued a clear statement regarding responsibility for managing risk. The purpose of the statement was to make it clear that risk management was the responsibility of all members of the company. Whilst the Board was ultimately responsible, each employee, in achieving their personal business objectives, needed to consider the risks they expose the group to and take appropriate action by reference to the stated policies, where appropriate. Where risks were not subject to any policy constraint, employees were expected to apply judgement to decide upon the acceptable level of risk or to defer to their line manager. This message was communicated through induction programs and reinforced in departmental meetings.

Case study - Roles and responsibilities

VIP formed a Risk Council, comprising the four divisional managing directors, the chief executives and function heads. The main purpose of the Council was to consider risks arising from new ventures. In addition, it also considered the appropriateness of the ongoing process by which the management of significant risks was reported to the Board as the business expanded.

4.2 The process for reviewing effectiveness

Put simply, a company's system of internal control has as its principal aim the management of risks that threaten the achievement of its business objectives. Therefore, in order to have effective internal control a company needs to:

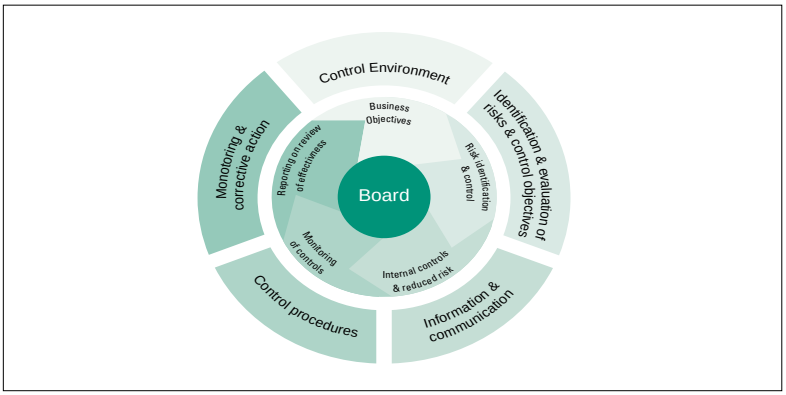
- identify its business objectives;
- identify and assess the risks which threaten the achievement of those objectives;
- design internal controls to manage those risks;
- operate the internal controls in accordance with their design specification; and
- monitor the controls to ensure they are operating correctly.

Turnbull and the Combined Code add the final two links in the chain:

- directors' should review the effectiveness of the system of internal control; and
- report to shareholders that they have done so.

This suggests a defined process for the Board's review of the effectiveness of internal control - a process starting with the identification of the business objectives and the identification and assessment of the related risks that would prevent the company achieving those objectives. By expressly identifying business objectives, the likelihood of overlooking key business risks will be reduced. It should be remembered that key risks include not only those that threaten the survival of the group, or could seriously weaken it, but also the risk of failing to identify significant opportunities.

This process, represented as follows, is discussed more fully in sections 4.3 to 4.6 below.



The outer circle represents the key components of a sound system of internal control introduced in the last chapter. The inner circle represents the process by which sound internal control is established and the ongoing review of the effectiveness of internal control achieved.

4.3 Business objectives

The Board should identify all of the strategic business objectives which are key to the success of the company. By making these explicit the likelihood of overlooking key business risks which threaten the survival of the company or could lead to a significant impact on its performance or reputation will be reduced.

Linking the identification of key business risks to the company's strategic business objectives may already be part of the normal financial calendar supporting the strategic planning and budgeting process. It will be important to ensure this process is sufficiently balanced in its appraisal of the financial and non-financial risks.

Case study - Objectives

VIP's aim is to maintain earnings growth at 15% per annum through the following strategic objectives:

- cost reduction by re-locating manufacturing to low cost areas;
- increasing market penetration by expanding into new and emerging markets; and
- rationalising its European operations and establishing shared service centres.

During the executives' strategic planning away day they identified a number of risks which threaten the achievement of these strategic objectives. These included:

- Fluctuating commodity prices; exchange rates; break in supply chain
- Political risks; market/economic risk
- EU developments; competitive activity.

It is important that the strategic objectives can be translated into business objectives. In order to deliver the strategy, it is necessary to understand how the business objectives, which operationalise the strategy, give rise to risks and indeed, whether significant additional risks arise. Let us take one of the business objectives, identified by management, as supporting the achievement of the first strategic objective - *relocation of the Scandinavian manufacturing site to a brown field site in the Czech Republic.*

Key considerations

- All objectives that are key to the success of the company should be identified.
- Objectives fall into one or more of the following categories: effectiveness and efficiency of operations; reliability of internal and external reporting; and compliance with applicable laws, regulations and internal policies.

4.4 Risk identification and assessment

The Board should formally identify the major business risks (or review the process by which they have been identified and formally endorse the conclusions) and be able to demonstrate that it is aware of the significant risks facing the business. Significant risks include those that threaten the survival of the group, or could seriously weaken it, along with the risk of failing to identify significant opportunities.

There are many techniques available for identifying risk. Some are detail-based and offer quantification, others are scenario-based or qualitative. The process can either be facilitated by specialists or carried out by questionnaire or a combination of both.

Techniques for identifying risks include:

PEST analysis A high level technique to understand the external environment affecting the industry and some of the specific external factors that may affect the business. It considers **P**olitical, **E**conomic, **S**ocial and **T**echnological factors and the risks to the business that flow from these.

Five Forces analysis This technique considers all the forces that influence the company, its industry and its market place. It helps to analyse why a business is successful or not. The five forces are the threat of new entrants, threat of substitute products or services, the bargaining power of suppliers and buyers, the competitors and the intensity of rivalry in the industry.

SWOT analysis SWOT is an acronym for **S**trengths, **W**eaknesses, **O**pportunities and **T**hreats to the business.

Facilitated methods (eg, brain storming) have the advantage of drawing upon those experienced in risk assessment, whilst maximising the input of management who should know the business best.

Case study - Risk identification

In addition to the risks threatening the achievement of the strategic objectives identified above, VIP's management used the PEST analysis technique to identify risks threatening the business objectives. Part of their PEST analysis in respect of the relocation of the Scandinavian operation to the Czech Republic is set out below:

Political		**Economic**	
Threats	*Opportunities*	*Threats*	*Opportunities*
Volatile political environment	Potential Government Grant to relocate	Cost of redundancy in Scandinavia	Low wage rates
Non EU country		Poor infrastructure - potential supply chain breakdown	
Social		**Technological**	
Threats	*Opportunities*	*Threats*	*Opportunities*
Language barrier	Strong work ethic	Poor IT links	E-commerce
Training needs/ re-education		Low grade technology support	
Cultural issues			

Turning to risk assessment, it is important that management consider the underlying gross risks, which are the risks faced by the business before any form of control, not merely the risks which are currently exposed after existing controls. This will enable the company to evaluate potentially critical controls and any significant under/over control.

For each identified risk a value judgement must be made on the impact, both financial and reputational, that its crystallisation would have on the business and the likelihood of the risk occurring.

Table of Guide Values

	Low	Medium	High
Financial impact	Minimal financial impact	Level at which the impact would be significant in monthly management accounts	Level at which the impact might invoke a profit warning
Image impact	Local press/media	National press/ media	International press/CNN
Likelihood/ frequency	Annually or less	Monthly	Daily

It is particularly important to consider the reputational impact as well as financial impact as the consequence of a risk crystallising may go beyond the initial financial impact. The effect on a company's reputation may over the medium term have a far greater cost than the perceived initial financial impact.

Regardless of the technique chosen, directors should:

- use a well defined analysis format;
- assess both the probability of the risk occurring and its likely impact;
- apply causation analysis to identify the root cause of risk; and
- be aware that risks can have single or multiple causes and single or multiple impacts. These interdependencies can be critical in identifying the real impact of risks, and hence the cost benefit analysis applied to their mitigation.

Illustration 4 - Lethal cocktail

Disasters can occur through 'lethal cocktails'. Consider some of the possible contributory factors to the 1997 air crash in Guam:

The pilot was flying a replacement aircraft of a different type to that which he normally flew; the outer marker beacons were not functioning and as a result air traffic control were talking to the pilot in English, a likely second language for both pilot and controller; the weather was poor; and unlike most international airports, the landing beacons stopped three kilometres short of the runway.

Whilst each factor when taken individually had compensating controls, the resulting cocktail of risk presented an altogether greater danger.

Once these steps have been performed it may be appropriate to apply more sophisticated measurement techniques to certain risk scenarios to establish the expected effect.

Armed with this prioritisation of the risks facing the business, informed choices as to the most appropriate means to mitigate loss to an acceptable level can be made.

An effective risk assessment process addresses both financial risks (such as credit, market and liquidity risk) and non-financial risks (such as operational, legal and environmental risk). Furthermore, the process should include an evaluation of the risks to determine which are controllable by the company and which are not.

"The Board must decide whether to accept the risk or withdraw from, or reduce the level of activity concerned."

For those risks that are controllable, the company must decide whether to accept those risks or whether to mitigate the risk through control procedures. For those risks that cannot be controlled, the Board must decide whether to accept the risks or to withdraw from, or reduce the level of business activity concerned. Contingency plans should be considered where the Board elects to accept uncontrollable significant risks.

Case study - Assessment of risk

VIP management then sought to identify both positive and negative risks arising from the proposed relocation.

The risks were prioritised using the following risk score matrix.

	Risk score			
	1	2	3	4
Financial impact	Insignificant	Moderate	Major	Catastrophic
Image impact	Individuals present	Local press	National media	Global media
Likelihood/ frequency	Unlikely	Moderate	Likely	Almost certain

A weighting factor, based on the directors' experience of the business was applied, and their risks were prioritised as follows:

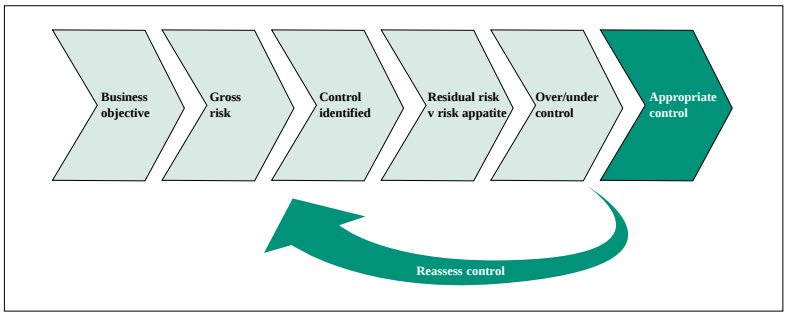
Risk	**PEST**	**Financial impact**	**Image impact**	**Likelihood/ frequency**	**Risk score**
Weighting factor		*4*	*4*	*2*	
Supply chain breakdown	E	4	2	3	30
Language barrier	S	2	2	4	24
Cost of redundancy in Scandinavia	E	2	2	4	24
E-commerce	T	3	1	4	24
Poor IT links	T	2	2	3	22
Volatile political environment	P	3	1	3	22
Etc					

Key considerations

- **Completeness** of risk identification.
- The **probability** that risks will materialise.
- The potential **consequences** (materiality) if the risk materialises.

4.5 Identification of appropriate controls

The Board should identify controls appropriate to maintain the key business risks within the defined risk tolerance levels set by the Board, bearing cost/benefit considerations in mind - or review the process by which this is done and endorse the conclusions. The Board should also be satisfied that suitable individuals have a clear responsibility for maintaining a dynamic risk identification and assessment process and related internal controls.



The Board may not know the fine detail of how all risks that could lead to a material loss are controlled but should be satisfied that proper control policies, procedures and activities have been established to support their control objectives. The design of controls should be based on generally accepted control criteria which have been approved by the Board for this purpose and include both preventative and detective controls.

.5 Identification of appropriate controls

Case study - Identification of controls

VIP used a responsibility matrix to formalise the responsibilities in respect of designing, evaluating, managing and monitoring risk and control.

Risk	Risk score	Control	Responsibility
Supply chain breakdown	30	Cyclic performance review of key suppliers	Operations director
Language barrier	24	Immediate employment of two full-time translators for expatriates for one year. Training programme for UK and Czech Republic staff	HR director
Cost of redundancy in Scandinavia	24	No control, accepted as part of Strategic objective. Long term benefit considered to outweigh short term costs.	N/A
E-commerce	24	Project to determine e-strategy	IT director
Poor IT links	22	Implement Information Management development project	IT manager
Volatile political environment	22	Monitored by receiving monthly reports and news feed analysis in head office.	Line manager
Etc ...			

Some of the less significant risks will be the responsibility of someone below Board level and will not be monitored by the Board. Decisions have to be made based on the risk appetite of the group, particularly where it is not possible to create a direct control. Where controls did not exist, VIP used control and risk self-assessment (see section 4.6) to identify appropriate controls.

Management reached a decision based upon the trade off between the threat of the risk crystallising and the cost saving benefits of relocating to the Czech Republic. The level of trade off will be defined by the Board's philosophy on the risk appetite.

If appropriate assurance over supply chain continuity exists, the Board are happy to proceed with proposals.

Key considerations

- The company's **risk appetite** - determining how much risk it wishes to accept.
- The balance between **preventive** versus **detective controls**.
- The **cost/benefit** of control - balance between the cost of control and the perceived benefits.

4.6 Monitoring of controls

The Board should establish procedures to ensure that monitoring the appropriateness and effectiveness of the identified controls is embedded within the normal operations of the company. This may require cultural changes.

Although monitoring controls is part of the overall system it is largely independent of the elements it is checking. Examples of monitoring procedures include:

- control self-assessment reviewed and tested (at least to a limited extent) by head office/internal audit;
  Control and risk self-assessment by local operational management is a popular option but needs to be carefully managed. Management already have an implicit responsibility for the design and operation of the system of internal controls within their businesses and self-certification is a means of formalising this responsibility. The approach can range from the use of detailed questionnaires (which may be subsequently validated by internal or external audit) through to a broader workshop based approach at which both business risks and related controls are investigated and assessed by the unit responsible for achieving the business objective - a bottom-up approach.

  Self-certification may not be sufficient on its own as the right amount of independent challenge may not be built into the process. The results should be independently reviewed (for example, by internal or external auditors) on behalf of the Board or Audit Committee. This independent review should independently challenge the:

- *completeness of the business objectives covered;*
- *process for the identification and assessment of the associated business risks;*
- *design and operation of the key mitigants;*
- *process for reporting any excess of residual risk beyond defined risk tolerance levels; and*
- *process for reporting any significant over/under control.*

- internal audit visits on a cyclical basis; and
  Although internal audit should maintain independence from management, they can perform more than just a monitoring role. In many companies they also act as facilitators and internal advisors to management on effective means of controlling business risks. Internal audit arrangements naturally vary, but they have the potential to play a central role within the monitoring process - see chapter 6.

- special reviews by external auditors or specialists on a cyclical basis.
  Responsibility for reviewing and concluding on the effectiveness of internal control rests with the Board. However, the external auditors are likely to have helpful knowledge and access to specialist consultants with expertise in specific aspects of risk management and control evaluation. Such procedures are outwith the scope of the statutory audit, but could be provided as part of a separate engagement.

Within a large organisation a balance must be struck between direct involvement by the directors and a high level review in which some areas of responsibility are delegated. Multi-site or multi-national organisations require involvement from both group and operating company management.

In order to make an objective assessment of the effectiveness of internal control, a set of criteria is required as a basis for making judgements.

4 Reviewing the effectiveness of internal control

Several models exist which provide a basis for the design and objective assessment of the effectiveness of control. By their nature, such models also provide criteria by which the effectiveness of the system of internal control can be judged. Two models that are currently accepted internationally are the COSO and CoCo systems. The COSO criteria being substantially similar to those set out in the ICAEW earlier guidance on internal financial control (the Rutteman report).

To assist directors in their assessment of the effectiveness of internal control, both COSO/Rutteman and CoCo criteria for assessing effectiveness are included in Appendix V. For comparison purposes, the CoCo criteria have been regrouped into the five-component structure of COSO/Rutteman.

The effectiveness of control cannot be judged solely on the degree to which each criterion, taken separately, is met. The criteria are interrelated, as are the control elements in an organisation. Control elements cannot be designed or evaluated in isolation from the business objectives and associated threats to the achievement of those objectives.

The Board's review of effectiveness

While effective monitoring throughout the group is an essential component of a sound system of internal control, the Board cannot rely solely on the embedded monitoring process to discharge its responsibilities. Turnbull requires that the Board should regularly receive and review reports on internal control. The Board should be informed about how the reviews giving rise to the reports have been undertaken. Unless the Board are aware of how such reviews have been undertaken, they will not be in a position to opine on the appropriateness of the output. Clearly a perfunctory report will not offer the same degree of comfort as one produced through a thoughtful process.

In addition, the Board should undertake an annual assessment exercise for the purposes of making its statement in the annual report to ensure that it has considered all significant aspects of internal control for the accounting period and the period up to the date of approval of the annual report and accounts.

.6 Monitoring of controls

The Board should define the process to be adopted for its review of the effectiveness of internal control and should ensure that it is provided with appropriately documented support for its statement on internal controls in the annual report and accounts. The Board need to consider both the scope and frequency of the reports it receives during the year, together with the process for its annual assessment.

'Regular' review process

The reports from management and/or others qualified to prepare them in accordance with agreed procedures, should provide a balanced assessment of the significant risks and the effectiveness of the system of internal control in the areas covered. Any significant control failings or weaknesses identified should be discussed in the reports, including the impact that they have had, could have had, or may have, on the group and the actions being taken to rectify them.

"The Board should regularly receive and review reports on internal control."

It is essential that there is a frank open dialogue between management and the Board on matters of risk and control.

When reviewing reports during the year, the Board should:

- consider what are the significant risks and assess how they have been identified, evaluated and managed;

  The Board must satisfy itself that all the significant risks threatening the achievement of its business objectives have been identified, assessed and controlled within its defined risk tolerances.

- assess the effectiveness of the related system of internal control in managing the significant risks, having regard, in particular, to any significant failings or weaknesses that have been reported;

  When considering the effectiveness of the related system of internal control, the directors should have regard to the principal characteristics of a sound system of internal control set out in Appendix V.

- consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and

  It is not sufficient for the Board to satisfy itself that weaknesses are being identified. It must also consider what remedial action is being taken and whether such steps are appropriate.

- consider whether the findings indicate a need for more extensive monitoring of the system of internal control.

  Where an weakness identified in one area of the business may be duplicated in other areas, it may be appropriate for the Board to commission a more comprehensive review. Alternatively, the Board may consider that either the degree of risk involved or the potential for control breakdown warrant further investigation.

Turnbull paragraph 31 (plain text)

Case study - Regular review

At the half year the Board had identified a shortfall in growth - it had only been 5%. As part of the revised forecast for the year, the executives asked each of the divisional managers to state what they could do to achieve 10% growth in the second half of the year. The directors also asked for a note of the additional risks that would be involved in striving to achieve this result. As a result of the responses, the directors revised the business objectives resulting in division A being asked to deliver 15% and division C, 5%.

Management recognised that the ability of each division to take on increased performance targets was dependent on different risk profiles and therefore provided risk adjusted performance targets.

.6 Monitoring of controls

The annual review exercise

The guidance requires that the Board's annual assessment should consider issues dealt with in the reports it has reviewed during the year together with additional information necessary to ensure the Board has taken account of all significant aspects of internal control for the company's accounting period and the period up to the date of approval of the annual report and accounts. This suggests that the Board must, at least, update its annual assessment directly before the annual report and accounts are approved.

"The Board should undertake an annual assessment for the purposes of making its statement in the annual report."

Compliance with Turnbull requires that the Board's annual assessment should, in particular, consider:

- changes since the last review in the nature and extent of significant risks and the company's ability to respond effectively to changes in its business and external environment;

  The Board should review the company's business and operational structure to identify changes which might alter the risk profile, a typical example might be either entry to, or withdrawal from, a volatile market.

  The ability to respond effectively to changed circumstances is vital. For example, a company attempting to establish a foothold in a volatile market place might respond to new competitors by providing heavily discounted products or services to secure its market position.

- the scope and quality of management's ongoing monitoring of risks and the system of internal control, and, where applicable, the work of its internal audit function and other providers of assurance;

  The Board will wish to consider whether management's approach to the ongoing monitoring of the system of internal control covers the key risks to the business in what they believe to be an appropriate cycle and with a level of diligence that they deem satisfactory. All directors, including the non-

executives directors, will need to form a view on how well the company is managed.

The internal audit function may provide significant additional comfort providing it has sufficient resources and authority to be effective.

- the extent and frequency of the communication of the results of the monitoring to the Board - or Board committees - which enables it to build up a cumulative assessment of the state of control in the company and the effectiveness with which risk is being managed;

  The Board should consider whether it receives the output from the monitoring process regularly enough for it to be able to form a timely opinion of the on-going effectiveness of the process. If the Board does not receive, review and act upon the results of the monitoring on a timely basis, strategic decision making may be impaired.

- the incidence of significant control failings or weaknesses that have been identified at any time during the period and the extent to which they have resulted in unforeseen outcomes or contingencies that have had, could have had, or may in the future have, a material impact on the company's financial performance or condition; and

  The Board will want to reflect on the incidence of control weaknesses which occurred during the period and the effect which those weaknesses had, or could have or still may have on the organisations results.

- the effectiveness of the company's public reporting process.

  The efficiency of the year end reporting process from all areas of the organisation will provide an indication of the level of management control throughout the organisation.

Turnbull paragraph 33 (plain text)

Should the Board become aware at any time of a significant failing or weakness in internal control, it should determine how the failing or weakness arose and reassess the effectiveness of management's ongoing processes for designing, operating and monitoring the system of internal control.

Case study - Monitoring by management and reviews by the Board

Key performance indicator	Head office monitor reports on the percentage of deliveries on time as part of their work on the monthly reporting pack.
Significant risks	
Supply chain breakdown	Operations director supplies CEO with weekly delivery performance figures.
Language barrier	Ongoing reports received from site management on the success of the linguistic classes. Including details of training seminars held and attendance figures. Regular site visits and written reports to the Group HR Director. Board updated quarterly by HR director on progress.
E-commerce	Regular management updates on the e-strategy project, including achievement milestones and benefits realisation assessment.
Etc ...	

The assurance provided over the above risks were the subject of independent scrutiny by VIP's internal audit function.

The Board's annual assessment

As part of the annual review, external facilitators challenged the risks associated with the African operation. It transpired that these were taking up 30% of executive time because of security issues, but were contributing less than 5% of profit. The Board had been under significant pressure in the latter part of the year as a result of a hostile bid. The Board agreed an exit strategy from the African business, thus freeing up executive time.

Investment in Chile had started through the sales director. No one at Board level had any experience of operating in South America and in the Board's review of risks, one of the non-executives asked what the key risks were for that operation. None of the Board knew, as the investment was less than 20% and no attention had been given to it. A follow up review identified that there was a significant quality problem which could have impacted on the reputation of VIP, as the main customer of the Chilean operation was the key customer in Spain -

one of VIP's most profitable accounts. This highlighted the importance of understanding the total exposure to certain risks.

Learning from the experience in Chile, the executives asked for a similar exercise to be undertaken in China. The key benefit of this was that a number of opportunities were identified. It was found that one competitor had a better relationship with the local suppliers. As a result, VIP entered into negotiations with its principle supplier in Germany who had been considering its own investment strategy in China. The outcome was a trading alliance in which VIP assisted its supplier in establishing itself in China, thus securing a better supply and managing one of its key strategic risks as a result.

Furthermore, the Board requested the purchasing director explore the possibility of securing similar strategic relationships with other suppliers.

Key considerations

- Has sufficient time and resource been allowed.
- Does the process for identifying, evaluating and managing the significant risks accord with the guidance.
- Can the whole Board satisfy itself as to the adequacy of the review.
- Is the Board's knowledge detailed enough for it to concur with the proposed statement.
- Does the Board's review take into account all significant events up to the date of approval of the annual report and accounts.

5 Disclosure

- Disclosure goes beyond internal financial control
- Emphasis is on how the Board has reviewed the process for identifying, evaluating and managing the company's key risks rather than a description of key controls in place

5.1 The new requirements

The foreword to the guidance states that the London Stock Exchange *'consider that compliance with the guidance will constitute compliance with Combined Code provisions D.2.1 and D.2.2 and provide appropriate narrative disclosure of how Code principle D.2 has been applied'.*

The required disclosures, which are outlined below, are designed to provide users of the annual report with meaningful high-level information. It is imperative that the Board ensures that these disclosures - and all other disclosures in the annual report and accounts - do not give a misleading impression. For groups of companies, the review of effectiveness of internal control and the report to the shareholders should be from the perspective of the group as a whole.

"Meaningful high-level information."

Turnbull paragraph	The Board's statement on internal control	
35	In its narrative statement of how the company has applied Code principle D.2, the Board should, as a minimum, disclose:	
	■ that there is an on-going process for identifying, evaluating and managing the significant risks faced by the company;	☐
	■ that it has been in place for the year under review and up to the date of approval of the annual report and accounts;	☐
	■ that it is regularly reviewed by the Board; and	☐
	■ accords with the guidance in this document.	☐
36	The Board may wish to provide additional information in the annual report and accounts to assist understanding of the company's risk management processes and system of internal control.	☐

5 Disclosure

37	The disclosures relating to the application of principle D.2 should include an acknowledgement by the Board that it is responsible for the company's system of internal control and for reviewing its effectiveness.	☐
37	It should also explain that such a system: ■ is designed to manage rather than eliminate the risk of failure to achieve business objectives; and	☐
	■ can only provide reasonable assurance against material misstatement or loss.	☐
38	In relation to Code Provision D.2.1, the Board should summarise the process it (where applicable, through its committees) has applied in reviewing the effectiveness of the system of internal control.	☐
38	It should also disclose the process it has applied to deal with material internal control aspects of any significant problems disclosed in the annual report and accounts.	☐
39	Where a Board cannot make one or more of the disclosures in paragraphs 35 and 38, it should state this fact and provide an explanation.	☐
39	The Listing Rules require the Board to disclose if it has failed to conduct a review of the effectiveness of the company's system of internal control.	☐
40	The Board should ensure that its disclosures provide meaningful, high-level information and do not give a misleading impression.	☐
41	Where material joint ventures and associates have not been dealt with as part of the group for the purposes of applying this guidance, this should be disclosed.	☐
See section 5.2 below	A company which adopts the transitional approach should indicate within its governance disclosures that it has done so.	☐
Turnbull paragraph	**The Board's statement on internal audit**	
47	If the company does not have an internal audit function and the Board has not reviewed the need for one, the Listing Rules require the Board to disclose these facts.	☐

.1 The new requirements

The disclosure required by paragraph 37 is essentially similar to elements of the disclosure previously required by the Listing Rules and the earlier ICAEW guidance for directors on internal financial control (the Rutteman guidance) - though specific reference to the Board's responsibility in respect of the *review* of the system of internal controls is now required.

The remaining disclosure requirements represent a significant change. The key issues are discussed below:

- The disclosures go beyond internal financial control. In fact, many of the disclosure requirements do not refer directly to control at all, but to risk. Nevertheless, risk and control are inexorably linked - the principal aim of the system of internal control being the identification and management of risks that threaten the achievement of business objectives.

- The disclosures are, in the main, concerned with how the Board - where applicable, through its committees - has reviewed the effectiveness of the system of internal control. A description of the key procedures designed to provide effective control is no longer required.

- No opinion on the effectiveness of the system of internal control is required. This is essentially no different from established practice. It is essential, however, that the Board's disclosures do not give a misleading impression.

- Additional disclosures are no longer required in respect of weaknesses in internal financial control that have resulted in material losses, contingencies or uncertainties which require disclosure in the financial statements or in the auditors report. Instead, the Board should disclose the process it has applied to deal with material internal control aspects of any significant problems *disclosed in the annual report and accounts.*

  Disclosure is not required in respect of breakdowns in control that result in 'near misses' - that are not disclosed in the annual report and accounts. It is important, however, that near misses are reported to management and corrective action taken where necessary.

5 Disclosure

The guidance aims to provide robust disclosure yet avoid verbosity that does not add to the users' understanding of the approach adopted. Turnbull states that 'the *Board should ensure that its disclosures provide meaningful high-level information and do not give a misleading impression*', however, it is crucial that the need to achieve the necessary high standards of corporate behaviour is not overlooked.

Companies in the habit of providing shareholders with meaningful governance disclosures should have few problems with the new disclosures. However, those companies who traditionally take a minimalist approach should not see the new requirements as an opportunity to disclose virtually nothing about their risk management process and system of internal control. Such an approach neither encourages high standards of corporate behaviour nor provides shareholders with a meaningful insight into how the Board has maintained a sound system of internal control to safeguard their investment and the company's assets. Indeed, the guidance encourages Boards to provide additional information in the annual report and accounts to assist understanding of the company's risk management processes and system of internal control.

Notwithstanding the above, there is a danger that such disclosures can sometimes degenerate into nothing more than 'boiler plates'. Boards should be vigilant in ensuring that disclosures remain meaningful and relevant over time.

.1 The new requirements

In making their statement on internal control, Boards should ask themselves the following questions:

- Is the statement factually correct? Before making a statement that there is an ongoing process that accords with the guidance, the Board should consider whether such a statement can be supported. Directors should not underestimate the amount of work necessary to support an internal control statement and inevitably some companies may be unable to establish procedures to implement the procedures set out in the guidance before December 1999.
- Will the statement be minimalist or expansionist? Whatever style the Board adopt, they should have regard to paragraph 40 of the guidance which states *'the Board should ensure that its disclosures provide meaningful high-level information and do not give a misleading impression'*. Furthermore, the Listing Rules require sufficient explanation to enable shareholders to evaluate how the principles of good governance have been applied.
- Where in the annual report and accounts will the statement be presented? The most obvious place is the narrative statement on how the Combined Code principles have been applied.
- Is there room for improvement? No system of internal control can provide absolute assurance against material misstatement or loss and weaknesses may well arise in the future. Consideration should be given to acknowledging any areas for improvement.
- Have unnecessary opinions - such as 'internal control is effective' - been avoided?

5.2 Implementation

In a letter from the London Stock Exchange to company secretaries and finance directors of all UK listed companies, the exchange set out transitional provisions to allow companies to take the necessary steps to adopt the new guidance.

Accounting periods ending on or after 23 December 1999 and up to 22 December 2000

Any company not complying in full with paragraphs 12.43A(a) and (b) of the Listing Rules (see section 1.1) will be required to:

- as a minimum, state in the annual report and accounts that procedures necessary to implement the guidance have been established or provide an explanation of when such procedures are expected to be in place; and
- report on internal financial controls pursuant to *Internal Control and Financial Reporting - Guidance for directors of listed companies registered in the UK* (the Rutteman guidance).

A company which adopts this transitional approach should indicate within its governance disclosures that it has done so.

Accounting period ending on or after 23 December 2000 or where the guidance has been fully adopted early

For accounting periods ending on or after 23 December 2000, full compliance with paragraphs 12.43A(a) and (b) of the Listing Rules will be required (see section 1.1).

5.3 Specimen statements on internal control

Specimen statements are set out in Appendix II for illustrative purposes only. They are not 'standard wording' and must be tailored to any company's individual circumstances.

.3 Specimen statements on internal control

For accounting periods ending on or after 23 December 1999 and up to 22 December 2000, see specimen statement A.

For accounting periods ending on or after 23 December 2000, or where the guidance has been fully adopted early, see specimen statement B.

"Companies that are confident of the strength of their governance should maximise the value by informing investors through clear and meaningful disclosure."

6 Internal audit

- Where a company does not have an internal audit function, the Board should assess the need for such a function annually
- Where an internal audit function exists, the Board should annually review its scope of work, authority and resources

6.1 Background

The Cadbury Committee regarded it as good practice for companies to set up an internal audit function to help discharge the directors responsibilities for the maintenance and review of internal controls, though this was not referred to in their Code of Best Practice.

The Committee on Corporate Governance (Hampel Committee) supported the Cadbury recommendation, but considered that there should be no hard and fast rule. Instead, they recommended that companies, and in particular Audit Committees, review *'from time to time'* the need for a internal audit function. Combined Code provision D.2.2 contained a similar recommendation, however, neither the final report of the Hampel Committee nor the Combined Code define what is meant by *'from time to time'*.

"Internal audit has the potential to be one of the most influential and value-added services available to the Board."

Furthermore, while compliance with the Combined Code requires companies that do not have an internal audit function to review the need for one, the Code contains no equivalent recommendation for companies that do have such a function. Turnbull closes this lacuna and effectively defines *'from time to time'*.

6.2 The revised requirements

> The Board of a company that does not have an internal audit function should assess the need for such a function annually having regard to the factors referred to in paragraphs 43 and 45 above. Where there is an internal audit function, the Board should annually review its scope of work, authority and resources, again having regard to those factors.
>
> Turnbull paragraph 46

The need for an internal audit function will vary depending on company specific factors including the complexity, diversity and scale of the company's activities, the number of employees and the company's corporate culture.

When assessing the need for an internal audit function, the Board should consider whether it has other means of obtaining sufficient and objective assurance regarding the effectiveness of the system of internal control. The Board should also have regard to any trends or current factors in the company's internal environment, markets or other aspects of its external environment that may have increased, or be expected to increase, the risks faced by the company. The guidance identifies the following trends:

- organisational restructuring (e.g. delayering of management);
- changes in reporting processes or underlying information systems;
- adverse trends evident from monitoring internal control systems; and
- increased incidence of unexpected or unacceptable results.

But this list is by no means exhaustive and other factors might be:

- movement into new or high risk markets;
- changes in the reward process for staff; and
- the culture of the organisation (blame or learning).

Where there is an internal audit function, Turnbull recommends that the Board should review its scope, authority and resources, having regard to the above factors.

KPMG recommends that Boards also consider the following questions:

- *How well does the internal audit function assist management and the Board in the achievement of corporate objectives?*
- *Is the internal audit function well respected across the company. Are they perceived as an asset or a liability?*
- *Does internal audit add value, and is that value measured?*
- *How often do internal audit report to the Audit Committee or full Board?*
- *Is internal audit responsive to changes in the business?*
- *Is a period in internal audit considered to be important in the development of senior members of the company?*
- *Is there a demand for internal audit staff to move into management roles?*

6.3 The role of internal audit

Internal audit has the potential to be one of the most influential and value-added services available to the Board. However some companies may wish to reposition their internal audit culture to provide a value adding discipline.

Traditional	Value added
■ Viewed as a policeman	■ Seen as a value adding resource
■ Compliance based approach	■ Process driven/value added approach
■ Viewed by management as the owners of control	■ Seen as a quasi-consultant to help with control
■ Purely finance orientated	■ Business objective orientated
■ Staffed by unqualified inexperienced staff	■ A mix of qualified auditors and business professionals
■ Seen as a 'green pasture ' prior to retirement	■ Seen as a training ground for a senior management

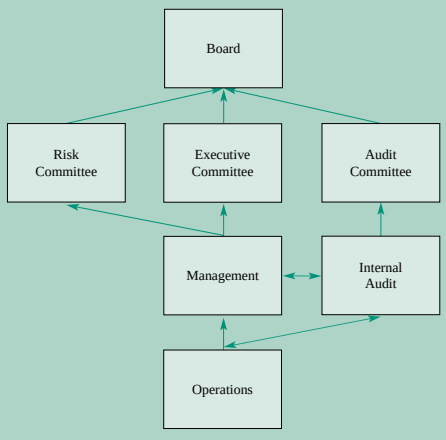
.3 The role of internal audit

When objective and adequately resourced, an internal audit function - or its equivalent where, for example, a third party is contracted to perform the work concerned - should be in a position to provide the Board with much of the assurance it requires regarding the effectiveness of the system of internal control.

In the absence of an internal audit function, management needs to apply other monitoring processes in order to assure itself, and the Board, that the system of internal control is operating as intended. Any process will need to provide the Board with sufficient and effective assurance.

The Institute of Internal Auditors define the primary role of an internal audit function as providing reasonable assurance to executive management and the Board about the adequacy and effectiveness of the risk management control framework in operation. The secondary role is to strengthen and improve the risk management and control framework through the promulgation of best practice. As such, an effective internal audit function acts as a change advocate.

Where does internal audit fit in?



Audit's precise role and relationship will vary within different companies. It is therefore important that there is clarity over who it does serve and what its purpose is. Its relationship with each of the key parties should be determined (ie, for each of the dotted and hard lines in the illustration above).

6.4 Other assurance providers

In conducting its annual assessment, the Board should *'consider the scope and quality of the ongoing monitoring of risks and internal control, and, where applicable the work of its internal audit function and other providers of assurance'*. It is important to remember that internal audit are not the only assurance providers - there may also be other functions within the group that provide assurance and advice covering specialist areas such as health and safety, regulatory and legal compliance, and environmental issues. This assessment should extend to those activities which may have been outsourced or supplied externally - for example, by an environmental assurance provider.

7 The KPMG guide for embedding risk management

In order to successfully implement a risk and control framework which will enable a company to maximise the value from successful risk management, the following steps are those we have found to be the most critical. This approach has been devised from, and is consistent with, KPMG's successful methodology

- **'The case for change' - Why should we do anything?**
  The case for change will need to be generated from within the Board who, will in turn, nominate one of the executive members of the Board to drive the implementation forward (the implementer), but overall responsibility remains with the whole Board. The case for change must, from the outset, articulate the benefits to performance that embedding risk management and control will bring. The implementer will in conjunction with another Board level sponsor such as the CEO develop a business case for presentation to, and approval by, the Board. The CEO will, as the appointed sponsor, demonstrate the commitment within the organisation to drive the process forward.

- **'As- is' - Where are we now?**
  The implementer will need to appoint a responsible officer within the company who will have responsibility to champion the process with management. The officer's first task will be to document, understand and assess the current process and environment - the 'as-is'. Together with the implementer, they should consider the composition of a Risk Committee.

- **'To-be' - Where do we want to be?**
  Before one can start on a journey it is necessary to develop a vision of what one expects to see, this will act as a framework or standard against which one can compare the actual results. It should describe what success looks like and determine the critical factors to achieving success. The responsible officer will develop outline options for the process and how it should work. Representatives from the management team and the assurance functions will assist in the development of the approach, and the Risk Committee will challenge the approach. The implementer will present the proposed process to the CEO and the Board.

- **Design - What needs to change?**
  The design of the new or the adaptation of the existing process will be undertaken by management with input from, and challenge by, the management team and assurance functions. The Risk Committee will seek to challenge the process for robustness, before it is submitted to the Board for approval.

- **Mobilise - How do we get there?**
  The responsible officer with assistance from the management team will determine the level of resources required in order to achieve the necessary momentum to make the process work. The Risk Committee will approve the resource level and the CEO will be required to sanction the commitment of the resources.

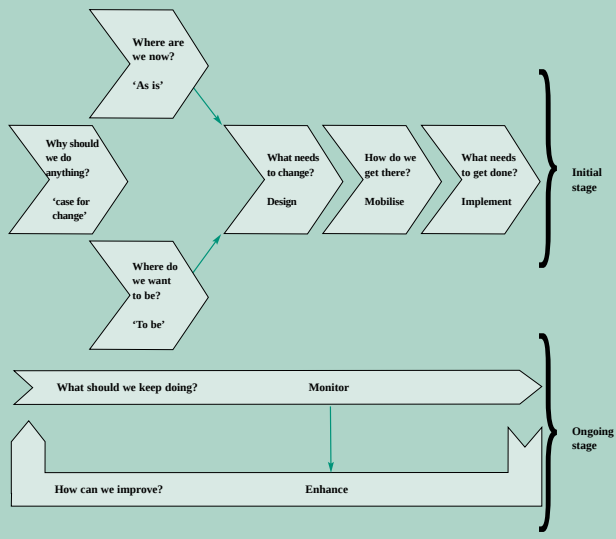
- **Implement - What needs to get done?**
  The management team with support and guidance from the responsible officer will implement the process under the leadership of the Board nominated implementer. The Risk Committee will review the on-going implementation and provide independent reports to the Board.

- **Monitor - What should we keep doing?**
  The management team will provide regular reports to the Risk Committee who will review them and provide regular summary reports to the Board. The assurance functions will support the Risk Committee by providing resource to analyse and follow up on key findings. They will also provide an independent view of the entire process to the Audit Committee who will provide summary reports to the Board.

- **Enhance - How can we improve?**
  The Board will undertake an annual review of the effectiveness of the internal control process. The designated implementer will lead the response to the annual review and management will action that response.

These steps can be summarised as follows:

The KPMG guide for embedding risk management



In future years, considerations similar to those outlined in the initial stage above, will form part of the annual assessment exercise.

Many parts of the company will be involved in the process. It is helpful to construct a role map so that all parties involved understand where their contribution fits within the overall process. An outline role map, showing some of the key contributors, is illustrated overleaf.

	Gaining commitment	Case for change	As-is	To be	Design	Mobilise	Implement	Monitor	Enhance
Chairman	1. Challenge board on what they intend to do to ensure compliance with Turnbull will bring benefits to business.								
Non-executives/ Audit Committee	2. Identify/nominate board member to take responsibility for 'process'.							4. Review assurance reports.	
CEO	3. Approve actions to assess/review current arrangements.	3. Sponsor and demonstrate support for process; obtain commitment.				3. Commit necessary resource.			
Board	4. Appoint a senior officer to manage 'process'. Form a risk committee to act as a challenge forum for process.	4. Approve business case.			3. Approve design.			5. Review Risk Committee reports & Audit Committee reports.	1. Annual assessment and review.
Board nominated sponsor/ implementer		2. Ensure support from entire board for need for 'process'. Present business case to board.		4. Select format option for forward process and present to board/CEO.			1. Leads implementation team.		2. Lead response to annual review.
Risk Committee				3. Challenge options.	2. Challenge robustness of design.	2. Approve resource.	4. Review implementation update.	3. Review management reports.	
Nominated responsible officer		1. Assist executive in preparation of business case.	1. Understand how current process works.	2. Prepare outline options for how process should work.		1. Determine resource required.	2. Co-ordinates implementation team.		
Assurance functions					1. Facilitate and challenge process.			2. Independent review.	
Management				1. Offer options	1. Construct model for process/adapt excisting process design.		3. Implement.	1. Regular reports.	3. Action response to annual review.

Appendix I

Recommended immediate actions and decisions

KPMG recommends that:

The Board demand a business case centred on the proposition that the enhancement of business performance is dependent on embedding risk management.

Clarity exists as to which member of the Board will champion the design and implementation of the review and monitoring process. Without sponsorship at Board level, the process risks getting relegated out of the Boardroom.

The Board consider whether aspects of the monitoring process are to be carried out by a sub-committee on behalf of the Board. If so, consideration must be given to the charter and capabilities of such committees.

For many organisations the formulation of a Risk Committee would be beneficial. It is important that Audit Committees do not become overburdened and deflected from their already significant obligations.

The onus should be on developing and implementing an embedded process. This may mean not being in a position to comply fully in year one, nevertheless, we believe this to be preferable to developing a 'make do' solution.

Companies should not rush into 'early compliance'. In our view this will be unrealistic for many companies. We are aware that even some of the largest groups have recognised that whilst they may believe they have all the necessary controls in place, they are not in a position to state so with confidence, or that all components that contribute to the system of internal control are adequately codified. We commend those companies that are mature enough to recognise that more needs to be done before stating compliance.

The Board should determine the type of information and assurances it wishes to receive from management, including internal audit. Without determining the quantity and quality of information at the outset, the Board, or appropriate sub-committee, risks information overload.

Appendix I

As far as possible, material joint ventures and associates should be dealt with as part of the group for the purposes of applying the Turnbull guidance.

The Board, should ensure that internal audit is in a position to provide the Board with much of the assurance it requires regarding the effectiveness of the system of internal control. It should not only assess the 'parts', but also the 'corporate glue' holding the parts together.

In reviewing the scope, authority and resources of internal audit, the Board should consider:

- How effectively does the internal audit function assist management and the Board in the achievement of corporate objectives?
- Is the internal audit function well respected across the company. Is it perceived as an asset or a liability?
- Does internal audit add value, and is that value measured?
- How often do internal audit report to the Audit Committee or full Board?
- Is internal audit responsive to changes in the business?
- Is a period in internal audit considered to be important in the development of senior members of the company?
- Is there a demand for internal audit staff to move into management roles?

Companies should assess how they currently manage risk, before embarking on a programme of change. It is important that existing practices are captured and codified so as not to 'throw the baby out with the bath water'.

The Board should reach a consensus over what the significant risks to strategic objectives are? Without clear focus, the review of internal controls will be compromised.

Appendix I

Companies should adopt/devise a framework as a standard against which to assess the effectiveness of its system of internal controls. As a minimum, we believe for any control model to work effectively and be relevant to the performance of the business, it must contain the following key components.

- Philosophy and policy - The Board should make its risk management expectations explicit. Managers must be clear as to both what is expected of them and what is not.

- Roles and responsibilities - The roles and responsibilities of all key constituencies in an organisation - in respect of the identification, evaluation, monitoring and reporting on risk - should be made explicit. In particular, the Board should determine their own role, together with that of any Board committees, responsible officers, management heads and internal audit.

- Converting strategy to business objectives - Risks, which include those which directly impact on the strategic objectives together with those which threaten the achievement of business objectives, should not be defined too narrowly. By making strategic and business objectives explicit, the likelihood of overlooking significant risks will be reduced. The link between strategy and business planning is therefore a critical risk management process which is often overlooked.

- Risk to delivering performance - The Board should formally identify the significant business risks (or review and endorse the process by which they have been identified) and be able to demonstrate that they are aware of such risks. Without a clear focus on the significant risks to strategic objectives, the review of internal controls will be compromised.

- Performance appetite - For each identified risk, the Board should consider the probability of the risk occurring and the impact its crystallisation would have on the business. Controls identified and implemented should be appropriate to maintain the key business risks within the Board's defined risk tolerance levels. Cost/benefit considerations apply here.

- Demonstration of performance and risk effectiveness - The Board should be periodically provided with an assessment of the effectiveness of control. However, a balance must be struck between direct involvement by the directors and a high level review in which some areas of responsibility are delegated. Performance should be monitored against the targets and indicators identified in the organisation's objectives and plans. This process has a degree of circularity as monitoring may signal a need to re-evaluate the company's objectives or control.

- Behaviour - Shared ethical values, including integrity, should be established, communicated and practiced throughout the organisation. Authority, responsibility and accountability should be clearly defined and support the flow of information between people and their effective performance toward achieving the company's objectives.

The Board should consider the most appropriate forum for undertaking the detailed review. This may or may not be the Audit Committee. Indeed a number of groups have set up risk management councils to undertake aspects of the Board's review. KPMG supports this approach where it enables sufficient resource and appropriate skills to be brought to bear.

All directors should ensure that they are satisfied that the Board's statement on internal control provides meaningful high-level information that enables shareholders to evaluate how the principles of good governance have been applied.

Appendix II

Specimen statements

Statement A - Accounting periods ending on or after 23 December 1999 and up to 22 December 2000

Any company not complying in full with paragraphs 12.43A(a) and (b) of the Listing Rules (see section 1.1) are required to:

- as a minimum, state in the annual report and accounts that procedures necessary to implement the guidance have been established or provide an explanation of when such procedures are expected to be in place; and
- report on internal financial controls pursuant to *Internal Control and Financial Reporting - Guidance for directors of listed companies registered in the UK* (the Rutteman guidance).

Where the guidance has been fully adopted early, see specimen statement B.

Internal control

The Board is ultimately responsible for the group's system of internal control and for reviewing its effectiveness. However, such a system is designed to manage rather than eliminate the risk of failure to achieve business objectives, and can provide only reasonable and not absolute assurance against material misstatement or loss.

The Combined Code introduced a requirement, that the directors' review the effectiveness of the Group's system of internal controls. This extends the existing requirement in respect of internal financial controls to cover all controls including, financial, operational, compliance, and risk management.

Guidance for directors *Internal Control: Guidance for Directors on the Combined Code* (the Turnbull guidance) was published in September 1999, however, the directors have taken advantage of the London Stock Exchange's transitional rules and have continued to review and report upon internal financial controls in accordance with the ICAEW's 1994 guidance *Internal Control and Financial Reporting.*

Nevertheless, the Board confirm that they have established procedures necessary to implement the Turnbull guidance such that they can fully comply with it for the accounting period ending on 31 December 2000.

Appendix II

Key elements of the group's system of internal financial controls are as follows:

Control environment The group is committed to the highest standards of business conduct and seeks to maintain these standards across all of its operations throughout the world. The group has adopted a Code of Business Conduct, approved by the main Board, which provides practical guidance for all staff. There are also in place supporting group policies and employee procedures for the reporting and resolution of suspected fraudulent activities.

The group has an appropriate organisational structure for planning, executing, controlling and monitoring business operations in order to achieve group objectives. Lines of responsibility and delegations of authority are documented.

Risk identification Group management are responsible for the identification and evaluation of key risks applicable to their areas of business. These risks are assessed on a continual basis and may be associated with a variety of internal or external sources including control breakdowns, disruption in information systems, competition, natural catastrophe and regulatory requirements.

Information and communication Group businesses participate in periodic strategic reviews which include consideration of long term financial projections and the evaluation of business alternatives. Operating units prepare annual budgets and three-year strategic plans; performance against plan is actively monitored at the Board and sector level supported by regular forecasts. Forecasts and results are consolidated and presented to the Board on a regular basis.

Through these mechanisms, group performance is continually monitored, risks identified in a timely manner, their financial implications assessed, control procedures re-evaluated and corrective actions agreed and implemented.

Control procedures The group and its operating units have implemented control procedures designed to ensure complete and accurate accounting for financial transactions and to limit the potential exposure to loss of assets or fraud. Measures taken include physical controls, segregation of duties, reviews by management and internal audit, and external audit to the extent necessary to arrive at their audit opinion.

A process of control self-assessment and hierarchical reporting has been established which provides for a documented and auditable trail of accountability. These procedures are relevant across group operations and

provide for successive assurances to be given at increasingly higher levels of management and, finally, to the Board. These documents are reviewed by the internal auditors for completeness and accuracy. Planned corrective actions are independently monitored for timely completion.

Monitoring and corrective action There are clear and consistent procedures in place for monitoring the system of internal financial controls. The Audit Committee meets at least three times a year and, within its remit, reviews the effectiveness of the group's system of internal financial controls. The committee receives reports from the group internal audit function and management.

Statement B - Accounting periods ending on or after 23 December 2000

For accounting periods ending on or after 23 December 2000, full compliance with paragraphs 12.43A(a) and (b) of the Listing Rules is required.

Internal control

The Board is ultimately responsible for the group's system of internal control and for reviewing its effectiveness. However, such a system is designed to manage rather than eliminate the risk of failure to achieve business objectives, and can provide only reasonable and not absolute assurance against material misstatement or loss.

Following publication of guidance for directors on internal control *Internal Control: Guidance for Directors on the Combined Code* (the Turnbull guidance), the Board confirm that there is an ongoing process for identifying, evaluating and managing the significant risks faced by the group, that has been in place for the year under review and up to the date of approval of the annual report and accounts, and that this process is regularly reviewed by the Board and accords with the guidance.

The Board have reviewed the effectiveness of the system of internal control. In particular, it has reviewed and updated the process for identifying and evaluating the significant risks affecting the business and the policies and procedures by which these risks are managed. This has been reinforced by the adoption of a Code of Business Conduct, approved by the main Board, which provides

practical guidance for all staff. There are also supporting group policies and employee procedures for the reporting and resolution of suspected fraudulent activities.

Management are responsible for the identification and evaluation of significant risks applicable to their areas of business together with the design and operation of suitable internal controls. These risks are assessed on a continual basis and may be associated with a variety of internal or external sources including control breakdowns, disruption in information systems, competition, natural catastrophe and regulatory requirements.

A process of control self-assessment and hierarchical reporting has been established which provides for a documented and auditable trail of accountability. These procedures are relevant across group operations and provide for successive assurances to be given at increasingly higher levels of management and, finally, to the Board. This process is facilitated by internal audit who also provide a degree of assurance as to the operation and validity of the system of internal control. Planned corrective actions are independently monitored for timely completion.

Management report regularly on their review of risks and how they are managed to both the Executive Committee and Risk Committee, whose main role is to review, on behalf of the Board, the key risks inherent in the business and the system of control necessary to manage such risks, and to present their findings to the Board. Internal audit independently review the risk identification procedures and control process implemented by management, and report to the Audit Committee on a quarterly basis. The Audit Committee reviews the assurance procedures, ensuring that an appropriate mix of techniques is used to obtain the level of assurance required by the Board. Both the Audit and Risk Committees present their findings to the Board on a quarterly basis or earlier as appropriate.

The managing director also reports to the Board on behalf of the Executive Committee on significant changes in the business and the external environment which affect significant risks. The finance director provides the Board with monthly financial information which includes key performance and risk indicators. Where areas for improvement in the system are identified, the Board considers the recommendations made by the Executive Committee, the Risk Committee and the Audit Committee.

Appendix II

The Risk Committee includes two non-executive directors, the finance director, the operations director, the head of internal audit and representatives from environmental review, insurance, health and safety review and legal and compliance. It reviews, on a bi-monthly basis, the risk management and control process and considers the:

- authority, resources and co-ordination of those involved in the identification, assessment and management of significant risks faced by the group;
- response to the significant risks which have been identified by management and others;
- monitoring of the reports from group management;
- maintenance of a control environment directed towards the proper management of risk; and
- annual reporting procedures.

Additionally, the Risk Committee keeps abreast of all changes made to the system and follows up on areas which require improvement. It reports to the Board at quarterly intervals or more frequently should the need arise.

Appendix III

Internal control benchmarking

Old way	New way
Control environment	
■ Primary objective is to demonstrate compliance at minimum cost. Secondary objective is to identify risks and control improvements	■ Risk identification and control considered fundamental to managing the business. Overall business performance improved by linking risk management to the fulfilment of business objectives
■ Board/Audit Committee only takes a passive interest in internal control, solely seeking compliance with Turnbull guidance	■ Board/Audit Committee takes an active interest in internal control
■ Learning on risk and control issues, including relevant training, is restricted to internal audit or finance personnel	■ Creation of an environment which promotes learning and training on risk and control issues throughout the company
■ Control awareness not actively developed through the entire group	■ Appropriate formalised and agreed levels of behaviour and control awareness throughout the company
■ Process is thought of as an annual initiative or just another disclosure issue	■ Process is ongoing and embedded within the company, prompting compliance with the 'spirit' of the guidance
■ The Audit Committee tasked with responsibility for internal control without consideration of relevant experience and resources	■ Consideration given to the resources and experience of the Audit Committee - and other relevant committees - before delegating certain aspects of the review process

Appendix III

Identification and evaluation of risks and control objectives	
■ Identification of risk on a fire fighting basis	■ Embedded process to identify and evaluate risks which significantly threaten business objectives
■ Risk and control objectives are pulled together only for Turnbull reporting purposes	■ Facilitated risk reviews used to identify business risk and drive control evaluation
■ Reliance on centralised control manual to dictate the internal controls	■ Operating units use self assessment to identify and evaluate their own controls in conjunction with a centralised control framework
■ The process is largely top down and restricted to senior levels of management	■ The philosophy is set by the Board but the process is cascaded throughout the company. Risks identified at all levels are discussed openly and not ignored
■ Risks are defined too narrowly, concentrating on known or comfort areas	■ Identification of business objectives leads to the assessment of associated risks and exposures, thereby defining risk in the widest sense

Appendix III

Information and communication	
■ Traditional performance indicators are adapted to allow management to monitor business activities on a monthly cycle	■ Systems are developed to provide relevant and reliable information - performance indicators - to the right people on a timely basis
■ Use of manuals (e.g. operations/ policy) to communicate control issues across the company	■ Policies are used to reinforce the direct communication of control issues
Control procedures	
■ Local management confirm control procedures in an annual letter of assurance under a self assessment process	■ Local management actively challenge the operation of controls as part of the self assessment process
■ Internal audit co-ordinates/ administers the review process	■ Internal audit facilitates and challenges local management reporting and conclusions
Monitoring and corrective action	
■ There is more emphasis on the 'fieldwork' and the initial phases of the risk management process, with little attention being paid to follow-up activities	■ Follow-up procedures are formally established and performed to ensure that fieldwork leads to appropriate change or action
■ Finance function is responsible for the system of internal control	■ The Board actively sponsors internal control initiatives
■ Report by exception to the Board/Audit Committee	■ Development of an ongoing monitoring process embedded within the company's overall business operations which provides the directors with regular reports on the state of the system of internal control
■ Internal audit checks on a routine basis	■ Internal audit assures the robustness of the ongoing monitoring process

Appendix IV

Board timetable

This Board timetable is based on a 31 December year end and phased implementation rather than early adoption.

October 1999

Consider what procedures will be necessary to implement the guidance. In particular, consider the key tasks to be completed; the resources available; and the time scale involved.

Reach consensus on the significant risks to strategic objectives and determine the type of information and assurances the Board wishes to receive from management.

Consider whether aspects of the monitoring process are to be carried out by a sub-committee on behalf of the Board and decide which director will champion the design and implementation of the review and monitoring process.

Consider the scope authority and resources of the internal audit function. If an internal audit function does not exist, consider whether one is needed and if not, how the Board satisfies itself that it receives sufficient and objective assurance.

December 1999

Consider what progress has been made in implementing the Turnbull guidance. In particular, whether:

- the system of internal control is embedded within the company;
- the questions set out in the appendix to the Turnbull guidance are being addressed; and
- policies and procedures are being adequately disseminated throughout the company.

February 2000	Consider work undertaken on risk and control. Identify possible significant problems and consider internal control disclosures in the light of implementation arrangements.
February 2000	Consider the statement on internal control/internal financial control that will be included in the annual report together with the supporting documentation.
April 2000/ September 2000	Business divisions report to Audit Committees, and other appropriate sub-committees, on progress towards embedding risk management and control. Internal audit independently review the risk identification procedures and control process implemented by management, and report to the Board via the Audit Committee. The Audit Committee reviews the assurance procedures, ensuring that an appropriate mix of techniques is used to obtain the level of assurance required by the Board. The Risk Committee reviews, and reports to the Board on the: ■ authority, resources and co-ordination of those involved in the identification, assessment and management of significant risks faced by the group; ■ response to the significant risks which have been identified by management and others; ■ monitoring of reports from management;

	■ maintenance of a control environment directed towards the proper management of risk; and ■ annual reporting procedures. Both the Audit and Risk Committees present their findings to the Board.
November 2000	As part of strategic and business planning cycle, undertake annual assessment (Turnbull paragraphs 32 and 33) - ensuring risks being focused on remain relevant. Consider the scope, authority and resources of the internal audit function. If an internal audit function does not exist, consider whether one is needed and if not, how the Board satisfies itself that it receives sufficient and objective assurance.
March 2001 Meeting to approve the annual report and accounts	Finalise or update the annual assessment of internal control before approving the Board's statement on internal control.

Appendix V

Criteria for reviewing the effectiveness of internal control

To assist directors in their assessment of the effectiveness of internal control, both COSO/Rutteman and the more contemporaneous Canadian (CoCo) criteria for assessing effectiveness are included below. For comparison purposes, the CoCo criteria have been regrouped into the five-component structure of COSO/Rutteman.

COSO/Rutteman Criteria	CoCo Criteria
Control environment	
■ A commitment by directors, management and employees to competence and integrity (eg, leadership by example, employment criteria) and the development of an appropriate culture to support these principles. ■ Communication of appropriate agreed standards of business behaviour and control consciousness to managers and employees (e.g. through written codes of conduct, formal standards of discipline, performance appraisal). ■ An appropriate organisational structure within which business can be planned, executed, controlled and monitored to achieve the company's objectives. ■ Allocation of sufficient time and resources by the Board, senior management and the company to internal control and risk management issues. ■ The creation of an environment that promotes learning within the company on risk and control issues, including the provision of relevant training. ■ Appropriate delegation of authority, with accountability, which has regard to acceptable levels of risk. ■ A professional approach to the public reporting of matters related to internal control.	■ Shared ethical values, including integrity, should be established, communicated and practiced throughout the organisation. ■ Human resource policies and practices should be consistent with an organisation's ethical values and with the achievement of its objectives. ■ Authority, responsibility and accountability should be clearly defined and consistent with an organisation's objectives so that decisions and actions are taken by the appropriate people. ■ An atmosphere of mutual trust should be fostered to support the flow of information between people and their effective performance toward achieving the organisation's objectives. ■ People should have the necessary knowledge, skills and tools to support the achievement of the organisation's objectives.

Appendix V

Identification and evaluation of risks and control objectives ■ Identification in a timely manner of the key business, operational, financial and compliance risks facing the company. Such risks include those associated with, for example, market, technological, reputational and business probity issues. ■ Consideration of the likelihood of those risks crystallising and the significance of the consequent impact on the business. ■ Establishment of priorities for the allocation of resources available for control and the setting and communicating of clear control objectives.	■ Objectives should be established and communicated. ■ The significant internal and external risks faced by an organisation in the achievement of its objectives should be identified and assessed. ■ Objectives and related plans should include measurable performance targets and indicators. ■ External and internal environments should be monitored to obtain information that may signal a need to re-evaluate the organisation's objectives or controls.
Information and communication ■ Performance indicators which allow management to monitor the key business activities and risks, and to identify developments which require intervention. ■ Information systems which provide ongoing identification and capture of relevant, reliable and up-to-date information from internal and external sources. The information systems should be secure and have appropriate contingency arrangements. ■ Systems which communicate relevant information to the right people at the right frequency and time in a format which exposes significant variances from operating plans, budgets and forecasts and allows prompt response.	■ Communication processes should support the organisation's values and the achievement of its objectives. ■ Sufficient and relevant information should be identified and communicated in a timely manner to enable people to perform their assigned responsibilities. ■ Plans to guide efforts in achieving the organisation's objectives should be established and communicated. ■ Information needs and related information systems should be reassessed as objectives change or as reporting deficiencies are identified.

Appendix V

Control procedures ■ Procedures to ensure complete and accurate accounting for transactions. ■ Appropriate authorisation limits for transactions that reasonably limit the company's exposures. ■ Procedures to ensure the reliability of data processing and the integrity of the information generated. ■ Controls that limit exposure to loss of assets/records or to fraud (e.g. physical controls, segregation of duties). ■ Checks which provide effective supervision of the control activities (e.g. site visits by senior management/routine and surprise checks). ■ Procedures to ensure compliance with laws and regulations that have significant financial implications. ■ Preparation of manuals (e.g. operations/policy) that facilitate the achievement of the above.	■ Policies designed to support the achievement of an organisation's objectives and the management of its risks should be established, communicated and practiced so that people understand what is expected of them and the scope of their freedom to act. ■ The decisions and actions of different parts of the organisation should be co-ordinated. ■ Control activities should be designed as an integral part of the organisation, taking into consideration its objectives, the risks to their achievement, and the inter-relatedness of control elements.
Monitoring and corrective action ■ An ongoing monitoring process embedded within the company's overall business operations which provides reasonable assurance to the Board that there are appropriate control procedures in place for all the company's significant business activities and that these procedures are being followed (e.g. consideration by the Board or Board committee of reports from management or from an internal audit function).	■ Performance should be monitored against the targets and indicators identified in the organisation's objectives and plans. ■ The assumptions behind an organisation's objectives should be periodically challenged. ■ Follow-up procedures should be established and performed to ensure appropriate change or action occurs.

■ Identification of change in the company and its environment which may require changes to the system of internal control. ■ Formal and timely procedures for reporting weaknesses and for ensuring appropriate corrective action. ■ The provision of adequate support for public statements by the Board on internal control.	■ Management should periodically assess the effectiveness of control in its organisation and communicate the results to those to whom it is accountable.

Appendix VI

Questions to ask when assessing the effectiveness of internal control

The Appendix to the Turnbull guidance includes questions which Boards may wish to consider and discuss with management when reviewing reports on internal control and carrying out their annual assessment. For convenience, these questions are reproduced below. The questions are not intended to be exhaustive and will need to be tailored to the particular circumstances of the company.

Risk assessment

- Does the company have clear objectives and have they been communicated so as to provide effective direction to employees on risk assessment and control issues? For example, do objectives and related plans include measurable performance targets and indicators?
- 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.)
- Is there a clear understanding by management and others within the company of what risks are acceptable to the Board?

Control environment and control activities

- 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?
- Do 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?
- Does senior management demonstrate, through its actions as well as its policies, the necessary commitment to competence, integrity and fostering a climate of trust within the company?
- Are authority, responsibility and accountability defined clearly such that decisions are made and actions taken by the appropriate people? Are the decisions and actions of different parts of the company appropriately co-ordinated?

Appendix VI

- Does the company communicate to its employees what is expected of them and the scope of their freedom to act? This may apply to areas such as customer relations; service levels for both internal and outsourced activities; health, safety and environmental protection; security of tangible and intangible assets; business continuity issues; expenditure matters; accounting; and financial and other reporting.
- Do 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?
- How are processes/controls adjusted to reflect new or changing risks, or operational deficiencies?

Information and communication

- Do management and the Board receive timely, relevant and reliable reports on progress against business objectives and the related risks that provide them with the information, from inside and outside the company, needed for decision-making and management review purposes? This could include performance reports and indicators of change, together with qualitative information such as on customer satisfaction, employee attitudes etc.
- Are information needs and related information systems reassessed as objectives and related risks change or as reporting deficiencies are identified?
- Are periodic reporting procedures, including half-yearly and annual reporting, effective in communicating a balanced and understandable account of the company's position and prospects?
- Are there established channels of communication for individuals to report suspected breaches of laws or regulations or other improprieties?

Monitoring

- Are there ongoing processes embedded within the company's overall business operations, and addressed by senior management, which monitor the effective application of the policies, processes and activities related to internal control and risk management? (Such processes may include control self-assessment, confirmation by personnel of compliance with policies and codes of conduct, internal audit reviews or other management reviews).

Appendix VI

- Do these processes monitor the company's ability to re-evaluate risks and adjust controls effectively in response to changes in its objectives, its business, and its external environment?
- Are there effective follow-up procedures to ensure that appropriate change or action occurs in response to changes in risk and control assessments?
- Is there appropriate communication to the Board (or Board committees) on the effectiveness of the ongoing monitoring processes on risk and control matters? This should include reporting any significant failings or weaknesses on a timely basis.
- Are there specific arrangements for management monitoring and reporting to the Board on risk and control matters of particular importance? These could include, for example, actual or suspected fraud and other illegal or irregular acts, or matters that could adversely affect the company's reputation or financial position?

Appendix VII

KPMG offices in the UK

United Kingdom

London
PO Box 695
8 Salisbury Square
London EC4Y 8BB
Tel: (0171) 311 1000
Fax: (0171) 311 3311

Aberdeen
37 Albyn Place
Aberdeen AB10 1JB
Tel: (01224) 591 000
Fax: (01244) 590 909

Belfast
Stokes House
17-25 College Square East
Belfast BT1 6DH
Tel: (01232) 243 377
Fax: (01232) 893 893

Birmingham
2 Cornwall Street
Birmingham B3 2DL
Tel: (0121) 232 3000
Fax: (0121) 232 3500

Bristol
100 Temple Street
Bristol BS1 6AG
Tel: (0117) 905 4000
Fax: (0117) 905 4001

Cambridge
37 Hills Road
Cambridge CB2 1XL
Tel: (01223) 366 692
Fax: (01223) 460 701

Cardiff
Marlborough House
Fitzalan Court
Fitzalan Road
Cardiff CF2 1TE
Tel: (01222) 468 000
Fax: (01222) 468 200

Derby
5 Stuart Street
Derby DE1 2EQ
Tel: (01332) 636 100
Fax: (01332) 636 261

Edinburgh
Saltire Court
20 Castle Terrace
Edinburgh EH1 2EG
Tel: (0131) 222 2000
Fax: (0131) 527 6666

Gatwick
1 Forest Gate
Brighton Road
Crawley
West Sussex RH11 9PT
Tel: (01293) 652 000
Fax: (01293) 652 100

Glasgow
24 Blythswood Square
Glasgow G2 4QS
Tel: (0141) 226 5511
Fax: (0141) 204 1584

Ipswich
6 Lower Brook Street
Ipswich IP4 1AP
Tel: (01473) 233 499
Fax: (01473) 204 486

Leeds
1 The Embankment
Neville Street
Leeds LS1 4DW
Tel: (0113) 231 3000
Fax: (0113) 231 3200

Leicester
1 Waterloo Way
Leicester LE1 6LP
Tel: (0116) 256 6000
Fax: (0116) 256 6050

Liverpool
8 Princes Parade
Liverpool L3 1QH
Tel: (0151) 473 5100
Fax: (0151) 473 5200

Manchester
St James' Square
Manchester M2 6DS
Tel: (0161) 838 4000
Fax: (0161) 838 4040

Milton Keynes
Norfolk House
499 Silbury Boulevard
Central Milton Keynes
MK9 2HA
Tel: (01908) 844 800
Fax: (01908) 844 888

Newcastle upon Tyne
Quayside House
110 Quayside
Newcastle upon Tyne
NE1 3DX
Tel: (0191) 401 3700
Fax: (0191) 401 3750

Appendix VII

Norwich
Holland Court
The Close
Norwich NR1 4DY
Tel: (01603) 620 481
Fax: (01603) 623 078

Nottingham
St Nicholas House
31 Park Row
Nottingham NG1 6FQ
Tel: (0115) 935 3535
Fax: (0115) 935 3500

Plymouth
Plym House
3 Longbridge Road
Marsh Mills
Plymouth
Devon PL6 8LT
Tel: (01752) 632 100
Fax: (01752) 632 110

Preston
Edward VII Quay
Navigation Way
Ashton-on-Ribble
Preston
Lancashire PR2 2YF
Tel: (01772) 722 822
Fax: (01722) 736 777

Reading
Arlington Business Park
Theale
Reading
RG7 4SD
Tel: (0118) 964 2000
Fax: (0118) 964 2222

St Albans
Aquis Court
31 Fishpool Street
St Albans
Herts AL3 4RF
Tel: (01727) 733 000
Fax: (01727) 733 001

Sheffield
The Fountain Precinct
1 Balm Green
Sheffield S1 3AF
Tel: (0114) 276 6789
Fax: (0114) 209 2421

South Coast
Dukes Keep
Marsh Lane
Southampton SO14 3EX
Tel: (01703) 202 000
Fax: (01703) 202 001

Stoke-on-Trent
Festival Way
Stoke-on-Trent ST1 5TA
Tel: (01782) 216 000
Fax: (01782) 216 050

Channel Islands
Guernsey
PO Box 20
Orbis House
20 New Street
St Peter Port
Guernsey GY1 4AN
Tel: (01481) 721 000
Fax: (01481) 722 373

Jersey
PO Box 453
38/39 The Esplanade
St Helier
Jersey JE4 8WQ
Tel: (01534) 888 891
Fax: (01534) 888 892

Isle of Man
Douglas
Heritage Court
41 Athol Street
Douglas, Isle of Man
Tel: (01624) 681 000
Fax: (01624) 681 098