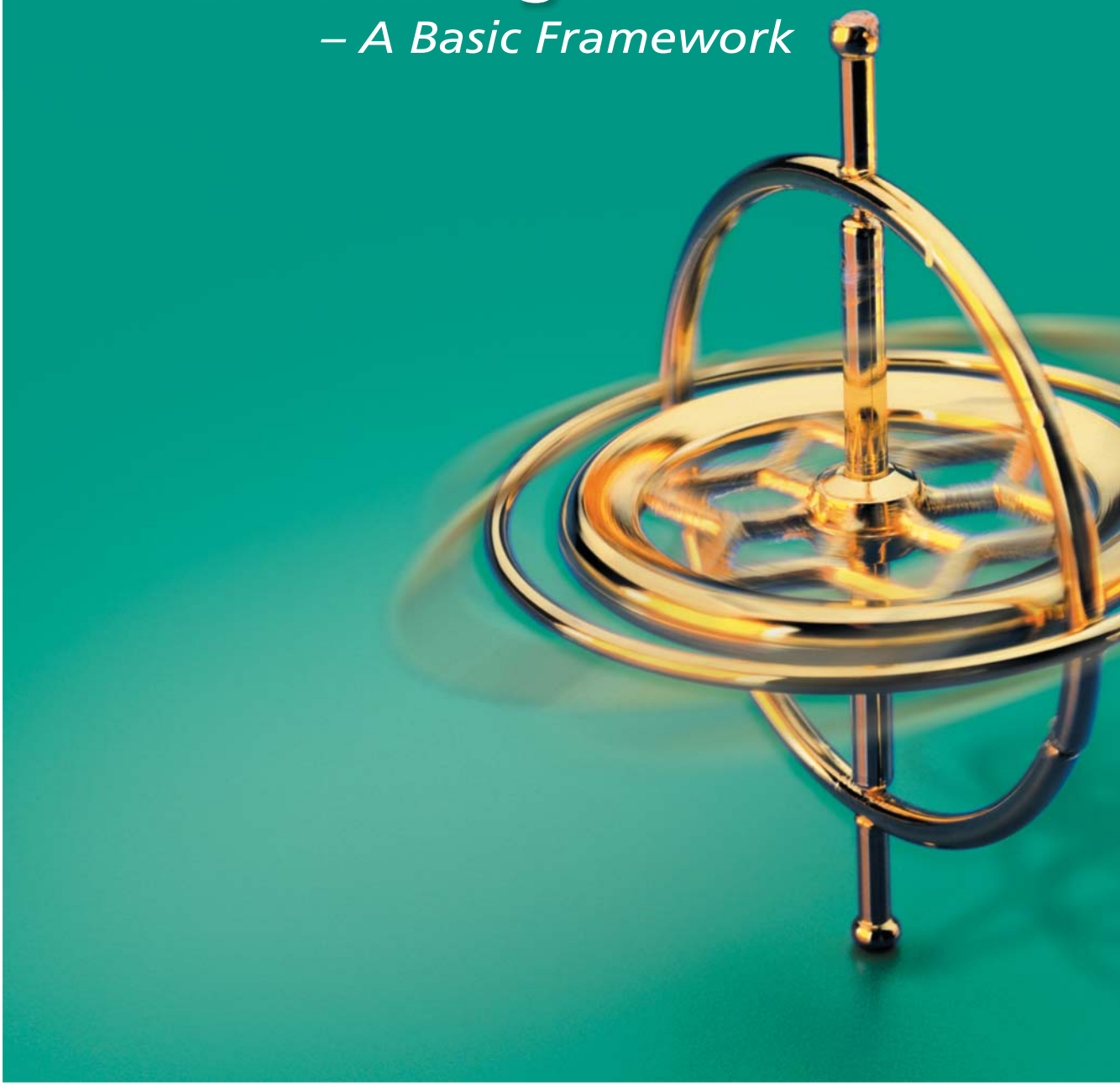
Hong Kong Institute of
Certified Public Accountants
香港會計師公會
The Success Ingredient

Internal Control *and* Risk Management

– A Basic Framework



FOREWORD

Since the formation of the Corporate Governance Committee in 1995, the Hong Kong Institute of Certified Public Accountants is proud to have been playing a leading role in promoting greater awareness and higher standards of corporate governance in Hong Kong. The Institute believes that good corporate governance is fundamental to attracting investment, stimulating economic growth and reducing the cost of capital. It is also vital to Hong Kong's role as one of the world's major financial centres and the premier international capital market for Mainland China and the region.

We are supportive, therefore, of the Stock Exchange of Hong Kong Limited's recent amendments to the Listing Rules to introduce the Code on Corporate Governance Practices ("the Code") and the requirements in relation to the Corporate Governance Report. These changes will raise the bar for listed companies in Hong Kong in terms of their corporate governance practices and disclosures.

This **guide** on internal control and risk management has been developed at the invitation of the Stock Exchange, with the primary objective of providing general guidance and recommendations on a basic framework of internal control and risk management. It draws on important overseas studies, which are acknowledged benchmarks of international good practice while, at the same time, takes into account the current situation of the Hong Kong market. We believe that the principles and recommendations contained in this **guide** should help listed companies to understand and implement the requirements in the Code relating to internal control, and to devise their own internal control procedures that have regard to the specific circumstances and characteristics of their business.

Enhancing corporate governance is not simply a matter of imposing rules and laws but about promoting and developing an ethical and healthy corporate culture. I hope that this **guide** makes it abundantly clear that establishing a sound system of internal control and reviewing its effectiveness is not an exercise in learning how to comply with unwelcome and onerous regulatory requirements but, rather, it is about implementing mechanisms that will help a company to achieve its corporate objectives and fulfil the expectations of its shareholders and stakeholders. At the basic level, the **guide** emphasises that, as a precondition for having effective controls, a company must ensure that it has clear objectives that are agreed by the board and well-understood by the senior management and employees. The company should then identify, assess and prioritise the risks that could prevent it from achieving those objectives, and establish processes to manage them effectively. It must also have in place early warning indicators so that if things go off course, the situation is quickly identified and brought to the attention of the appropriate people for action. For this to happen, there also needs to be good communication and an effective flow of information, both internally and with external parties, such as auditors and regulators. Finally, ongoing monitoring and reviews of the system are required because the business environment and conditions continue to change.

Unfortunately, there are far too many companies where some, or all, of these elements have been lacking and, indeed, some of them have failed because of it, despite having, on paper, good business prospects. Some have grown too fast, and generally outrun the ability of their internal control and risk management mechanisms to cope, others have failed to install proper internal checks and balances and have thus failed to identify the early signs of problems, and yet others have succumbed to the force of personality of dominant board members and controlling shareholders, whose ethical values fall short of market

expectations and the public interest. We are all familiar with examples of the type and should learn from them. While good internal controls cannot be a panacea for all corporate problems, they can help to provide a reasonable assurance that a sound business in the hands of decision makers with good sense and judgement will succeed in its objectives.

I hope that it will be obvious to the reader of this **guide** that it focuses as much on protecting the business and creating an environment where it can thrive and increase shareholder value, as it does on compliance with rules and regulations. Good ethical governance embraces good corporate governance, and an effective system of corporate governance should enable both compliance and performance to be achieved to the reasonable expectation of shareholders and stakeholders. This is why effective internal controls and risk management mechanisms should be incorporated within a company's normal management and governance processes, and should constitute part of its framework of accountability and regular reporting to shareholders.

In keeping with the Code, the immediate targets of this **guide** are listed companies and their subsidiaries and, beyond this, other companies in the group. However, I hope that companies that are not (or not yet) listed and other interested parties will also find this **guide** to be a useful reference.

Edward K.F. Chow
President, and Chairman, Internal Control and Risk Management Guide Task Force
Hong Kong Institute of Certified Public Accountants

June 2005

COMPOSITION OF THE INSTITUTE'S 2005 CORPORATE GOVERNANCE COMMITTEE

Chairman:	Chew Fook Aun	Kyard Ltd.
Deputy Chairmen:	Michael K.H. Chan	Lam Soon (Hong Kong) Ltd.
	Richard George	Deloitte Touche Tohmatsu
Members:	Nicholas Allen	PricewaterhouseCoopers
	David Cheng	HLB Hodgson Impey Cheng
	Gordon W.E. Jones	Companies Registry
	Quinn Y.K. Law	The Wharf (Holdings) Ltd.
	Stephen Lee	KPMG
	Kenneth G. Morrison	Moores Rowland Mazars
	Peter Nixon	Potential Associates Ltd.
	Keith Pogson	Ernst & Young
	James Siu	Li & Fung Ltd.
	Tommy Tam	National Electronics (Consolidated) Ltd.
	Nancy Tse	Hospital Authority
	Jim Wardell	Horwath Corporate Advisory Services Ltd.
Secretaries:	Peter Tisman	Director, Specialist Practices, Hong Kong Institute of CPAs
	Mary Lam	Assistant Director, Specialist Practices, Hong Kong Institute of CPAs

COMPOSITION OF THE INTERNAL CONTROL AND RISK MANAGEMENT GUIDE TASK FORCE

Chairman:	Edward K.F. Chow	China Infrastructure Group Holdings Plc.
Members:	Chew Fook Aun	Kyard Ltd.
	Michael K.H. Chan	Lam Soon (Hong Kong) Ltd.
	Richard George	Deloitte Touche Tohmatsu
	Stephen Lee	KPMG
	Guy Look	Sa Sa International Holdings Ltd.
	Peter Nixon	Potential Associates Ltd.
	James Siu	Li & Fung Ltd.
Secretaries:	Peter Tisman	Director, Specialist Practices, Hong Kong Institute of CPAs
	Mary Lam	Assistant Director, Specialist Practices, Hong Kong Institute of CPAs

CONTENTS

A. OBJECTIVES

1.0 Background

1.1 The Stock Exchange of Hong Kong Limited ("Stock Exchange") published the Code on Corporate Governance Practices ("the Code") and Corporate Governance Report in November 2004. These were subsequently incorporated into Appendices 14 and 23 of the Main Board Listing Rules and Appendices 15 and 16 of the Growth Enterprise Market ("GEM") Listing Rules respectively. The Code, with one exception, became effective for accounting periods commencing on or after 1 January 2005. The exception is in respect of Code provision C.2 on internal controls and the proposed disclosure requirements in the Corporate Governance Report relating to listed issuers' internal controls, which take effect for accounting periods commencing on or after 1 July 2005.

1.2 The Stock Exchange invited the Hong Kong Institute of Certified Public Accountants ("the Institute") to issue further guidance to help listed issuers understand and implement the Code requirements relating to internal control and devise their internal control procedures.

1.3 The Institute agreed to take up the Stock Exchange's invitation. A task force, set up under the Corporate Governance Committee and including representatives from the Auditing and Assurance Standards Committee and the Professional Accountants in Business Committee, was formed to undertake the project.

2.0 Listing Rule requirements on internal control

2.1 Principle C.2 of the Code states that: "*The board should ensure that the issuer maintains sound and effective internal controls to safeguard the shareholders' investment and the issuer's assets*."

2.2 Code provision C.2.1 on "Internal Controls" states that: "*The directors should at least annually conduct a review of the effectiveness of the system of internal control of the issuer and its subsidiaries and report to shareholders that they have done so in their Corporate Governance Report. The review should cover all material controls, including financial, operational and compliance controls and risk management functions.*"

2.3 The recommended best practices in relation to reviewing internal controls and the related disclosures are set out in C.2.2 to C.2.5 of the Code. Listed companies are encouraged to adopt the recommended best practices.

2.4 The note to paragraph 2 of Appendix 23 (Main Board Listing Rules) and Appendix 16 (GEM Listing Rules), which sets out the specific disclosures pertaining to the Code provisions that a listed issuer is expected to make in its Corporate Governance Report, contains the following disclosure in relation to the Code provision on "Internal Controls":

> "*(3) a statement that the board has conducted a review of the effectiveness of the system of internal control of the issuer and its subsidiaries (C.2.1 of the Code).*"

2.5 Where a listed issuer includes a statement on the review of its system of internal control in the annual report, pursuant to provision C.2.1 of the Code, it is encouraged to disclose the details set out in paragraph 3(d) of Appendix 23 of the Main Board Listing Rules and Appendix 16 of the GEM Listing Rules, as appropriate.

3.0 Objectives of the guide

3.1 The primary objective of this guide is to provide general guidance and recommendations on a basic framework of internal control. This should help listed issuers understand and implement the requirements in the Code relating to internal control, and to devise their own internal control procedures that take account of the particular circumstances and characteristics of their own business and operation. The guide is not intended to be exhaustive or prescriptive, but should nevertheless be useful to directors, managers and other personnel that are accountable for control in a company.

3.2 It is also intended to:

(i) help improve understanding of the conceptual framework of internal control and risk management;

(ii) help provide a framework/basis that can be used to develop and assess the effectiveness of internal control in a company; and

(iii) reflect sound business practice whereby internal control is embedded in the business and management processes by which a company pursues its objectives.

3.3 The Stock Exchange indicated that in preparing the Code, it had, in particular, taken into account the principles and guidelines set out in the revised Combined Code on Corporate Governance ("the Combined Code") issued by the Financial Reporting Council in the United Kingdom ("UK") in July 2003. The Preamble to the Combined Code makes reference to specific guidance on how to comply with particular parts of the Combined Code. *Internal Control: Guidance for Directors on the Combined Code* ("the Turnbull Guidance")[1] is the guidance relevant to the provisions on internal control. In preparing this guide, the Institute has referred to the Turnbull Guidance.

3.4 The Institute considers that the report, *Internal Control – Integrated Framework*, issued by the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") in the United States, in 1992, contains a definition of internal control and a conceptual framework that are constructive and relevant. Where appropriate, therefore, this guide adopts the approach outlined in the COSO report.

[1] *Internal Control: Guidance for Directors on the Combined Code* published by the Institute of Chartered Accountants in England and Wales in the UK in September 1999.

3.5 Boards of listed companies are encouraged to make reference to this guide in:

- assessing how the company has applied Code principle C.2;
- implementing the requirements of Code provision C.2.1; and
- reporting on these matters to shareholders in the Corporate Governance Report.

3.6 Directors are expected to exercise judgement in reviewing how the company has implemented the requirements of the Code relating to internal control and reporting to shareholders thereon.

3.7 The guidance set out herein in relation to establishing a sound system of internal control and reviewing its effectiveness should be incorporated by the company within its normal management and governance processes, from a corporate governance point of view, as part of the accountability of a company's board and management to shareholders, and should not be treated as a separate exercise undertaken to meet regulatory requirements issued and enforced by a securities market regulator.

4.0 Applicability of the guide

4.1 This guide is aimed primarily at listed companies and their subsidiaries, to which Code provision C.2.1 applies. However, listed companies are very diverse in nature. Internal controls should be tailored to an individual company's own particular characteristics and circumstances, which may depend upon, for example, its industry, size and organisational structure. Accordingly, it is not appropriate to adopt a "one size fits all" approach.

4.2 It is believed that the principles and recommendations contained in this guide will provide a useful reference for most listed companies, although they may need to be adapted according to the circumstances of the company concerned. All companies that are part of a listed group are encouraged to take on board these principles and recommendations, and it is hoped that companies in general that wish to implement or enhance their system of internal control will find this guide to be a useful reference.

4.3 Throughout the guide, where reference is made to "company", it should be taken, where applicable, as referring to the group of which the reporting company is the parent company. For groups of companies, the review of the effectiveness of internal control and the report to the shareholders should be from the perspective of the group as a whole, e.g., groups of companies should review the effectiveness of all significant controls at all significant locations.

4.4 Where material joint ventures and associates have not been dealt with as part of the group for the purposes of applying this guidance, companies are encouraged to disclose this. Where they exist, alternative sources of risk management and internal control assurance applied to these entities should also be disclosed.

B. IMPLEMENTING INTERNAL CONTROL AND RISK MANAGEMENT

1.0 Framework and scope of internal control

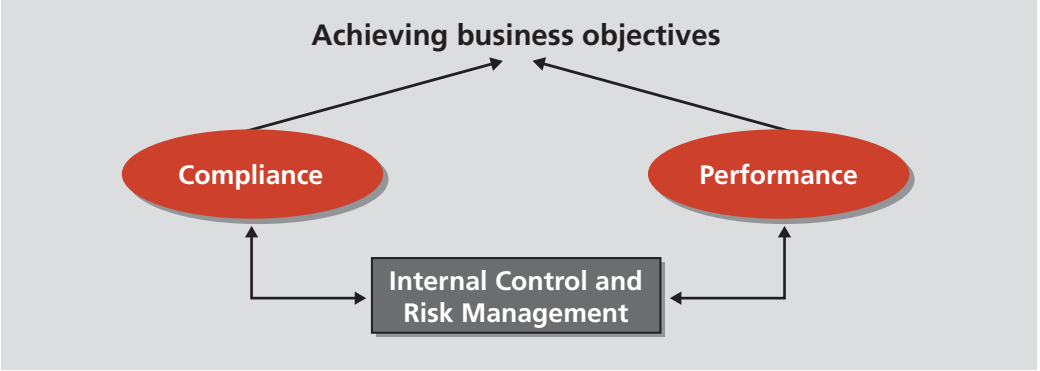
1.1 There is no simple definition of "internal control". However, as indicated in paragraph A.3.4 above, where appropriate, this guide adopts the definition and conceptual framework described in the COSO report, which the Institute regards as a useful model. (See also Appendix I).

1.2 The COSO report defines internal control as a process designed to provide reasonable assurance regarding the achievement of objectives in relation to the following:

- *Effectiveness and efficiency of operations*
- *Reliability of financial reporting*
- *Compliance with applicable laws and regulations*

1.3 Internal control is fundamental to the successful operation and day-to-day running of a business and it assists the company in achieving its business objectives. As indicated above, the scope of internal control is very broad. It encompasses all controls incorporated into the strategic, governance and management processes, covering the company's entire range of activities and operations, and not just those directly related to financial operations and reporting. Its scope is not confined to those aspects of a business that could broadly be defined as compliance matters, but extends also to the performance aspects of a business. (See Figure 1.)

Figure 1: Internal Control Framework



1.4 Internal controls need to be responsive to the specific nature and needs of the business. Hence, they should seek to reflect sound business practice, remain relevant over time in the continuously evolving business environment and enable the company to respond to the specific needs of the business or industry.

1.5 It is important that control should not be seen as a burden on business but, rather, the means by which business opportunities are maximised and potential losses associated with unwanted events reduced. Furthermore, successful companies should not allow themselves to become complacent or blinded by their own success. There are numerous examples of companies whose success has been jeopardised by a lack of, or deficiencies in, internal controls.

1.6 At the same time, the cost/benefit equation is also relevant to any internal control system. Cost/benefit considerations should be taken into account both in the overall design of the system and in the context of risk identification, assessment and prioritisation.

Function of internal control

1.7 Control is not synonymous with managing and does not constitute everything involved in the management of a company. While it aims to support the achievement of business objectives, and should serve as an early warning system of possible impediments to achieving those objectives, internal control does not, on the other hand, indicate what objectives to set. While it can help to ensure that reliable information is made available for decision-making, implementation and monitoring, and can facilitate assessment and reporting on the results of actions taken, it does not take the place of the management in making strategic and operational decisions. In addition, decisions about whether to act and what action to take are outside the scope of internal control.

1.8 It follows from the above that there are inherent limitations in control. A sound and well-designed system of internal control reduces, but cannot eliminate, the possibility of poor judgement in decision-making; human error or mistake; control activities and processes being deliberately circumvented by the collusion of employees or others; management overriding controls; and the occurrence of unforeseeable circumstances.

1.9 A sound system of internal control therefore helps to provide reasonable, but not absolute, assurance that a company will avoid being hindered in achieving its business objectives, or in the orderly and legitimate conduct of its business, by circumstances that may reasonably be foreseen. A system of internal control cannot, however, provide protection with certainty against a company failing to meet its business objectives or against all material errors, losses, fraud, or breaches of laws or regulations.

1.10 As noted in paragraph A.4.1 above, no two companies will, or should, have identical internal control systems. Companies and their control differ by industry, size and organisational structure, and by culture and management philosophy. Therefore, while all companies need each of the components (referred to in paragraph B.2.2 below) to ensure adequate control over their activities, each will have a unique internal control system tailored to meet its own circumstances. The management will have to exercise its judgment, driven by the particular needs of the company, to determine the nature of the controls that should be in place and whether they are functioning effectively in achieving the company's objectives.

2.0 Elements of a sound system of internal control

2.1 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 in relation 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; and
- help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business.

2.2 Internal control can be analysed into five inter-related components, which also serve as criteria for the effectiveness of the internal control system in supporting the achievement of the separate but overlapping operational, financial reporting and compliance objectives. This is illustrated in Figure 2. The components are:

(i) Control environment – the foundation for the other components of internal control, which also provides discipline and structure. Factors include ethical values and competence (quality) of personnel, direction provided by the board and effectiveness of management.

(ii) Risk assessment – identification and analysis of risks underlying the achievement of objectives, including risks relating to the changing regulatory and operating environment, as a basis for determining how such risks should be mitigated and managed.

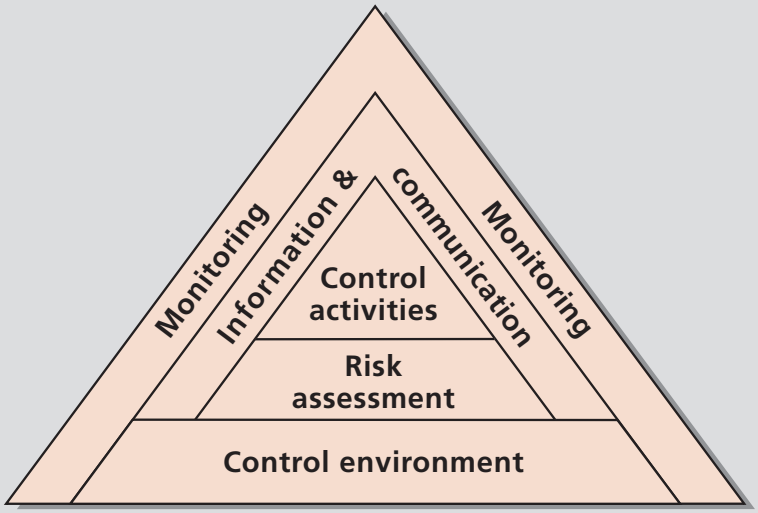
(iii) Control activities – a diverse range of policies and procedures that help to ensure management directives are carried out and any actions that may be needed to address risks to achieving company objectives are taken.

(iv) Information and communication – effective processes and systems that identify, capture and report operational, financial and compliance-related information in a form and timeframe that enable people to carry out their responsibilities.

(v) Monitoring – a process that assesses the adequacy and quality of the internal control system's performance over time. Deficiencies in internal controls should be reported to the appropriate level upstream, which may be, for example, senior management, the audit committee, or the board.

A more detailed description and breakdown of the five components and their relationships is contained in Appendix II.

Figure 2: Internal Control Components



Adapted from *Internal Control – Integrated Framework*, COSO

2.3 A company's system of internal control will reflect its control environment, which encompasses its organisational structure.

2.4 The system of internal control should:

- be embedded in the operations of the company and form part of its culture;
- be capable of responding quickly to evolving risks to the business arising from factors within the company and changes in the business environment; and
- 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.

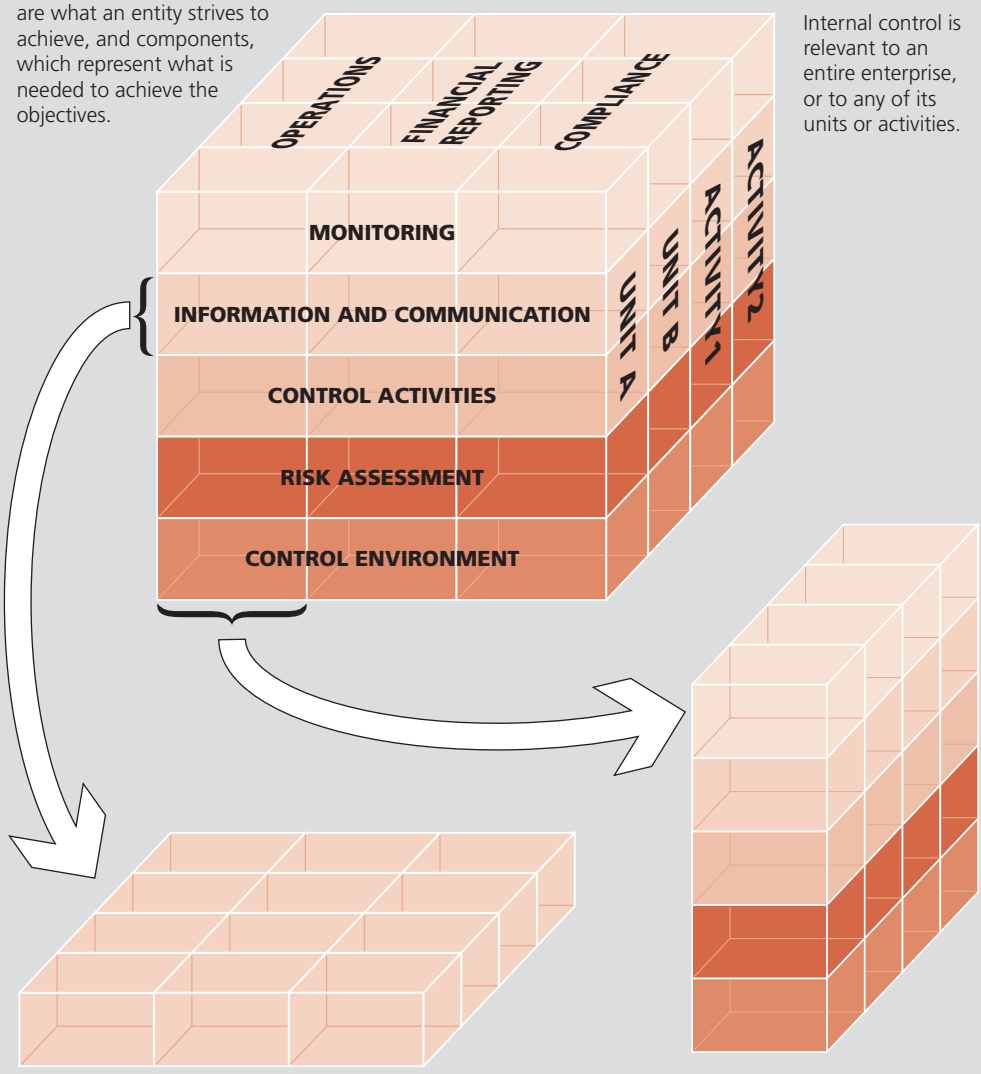
2.5 Internal control procedures should, as far as possible, given the nature of the individual company concerned, be kept simple and straightforward, and have regard to the need to ensure that (a) the costs do not outweigh the benefits and (b) staff at all levels can "buy into" the importance of maintaining adequate control and are not alienated by unnecessary complexity in implementing it.

2.6 There is a direct relationship between a company's objectives and the components of internal control that are required to achieve them. A graphical representation of this is reproduced in Figure 3. All of the components apply to the three categories of objectives referred to in paragraph B.1.2 above. The third dimension in Figure 3 represents subsidiaries, divisions, or other business units, and functional or other activities, such as purchasing, production and marketing. This reflects the fact that internal control is relevant not only to an enterprise as a whole, but also to parts of that enterprise.

Figure 3: Relationship between Objectives and Components

There is a direct relationship between objectives, which are what an entity strives to achieve, and components, which represent what is needed to achieve the objectives.

Internal control is relevant to an entire enterprise, or to any of its units or activities.



Information is needed for all three objectives categories – to effectively manage business operations, prepare financial statements reliably and determine compliance.

All five components are applicable and important to the achievement of operations objectives.

Extracted from *Internal Control – Integrated Framework*, COSO

3.0 Need for training

3.1 Directors and management should be provided with appropriate training to enable them to gain a proper understanding of internal controls, their function and scope, including reporting. While this should help to facilitate compliance with the regulatory requirements on internal controls, equally importantly, it should also provide greater assurance that business objectives can be achieved. Training programmes may be provided in-house, or through training institutes or professional bodies.

4.0 Risk management

4.1 The process of risk management involves:

- understanding organisational objectives;
- identifying the risks associated with achieving or not achieving them and assessing the likelihood and potential impact of particular risks;
- developing programmes to address the identified risks; and
- monitoring and evaluating the risks and the arrangements in place to address them.

4.2 Risk may affect many areas of activity, such as strategy, operations, finance, technology and environment. In terms of specifics it may include, for example, loss of key staff, substantial reductions in financial and other resources, severe disruptions to the flow of information and communications, fires or other physical disasters, leading to interruptions of business and/or loss of records. More generally, risk also encompasses issues such as fraud, waste, abuse and mismanagement.

4.3 Appendix III illustrates some of the types of risks that may need to be considered, but this list should not be regarded as exhaustive and it is not industry specific. Actual risks faced by a company are likely to include more industry-specific types of risks and to relate to the particular circumstances of the company.

4.4 Risk management is essential for reducing the probability that corporate objectives will be jeopardised by unforeseen events. The board must determine the type and extent of risks that are acceptable to the company, and strive to maintain risk within these levels. Internal control is one of the principal means by which risk is managed.

4.5 In the business world, a company's objectives and the environment in which it operates are continually evolving and, as a result, the risks that it faces also change. A sound system of internal control depends on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed. The systems and processes of control need to be sufficiently flexible to be able to change and adapt as the environment and the company's organisation, objectives and activities develop over time.

4.6 Since profits and increases in shareholder value are, in part, the reward for successful risk-taking in business, the purpose of internal control is to help manage and control risk appropriately, rather than to eliminate it.

4.7 The fundamentals of good risk management and internal control and an indication of some potential benefits of effective risk management and internal control are illustrated below in Figures 4 and 5 respectively.

Figure 4: Fundamentals of Good Risk Management and Internal Control

Adapted from *Implementing Turnbull – A Boardroom Briefing*, ICAEW

Figure 5: Potential Benefits of Effective Risk Management and Internal Control

Adapted from *Implementing Turnbull – A Boardroom Briefing*, ICAEW

Internal financial control

4.8 Effective financial controls are a vital element of internal control. They help in identifying and managing liabilities to ensure that the company is not unnecessarily exposed to avoidable financial risks (e.g., losses from derivatives and financial instruments) and that financial information used within the business and for publication is reliable. They also contribute to the safeguarding of assets from inappropriate use or loss, including the prevention and detection of fraud.

4.9 Internal financial control is also a key part of the fundamentals of good risk management that should underpin the wider aspects of business risk. It is needed to provide the board and senior management with information of sufficient quality to make good business decisions and meet their regulatory obligations. Important areas include the maintenance of proper financial records in support of financial budgets, projections, other management information (e.g., monthly management accounts and reports, comparison of budgetary versus actual performance) and reliable interim and year-end reporting.

Business Planning and Budgeting

4.10 Budgeting is an important management tool and a key control process in business planning. An efficient and effective budgetary system should be linked to business plans, containing measurable statements of the company's objectives, policies and priorities, strategies for achieving objectives/targets and a resource framework. This encourages a clearer company vision, enables proper forward planning to take place and facilitates the best use of resources. The assessment of risk is, therefore, also relevant to the budgeting and business planning process, at both the preparation and monitoring stages. It is important to conduct regular reviews of business plans and budgets for their continuing relevance and to monitor performance and progress against the budgets.

5.0 Embedding the process

5.1 Many employees may have some responsibility for internal control as part of their accountability for achieving objectives. Some of the key personnel are referred to in section C.5.0 below, but others also have a role to play. They, collectively, need to have the necessary knowledge, skills, information and authority to establish, operate and monitor the system of internal control. This will require an understanding of the company, its objectives, the industries and markets in which it operates and the risks that it faces.

5.2 Control should be embedded within the business processes by which a company pursues its objectives. It follows that, rather than developing separate risk reporting systems, it is best to build early warning mechanisms into existing management information systems. Overly cumbersome or elaborate risk management processes can be a distraction from the key point, which is that incorporating control within existing processes enables each person in the organisation to become more focused on meeting the business objectives and in managing significant risks that relate to the tasks that he or she performs.

5.3 Opportunities exist through embedding risk management to remove duplicate or unnecessary controls and to create an environment where, subject to sound risk management practices, there is more empowerment for people within the company to work to satisfy the needs of customers/clients.

5.4 A key issue that can be addressed is the extent to which executive management puts significant risk management issues on its agenda. Where there is a risk committee, it should avoid usurping the role of the executive management. It can encourage and foster good risk management and awareness, but it should not take over the role of the executive management.

5.5 Senior management and the board need to ask whether they have enough timely, relevant and reliable reports on progress against business objectives and significant risks. For instance, do they have enough qualitative information on customer satisfaction and employee attitudes? Also, as risks change, do they have the necessary business information to respond effectively?

C. RESPONSIBILITIES FOR INTERNAL CONTROL AND RISK MANAGEMENT, AND THE PROCESS OF REVIEW

1.0 The Board

1.1 Broadly speaking, the purpose of a system of internal control is to keep a company on course towards achieving its performance and profitability goals and its overall mission. In this regard it is important that the board agrees on a set of clearly-defined objectives and goals, which should be communicated throughout the company. As previously stated, the immediate aim of internal control is to help to provide a reasonable level of assurance that a company will meet the agreed objectives and goals. It has a key role in the management of risks that are significant to the fulfilment of business objectives.

1.2 Principle C.2 of the Code states that it is the board's responsibility to ensure that the company maintains sound and effective internal controls to safeguard the shareholders' investment and the issuer's assets at all times. To fulfil this responsibility, the directors should at least annually conduct a review of the effectiveness of the system of internal control of the company and its subsidiaries and report to shareholders that they have done so in their Corporate Governance Report. The review should cover all material controls, including financial, operational and compliance controls and risk management functions (Code provision C.2.1).

1.3 It is also a good practice for the board, prior to the date of each interim report, to evaluate any change in the company's internal control that has occurred during the interim reporting period, and which has materially affected, or is reasonably likely to materially affect, the company. Consideration should also be given to disclosing any significant failing or weakness in internal control and its impact on the company in the interim report, in order to enable investors and the public to appraise the position of the company.

Review of the effectiveness of internal control and risk management

1.4 Reviewing the effectiveness of internal control is an essential part of the board's responsibilities, while the management is accountable to the board for designing, operating and monitoring the system of internal control and for providing assurance to the board that it has done so. The board will need to form its own view on effectiveness after due and careful enquiry based on the information and assurances provided to it.

1.5 The board may delegate detailed aspects of the review work to board committees, e.g., the audit committee (see also section C.4.0), the risk management committee, etc. The scope of review of such committees is for the board to decide and will depend upon factors such as the size and composition of the board, the scale, diversity and complexity of the company's operations, and the nature of the significant risks that the company faces.

1.6 To the extent that designated board committees carry out, on behalf of the board, tasks that are attributed in this guide to the board, the results of the relevant committees' work should be reported to, and considered by, the board. The board as a whole should form its own view on the adequacy of the review, after due and careful enquiry, given that the board takes ultimate responsibility for the disclosures on internal control in the Corporate Governance Report.

The process of review

1.7 Effective monitoring on a continuous basis is an essential component of a sound system of internal control. The board should not, however, be passive and rely solely on the embedded monitoring processes within the company to discharge its responsibilities. It should regularly receive and review reports on internal control.

1.8 In addition, the board is required to undertake an annual assessment of the effectiveness of the system of internal control of the company and its subsidiaries for the purposes of making its public statement on internal control in the Corporate Governance Report. The assessment should cover the period to which the financial statements relate and, if appropriate, any very significant matters up to the date of approval of the annual report and financial statements.

1.9 The board should define the process to be adopted for its review of the effectiveness of internal control. This should encompass both the scope and frequency of the reports that it receives and reviews during the year, and also the process for its annual assessment, so that it will be provided with sound, appropriately-documented, support for its statement on internal control in the company's Corporate Governance Report.

1.10 The reports from the management or others tasked with commenting upon internal controls (e.g., internal auditors) should be made to the board, or such committees of the board designated for the purpose, on a sufficiently frequent basis so as to provide the board with an up-to-date picture of the company's current control situation. It is effectively a process of continuous assessment, which needs to ensure that all significant aspects of the business have been addressed.

1.11 The board should make it clear that, in relation to the areas covered by the reports, the board expects the reports to provide a balanced assessment of the significant risks and the effectiveness of the system of internal control in managing those risks. Any significant control failings or weaknesses identified should be discussed in the reports, including the impact on the company that they have already had, could have had, or may have, and the actions being taken to rectify them. It is essential that there be openness of communication by the management with the board on matters relating to risk and control.

1.12 Key risk indicators and the results of embedded monitoring should be supplied to the board or designated committees on an ongoing basis, and the chairman of the board should encourage discussion of risk management and internal control issues at each board meeting, as appropriate, as an additional item to the normal board agenda. Reports from other committees, such as the executive and audit committees, also provide opportunities to discuss risk and control.

1.13 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 in internal control 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.

1.14 The board's annual assessment exercise for the purpose of making its public statement on internal control in the Corporate Governance Report should consider issues dealt with in the relevant reports reviewed by it during the year, together with any additional information necessary to ensure that it has taken account of all significant aspects of internal control for the company, including financial, operational and compliance controls and risk management functions, for the year under review, and up to the date of approval of the annual report and financial statements.

1.15 In the annual assessment, the board is also encouraged to consider, the various matters set out as recommended best practices in section C.2.2 of the Code.

1.16 If the board becomes aware at any time of a significant failing or weakness in internal control, it should determine how the failing or weakness arose and re-assess the effectiveness of management's ongoing processes for designing, operating and monitoring the system of internal control. The board may need to consider whether timely disclosure should be made of any significant failing or weakness in internal control and its impact on the company, in order to enable investors and the public to appraise the position of the company, in particular, in relation to information that could be considered to be price-sensitive.

1.17 In order to make an objective assessment of the effectiveness of internal control, a set of criteria should be developed by directors and management as a basis for making judgements.

Reporting on internal control and risk management

1.18 In its narrative statement of how the company has applied Code principle C.2, the board should, where applicable, disclose, at least, that:

- there is an ongoing process for identifying, evaluating and managing the significant risks faced by the company that threaten the achievement of its business objectives;
- the system of internal control has been in place for the year under review, and up to the date of approval of the annual report and financial statements; and
- the system of internal control has been reviewed by the board during the year under review.

1.19 The board may also consider disclosing that the system of internal control is consistent with the principles outlined in this guide.

1.20 The board may wish to provide additional information in the Corporate Governance Report to assist understanding of the company's risk management processes and system of internal control.

1.21 The disclosures relating to the application of Code principle C.2 should include an acknowledgement by the board that it is responsible for ensuring that the company maintains a sound and effective system of internal control, and for reviewing its effectiveness.

1.22 The board should also explain that such a system is designed to manage, rather than eliminate, the risk of failure to achieve business objectives, and that it can provide only a reasonable, and not an absolute, assurance in this respect. In addition, it cannot guarantee against material misstatement or loss.

1.23 In relation to Code provision C.2.1, the board should summarise the process it (and, where applicable, any relevant committee) has applied in reviewing the effectiveness of the system of internal control. 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 financial statements.

1.24 Paragraph 3 of Appendix 23 (Main Board Listing Rules) and Appendix 16 (GEM Listing Rules) sets out the recommended disclosures in the Corporate Governance Report in relation to internal controls. These are the areas that listed companies are encouraged to comment on in their Corporate Governance Report, but the level of detail required may vary with the nature and complexity of the company's business activities.

1.25 Where a board cannot make one or more of the disclosures in paragraphs C.1.18 and C.1.23, it should also consider stating the fact and providing an explanation. The Code requires an issuer to disclose and give considered reasons if it has failed to conduct a review of the effectiveness of the system of internal control of the company and its subsidiaries, or any part thereof.

1.26 The board should ensure that its disclosures provide meaningful information and do not give a misleading impression. Reference should be made to Rule 2.13(2) of the Main Board Listing Rules on the general principles to be adopted by listed companies and their directors in disclosing information.

2.0 Board policies

2.1 A system of internal control is effected by a number of parties and many individuals within a company have a role to play, and responsibilities in relation to internal control, as part of their accountability for achieving objectives.

2.2 As indicated above (see paragraph C.1.2), the board of directors is ultimately responsible for the company's system of internal control. It should set appropriate policies on internal control and should request, receive and assess, relevant materials prepared by the executive management, and the company's auditors and other relevant parties (if appropriate) on each of the components of the internal control structure (see paragraph B.2.2 above), that will enable it to satisfy itself that the system and processes are functioning effectively.

2.3 The board must further ensure that the system of internal control is effective in monitoring and managing risks in the manner and to the level that it has approved.

2.4 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 that the board regards as acceptable for the company to bear;
- the likelihood of the risks 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.

2.5 It is essential that the board sets the right tone at the top and that it communicates a clear message that control responsibilities must be taken seriously. In order to achieve this, the board should consider asking itself questions such as: **Does the company have the right attitude to risk management and internal control?** Concerns that would indicate the need for a change in behaviour and mindset in relation to risk management and internal control would include:

- the board thinks that risk management is "not its problem";
- the company is focused only on internal financial control rather than the wider scope of internal control;
- there is no consensus amongst the board on what are the business objectives;
- reviewing internal control is regarded only as a regulatory exercise for the purpose of making a public statement, rather than an embedded part of the business;
- risk management is seen as the responsibility of one function, such as audit or insurance;
- no key risk indicators have been determined; and
- employees have no training or experience in risk awareness.

2.6 The boards of many companies carry out their duties through functional committees, e.g., audit, remuneration and nomination committees. The various committees can each bring a different perspective to the components of internal control and may be in a position to advise or assist the board on relevant policy issues.

3.0 Internal audit function

3.1 Provision C.2.5 of the Code states that companies that do not have an internal audit function should review the need for one on an annual basis and should disclose the outcome of such review in the company's Corporate Governance Report.

3.2 It is a good practice for companies to establish an internal audit function to undertake regular monitoring of key controls and procedures. Such regular monitoring is an integral part of a company's system of internal control and helps to ensure its effectiveness.

3.3 Internal audit can make a significant and valuable contribution to the company by:

- providing advice on the management of risk, especially those issues surrounding the design, implementation and operation of systems of internal control;
- enhancing efficient and effective risk and control management by identifying opportunities to save on costs of control and/or by the avoidance of operational and similar losses; and
- promoting risk and control concepts within the company, e.g., by running or facilitating control self-assessment programmes.

3.4 Various benefits can be provided by an internal audit function. With the right level of resources, it should be able to:

(a) provide objective assurance to the board and management as to the adequacy and effectiveness of the company's risk management and internal control framework;

(b) assist the management to improve the processes by which risks are identified and managed; and

(c) assist the board with its responsibilities to strengthen and improve the risk management and internal control framework.

3.5 Nevertheless, the need for an internal audit function will vary depending on company-specific factors, including the scale, structure, diversity and complexity of the company's activities, the number of employees, the company's corporate culture, as well as cost/benefit considerations. Senior management and the board may desire objective assurance and advice on risk and control. An adequately-resourced internal audit function (or its equivalent where, for example, a qualified, independent third party is contracted to perform some or all of the work concerned) may provide such assurance and advice. There may be other functions within the company that also provide assurance and advice covering specialist areas, such as health and safety, regulatory and legal compliance and environmental issues.

3.6 In the absence of an internal audit function, the management needs to apply other monitoring processes in order to assure itself, and the board, that the system of internal control is functioning as intended. In these circumstances, the board will need to assess whether such processes provide sufficient and objective assurance.

3.7 When undertaking its assessment of the need for an internal audit function, the board should consider whether there are any trends or current factors relevant to the company's activities, markets or other aspects of its external environment, that have increased, or are expected to increase, the risks faced by the company. Such an increase in risk may also arise from internal factors, such as organisational restructuring, or from changes in reporting processes or underlying information systems. Other matters to be taken into account may include adverse trends evident from the monitoring of internal control systems or an increased incidence of unexpected occurrences.

3.8 When the board of a company, which does not have an internal audit function, carries out its annual assessment of the need for such a function, it should consider the factors referred to in paragraphs C.3.5 and C.3.7 above, amongst others.

3.9 Where there is an internal audit function, the board is recommended to annually review its scope of work, authority and resources, again having regard to those factors referred to in paragraphs C.3.5 and C.3.7 above.

4.0 Audit committee

4.1. The audit committee plays an important role in the control and risk management framework of a company, including, in the review process. The Listing Rules (Main Board – Rule 3.21, GEM – Rule 5.28) require every listed issuer to establish an audit committee.

4.2 The terms of reference of the audit committee should include the duties specified in Code provision C.3.3. Amongst these are the following duties relating to oversight of the issuer's financial reporting system and internal control procedures:

- to review the issuer's financial controls, internal control and risk management systems;
- to discuss with the management the system of internal control and ensure that the management has discharged its duty to have an effective internal control system;
- to consider any findings of major investigations of internal control matters as delegated by the board, or on its own initiative, and the management's response;
- where an internal audit function exists, to ensure co-ordination between the internal and external auditors, and to ensure that the internal audit function is adequately resourced and has appropriate standing within the issuer, and to review and monitor the effectiveness of the internal audit function;
- to review the group's financial and accounting policies and practices; and
- to review the external auditor's management letter, any material queries raised by the auditor to management in respect of the accounting records, financial accounts or systems of control and management's response.

(Further general guidance on the role and duties of an audit committee can be found in "*A Guide For Effective Audit Committees*", published by the Institute in February 2002.)

5.0 Other parties in the system

Executive management

5.1 The executive management is directly responsible for implementing the overall strategy and policies decided by the board and for all activities of a company, including the operation of the internal control system. However, management at different levels will have different internal control responsibilities, depending on the characteristics of the company.

Senior executives

5.2 The chief executive should have line responsibility for all aspects of executive management, and is accountable to the board for the performance of the company and the implementation of the board's strategy and policies, including policies on risk and control.

5.3 The chief executive, together with other senior executives, should identify and evaluate the risks faced by the company for consideration by the board, and should take charge of designing, operating and monitoring a suitable system of internal control that implements the policies set by the board. They should ensure the existence of a positive control environment and that all the components of internal control are in place. They should also provide leadership and direction to other senior managers responsible for the major functional areas, periodically reviewing their responsibilities and the way they are controlling the business.

5.4 The Listing Rules (Main Board – Rule 3.24, GEM – Rule 5.15) require every listed company to employ a full-time "qualified accountant", who is a member of the senior management and whose responsibility "*must include oversight of the issuer and its subsidiaries in connection with its financial reporting procedures and internal controls and compliance with the requirements under the Exchange Listing Rules with regard to financial reporting and other accounting-related issues*". Under the Listing Rules, therefore, the qualified accountant has a particular responsibility for oversight of internal controls relating to the finance function.

5.5 The chief financial officer (CFO), who may also be the qualified accountant, commonly plays an important monitoring role. The CFO is generally involved in developing and preparing company-wide budgets and plans, which necessitates tracking and analysing the performance of the whole company, not only the financial aspects, but also from the perspective of its operations and compliance, covering the activities of all divisions, subsidiaries and other units. As such, the CFO is commonly a central point of management control.

5.6 Given his/her role, the CFO should be involved in the process when, e.g., the company's objectives are established and strategies decided, risks are analysed and decisions are made on how changes/risks affecting the company will be managed. The CFO can provide valuable input and direction in relation to the above matters, and is well positioned to focus on monitoring and following up on the agreed actions.

Compliance officer

5.7 The responsibilities of a compliance officer, where the position exists, should include, as a minimum, the following matters:

(i) ensuring that the board is kept fully informed of the parameters within which it should operate;

(ii) ensuring that board procedures are properly followed; and

(iii) advising on, and assisting the board in implementing, procedures to ensure that the company complies with all applicable laws and regulations and relevant statements of best practice.

Operational personnel

5.8 Senior managers in charge of organisational units (i.e., individual departments/sections) may be assigned responsibility for guiding the development and implementation of internal control policies and procedures that address their unit's objectives, and ensuring that these are consistent with the company-wide objectives.

5.9 Unit managers usually play a more hands-on role in devising and executing particular internal control procedures for the unit's function. They may be expected to make recommendations on the controls, monitor their application, and meet with upper level managers to report on the functioning of the relevant controls.

5.10 Supervisory personnel are directly involved in executing control policies and procedures at a detailed level. They may be expected to take action on exceptions and other problems as they arise, and to report upwards to higher-level management any significant matters, whether pertaining to a particular transaction or an indication of larger concerns.

APPENDIX I

The concept and scope of internal control

1. The **Cadbury Report**[2] states that for directors to meet their responsibilities for maintaining adequate accounting records, they need in practice to maintain a system of internal control over the financial management of the company, including procedures designed to minimise the risk of fraud.

2. The **Rutteman Guidance**[3] defines "internal financial control" as internal controls over the safeguarding of assets, the maintenance of proper accounting records and the reliability of financial information used within the business or for publication. The Rutteman guidance also encourages directors to review and report on all aspects of internal control, including controls to ensure effective and efficient operations and compliance with laws and regulations.

3. The **report of the Committee of Sponsoring Organizations of the Treadway Commission (COSO)**[4], *Internal Control – Integrated Framework* (1992), defines internal control as "*a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:*

   - *Effectiveness and efficiency of operations*
   - *Reliability of financial reporting*
   - *Compliance with applicable laws and regulations"*

4. The COSO definition provides some insights into the fundamental concepts of internal controls, in particular:

   - Internal control is a ***process*** and a means to an end, not an end in itself.
   - Internal control can be expected to ***provide only reasonable assurance***, not absolute assurance.
   - Internal control is ***effected by people*** at every level of a company and is geared to the ***achievement of objectives***.

---

2 Report of the Committee on The Financial Aspects of Corporate Governance, UK, December 1992.

3 *Internal Control and Financial Reporting: Guidance for directors of listed companies registered in the UK* issued by the Rutteman Working Group, UK, December 1994. The working group was established to develop criteria for assessing effectiveness, and guidance for directors in relation to reporting on internal controls.

4 COSO is a private sector initiative. It was originally formed in 1985 and was jointly sponsored by five major financial professional associations in the United States – the American Accounting Association, the American Institute of Certified Public Accountants, the Financial Executives Institute, the Institute of Internal Auditors, and the National Association of Accountants (now the Institute of Management Accountants). COSO's goal was to improve the quality of financial reporting by focusing on corporate governance, ethical practices, and internal control.

5. ***Guidance on Control*, issued by the Criteria of Control Board of The Canadian Institute of Chartered Accountants ("CoCo")**[5], builds on the concepts in the COSO report and defines control as comprising "*those elements of a company (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organisation's objectives*". The CoCo report also states that from another perspective, "*control is effective to the extent that the remaining (uncontrolled) risks of the organisation failing to meet its objectives are deemed acceptable*".

[5] *Guidance on Control*, Canada, November 1995, issued by the Criteria of Control Board (currently known as The Risk Management and Governance Board) of The Canadian Institute of Chartered Accountants.

APPENDIX II

Further information on the components of a system of internal control

(1) Control environment

As noted in paragraph B.2.2 above, the *control environment* is the foundation for the other components of internal control and provides discipline and structure. Factors include ethical values and competence (quality) of personnel, direction provided by the board and effectiveness of management.

The control environment should include a strong commitment to integrity and high ethical values. In this regard senior management must explicitly communicate the entity's values and behavioural standards to employees, e.g., through a formal code of conduct, and encourage compliance by their actions and examples. The imposition of appropriate penalties on persons who violate codes of conduct is also an important part of ensuring that they are complied with and become ingrained in the corporate culture.

Incentives and temptation are amongst the pitfalls that could potentially undermine a strong ethical culture. The former includes pressure to meet unrealistic performance targets, particularly for short-term results, and high performance-dependent rewards. The latter includes non-effective controls, such as poor segregation of duties in sensitive areas that offer temptations to misappropriate or conceal poor performance; a weak internal audit function that is unable to detect and report improper behaviour and an ineffective board that does not provide objective oversight of senior management.

Other aspects of the control environment include:

- *A commitment to competence*: the management should specify the competence levels of particular jobs and translate those into necessary knowledge and skills.
- *An active and involved board and audit committee*: the board must possess an appropriate degree of management, technical and other expertise, coupled with the necessary stature and mindset to perform its strategic and oversight functions. Board members must be objective and willing to question the management's activities. The audit committee also should have suitably experienced, qualified, independent and active members.
- *Assignment of authority and responsibility, and accountability for actions*: this includes the establishment of reporting relationships and authorisation protocols. A major challenge is to delegate only to the extent required to achieve objectives, which in turn requires ensuring that risk acceptance is based on sound practices for identification and minimisation of risk. Another important challenge is to ensure that all personnel understand the entity's objectives. The control environment depends significantly upon the extent to which individuals appreciate that they will be held accountable.

- *Organisational structure*: the entity's structure needs to be organised to best carry out the strategies designed to achieve specific objectives and, in particular, to provide the necessary information flow to properly manage its activities.
- *Human resource policies and practices*: ongoing education and training in relation to, e.g., ethical conduct, roles and responsibilities, and technological and market developments are very important, as are performance feedback and appraisals and competitive compensation packages to hire competent staff.

(2) Risk assessment

As noted above (see paragraph B.2.2 above), *risk assessment* involves the identification and analysis of risks underlying the achievement of objectives, including risks relating to the changing regulatory and operating environment and business strategy, as a basis for determining how such risks should be mitigated and managed.

Setting objectives

Risk affects an entity's ability to survive and successfully compete. The board and management must decide how much risk can be prudently accepted and strive to maintain risk within this level. Setting objectives is a pre-condition to risk assessment and management. It is a prerequisite for and enabler of internal controls, although not a component as such.

It is important, therefore, that clear business objectives be set. These should be expressed around the future rather than the past or present and should be focused on achievable goals. The board should consider whether any existing objectives are able to meet the challenges that it is likely to face over, at least, the next two to three years.

By setting high level objectives at the entity level and more specific objectives at the activity level, an entity can identify factors that are critical to the achievement of goals.

Objectives can be defined in terms of the following broad categories, although some individual objectives may overlap between categories:

- *Operations objectives*: these relate to the achievement of an entity's fundamental mission and address the effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding resources against loss.
- *Financial reporting objectives*: these relate to the preparation of reliable published financial statements, including interim and summary financial reporting and related information. They are driven primarily by external requirements.
- *Compliance objectives*: these relate to adherence to laws, rules and regulations to which the entity is subject, such as requirements concerning markets (including continuing listing obligations and specific industry regulations), pricing, taxes, the environment, employee welfare and international trade.

Entity-wide objectives should be broken down into sub-objectives, consistent with the overall strategy and linked to activities throughout the organisation. Activity objectives also need to be clear and readily understood by the staff undertaking the relevant activities, and they should be measurable.

Risk identification and assessment

There are various techniques use to identify risks, including those developed by external and internal auditors to define the scope of their activities, periodic reviews of economic and industry factors affecting the business, senior management conferences and meetings with industry analysts. Whatever method(s) is/are adopted, the management needs to consider carefully the factors that contribute to or increase risk, including issues such as past experience of failure to meet objectives; quality of personnel; significant changes, such as increased competition; legislative, regulatory and personnel changes; market developments, and the significance of particular activities to the entity and their complexity.

Risk should also be identified at the activity level, which can help to focus risk assessment on major business units or functions and also contribute to maintaining acceptable levels at the entity-wide level.

Following the initial identification of the significant risks to the company achieving its objectives, it may be useful to consult throughout the company on issues such as:

- awareness of the company's business objectives, business strategy and related significant risks;
- the company's risk management policy;
- whether the control strategies adopted are effective and what needs to be done to put them into effect;
- the fundamentals of good risk management and internal control;
- ways in which improvements can be made in order to mitigate the significant risks affecting the ability of the company to achieve its business objectives; and
- changing behaviour.

This consultation can help to identify whether senior management has identified all the significant risks relevant to the objectives. It can also provide the board with a solid foundation for its review of the effectiveness of internal control and for its reporting to shareholders on control.

Following the identification of entity-wide and activity risks, a risk analysis should be performed. Once the significance and likelihood of risk have been assessed, the management needs to consider how the risk should be managed. Actions that can be taken to reduce the significance or likelihood of a risk occurring, depending upon the nature of the risk, range from, e.g., identifying alternative suppliers, to obtaining more relevant operating reports, to improving training programmes. Fundamental to risk assessment is a process to identify changed conditions and take action as necessary. Relevant changes could include matters such as the following:

- *Changes in operating conditions*: e.g., due to deregulation, increased public pressure on pricing, etc.

- *New personnel*: changes in key personnel; high staff turnover, putting greater pressure on training and supervision.
- *New information systems*: normally effective controls can break down when new systems are developed, especially under tight time constraints.
- *Unexpectedly rapid growth*: when operations expand significantly and quickly, existing control systems may be strained to breaking point.
- *New product lines or activities*: when an entity enters a business or engages in transactions with which it is not familiar, existing controls may be inadequate.
- *Corporate restructuring*: restructuring and cost-reduction programmes could result in a loss of staff and inadequate supervision and/or segregation of duties.
- *Overseas expansions*: expansion into foreign markets may bring about unique risks due to the differences in market conditions, local culture, etc.

Mechanisms to identify relevant and important changes should, as far as possible, be forward-looking and early warning systems should be in place to identify data signalling new risks.

Prioritising risks

Risks may be prioritised according to their impact and likelihood, e.g:

A. Require immediate action

B. Consider action and have a contingency plan

C. Consider action

D. Keep under periodic review

The impact should be considered not merely in financial terms, but more importantly, in terms of potential effect on the achievement of the company's objectives. Not all risks will be identified as significant. Non-significant risks should be reviewed regularly, particularly in the light of changing external events, to check that they remain non-significant.

Having identified and then prioritised the significant risks in gross terms, it is then helpful to determine for each of these, (a) do the directors wish to accept this risk, (b) what is the control strategy to avoid or mitigate the gross risk, (c) who is accountable for managing the risk and maintaining and monitoring the controls, (d) what is the residual risk, that is the risk remaining after the application of the control processes, and (e) what is the early warning mechanism?

Taking each of these points in turn:

(a) Each gross risk is considered in the context of the company's objectives. The board decides whether the identified risks exceed the benefits that will be obtained by achieving the objectives i.e., is it worthwhile to continue with a particular objective if the risks outweigh the reward? If the decision is to carry on, the board must decide how to respond to the risk by adopting specific control strategies.

(b) Control strategies include:

- accepting the risk;
- transferring the risk (e.g., passing it to another party by changing contractual terms);
- elimination (by adopting an exit strategy);
- control (by building control into the operational process, additional quality control, involving your best people in managing it);
- sharing the risk with another party; and
- insuring against some or all of the risk.

(c) Delegation of responsibility for managing risk in totality should not be allocated to a single individual. Ideally, it would be spread across those responsible for managing different business activities.

(d) Consideration could be given to determining the level of risk remaining after the application of the control strategy. A key point to note, as indicated above, is that it is not possible to eliminate risk entirely. A company needs to know its risk profile and how to manage it. Where there are risks, they need to be sensible risks and not reckless or ill-considered ones. The company's business objectives need to be appropriate to the risk appetite of the board. The board needs to determine its risk appetite, i.e., the amount of risk that it is willing to accept. This involves considering, for significant risks, whether the risk/reward ratio is appropriate.

(e) Early warning mechanisms are reporting processes which enable the board and senior management to be alerted before a problem becomes a disaster, and at a stage when action can be taken to mitigate or overcome the situation. "Key Risk Indicators" can be established (as a form of early warning mechanism), the idea being to give early indication of potential problems in order that corrective action may be taken promptly.

It should be noted that, while risk assessment is a part of the internal control system, the plans, programmes and other actions deemed necessary to address the risks are an essential part of the overall management process but are not regarded as an element of the internal control system.

(3) Control activities

As previously noted (see paragraph B.2.2 above), *control activities* comprise a diverse range of policies and procedures that help to ensure that relevant management directives are carried out and any actions that may be needed to address risks to achieving company objectives are taken. These may include approvals and verifications, reviews, safeguarding of assets and segregation of duties. Control activities can also be divided into operations, financial reporting and compliance, although there may be, on occasions, some overlap between them. Among the common control activities performed by personnel at different levels in an entity are the following:

- *Top-level reviews*: e.g., conducting reviews of actual performance versus budgets, forecasts, prior periods and competitors.
- *Direct functional or activity management*: reviews of performance reports conducted by managers in charge of functions or activities.
- *Information processing*: performing a variety of controls to check accuracy, completeness and authorisation of transactions, e.g., exception reports.
- *Physical controls*: ensuring equipment, inventories, securities and other assets are safeguarded and subjected to periodic checks.
- *Performance indicators*: carrying out analyses of different sets of data, operational or financial, and the relationships between them, and investigative and/or corrective action. By investigating unexpected results or unusual trends, the management can identify circumstances where the underlying activity objectives are in danger of not being achieved.
- *Segregation of duties*: dividing and segregating duties amongst different people, to strengthen checks and minimise the risk of errors or abuses.

Although, generally, the internal control processes of smaller entities may be less formal and more flexible, it is nevertheless important that relevant policies and the procedures for implementing them are carried out thoughtfully, conscientiously and consistently.

Assessing risk is only one part of the overall picture and along with risk assessment, the management needs to identify and put into effect actions needed to address the risks. Such actions also serve to focus attention on control activities, the aim of which is to ensure that the necessary actions are carried out in an effective and timely manner.

Given the critical reliance on information systems for financial and other data, controls are needed over such systems. These include what the COSO report refers to as (a) "general controls", i.e., controls to ensure the continued proper operation of the system, such as back-up and recovery procedures, contingency or disaster recovery planning, and system security; and (b) "application controls", which include steps within the application software and related manual procedures to control the processing of various types of transactions.

(4) Information and communication

As previously noted (see paragraph B.2.2 above), *information and communication* refers to effective processes and systems that identify, capture and report operational, financial and compliance-related information in a form and time frame that enable people to carry out their responsibilities. This includes, in its broadest sense, communication from the top about the importance of control-related matters and the role of individuals, channels for communicating significant information upstream, and also effective communication with external stakeholders.

Information

Relevant information must be identified, captured and communicated in a form and time frame to enable people to make decisions and act on it.

Information systems provide operational, financial and compliance-related information, both internally-generated and external, that facilitates the running and control of a business and is necessary for informed decision-making and external reporting.

Such systems must be able to adapt with the need to support new entity objectives in the face of fundamental industry changes, particularly in industries that are very innovative and fast-moving.

Information systems can be formal or informal. The latter could include discussions with customers, suppliers, regulators and employees, which can provide useful information to assist in the identification of risks and opportunities. Attendance at business seminars and membership of trade, professional and other bodies can also provide a source of relevant information.

The quality of system-generated information affects the ability of the management to make appropriate decisions. It is critical that reports contain sufficient relevant data to support effective control and the system design should address this. The quality of information requires ascertaining the answers to questions such as:

- *Content*: Is the content appropriate?
- *Timeliness*: Is it available when required?
- *Up-to-date*: Is it the latest information?
- *Accuracy/reliability*: Is it correct and reliable?
- *Accessibility*: Can all relevant parties access it easily?

Communication

More broadly, effective communication must flow in all directions throughout the organisation. Employees should be given a clear message from the senior management that control responsibilities must be taken seriously. They must understand their own role in the internal control system and how individual activities relate to the work of others. They must also have a means of communicating significant information upstream, which entails having open channels of communication and a willingness on the part of more senior personnel to listen. An environment in which employees fear reprisals for reporting relevant information will defeat the object.

Personnel should be made aware that, whenever the unexpected occurs, attention should be given not only to the event itself, but also to determining the cause. They need to know how their activities relate to the work of others and what behaviour is expected or acceptable, and what is not.

Communication between the management and the board and board committees is critical. The management must keep the board up to date on performance, developments, significant risks, major initiatives and other relevant issues. The board, in turn, should communicate to management what information it needs and should provide direction and feedback.

There is also a need for effective communication with external parties, such as shareholders, customers, suppliers and regulators. Customers and suppliers can provide very useful input on, e.g., the design and quality of products and services, and communications from external parties, such as external auditors and regulators, can provide valuable feedback on the functioning of an entity's internal control system. Open communication with shareholders, financial analysts, etc., can point to the information that is relevant to their needs.

(5) Monitoring

Internal control systems need to be monitored. As noted above (see paragraph B.2.2), *monitoring* entails a process that assesses the quality of the internal control system's performance over time. This is accomplished through ongoing monitoring activities and/or separate evaluations. Deficiencies in internal control should be reported to the appropriate level upstream, which may be, for example, senior management, the audit committee, or the board.

Monitoring ensures that internal control continues to operate effectively. It involves assessment by appropriate personnel of the design and operation of controls and the taking of suitable follow-up action. It applies to activities within an entity and may also apply to outside contractors that provide relevant services to the entity.

The frequency of separate evaluations needed for management to have a reasonable assurance about the effectiveness of the internal control system, is a matter of judgement. Relevant factors would include: the nature and degree of changes occurring and their associated risks, the competence and experience of personnel implementing the controls, and the results of ongoing monitoring. As ongoing monitoring procedures are built into the recurring operating activities of an entity, are performed on a real-time basis and should be reacting to changes, in principle, they should be more effective than procedures performed in connection with separate evaluations.

Who to evaluate?

Often evaluations will take the form of a self-assessment, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. The chief executive of a division might initiate the evaluation and personally assess the control environment factors. Line managers might focus primarily on operations and compliance objectives and the divisional controller might focus on the financial reporting objectives. The corporate management would review the division's assessment, together with the evaluations of other divisions.

Internal auditors usually perform internal control evaluations as part of their regular duties, or upon request by the board or senior management. The work of the external auditors may also be used in considering the effectiveness of internal control.

Documentation

The extent to which the system of internal control is documented may vary with the entity's size, complexity, etc. Larger organisations are more likely to have written policy manuals, formal organisation charts, written job descriptions, operating instructions, information system flowcharts and so on. Smaller companies are likely to have less documentation, although this does not necessarily mean that their internal control is less effective. However, an appropriate level of documentation can make an evaluation more efficient. It also facilitates employees' understanding of how the system works and their role in it, and it makes it easier to modify the system when necessary.

Reporting deficiencies

All internal control deficiencies that can affect the entity's attainment of its objectives should be reported to those who are in a position to take necessary action.

Information generated by employees in conducting regular operating activities is usually reported through normal channels to their supervisor, who may in turn report it upstream or laterally, as appropriate. There should be an alternative channel for reporting very sensitive information, such as illegal or improper acts. Findings of deficiencies should usually be reported not only to the individual responsible for the function or activity involved, who is able to take corrective action, but also to at least one level of management above that person. This procedure enables more senior level oversight and support for taking corrective action and facilitates communication to others within the organisation whose activities may also be affected.

Providing information on internal control deficiencies to the right party is critical to the continued effectiveness of the system. Protocols can be established to identify what information is needed at a particular level for decision-making. Parties to whom deficiencies are to be communicated may prescribe specific directives regarding information to be reported. The board or audit committee, for example, may ask the management, or the internal or external auditors, to communicate only those findings of deficiencies that reach a certain threshold of seriousness or importance.

APPENDIX III

Possible risks faced by a company

Business risks

- Wrong business strategy
- Competitive pressure on price / market share
- General / regional economic problems
- Industry sector in decline
- Political risks
- Adverse government policy
- Inattention to information technology (IT) aspects of strategy and implementation
- Obsolescence of technology
- Substitute products
- Takeover target
- Inability to obtain further capital
- Bad acquisition
- Too slow to innovate and reengineering
- Too slow to respond to demands from market and customers

Financial risks

- Market risk
- Credit risk
- Interest risk
- Currency risk
- Treasury risk
- Liquidity risk
- Overtrading
- High cost of capital
- Misuse of financial resources
- Going concern problems
- Occurrence of types of fraud to which the business is susceptible
- Misstatement risk related to published financial information
- Breakdown of accounting system
- Unreliable accounting records
- Unrecorded liabilities
- Penetration and attack of IT systems by hackers
- Decisions based on incomplete or faulty information
- Too much data and not enough analysis
- Unfulfilled promises/pledges to investors

Compliance risks

- Breach of Listing Rules
- Breach of financial regulations
- Breach of Companies Ordinance requirements
- Breach of competition regulations

- Breach of other regulations and laws
- Litigation risk
- Tax problems
- Health and safety risks
- Environmental problems

Operational and other risks

- Inefficient / ineffective management process
- Business processes not aligned to customer / market demand and strategic goals
- Loss of entrepreneurial spirit
- Missed or ignored business opportunities
- Other business probity issues
- Other issues giving rise to reputational problems
- Poor brand management
- Failure of major change initiative
- Inability to implement change
- Stock-out of raw materials
- Skills shortage
- Physical disasters (e.g., fire and explosion)
- Computer viruses or other system malfunctions
- Failure to create and exploit intangible assets
- Loss of intangible assets
- Loss of physical assets
- Loss of key people
- Loss of key contracts
- Lack of orders
- Lack of business continuity
- Succession problems
- Inability to reduce cost base
- Over-reliance on key suppliers or customers
- Onerous contract obligations imposed by major customers
- Failure of new products or services
- Failure to satisfy customers
- Poor service levels
- Quality problems
- Product liability
- Failure of major projects
- Failure of big technology related projects
- Failure of outsource providers to deliver
- Lack of employee motivation or efficiency
- Industrial action
- Problems arising from exploiting employees in developing countries
- Inefficient / ineffective processing of documents
- Breach of confidentiality

Adapted from *Implementing Turnbull – A Boardroom Briefing*, ICAEW

APPENDIX IV

Bibliography and other references

1. *A Guide For Effective Audit Committees (2002)*
   Hong Kong Institute of Certified Public Accountants

2. *Rules Governing the Listing of Securities on The Stock Exchange of Hong Kong Limited ("Main Board Listing Rules")*
   The Stock Exchange of Hong Kong Limited

3. *Rules Governing the Listing of Securities on the Growth Enterprise Market of The Stock Exchange of Hong Kong Limited ("GEM Listing Rules")*
   The Stock Exchange of Hong Kong Limited

4. *Report of the Committee on the Financial Aspects of Corporate Governance ("Cadbury Report") (1992)*
   Committee on the Financial Aspects of Corporate Governance ("Cadbury Committee"), UK

5. *Internal Control and Financial Reporting: Guidance for directors of listed companies registered in the UK ("Rutteman Guidance") (1994)*
   Rutteman Working Group, UK

6. *Committee on Corporate Governance: Final Report ("Hampel Report") (1998)*
   Committee on Corporate Governance, UK

7. *Internal Control: Guidance for Directors on the Combined Code ("Turnbull Guidance") (1999)*
   The Institute of Chartered Accountants in England and Wales, UK

8. *Implementing Turnbull – A Boardroom Briefing*
   The Institute of Chartered Accountants in England and Wales, UK

9. *Internal Control – Integrated Framework (1992)*
   Committee of Sponsoring Organizations of the Treadway Commission, US

10. *Board Briefing on IT Governance, 2nd Edition (2003)*
    IT Governance Institute, US

11. *Enterprise Risk Management – Integrated Framework (2004)*
    Committee of Sponsoring Organizations of the Treadway Commission, US

12. *Internal Control Reporting – Implementing Sarbanes-Oxley Section 404 (2004)*
American Institute of Certified Public Accountants

13. *Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports – Frequently Asked Questions (2004)*
Office of the Chief Accountant Division of Corporation Finance, U.S. Securities and Exchange Commission

14. *Guidance on Control (1995)*
The Risk Management and Governance Board (previously known as the Criteria of Control Board), Canadian Institute of Chartered Accountants, Canada

15. *International Standards for the Professional Practice of Internal Auditing*
The Institute of Internal Auditors

Hong Kong Institute of Certified Public Accountants
Tel: (852) 2287 7228
Fax: (852) 2865 6603
Email: hkicpa@hkicpa.org.hk
Website: www.hkicpa.org.hk