Professional Accountants in Business Committee

Exposure Draft

December 2011

Comments requested by February 29, 2012

International Good Practice Guidance

Evaluating and Improving Internal Control in Organizations

REQUEST FOR COMMENTS

The Professional Accountants in Business (PAIB) Committee of IFAC approved this Exposure Draft of the proposed International Good Practice Guidance (IGPG), *Evaluating and Improving Internal Control in Organizations*, for publication in December 2011. This proposed IGPG may be modified in light of comments received before being issued in final form.

Respondents are asked to submit their comments **electronically** through the IFAC website (www.ifac.org), using the Submit a Comment button. Please note that first-time users must register to use this feature. All comments will be considered a matter of public record and will ultimately be posted on the PAIB Committee website.

Comments can also be faxed to the attention of the PAIB Committee at +1 (212) 286-9570, or mailed to:

PAIB Committee
International Federation of Accountants
545 Fifth Avenue, 14th Floor
New York, NY 10017 USA

Comments should be submitted by **February 29, 2012.**

Copies of this exposure draft may be downloaded free of charge from the PAIB section of the IFAC website at www.ifac.org/paib.

Other recent publications by the PAIB Committee include *Competent and Versatile: How Professional Accountants in Business Drive Sustainable Organizational Success* (2011), which outlines the diverse roles of professional accountants in business and the many ways they serve their employers and the public interest. Copies of *Competent and Versatile* and this IGPG may be downloaded free of charge at www.ifac.org/paib.

The *Preface to IFAC's International Good Practice Guidance* sets out the scope, purpose, and due process of the PAIB Committee's IGPG series.

IFAC's mission is to serve the public interest by:

- contributing to the development, adoption, and implementation of high-quality international standards and guidance;
- contributing to the development of strong professional accountancy organizations and accounting firms, and to high-quality practices by professional accountants;
- promoting the value of professional accountants worldwide; and
- speaking out on public interest issues where the accountancy profession's expertise is most relevant.

The PAIB Committee serves IFAC member bodies and professional accountants worldwide who work in commerce, industry, financial services, education, and the public and not-for-profit sectors. Its aim is to promote and contribute to the value of professional accountants in business. To achieve this objective, its activities focus on:

- increasing awareness of the important roles professional accountants play in creating, enabling, preserving, and reporting value for organizations and their stakeholders; and
- supporting member bodies in enhancing the competence of their members to fulfill those roles. This is achieved by facilitating the communication and sharing of good practices and ideas.

The PAIB Committee extends its appreciation and thanks to its Risk Management and Internal Control Task Force for preparing and assisting the committee in developing this proposed IGPG. The Risk Management and Internal Control Task Force consists of PAIB Committee members Henny Kapteijn (chair), Alan Johnson, and Yacoob Suttar; and PAIB Committee technical advisors Khalid Rahman, Carol Scott, and Karlijn Tesselaar. The task force thanks the following external specialists for their contributions: Ken Witt and Kayla Briggs (both American Institute of Certified Public Accountants), Paul Moxey (Association of Chartered Certified Accountants), Gigi Dawe (Canadian Institute of Chartered Accountants), Gillian Lees (Chartered Institute of Management Accountants), Gord Cummings (Certified Management Accountants of Canada), Vanessa Jones (Institute of Chartered Accountants of England and Wales), Cees Klumper (GAVI Alliance, Switzerland), Urjan Claassen (Nyenrode Business University, Netherlands), Roger Debreceny (University of Hawaii, US), and Steve Jameson (Institute of Internal Auditors, US).

Guide for commentators

The aim of this IGPG, *Evaluating and Improving Internal Control in Organizations*, is to establish a benchmark for good practice in maintaining effective internal control, and, in particular, to help professional accountants in business and their organizations create a cycle of continuous improvement for their internal control systems.

In encapsulating good practice in nine fundamental principles, the emphasis of this IGPG, as is the case with the PAIB Committee's other IGPGs, is to support professional accountants in business by helping them consider how to apply good practice principles rather than instructing them on implementing specific internal controls.

The PAIB Committee would like to receive comments on all topics addressed in this proposed IGPG. Anyone offering comments should refer to specific paragraphs, include the reasons for the comments, and, where appropriate, make explicit suggestions for proposed changes to wording. The PAIB Committee is particularly interested in comments on the matters set out below.

The terminology

1. Does the title *Evaluating and Improving Internal Control in Organizations*, as well as the term *internal control*, fit in the context of this IGPG, or should it be replaced by a different or more refined title or term?
2. Are the internal control definitions in Appendix A suitable for this guidance? Can or should they be further clarified?

The principles

3. Do the principles cover all the fundamental areas for evaluating and improving internal control in organizations, especially those areas where internal control is often applied incorrectly in organizations?

The guidance

4. Is the application guidance for each principle adequate to guide good practice?
5. Are there other resources on internal control that should be considered for inclusion in the appendices?

Other issues

6. Does there need to be a subsequent IGPG on risk management?

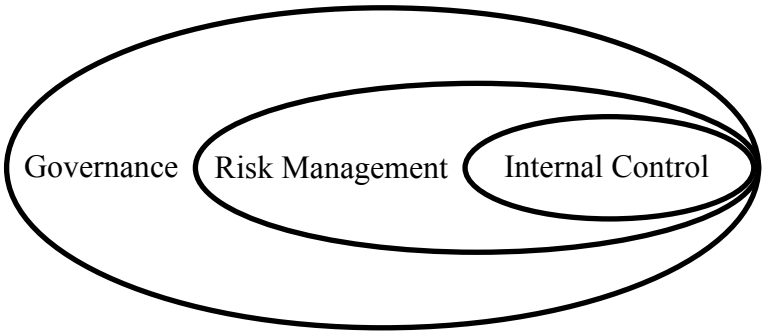
INTERNATIONAL GOOD PRACTICE GUIDANCE
EVALUATING AND IMPROVING INTERNAL CONTROL IN ORGANIZATIONS

CONTENTS

1. Introduction

1.1 One of the best defenses against business failure, as well as an important driver of business performance, is strong internal control, which mitigates risk and adds sustainable value. Successful organizations know how to exploit and manage risks, in many instances through internal control, and therefore realize long-term sustainable performance. This is true for organizations globally and was clearly reinforced by various financial crises in recent years.

1.2 Internal control can be considered an integral part of an organization's governance and risk management system—effected, understood, and actively followed by the governing body, management, and other personnel—to exploit the opportunities and to manage the risks in achieving the organization's objectives.[1]



1.3 Professional accountants in business across the globe are involved in the design, implementation, operation, audit, evaluation, and improvement of their organizations' internal control systems. This International Good Practice Guidance (IGPG) covers the main issues professional accountants in business should address to improve these internal control systems.

1.4 This IGPG identifies what is often applied incorrectly in organizations, with respect to internal control, and contains principles that demonstrate how professional accountants in business can support their organizations in evaluating and improving their internal control system. The guidance is not intended to be prescriptive, but rather considers the areas organizations need to continuously improve and the issues they need to address.

1.5 This guidance is directed at professional accountants in business working for all types of organizations, as all organizations, no matter their size or structure, private or public, should have an appropriate internal control system in place.

2. Why Internal Control is Important

2.1 Internal control is a crucial aspect of an organization's governance and risk management systems, and is fundamental to supporting the achievement of the organization's objectives and creating and protecting stakeholder value. The

[1] See Appendix A of this guidance for further definitions of governance, risk management, and internal control.

imposition of additional rules and requirements that results from high-profile organizational failures, as well as the resultant time-consuming and costly compliance efforts, obscure the fact that the right kind of internal controls—focused on the most important opportunities for and threats to an organization—can actually save time and money, and promote the creation and preservation of value.

2.2 According to IFAC's interviews with 25 key business leaders, summarized in the brochure *Integrating the Business Reporting Supply Chain* (2011), ongoing risk management and internal control should be key parts of governing body oversight. Various financial crises in recent years have demonstrated that in some organizations—especially in some financial institutions—risk management and internal control practices were flawed. According to the business leaders interviewed, these organizations did not fully comprehend the risks to which they were exposed. Before the latest string of financial crises, many organizations were overly focused on financial reporting controls. These crises highlighted the fact that many, if not most, of the risks that affected organizations derived from external circumstances. Moving forward, risk management and related internal control systems need to encompass a wider perspective, considering that organizations are impacted by many variables, often outside their direct control. Ongoing risk management and internal control should be a key part of integrated governance at every level of an organization and across all operations.

2.3 IFAC's *Global Survey on Risk Management and Internal Control* (2011), with more than 600 respondents from around the globe and from all types of organizations, revealed that: (a) more awareness of the benefits of implementing risk management and internal control systems should be created, and (b) risk management and internal control systems should be better integrated into organizations' overall governance, strategy, and operations. According to survey respondents, the drive to integrate risk management and internal control systems is gaining momentum, but the tools and guidance to develop and implement a genuinely integrated system do not really exist. Currently, risk management guidelines are often separate from internal control guidelines. The first step to strengthening guidance in this area, according to respondents, is to combine these separate guidelines into one integrated set. Bringing these guidelines together would help increase the general understanding that both risk management *and* internal control are integral parts of an effective governance system.

2.4 Despite the existence of sound internal control frameworks, it is often the application of such frameworks that fails or could be further improved in many organizations. With this publication, the Professional Accountants in Business (PAIB) Committee aims to provide a practical guide—complementary to already existing internal control frameworks and based on those internal control issues that are often applied incorrectly—that focuses on the role of professional accountants in business and how they can support their organizations in evaluating and improving internal control as an integrated part of organizations' governance, risk management, and internal control systems.

The Roles of Professional Accountants in Business

2.5 Worldwide, more than one million professional accountants work to support organizations in commerce, industry, financial services, education, and the public and not-for-profit sectors, making those organizations more successful and sustainable. They form a very diverse constituency, and can be found working as employees, consultants, and self-employed owner-managers or advisors.

2.6 As further explained in *Competent and Versatile—How Professional Accountants in Business Drive Sustainable Organizational Success* (2011), the roles professional accountants in business perform can broadly be described as creators, enablers, preservers, and reporters of sustainable value creation for organizations.

2.7 Within organizations, many professional accountants are in a position of strategic or functional leadership, or are otherwise well placed to partner with other disciplines in the planning, implementation, execution, evaluation, or improvement of internal control. In addition, many professional accountants in business have a responsibility to provide objective, accurate, and timely information and analyses to support all of these activities.

3. Key Principles of Evaluating and Improving Internal Control

3.1 The principles below represent good practice for evaluating and improving internal control systems.

3.2 These principles are not formulated to design and implement a system of internal control, for which other existing frameworks are referenced (see Appendix B), but to evaluate and improve existing internal control systems by highlighting a number of areas where the practical application of such frameworks often fails in many organizations.

A. Supporting the Organization's Objectives

Internal control should be used to support the organization in achieving its strategic and operational objectives, while complying with rules and regulations, by managing its significant risks. The organization should therefore integrate internal control as part of risk management and make it a natural part of its overall, integrated governance system.

B. Determining Roles and Responsibilities

The organization should determine the various roles and responsibilities with respect to internal control (including governing body, audit committee, management at all levels, internal and external auditors, and external specialists), as well as coordinate the collaboration among participants.

C. Linking to Individual Performance

Management should link achievement of the organization's internal control objectives to individual performance objectives. Each person within the organization should be held accountable for the achievement of the assigned internal control objectives.

D. Ensuring Sufficient Competency

The governing body, management, and other participants in the organization's governance system should be sufficiently competent to fulfill the internal control responsibilities associated with their roles.

E. Supporting Organizational Culture

Management should foster an organizational culture that motivates members of the organization to act in line with risk management strategy and policies on internal control set by the governing body to achieve the organization's objectives. The tone and action at the top are critical in this respect.

F. Responding to Risk

Internal controls should always be selected, implemented, and operated as a response to specific risks and their potential interactions.

G. Communicating Regularly

Management should ensure that regular communication regarding the internal control system, as well as the outcomes, takes place at all levels of the organization to make sure that the system of internal control is fully understood and the internal control principles are applied by all.

H. Monitoring and Evaluating Controls

Both individual controls as well as the internal control system as a whole should be regularly monitored and evaluated. Identification of unmanaged significant risks, system weaknesses, control failures, or previously undetected errors that are outside the tolerance level is usually a sign that an individual control or the internal control system is not achieving its objectives and needs to be improved.

I. Providing for Accountability and Transparency

The governing body, together with management, should periodically report to stakeholders the major risks the organization faces as well as the actual performance of the organization's internal control system.

3.3 The next section contains practical guidance on implementing these principles.

4. Practical Guidance on Implementing the Principles

What should the scope of internal control be?

4.1 Internal control is often perceived and treated as a compliance requirement, rather than as an enabler of improved organizational performance. Effective internal control can help organizations improve their performance by enabling them to take on additional opportunities, challenges, and risk in a more controlled way. Therefore, there needs to be a better connection between performance, risks, and controls, and how they interact.

PRINCIPLE A—Supporting the Organization's Objectives

Internal control should be used to support the organization in achieving its strategic and operational objectives, while complying with rules and regulations, by managing its significant risks. The organization should therefore integrate internal control as part of risk management and make it a natural part of its overall, integrated governance system.

A1. Risk taking is vital for organizations seeking long-term sustainable success. Proper risk assessment and internal control enable organizations to make informed decisions about the challenges and risks that they want to take in pursuit of the organizations' objectives and can help them target their resources to achieve sustainable success. However, risks cannot be taken without an explicit understanding of their influence on achieving an organization's objectives and of the impact on the organization should the risks materialize. Therefore, senior decision makers require relevant and reliable information, partly or wholly produced by the internal control system.

A2. In recent years, focus has shifted from the concept of internal control as a separate issue, toward internal control as an integrated part of risk management. For example, corporate governance frameworks worldwide have put greater emphasis on risk management than on internal control. Internal control can be most effective when it is integrated with risk management and embedded in all the processes of an organization. Risk management and internal control should therefore be viewed as two sides of the same coin, in that risk management concerns identification of threats and opportunities, while an internal control system is designed to effectively manage such threats and opportunities. Internal controls are risk controls, and once this is properly understood, the barriers to integration will be removed.

A3. Sustainable organizational success depends on how well organizations can integrate risk management and internal control into a wider corporate governance framework as an integral part of the organization's overall activities and business processes, not as separate and distinct systems. A strong, integrated governance framework is a key and integral part of managing a disciplined and controlled organization. If effectively integrated, it can result in an enterprise-wide governance, risk, and control system that:

- supports management in moving an organization forward in a cohesive, integrated, and aligned manner to improve performance, while operating effectively, efficiently, ethically, and legally within established risk-taking tolerances; and
- integrates and aligns activities and processes related to planning, risk management, policies and procedures, culture, competence, implementation, performance measurement, monitoring, continuous improvement, and reporting.

A4. An excessive and exclusive focus on financial reporting controls distracts management from ensuring that operational controls exist or are functioning as intended. Many times, root-cause analyses of financial reporting failures identify problems at the operational level that ultimately impact the financial statements. The challenge is to recognize that key financial controls might be able to pass a validation test, while underlying ineffective operational controls still expose the organization to risks. For example, ensuring the effectiveness of financial accounting controls on inventory does not necessarily lead to sufficient mitigation of inventory risk, such as wastage, obsolescence, or theft.

A5. Evaluating and improving risk management and internal control systems are among the core competencies of many professional accountants in business. Therefore, professional accountants should play a leading role in ensuring that risk management, including internal control, forms an integral part of an organization's governance framework. With an integrated, organization-wide approach to risk management and internal control, professional accountants in business also encourage the practice that risks be viewed and managed in a more holistic way. Strategic business decisions should be based on a rigorous analysis of risk and return, including an assessment of risk interactions and risk sensitivities related to organizational objectives, so that individual risks are not assessed and dealt with in isolation or in a linear, unconnected way. Relevant questions in this respect are:

- Are the various departments that are dealing with risk actually working together?
- Does the organization have a complete overview of all relevant risks?
- Does the organization understand how the various risks are interrelated or influence each other?
- How are risks evaluated?
- Are risks only managed on an individual basis, or should consideration also be given to interrelationships between risks and the risk exposure of the organization as a whole?

Who should be responsible for internal control?

4.2 Authority with respect to internal control should reside with executives who have the highest level of authorization, instead of being delegated to staff functionaries who lack executive powers.

PRINCIPLE B—Determining Roles and Responsibilities

The organization should determine the various roles and responsibilities with respect to internal control (including governing body, audit committee, management at all levels, internal and external auditors, and external specialists), as well as coordinate the collaboration among participants.

B1. Responsibilities for internal control:

- The governing body should assume overall responsibility for the organization's internal control strategy, policies, and system, and act accordingly. It should define risk strategy, approve the limits for risk taking and criteria for internal control, and make sure that management has effectively undertaken its responsibilities relating to management of risks and corresponding internal controls.
- Management should design, implement, maintain, and report on the organization's system of internal control appropriate to the risk strategy and policies on internal control, as approved by the governing body.
- Each person within the organization—management and other employees alike—should be held accountable for internal control and the management of specific risks within his or her span of control.
- Staff in support functions (e.g., risk officers) or external experts can have facilitating or supporting roles but should not assume line responsibility for internal control.
- Both internal and external auditors play an important role in monitoring and evaluating the internal control system and providing assurance to the governing body, usually through the audit committee. However, they should not assume responsibility for internal control in the organization.

B2. A governing body could have an audit or risk subcommittee, to which it could entrust some of its tasks with respect to internal control. However, the governing body as a whole should retain overall responsibility.

B3. In some organizations separate risk functions exist. In such cases, the risk officer should be an enabler of broad risk and internal control awareness across the organization, rather than an enforcer of compliance. Risk officers can strengthen the risk and control competence of governing bodies, management, and employees but should never take over their risk and control responsibilities.

B4. The professional accountant in business, with his or her specific attitude and mindset,[2] is in a good position to support management in maintaining operational oversight of the management of risks. Professional accountants may also serve as risk officers in organizations.

How could management's genuine attention on internal control objectives be obtained?

4.3 In order to get the appropriate attention of executive and line management, as well as of all other employees in an organization, internal control objectives should not only be linked to the organization's objectives but also to individual performance objectives.

PRINCIPLE C—Linking to Individual Performance

Management should link achievement of the organization's internal control objectives to individual performance objectives. Each person within the organization should be held accountable for the achievement of the assigned internal control objectives.

C1 The crucial importance of internal control to sustainable organizational success cannot be overemphasized. Achieving one's objectives and staying in control are inextricably linked. Sustainable success is based on people who create opportunities and also properly control their business. Line managers should therefore be held explicitly accountable for being in control, for example, by issuing in-control statements or letters of representation.

C2 An interesting view emerged from the UK's *Review of the Turnbull Guidance on Internal Control—Evidence Paper*, 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."[3]

C3 The professional accountant in business should ensure that information on control objectives and control performance is incorporated into the various organizational and personal and/or team performance management systems.

How should those involved in the internal control system live up to their responsibilities?

4.4 There is a risk that people with assigned internal control responsibilities might have insufficient knowledge, experience, skills, or time to adequately fulfill those responsibilities. This can seriously weaken and even jeopardize the internal control system.

---

2 *Competent and Versatile: How Professional Accountants in Business Drive Sustainable Organizational Success* (IFAC, 2011), 19.

3 *Review of the Turnbull Guidance on Internal Control—Evidence Paper* (Financial Reporting Council, 2005)

PRINCIPLE D—Ensuring Sufficient Competence

The governing body, management, and other participants in the organization's governance system should be sufficiently competent to fulfill the internal control responsibilities associated with their roles.

D1 Competence in this respect means:

- Having sufficient understanding of the organization's objectives, the external and internal environment, activities, processes, and systems, as well as the occurring risks and interdependent relationships.
- Knowing how the significant risks are being or can be managed with internal controls and other measures, and being capable of implementing those controls and measures.
- Being able to manage, execute, and/or monitor the controls and other measures, and deal with any uncovered risks, as well as with possible control weaknesses or failures.
- Having sufficient internal control resources available.
- Being able to judge, and/or execute, the evaluation and improvement of the organization's internal control system.
- Knowing and fulfilling one's responsibilities with respect to internal control as part of the governance system of the organization.

D2 The professional accountant in business can support the organization as a coach and provide on-the-job training on risk management and internal control. In this way the professional accountant in business can help enhance the level of internal control competence within the organization.

What else, beyond their formal responsibilities, should be expected from the governing body and management with respect to internal control?

4.5 Poor "tone at the top" has been widely quoted as a significant factor in organizational failures.

PRINCIPLE E—Supporting Organizational Culture

Management should foster an organizational culture that motivates members of the organization to act in line with risk management strategy and policies on internal control set by the governing body to achieve the organization's objectives. The tone and action at the top are critical in this respect.

E1 Management should fully acknowledge the importance of the "tone at the top"—the culture, and the ethical framework of the organization—which are essential to the successful implementation of an internal control system. Management has to lead by example with respect to internal control, and should also continuously convey the importance of maintaining an appropriate degree of internal control and the importance of

everyone's responsibility in achieving it. For example, if senior management appears unconcerned with ethics and controls and the focus is only on profitability, then employees down the line will be more inclined to feel that ethical conduct is not a priority.

E2 Another important element of leadership is to ensure that the values of the organization with respect to internal control are communicated from the top as key values of the organization. This concept needs to be part of a broader culture. A code of conduct can support and enable the desired types of employee behavior and point out the consequences of violating the principles of conduct.[4]

E3 Good "tone-at-the-top" includes the creation of clear roles and responsibilities with respect to risk management and internal control, as well as assigning these topics high priority at regular governing body and management meetings. Other examples are a "hands-on" approach in the operation of internal controls, effective whistle-blowing procedures, and appropriate follow-up on control weaknesses or failures.

E4 Professional accountants in business in senior positions within the organization can create awareness among their colleagues regarding the importance of internal controls.

How should internal controls be selected, implemented, and operated?

4.6 Often, organizations implement internal controls without adequate assessment of the external and internal environment, as well as their objectives, activities, processes, or systems, and the occurring risks.

PRINCIPLE F—Responding to Risk

Internal controls should always be selected, implemented, and operated as a response to specific risks and their potential interactions.

F1 Internal controls are a means to an end—the effective management of risks. When designing, implementing, operating, or assessing an internal control, the first question should be what risk or combination of risks the control is supposed to mitigate?

F2 Important considerations for adequate selection, implementation, and operation of internal controls are:

- the nature (cause, effect, and likelihood) of the corresponding risks;
- the organization's threshold for the particular risk;
- the suitability of the mix of controls;
- the cost effectiveness of the controls; and
- the continuous changes that can make existing controls ineffective or obsolete and drive the need for periodic assessment of the appropriate mix of controls.

[4] *Defining and Developing an Effective Code of Conduct for Organizations* (IFAC, 2007).

Organizations also need to remain agile and not become overly bureaucratic. Internal control should enable, not hinder, the achievement of organizational objectives.

F3 Organizations should have a built-in mechanism in all their strategic and operational decision-making to assess risks, including risk interaction, and to implement corresponding controls. All important deviations from the intended outcome need to be assessed. Controls should be implemented as close to the cause of a risk or as early in an activity or process as technically or economically feasible.

F4 Organizations should be aware that the various individual risks can mutually reinforce one another, making the combined effect bigger than anticipated. Therefore, risks should be assessed and controls designed taking the interaction between risks and the possible consequences into account. For example, a flood can create a domino effect of consequences, starting with damage to assets (via interruption of the supply chain and the consequential loss of production), falling sales, increasing liquidity shortages, and other similar difficulties, which could eventually lead to bankruptcy.

F5 The effort to plan, execute, and monitor internal control must be properly balanced with the effort to plan, execute, and monitor the organizational business plan. With too little attention on internal control, business objectives will not be achieved. On the other hand, too much attention on control can paralyze the organization: internal control becomes a goal in itself.

F6 Internal controls should only be applied where they are the appropriate response to manage risks. However, not every significant risk needs to be mitigated via internal controls, as there may be other ways to deal with those risks. Depending on the risk strategy and policies on internal control of the organization, organizations can also decide to accept a certain risk (by doing nothing), to hedge a risk (by insuring against the risk), to avoid a risk (by terminating the activity), or even to take on additional risk in pursuit of higher reward (by increasing the risk or lowering the level of internal control). Those decisions should be made explicitly and consciously.

F7 Controls should also be cost-effective in a broad sense: the overall benefits—taking into account economic, environmental, and social considerations and regulation—should be larger than the costs, and the greater the difference, the more cost-effective the control. It should be recognized that some risks, albeit relatively small from a monetary perspective, can nevertheless have very significant consequences if they materialize, warranting a greater degree of control than a purely quantitative approach might suggest. For example, the payment of even a small bribe can cause very serious reputational damage to any organization.

F8 The balance between risks and related controls is continuously changing in a dynamic environment and controls should be continuously reevaluated and re-optimized. Risk assessment and adjustment of internal controls should be carried out on a continuous cycle. For each business cycle, when management revisits strategy, the related risk and control policies also need to be reassessed. Changes in risk-taking strategy lead to changes in the amount of risk taken on and/or the level of controls applied. Finally, external developments may necessitate changes in internal controls.

F9 Professional accountants in business can support their organizations by making controls more cost effective, for example, by altering the mix of controls or by better embedding controls into the normal course of business (more "built-in" and less "add-on" controls).

How can internal control be better ingrained into the DNA of the organization?

4.7 In many organizations, the internal control system exists in handbooks and written procedures, but is not sufficiently present in everyday management or actual operations.

PRINCIPLE G—Communicating Regularly

Management should ensure that regular communication regarding the internal control system, as well as the outcomes, takes place at all levels of the organization to make sure that the system of internal control is fully understood and the internal control principles are applied by all.

G1 Internal controls can only work effectively when they are clearly understood and carried out by those involved. Therefore, controls should not be documented and communicated in isolation, but integrated into the environment in which they are intended to operate, including the objectives, activities, processes, systems, risks, and responsibilities.

G2 Proper documentation and communication are vital for effective internal control. When documenting and communicating internal controls, attention should be paid to the usability and understandability of the various policies, procedures, etc. The use of common language supports effective internal control. This common language should meet professional and technical standards but also be understandable for non-professionals in this area, such as line managers or process owners.

G3 Documentation is only the beginning; internal control should also be embedded into the way people work. Therefore, management should ensure, through active communication, that what is written in a policy document or handbook is understood widely across the organization and applied in practice by employees. A natural way of internalizing internal control is to actively engage people, through training and team meetings, in the management of their "own" risks and the development, implementation, operation, and evaluation of the related internal controls. This is especially important when people change roles—the occurring risks and corresponding controls in place should get fully passed along to incoming staff.

G4 Changes in the internal control system should be reflected in updated documentation and additional communication. This requires identifying, documenting, and communicating who makes the decisions; assigning authority for various processes; and determining how changes in the internal control system are to be made and approved. It is crucial to test the design of newly implemented and documented controls, followed by monitoring of their operating effectiveness.

G5 The common use of online systems both facilitates and challenges the effective documentation and communication of internal control. This reality must be considered in ensuring effective dissemination of the organization's internal controls, including updates.

G6 Professional accountants in business are frequently engaged in the improvement of documentation and communication of internal control systems. In addition, the professional accountant in business can support the organization in establishing an understandable common internal control language that meets professional and technical standards.

How should internal control be monitored and evaluated?

4.8 The organization should become aware that a problem with either an individual internal control or the system has occurred as soon as possible, so that further damage can be prevented or contained and the issue rectified. In many cases, however, not enough attention is given to defining what, exactly, should be monitored and evaluated with respect to internal control, how this should be done, and by whom.

PRINCIPLE H—Monitoring and Evaluating Controls

Both individual controls as well as the internal control system as a whole should be regularly monitored and evaluated. Identification of unmanaged significant risks, system weaknesses, control failures, or previously undetected errors that are outside the tolerance level is usually a sign that an individual control or the internal control system is not achieving its objectives and needs to be improved.

H1 Many people confuse the monitoring and evaluation of the internal control system with the monitoring and evaluation of the individual controls. At first glance, an individual control might seem to be adequate, but it should also be reviewed in the context of how the overall internal control system is intended to work. Monitoring and evaluation of both the individual internal controls (see H2) and the overall internal control system (see H3) completes the "Plan-Do-Check-Act cycle" with respect to internal control.[5]

H2 Monitoring, evaluation, and improvement of individual controls

H2.1 Internal controls that have previously been proven to be effective can weaken or fail. Possible causes for internal control weaknesses or failures include:

- a risk was not identified, or the risks or circumstances have changed so that the control is no longer effective;
- the probability or impact of a risk was incorrectly assessed or has changed;
- controls were not appropriate for the related risk (a design fault);
- a control was not properly executed (an operational fault);
- excessive residual risk remained; or
- a change was made in personnel performing control procedures.

[5] An iterative four-step management process typically used in organizations.

H2.2 Possible underlying causes could include:

- constant changes in the organization and its environment that can make existing controls become obsolete even if they still operate;
- insufficient care or other adverse personal behavior accepting false assurance;
- acceptance of unsubstantiated third-party assurance;
- a lack of understanding of the business;
- a lack of control resources; or
- a lack of information.

For example, hacking of corporate and government computer systems has become much more sophisticated, and, therefore, what was good practice only a year or two ago is inadequate today.

H2.3 When should monitoring controls be done? Periodically and, in some cases, continuously, depending on factors such as: volatility of the environment, the importance of the control, the nature of the control (e.g., routine or non-routine controls), the stability of the control, the history of failures of the control, the existence of compensating controls, and cost-benefit considerations.

H2.4 Who is responsible for monitoring controls? In general, monitoring should be performed by a person or persons who are: (a) sufficiently independent from the operation of the control, and (b) sufficiently competent. Internal and external audit could provide additional, independent evaluations and assurance.

H2.5 Since management is responsible for the effective operation of the controls, ongoing monitoring is usually the most effective practice, as it is performed close to the operation of the control and earlier in the process (as compared to separate evaluations that tend to be performed less frequently). Additionally, it reinforces the message that controls are a part of everyone's day-to-day responsibilities.

H2.6 How should monitoring controls be executed? Review and monitoring of the effectiveness of applicable internal controls should be part of an individual's job responsibilities. Therefore, all employees should understand how risk management and related internal controls are critical to the success of the organization's goals and objectives. Management should also communicate methods for employees and others to report deficiencies in or breaches of established internal controls as part of the overall governance system.

H2.7 When evaluating internal controls, professional accountants should help their organizations recognize the value of direct evidence of effectiveness, such as error rates, customer complaints, and numbers and amounts of unmatched cash items. In fact, this is one of the best sources of information for risks that occur frequently.

H2.8 Actions arising from the evaluation include:

- determining whether the control is working the way it is intended to work;
- correcting failures or mistakes, understanding why the failure happened or the mistake was made, and making sure that it will not happen again, all of which should be part of the continuous improvement cycle;
- properly documenting the corrections of the internal controls and communicating them to all those involved; and
- summarizing the various individual control failures as input for the evaluation of the internal control system, as many failures of individual controls may indicate weaknesses in the overall internal control system.

H3 Monitoring and evaluation of the internal control system

H3.1 Even where internal control systems were previously effective, over time they can lose their effectiveness to the point where significant weaknesses or failures can start occurring. Therefore, the organization should periodically monitor and evaluate whether all elements necessary for an effective and cost-efficient internal control system—as identified in the various internal control frameworks—are in place and functioning well, for example, in accordance with this guidance.

H3.2 Organizations need a structured process to ensure that the internal control system is being thoroughly evaluated on a timely basis.

H3.3 When should internal control system monitoring be done? For example, periodically in tandem with revision of strategy, or when there are indications of reduced effectiveness, such as several failures of individual controls. The actual timing should at least be dependent on the pace of internal and external change.

H3.4 Who should monitor the internal control system? The governing body, possibly supported by the audit committee, should ensure that the internal control system is monitored and evaluated when necessary. The actual assessment can be done by the organization's management or the finance or internal audit function.

H3.5 How should the internal control system be monitored? The internal control system should be monitored and evaluated against risk management strategy and policies on internal control, taking into account strategic, financial, and operational performance and the risk levels associated with achieving those performance levels. Elements should include re-examining the underlying choices, principles, and assessments made in arriving at the current system; review of reported incidences of control failures since the last evaluation; review of external and internal developments that, taken together, could suggest that overall choices may need to be re-considered.

H3.6 Actions arising from the evaluation should include combining the results of the previous cycle with new input, so that the organization can quickly and effectively react to departures from its plan and adapt to environmental changes that impact its ability to achieve its objectives within approved risk limits.

H3.7 An integral part of the monitoring and evaluation of the internal control system is feedback on the outcomes to the governing body as part of its oversight function.

How should the organization report on internal control performance?

4.9 The various internal and external stakeholders have a justified interest in the existence and performance of the organization's risk management and internal control.

PRINCIPLE I—Providing for Accountability and Transparency

The governing body, together with management, should periodically report to stakeholders the major risks the organization faces as well as the actual performance of the organization's internal control system.

I1 Organizations should transparently account for the structure and performance of their risk management and internal control system in their various reports to internal and external stakeholders, such as through their periodic accountability reports and/or on the organization's website.

I2 However, organizations should account not only for the existence of their system, but also about major risks the organization faces; what controls it has established; how internal control is monitored and evaluated; how the internal control system works; and what has been done to remediate any control failures or weaknesses.

I3 With respect to the scope and the depth of the reporting, organizations should assess the information various stakeholders need to make sufficiently informed decisions about the organization. Establishing open communication with stakeholders about the organization's risk management and internal control is instrumental in this respect.

I4 Organizations should develop a mechanism to incorporate relevant feedback from the various stakeholders into their internal control system.

Appendix A: Internal Control Definitions

Internal control:

An enriched definition of internal control, taking into account some of the suggestions of IFAC's *Global Survey on Risk Management and Internal Control* (2011), could be:

Internal control is an integrated part of an organization's governance and risk management system, which is effected, understood, and actively followed by the organization's governing body, management, and other personnel, to exploit opportunities and to manage the risks in achieving the organization's objectives through:

1. effective and efficient strategic and operational processes;
2. providing reliable information to internal and external users for timely and effective decision making;
3. ensuring conformance with applicable laws and regulations, as well as with the organization's own policies, procedures, and guidelines;
4. safeguarding the organization's resources against loss, fraud, misuse, and damage; and
5. safeguarding the availability, confidentiality, and integrity of the organization's information systems, including IT.

Risk management:

Taken from IFAC's Evaluating and Improving Governance in Organizations (2009)

The process of planning, organizing, leading, executing, and controlling the activities of an organization to maximize value and minimize the risk of events that diminish value. Risk management covers all categories of risk (threats as well as opportunities), including financial, strategic, operational, and reputational risks (see Committee of Sponsoring Organizations of the Treadway Commission and International Organization for Standardization in Appendix B). Depending on the type of risk, it can be managed in various ways, such as acceptance, avoidance, insurance, or via the implementation of internal controls.

Jointly, risk management and internal control are integrated parts of an organization's overall governance and management system that are:

1. effected and understood by the organization's governing body, management, and other personnel;
2. applied in strategy setting, both across the organization's operations and in its stakeholder communications;
3. designed to help its users identify, understand, and assess potential risks and opportunities and their interaction that might affect the organization;

in order to:

1. manage those risks and opportunities to be in line with the organization's risk management strategy; and

2. provide reasonable assurance regarding the achievement of organizational objectives and proper disclosure regarding the effectiveness of the risk management and internal control systems.

Governance: the set of responsibilities and practices exercised by the governing body with the goal of: (a) providing strategic direction, (b) ensuring that objectives are achieved, (c) ascertaining that risks are managed appropriately, and (d) verifying that the organization's resources are used responsibly.[6] This definition reflects both the performance and conformance aspects of governance.

Governing body: the person(s) or body (e.g., a board of directors) with primary responsibility for overseeing: (a) the strategic direction of the organization, and (b) the accountability of the organization. This includes overseeing the financial reporting process. Governing bodies can be made up of independent and non-independent directors and can have various subcommittees, such as the audit committee, the remuneration committee, and the ethics committee. In some entities in some jurisdictions, the governing body may include management personnel, executive members of a governance board of a private or public sector entity, or an owner-manager.

Integrated governance system: the governing body and subsequent levels of management integrating governance into strategy, management, oversight, and accountability, in order to achieve sustainable organizational success.

Conformance: compliance with laws and regulations, best practice governance codes, accountability, and the provision of assurances to stakeholders in general. The term can refer to: (a) internal factors defined by the officers, shareholders, or constitution of an organization, as well as (b) external forces, such as consumer groups, clients, and regulators.

Performance: policies and procedures that: (a) focus on opportunities and risks, strategy, value creation, and resource utilization, and (b) guide an organization's decision making.

Stakeholder: any person, group, or entity that has an interest in an organization's activities, resources, or output, or that is affected by that output. Stakeholders can include regulators, shareholders, debt holders, employees, customers, suppliers, advocacy groups, governments, and society as a whole.

Stakeholder value: organizational value that is generated for stakeholders by creating, implementing, and managing effective strategies, processes, activities, assets, etc. Sustainable value creation for stakeholders occurs when the benefits to them are greater than the resources they expend. Value is generally measured in financial terms, as in the case of shareholders, but it can also be measured as a societal or environmental benefit, as in the case of both shareholders and other stakeholders.

[6] *Board Briefing on IT Governance, 2nd Edition* (IT Governance Institute, 2003)

Appendix B: Important Sources of Information

This list of resources is not intended to be exhaustive. Use the IFACnet at www.ifac.org to search IFAC and many of its member body websites for additional information (click on the search function and select IFACnet).

- The IGPG *Defining and Developing an Effective Code of Conduct for Organizations* (2007) helps organizations encourage an ethics-based culture and define and develop a code of conduct. It also refers to the most significant resources in this area.
- In the PAIB paper *Internal Control from a Risk-Based Perspective* (2007), 10 senior-level professional accountants in business share their experiences and views on establishing effective internal control systems.
- IFAC's *Global Survey on Risk Management and Internal Control—Results, Analysis, and Proposed Next Steps* (2011) received over 600 responses from around the globe. This information paper provides an analysis of the survey results and summarizes respondents' recommendations for the next steps in this area.
- The IGPG *Evaluating and Improving Governance in Organizations* (2009) includes a framework—consisting of a series of fundamental principles, supporting guidance, and references—for how professional accountants can contribute to evaluating and improving governance in organizations.
- In the report *Integrating the Business Reporting Supply Chain* (2011), 25 prominent business leaders provide their recommendations on what should be done to effectively improve governance, the financial reporting process, audit, and the usefulness of business reports in the aftermath of the financial crisis of 2008. The report provides a summary of interviewees' recommendations in each area and highlights some of IFAC's related initiatives.
- *Competent and Versatile: How Professional Accountants in Business Drive Sustainable Organizational Success* (2011) outlines the diverse roles of professional accountants in business and the many ways they serve their employers and the public interest.
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has published *Enterprise Risk Management—Integrated Framework* (2004), which expands on internal control and provides key principles and concepts on the broader subject of enterprise risk management. A summary can be downloaded at their website at www.coso.org.
- COSO is also set to release an Exposure Draft of its update of *Internal Control—Integrated Framework* in December 2011. Visit the COSO website for further information.
- *Standard 31000—Risk Management* (International Organization for Standardization, 2009) sets out principles, a framework, and a process for the management of risk that are applicable to any type of organization in the public or private sector. It does not mandate a "one size fits all" approach, but rather emphasizes the fact that the management of risk must be tailored to the specific needs and structure of the particular organization.

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