Professional Accountants in Business Committee

Information Paper
August 2006

Internal Controls—A Review of Current Developments

International Federation of Accountants

Professional Accountants in Business Committee
International Federation of Accountants
545 Fifth Avenue, 14th Floor
New York, New York 10017 USA

This information paper was prepared by the Professional Accountants in Business (PAIB) Committee of the International Federation of Accountants (IFAC). The PAIB Committee serves IFAC member bodies and the more than one million professional accountants worldwide who work in commerce, industry, the public sector, education, and the not-for-profit sector. Its aim is to enhance the role of professional accountants in business by encouraging and facilitating the global development and exchange of knowledge and best practices.

This information paper may be downloaded free-of-charge from the IFAC website: http://www.ifac.org. The approved text is published in the English language.

The mission of IFAC is to serve the public interest, strengthen the worldwide accountancy profession and contribute to the development of strong international economies by establishing and promoting adherence to high-quality professional standards, furthering the international convergence of such standards and speaking out on public interest issues where the profession's expertise is most relevant.

INTERNAL CONTROLS—A REVIEW OF CURRENT DEVELOPMENTS

CONTENTS

INTERNAL CONTROLS—A REVIEW OF CURRENT DEVELOPMENTS

1. Introduction and Context

Following the publication of their information paper entitled *Enterprise Governance—Getting the Balance Right*, the Professional Accountants in Business (PAIB) Committee of the International Federation of Accountants (IFAC) issued an exposure draft entitled *Guidance for the Development of a Code of Conduct*. Extending its work in the governance area, the PAIB Committee has included internal control in its work program as a major area of activity. The first phase of this program is a scene setting article briefly describing much of the current guidance available and the regulatory regime surrounding the topic.

As the severity of high-profile corporate accounting failures has increased steadily over the last decade, there has been a corresponding increase in the development of new legislation, standards, codes and guidelines to assist organizations in improving their corporate governance. While these standards and guidelines originated from a variety of sources, they share a core principle: that good governance, by its nature, demands effective systems of internal control.

Recognition of the critical importance of internal control is evident in the key frameworks and guidelines on the subject. In the 1990s internal control frameworks such as the COSO[1] (USA), Turnbull[2] (UK) and CoCo[3] (Canada) emerged, some of which have recently been reviewed and updated or supplemented. In addition, there are many other publications on the theory and benefits of internal control.

Corporate governance and internal control became a highly pertinent and topical business issue at the beginning of the 21st century following a series of large corporate scandals and failures. These failures led to calls for enhanced corporate governance, risk management and internal control. Governments and legislators, regulators, and standard setting groups came under increasing pressure to take measures to assist in preventing similar shareholder losses from occurring in the future.

In response, various new laws, regulations and listing standards were issued. One such example is the US Sarbanes-Oxley Act of 2002—commonly known as SOX—in which Section 404 requires that companies registered with the US SEC report on their internal controls over financial reporting. The requirements are prescriptive, focusing on compliance and accountability. At that time, there were concerns that this would become the international "standard" for internal control, particularly as all companies in the US and elsewhere registered with the SEC were required to comply with Section 404, albeit with varying implementation timetables. This heavy emphasis on SOX, in particular the need to comply with its reporting requirements, meant that the internal control debate was being driven primarily from a compliance viewpoint.

---

1 *Internal Control—Integrated Framework (1992),* Committee of Sponsoring Organizations of the Treadway Commission, US

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

3 *Guidance on Control (1995),* Canadian Institute of Chartered Accountants, Canada

This document reviews current developments and some of the latest thinking in the area of internal control, while setting the recent US legislation in context.

1.1 General Comments

Shareholders expect those charged with governance of the company to manage the significant risks the company is facing and to put controls in place to deal with such risks. These risks encompass those risks related to business operations as well as risks related to compliance with laws and regulations, and financial reporting.

A company's system of internal control therefore has a key role in the management of risks that are significant to the fulfillment of its business objectives. A sound system of internal control contributes to safeguarding the shareholders' investment and the company's assets.

A company's objectives, its internal organization and the environment in which it operates are continually evolving and, as a result, the risks it faces are continually changing. A sound system of internal control therefore depends on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed. Since profits 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.

2. Internal Control Pre-2002

A number of key internal control frameworks, such as the COSO (USA), Turnbull (UK), and CoCo (Canada), were developed prior to the high-profile accounting scandals at the turn of the century. These frameworks described internal control as a "process" established, operated and monitored by those charged with the governance and management of a company, to provide reasonable assurance regarding the achievement of the company's objectives. The term process is used in a broad sense; it goes beyond procedures to include elements such as corporate culture and policies, as well as systems and tasks.

COSO's Internal Control Integrated Framework (1992) and Turnbull's Guidance on Internal Control (1999) both took a much broader approach to internal control than Sarbanes-Oxley, in terms of scope, objectives and approach. They focused on all controls covering the company's entire range of activities and operations, not just those directly related to financial reporting and adopted a risk-based approach to internal control.

2.1 The Committee of Sponsoring Organizations of the Treadway Commission

In 1992, The Committee of Sponsoring Organizations of the Treadway Commission (COSO[4]) defined 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.*

[4] The sponsoring organizations include the American Accounting Association, the American Institute of Certified Public Accountants, the Financial Executives International, the Institute of Management Accountants and the Institute of Internal Auditors.

- *Reliability of financial reporting.*
- *Compliance with applicable laws and regulations.*

This is very similar to the definition used in the other two key frameworks established in the 1990s.

COSO stated that internal control consists of five interrelated components which are derived from the way management runs a business and are integrated with the management process. They apply to entities of all sizes, although smaller organizations are likely to implement them in a more informal manner. The components are:

Control Environment—This sets the tone for the organization, providing the foundation for all other components of internal control. It includes integrity, ethical values and the competence of the people.

Risk Assessment—This is the identification and analysis of relevant risks, internal and external, to the achievement of the objectives, forming a basis for determining how the risks should be managed.

Control Activities—These help ensure that the necessary actions are taken to address risks relating to the achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions.

Information and Communication—Internal and external information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also must occur in a broader sense, flowing down, across and up the organization.

Monitoring—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.

COSO states that:

> *There is synergy and linkage among these components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons. Internal control is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise. "Built in" controls support quality and empowerment initiatives, avoid unnecessary costs and enable quick response to changing conditions.*

2.2 Internal Control: Guidance for Directors on the Combined Code

Internal Control: Guidance for Directors on the Combined Code,[5] commonly referred to as Turnbull guidance, was issued by the Institute of Chartered Accountants of England and Wales

[5] *Internal Control: Guidance for Directors on the Combined Code (1999)*, Institute of Chartered Accountants in England and Wales, UK

(ICAEW) at the request of the London Stock Exchange to provide guidance to directors of listed companies in implementing the requirements in the Combined Code[6] relating to internal control.

The Turnbull guidance views internal control as a system which encompasses the policies, processes, tasks, behaviors 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;
- Help ensure the quality of internal and external reporting; and
- Help ensure compliance with applicable laws and regulations, as well as internal policies with respect to the conduct of business.

Turnbull strongly favors a principles-based approach in which, reflecting sound business practice, internal control is embedded in the organization's business processes, whilst remaining relevant over time and through the organization's changing circumstances. It argues that internal control should be incorporated within the normal management and governance processes of an organization and not treated as a separate exercise undertaken to meet regulatory requirements. Turnbull strongly emphasizes that the guidance is intended to enable application in a manner which takes account of each company's particular circumstances. Turnbull further states that, "For the purposes of this guidance, internal controls considered by the board should include all types of controls including those of an operational and compliance nature, as well as internal financial controls."

Turnbull places responsibility for managing risk firmly at board level, requiring a company's board to take a risk-based approach to establishing a system of internal control. It also notes management's role in implementing board policies on internal control, and that all employees have some responsibility for internal control as part of their accountability for achieving objectives.

2.3 CICA's Criteria of Control Board Guidance on Control

CICA's Criteria of Control Board Guidance on Control (CoCo) defines control as comprising "those elements of an organization (including its resources, systems, processes, culture and tasks) that, taken together, support people in the achievement of the organization's objectives." This guidance defines control and sets out criteria that can be used to assess the effectiveness of control. Control is seen as encompassing the entire organization starting with its smallest unit, the individual person. CoCo uses four essential elements as groupings within which it articulates 20 criteria of control.

Purpose criteria provide a sense of the organization's direction. They address its objectives, risks and opportunities, policies, planning and performance targets and indicators.

Commitment criteria provide a sense of the organization's identity and address its ethical values, human resource policies, authority, responsibility and accountability and mutual trust.

---

[6] *Combined Code on Corporate Governance* ("the Combined Code"), Financial Reporting Council, UK

Capability criteria provide a sense of the organization's competence. They deal with knowledge, skills and tools, communication processes, information, co-ordination and control activities.

Monitoring and Learning criteria provide a sense of the organization's evolution. They involve reviewing internal and external environments, monitoring performance against targets, challenging assumptions, reassessing information needs and systems, establishing follow-up procedures and assessing the effectiveness of control.

These criteria are interrelated and together they provide the framework for looking at the whole organization from a control perspective. The guidance is intended to be useful in making judgments about designing, assessing and reporting on control. It is not intended as prescriptive minimum requirements.

2.4 Comparison of COSO, CoCo and Turnbull

As internal control frameworks, COSO, Turnbull and CoCo complement each other. They each see internal control as a process/set of processes designed to facilitate and support the achievement of business objectives. Each of the frameworks takes the wider approach to internal control covering consideration of significant risks in operations, compliance and financial reporting. Objectives such as improving business effectiveness are included, as are compliance and reporting objectives. The narrow approach to internal control is usually restricted to internal control over financial reporting.

Underlying each of the three frameworks is the fundamental principle that effective internal control is a process effected by people that supports the organization in several ways, enabling it to provide reasonable assurance regarding risk and to assist in the achievement of objectives.

Fundamental to each of the frameworks is that internal control is integral to the activities of the company, and not something practiced in remote corners.

2.5 Control Objectives for Information and Related Technology

The application of information technology (IT) has become central to the strategy and business processes of many entities. So, just as IT has become an integral part of the business, IT governance is now seen as an integral part of enterprise governance.

In recognition of the importance of IT governance, an IT governance framework, *Control Objectives for Information and Related Technology*[7] (COBIT) was developed in 1996 as a reference framework for developing and managing internal controls and appropriate levels of security in IT. COBIT provides a set of generally accepted IT control objectives to assist entities in maximizing the benefits derived through the use of IT and developing the appropriate IT governance and control in a company. COBIT supports IT governance by providing a framework to ensure that:

- IT is aligned with the business;
- IT enables the business and maximizes benefits;

[7] *Control Objectives for Information and Related Technology (1996),* IT Governance Institute and the Information Systems, Audit and Control Foundation, US

- IT resources are used responsibly; and
- IT risks are managed appropriately.

COBIT adapted its definition of internal control from COSO*: "the set of policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives are achieved and that undesirable events are prevented, detected and corrected."*

While COSO and Turnbull focus on the achievement of business objectives at the overall entity level, COBIT focuses specifically on information technology. Therefore while the concept of internal control presented in COBIT complements the other two frameworks, it applies this concept to controls over IT, and not the business as a whole.

3. 2002: the Sarbanes-Oxley Act in the US

In the early 2000s, a number of high-profile corporate accounting scandals resulted in some investors, company personnel and other stakeholders suffering significant losses. These scandals resulted in demands for a greater emphasis on corporate governance. In the US this has led to what many observers have seen as hastily prepared, radical and sometimes controversial new legislation that would significantly impact US corporate governance, aspects of reporting and the practice of public accounting. It has had ramifications in a number of countries outside the US.

In July 2002, the United States Congress passed the Sarbanes-Oxley Act (SOX) in an effort to reduce public concern over a number of high profile corporate failures in the US. It was hoped that SOX would assuage the concerns of investors and restore confidence in corporate reporting. The official title of SOX is in itself informative: "An Act to Protect Investors by Improving the Accuracy and Reliability of Corporate Disclosures made Pursuant to the Securities Laws and for other Purposes."

The main requirements were, in addition to the rules regarding internal control, covered in ensuing paragraphs which addressed:

- Independent audit committees;
- Various certifications by "signing officers" to be included in periodic financial reports under S302 of SOX;
- Codes of Conduct, whistle-blowing procedures; and
- Greater involvement of boards and audit committees in control activities.

SOX was far-reaching and contained many new regulations. Of particular interest to this document were the new rules regarding the reporting of evaluations related to internal control over financial reporting. These were required by Section 404(a): Management Assessment of Internal Controls which requires each annual report of an issuer to contain an "internal control report," which shall:

- State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

- Contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

In addition, SOX, via Section 404(b) which covers Internal Control Evaluation and Reporting, requires, that the organization's auditor shall "attest to, and report on the assessment made by management" in respect of the internal control assessment. 404(b) noted that the attestation shall be made in accordance with standards for attestation engagements issued by the Public Company Accounting Oversight Board and that any such attestation shall not be the subject of a separate engagement. In June 2004, the PCAOB issued Auditing Standard Number 2, *An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements.*

SOX applies to all companies worldwide that are registered with the Securities and Exchange Commission (SEC) and its implementation can be time consuming and costly. The new SEC rules brought about by SOX focused on internal control in relation to financial reporting and on the controls over information filed with the SEC.

SOX focuses on one specific aspect of internal control, that related to internal control over financial reporting whereas, as been previously noted, the key internal control frameworks such as COSO, Turnbull and CoCo take a wider business-led approach and cover all controls. Assessments of internal control using the SOX definition are less likely to focus on the business benefits that can result from a review of the wider aspects of internal control and the related processes for risk management.

As discussed later in this document, the emphasis of SOX on the compliance and reporting aspects of internal control led to concern that it would undermine the importance of internal control in business performance.

The US SEC has published a Concept Release as a prelude to forthcoming guidance for management in assessing a company's internal controls for financial reporting. It can be found online at http://www.sec.gov/news/press/2006/2006-112.htm.

4. Recent Developments in Internal Control

Since 2002, a number of bodies around the world have looked at current guidelines and best practice in the area of internal control in response to the same business scandals that prompted SOX. In the UK during 2004 and 2005, the Turnbull Review Group reviewed the 1999 guidance, making very few changes. In Hong Kong, the Hong Kong Institute of Certified Public Accountants (HKICPA) produced a document entitled *Internal Control and Risk Management—A Basic Framework* in June 2005. In the US in 2004, COSO produced the *COSO Enterprise Risk Management—Integrated Framework,* which supplements the 1992 internal control framework.

At a European level, the Fédération des Expert Comptables Européens (FEE) produced a discussion paper in March 2005 which includes a review of best practice amongst companies in risk management and internal control, a review of regulatory developments in the US and EU in response to the high-profile accounting scandals, and a survey of regulatory requirements on risk management and internal control in EU Member States.

4.1 Turnbull Review 2004–2005

The Turnbull Review Group of the Financial Reporting Council (FRC) conducted a substantial evidence-based review of the impact of the Turnbull guidance since its introduction in 1999, and considered whether it needed to be updated.

In December 2004, the Review Group issued an evidence gathering consultation paper. The evidence gathered from responses and from other sources represented the views and experience of a significant proportion of the London market, including companies and investors as well as auditors. These views carried considerable weight in determining whether any changes were needed.

There was a strong degree of consistency of opinion on the main issues, with the overwhelming view being that the Turnbull guidance had contributed to better understanding and management of risk and improvements in internal control in UK listed companies. It was the strong view of both companies and investors that this success was in large part attributable to the breadth and principles-based approach of the guidance.

By covering all material controls and linking internal control to risk management, it allowed companies to focus on the most significant risks facing them. By setting out high-level principles rather than detailed processes, it required boards to think broadly about their company's risks and enabled them to apply the guidance in a way that suited the circumstances of their company.

The Review Group considered whether the disclosure requirements of Section 404 of SOX would constitute an appropriate model for disclosures made in the UK under the Combined Code and Turnbull guidance, and concluded that they did not. There was little encouragement from investors for Section 404 style disclosures, and the Review Group concluded that the potential benefit of such a statement to shareholders was not sufficient to outweigh the associated costs.

However, the Review Group considered that companies should be encouraged to make the internal control statement more informative for shareholders.

The Review Group also considered whether the remit of the external auditor should be extended beyond the existing requirements which are to review the board's internal control compliance statement, drawing also on the knowledge of the company that they have obtained during the audit of the financial statements. There is no requirement on the auditor to express a view publicly on the effectiveness of the company's internal control system.

There was virtually no demand from investors or companies for an increased role for external auditors. The existing powers and remit of the external auditors were considered sufficient; in particular, there was no support for the external auditor being required to attest as to the effectiveness of the company's internal controls. The Review Group therefore recommended that there should be no expansion of the external auditors' responsibilities in relation to the company's internal control statement.

Only limited changes were made to the Turnbull guidance. The most significant of these relate to disclosure. Boards will now be required to confirm in the annual report that necessary action has

been or is being taken to remedy any significant failings or weaknesses identified from their review of the effectiveness of the internal control system, and to include in the annual report such information as they consider necessary to assist shareholders' understanding of the main features of the company's risk management processes and system of internal control.

The Review Group published its conclusions and began consultation on proposed changes to the Turnbull guidance in June 2005. These changes enjoyed broad support, with the result that revised guidance was issued in October 2005, to apply to financial years beginning on or after January 1, 2006.

4.2 COSO Enterprise Risk Management—Integrated Framework

In 2004, after a long period of development COSO supplemented its 1992 internal control framework with an additional framework to cover risk management and strategic risks and labeled the approach Enterprise Risk Management (ERM).

The ERM framework recognizes that an effective enterprise risk management process must be applied within the context of strategy setting. It starts with the top of the organization and supports the organization's major mission.

This framework defines internal control as an integral part of risk management. It sees risk management as concerned with the wider external and internal risks relevant to the determination of the entity's strategy to reach its objectives. It also sees internal control as part of that process, whereby internal control structures and procedures are instrumental in ensuring these objectives are achieved. The framework defines enterprise risk management as follows:

> *Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*

The key point here is that, as in the Turnbull guidance, those charged with governance should adopt a risk-based approach to internal control and any internal assessment of its effectiveness. COSO ERM believes that this approach should be incorporated into the strategic, governance and management processes of the company and should encompass the wider aspects of internal control, not just those directly related to financial reporting.

4.3 COBIT Version 4.0

COBIT, the IT governance framework that allows managers to bridge the gap between control requirements, technical issues and business risks, was first released in 1996 and has since been researched and updated.

The fourth edition, released in late 2005, is the first update since 2000, and emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment of IT operations with business operations, and supports continuous improvement in IT governance. It underlines the importance of continuous improvement and adding value in addition to regulatory compliance.

4.4 The Fédération des Experts Comptables Européens

In July 2003, The Fédération des Experts Comptables Européens (FEE) emphasized the business case for risk management in its *Discussion Paper on the Financial Reporting and Auditing Aspects of Corporate Governance.*[8] "Systems of internal control and risk management are fundamental to the successful operation of any company, not only for financial reporting purposes but also for the day-today running of the company to help it achieve its business objectives."

In its March 2005 *Discussion Paper on Risk Management and Internal Control in the EU*, FEE stated that it is not supportive of implementing an EU equivalent of Sarbanes-Oxley Section 404 in Europe. It argues that there are alternatives to hard and fast legal requirements, which can be more efficient in bringing about changes in behavior, particularly in jurisdictions where shareholders have effective powers.

It instead advocates mechanisms that encourage wider risk management and internal control. FEE sees the need to promote discussion and evidence gathering to encourage coordination and convergence of the development of risk management and internal control at EU level.

4.5 Developments in Some Other Countries

4.5.1 Hong Kong Institute of Certified Public Accountants

The Hong Kong Stock Exchange issued the *Code on Corporate Governance Practices* ("the Code," effective for accounting periods after January 1, 2005) and the *Corporate Governance Report* (the disclosure elements of which are effective after July 1, 2005) in November 2004.

The Code requires sound and effective internal control systems to be maintained and also requires that directors should at least annually review the effectiveness of their internal control systems. That review should cover all material controls, including financial, operational and compliance controls as well as risk management functions.

The Hong Kong Stock Exchange, in developing the Code, took into account the revised *Combined Code on Corporate Governance* ("the Combined Code") issued by the Financial Reporting Council in the United Kingdom in July 2003.

The HKICPA document, *Internal Control and Risk Management—A Basic Framework* (June 2005) was developed at the invitation of the Stock Exchange and focuses on allowing companies to develop their own internal control systems that have regard to the specific characteristics and circumstances of their business. It is intended to help improve an understanding of the conceptual framework of internal control and risk management; to help provide a framework/basis that can be used to develop and assess the effectiveness of internal control in a company; and to reflect sound business practice whereby internal control is embedded in the business and management processes by which a company pursues its objectives

[8] http://www.fee.be

The HKICPA guide draws on the UK Turnbull Guide whilst taking into account the local Hong Kong market and business structures and also uses the COSO definition of internal control and the portions of its conceptual framework that are relevant.

4.5.2 The King Report on Corporate Governance for South Africa

The King Report on Corporate Governance for South Africa was published in 2002 and recommends that:

> *The board should make use of generally recognized risk management and internal control models and frameworks in order to maintain a sound system of risk management and internal control to provide a reasonable assurance regarding the achievement of organizational objectives with respect to:*
>
> - *effectiveness and efficiency of operations;*
> - *safeguarding of the company's assets (including information);*
> - *compliance with applicable laws, regulations and supervisory requirements;*
> - *supporting business sustainability under normal as well as adverse operating conditions;*
> - *reliability of reporting; and*
> - *behaving responsibly towards all stakeholders.*

Again the King Report recommends that risk management and internal control should be practiced throughout the company by all staff, and should be embedded in day-to-day activities.

4.5.3 Corporate Governance and Internal Control in The Netherlands

The Dutch approach is based on managing and controlling, responsibility and right of say, and on accountability and supervision. Integrity and transparency are key issues. The strength of internal control is based on creating checks and balances between key stakeholders and by identifying separate responsibilities for the:

- (Independent) Supervisory Board;
- Management Board (Two tier board system);
- Annual Meeting of Shareholders; and
- External Auditor.

Corporate governance and internal control was formalized in 1997 by the Peter's Committee report, *Corporate Governance in the Netherlands: the Forty Recommendations*. The report provided voluntary recommendations applicable to both listed and other types of enterprises, including not-for-profit.

The implementation of its recommendations was reviewed in 2002 in the report, *Corporate Governance in The Netherlands 2002: the state of affairs*. This report identified the following areas as requiring improvement: discussion in the annual report of the strategic direction of the company, risk management, review of internal control systems and performance of the Supervisory Board. It also identified a lack of shareholder activism in following up companies' implementation of the recommendations. The report concluded that the principles of corporate governance and internal control needed legal enforcement.

Consequently, the forty recommendations from the Peters Committee have been replaced in 2003 by *The Dutch Corporate Governance Code* developed by the Tabaksblat Committee, which was chaired by the former CEO of Unilever, Morris Tabaksblat. The corporate governance principles in the Code reflect the latest views on good corporate governance which now enjoy wide support. Listed companies are obligated to explain in their annual report whether, and if so why and to what extent, they do not apply the best practice provisions of the corporate governance code i.e., the "comply or explain" principle. This is legally enforced by Dutch civil law and compliance to the Code also requires approval by the general meeting of shareholders.

Best practice provisions create a set of standards governing the conduct of management board and supervisory board members (also in relation to the external auditor) and shareholders. They reflect the national and international best practice and may be regarded as an elaboration of the general principles of good corporate governance.

These provisions state that the management board will mention in the annual report the main elements of:

(a) The operational and financial objectives of the company;

(b) The strategy designed to achieve the objectives; and

(c) The parameters to be applied in relation to the strategy.

Provisions also state the company shall have an internal risk management and control system that is suitable for the company. It shall, in any event, employ as instruments of the internal risk and management and control system:

(a) Risk analyses of the operational and financial objectives of the company;

(b) A code of conduct which should be published on the company's website;

(c) Guides for the layout of the financial reports and the procedures to be followed in drawing up the reports; and

(d) A system of monitoring and reporting.

According to the provisions, the management board shall declare in the annual report that the internal risk management and control systems are adequate and effective and shall provide clear substantiation of this. In the annual report, the management board shall report on the operation of the internal risk management and control system during the year under review. In doing so, it must describe any significant changes that have been made and any major improvements that are planned, and confirm that these have been discussed with the audit committee and the supervisory board.

5. Enterprise Governance

In 2004 IFAC, in co-operation with the Chartered Institute of Management Accountants (CIMA), published a report entitled *Enterprise Governance—Getting the Balance Right*. This report focused on the reasons corporate governance failed in certain organizations and, more importantly, what is required to avoid such failures and "get it right."

The report used the Information Systems Audit and Control Foundation's definition of enterprise governance which is "the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly."

Enterprise governance constitutes the entire accountability framework of the organization. There are two dimensions of enterprise governance: conformance and performance. Conformance covers issues such as board structures and roles, executive remuneration, and compliance with regulation. The conformance dimension focuses on accountability and assurance while the performance dimension focuses on strategy and value creation.

At the heart of enterprise governance is the argument that good corporate governance (i.e., meeting conformance objectives) on its own cannot make a company successful. Companies must balance conformance with performance. While the conformance dimension is essential, its focus should also be on helping the board to make strategic decisions through understanding its appetite for risk and its key drivers of performance, and identifying its key points of decision-making.

The joint IFAC/CIMA report emphasizes the importance of enterprise risk management (ERM), whereby strategic risks are considered at all times in the strategic process. COSO's ERM framework is referred to as a means of developing the risk element of enterprise governance risk management. ERM reconciles both:

- The assurance requirements of the board and external interests (i.e., that the business understands its risks and is managing them actively) —conformance; and
- The need to better integrate risk management in decision-making activity at all levels—performance.

It is clear that the overriding belief is that the primary objective of the governance and internal control processes should not be to report and disclose what is happening within the business, but to improve the performance of the business.

Internal control, therefore, sits within this framework on the conformance side but also contributes significantly to performance through the provision of relevant, pro-active information that determines whether or not strategic objectives can be achieved.

IFAC responded to the FEE Discussion Paper[9] supporting FEE's conclusion that regulation along the lines of SOX is inappropriate. The response emphasized that an appropriate balance must be struck between conformance and performance and that the compliance and reporting aspects of risk management and internal control should not be overemphasized. FEE subsequently noted that the debate remains open on the best model for corporate reporting on risk management and internal controls and that practice continues to evolve where Section 404 of SOX applies.

[9] http://www.fee.be/fileupload/upload/PAIB2742006481424.pdf

The IFAC response also emphasized that good governance, risk management and internal control are important in all entities, whether a small or medium sized enterprise or large listed company. IFAC argued the importance of international debate as to what risk management and internal control comprise and how they may be improved. This would be better facilitated through an inclusive approach that is applicable to all entities, large and small.

6. Convergence of Thinking on Internal Control

It is important to note that the over the past 12 to 18 months, the majority of outputs on internal control have agreed on a principles-based, risk-focused approach and there have been no recommendations of note for the introduction of prescriptive or legislative requirements as might have originally been anticipated in 2002. A principles-based, non-prescriptive approach should continue to be advocated in recognition of the need for organizations to develop an internal control system particular to their own specific internal and external environments.

The preference appears to be for an internal control system that sits within a risk management framework and there is consensus that internal control needs to be embedded within the organization, with employees informed as to how it impacts on their roles and their responsibilities in terms of monitoring and reporting.

The importance of the "tone at the top" and the culture and ethical framework of the organization is fully acknowledged and considered essential to the successful implementation of an internal control system. Poor "tone at the top" has often been quoted as a very significant factor in the recent high-profile accounting scandals.

Section 404 is the product of the US regulatory framework which, to some extent, is unique in that it is usually characterized as being rules-based. The approach in many other jurisdictions has tended to be principles-based and market-led. This alternative approach has recently been endorsed or re-endorsed in the UK, Europe and Hong Kong.

For companies registered with the SEC, however, SOX and its related guidance for auditors continues to set much of the agenda, due to its detailed and costly compliance requirements. It would appear that, in some organizations, this concentration on internal control over financial reporting may be to the possible detriment of the broader aspects of internal control and risk management. Those organizations required to comply with Section 404 need to be encouraged to do so within a broader enterprise governance framework, thus ensuring that the business benefits outweigh the often substantial costs of compliance.

An interesting fact emerged from the Turnbull Review, which stated that:

> *It was felt that those companies that viewed internal control as sound business practice were more likely to have embedded it into their normal business processes, and more likely to feel that they had benefited as a result, than those that viewed it primarily as a compliance exercise.*

It has long been accepted that good governance requires effective systems of internal control. For the benefit of all, organizations should be encouraged and supported in implementing good internal control systems. While a number of key internal control frameworks and many related

supporting “theory” documents are available, some consider that there is a need for support in the practical implementation of internal control systems.

This document has demonstrated that the general consensus is that, whatever form this support may take, it should take a principles- and market-based, risk-focused approach, in recognition of the need for an organization to develop an internal control system particular to its internal and external environment. Prescriptive and legislative requirements are often not recommended as a means of encouraging good internal control systems, as under these circumstances organizations are more likely to view internal control as merely a compliance exercise rather than an integral part of good business practice.

International Federation of Accountants
545 Fifth Avenue, 14th Floor, New York, NY 10017 USA
Tel +1 (212) 286-9344 Fax +1(212) 286-9570 www.ifac.org