Final Pronouncement
June 2012

Professional Accountants in Business Committee
International Good Practice Guidance

Evaluating and Improving Internal Control in Organizations

International Federation of Accountants

The mission of the International Federation of Accountants (IFAC) 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; 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.

Copyright © June 2012 by the International Federation of Accountants (IFAC). For copyright, trademark, and permissions information, please see page 24.

GOOD PRACTICE GUIDANCE

EVALUATING AND IMPROVING INTERNAL CONTROL

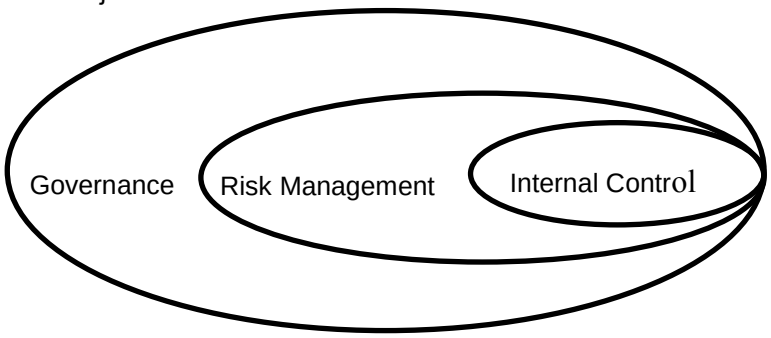
IN ORGANIZATIONS

CONTENTS

1. Introduction

1.1 One of the best defenses against business failure, as well as an important driver of business performance, is having an effective internal control system, which manages risk and enables the creation and preservation of value. Successful organizations know how to take advantage of opportunities and counter threats, in many instances through effective application of controls, and therefore improve their performance.

1.2 Internal control is an integral part of an organization's governance system and ability to manage risk, which is understood, effected, and actively monitored by the governing body, management, and other personnel to take advantage of the opportunities and to counter the threats to achieving the organization's objectives.[1]



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

1.4 This IGPG identifies why internal control systems in organizations are not always effective, and contains principles that demonstrate how professional accountants in business can support their organization in evaluating and improving their internal control system. The guidance is not intended to be prescriptive, but rather considers the internal control areas an organization needs 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, or whether they are 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 system and ability to manage risk, and is fundamental to supporting the achievement of an organization's objectives and creating, enhancing, and protecting stakeholder value. High-profile organizational failures typically lead to the imposition of additional rules and requirements, as well as to subsequent time-consuming and costly compliance efforts. However, this obscures the fact that the right kind of internal controls—enabling an organization to capitalize on opportunities while offsetting the threats—can actually

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

save time and money, and promote the creation and preservation of value. Effective internal control also creates a competitive advantage, as an organization with effective controls can take on additional risk.

2.2 According to IFAC's interviews with 25 key business leaders, summarized in the brochure *Integrating the Business Reporting Supply Chain* (2011), ensuring effective, integrated risk management and internal control should be a key part 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 or ineffective. 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 areas other than financial reporting including operations and 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. Effective risk management and internal control should be a key part of good 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 guidelines, it is often the application of such guidelines 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 that focuses on how professional accountants in business can support their organization in evaluating and improving internal control as an integral part of its governance system and risk management. This guidance is complementary to existing internal control guidelines and is based on those internal control matters that often cause difficulties in practice.

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

A. Supporting the Organization's Objectives

Internal control should be used to support the organization in achieving its objectives by managing its risks, while complying with rules, regulations, and organizational policies. The organization should therefore make internal control part of risk management and integrate both in its overall governance system.

B. Determining Roles and Responsibilities

The organization should determine the various roles and responsibilities with respect to internal control, including the governing body, management at all levels, employees, and internal and external assurance providers, as well as coordinate the collaboration among participants.

C. Fostering a Motivational Culture

The governing body and 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.

D. Linking to Individual Performance

The governing body and 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 assigned internal control objectives.

E. 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.

F. Responding to Risk

Controls should always be designed, implemented, and applied as a response to specific risks and their causes and consequences.

G. Communicating Regularly

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

H. Monitoring and Evaluating

Both individual controls as well as the internal control system as a whole should be regularly monitored and evaluated. Identification of unacceptably high levels of risk, control failures, or events that are outside the limits for risk taking could be a sign that an individual control or the internal control system is ineffective and needs to be improved.

I. Providing for Transparency and Accountability

The governing body, together with management, should periodically report to stakeholders the organization's risk profile as well as the structure and factual performance of the organization's internal control system.

4. Practical Guidance on Implementing the Principles

What should the scope of internal control be?

A. 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 and challenges in a more controlled way. Therefore, there needs to be a better understanding of how organizational performance relates to effective risk management and the role and effectiveness of internal control.

PRINCIPLE A—Supporting the Organization's Objectives

Internal control should be used to support the organization in achieving its objectives by managing its risks, while complying with rules, regulations, and organizational policies. The organization should therefore make internal control part of risk management and integrate both in its overall governance system.

A.1 Organizations always face uncertainty in achieving their strategic, operational, and other objectives. However, they can decide the level of risk they wish to be exposed to in the pursuit of those objectives. Proper risk assessment and internal control assist organizations in making informed decisions about the level of risk that they want to take, and implementing the necessary controls, in pursuit of the organizations' objectives. However, risks should not be taken without an explicit understanding of their potential consequences for achieving an organization's objectives. Therefore, decision makers require relevant and reliable information, produced through the internal control system, to effectively implement and execute their strategic and operational plans.

A.2 In recent years, focus has shifted from internal control as a separate concept to internal control as an integrated part of risk management and governance. For example, corporate governance codes worldwide now generally put greater emphasis on effective risk management than just on internal control. Internal control can be most effective when it is integrated with risk management and both are embedded in all the governance processes of an organization. Risk management and internal control should therefore be viewed as two sides of the same coin, in that risk management focuses on the identification of threats and opportunities, while controls are designed to effectively counter threats and take advantage of opportunities.

A.3 Sustainable organizational success depends on how well an organization can integrate risk management and internal control into a wider governance system as an integral part of its overall activities and decision-making processes. A strong, integrated governance system is an integral part of managing a disciplined and controlled organization. Effective integration can result in an enterprise-wide governance, risk management, and internal 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 limits for risk-taking; and
- integrates and aligns activities and processes related to objective setting, planning, policies and procedures, culture, competence, implementation, performance measurement, monitoring, continuous improvement, and reporting.

A.4 An excessive and exclusive focus on financial reporting controls distracts management from ensuring that operational or strategic controls exist and are functioning as intended. Root-cause analyses of business failures frequently identify insufficiently controlled risks at the operational level that caused significant problems before the financial statements could even be prepared. The challenge is to recognize that key financial controls might be able to pass a validation test, while underlying ineffective controls still expose the organization to unacceptable levels of risk. For example, ensuring the effectiveness of financial reporting controls on inventory does not necessarily lead to sufficient reduction of inventory risk, such as waste, obsolescence, or theft. Organizations should, therefore, take an approach that manages all types of risk in line with the guidance under Principle F, *Responding to Risk*.

A.5 Evaluating and improving risk management and internal control are among the core competencies of many professional accountants in business. Therefore, professional accountants can play a leading role in ensuring that risk management, including internal control, forms an integral part of an organization's governance system. 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 treated in a more holistic way. Therefore, all important business decisions should be based on proper risk assessment that defines the overall effect of uncertainty on the organization's objectives, so that individual risks are not assessed and dealt with in isolation or in a linear, unconnected way. Relevant questions in this respect include:

- Are the various departments that are dealing with a particular risk or are responsible for associated controls actually working together?
- Does the organization have an accurate and comprehensive understanding of its current risks?

- Does the organization understand how various risks might have common causes or mutually reinforcing consequences?
- Are the organization's risks within the limits for risk taking as determined in its risk management strategy and policies on internal control?
- Are risks only treated on an individual basis or does the organization understand the overall effect of uncertainty on its objectives?
- Does the organization sufficiently know the effectiveness of its controls and how they could be further improved?
- How can the organization be certain it knows the correct answers to the preceding questions? What are its processes for monitoring and evaluation and are they effective?

Who should be responsible for internal control?

B. Responsibility with respect to internal control should reside with those who have the highest level of authority, instead of being delegated to staff 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 the governing body, management at all levels, employees, and internal and external assurance providers, as well as coordinate the collaboration among participants.

B.1 Responsibilities for internal control are distributed among numerous groups.

- The governing body should assume overall responsibility for the organization's internal control strategy, policies, and system, and act accordingly. It should define risk management 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 (i.e., the oversight function).[2]
- Management, as the primary risk owner, should design, implement, maintain, monitor, evaluate, and report on the organization's internal control system in accordance with 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 proper understanding and execution of risk management and internal control within his or her span of authority.
- Staff in support functions (e.g., risk officers) or external experts can have facilitating or supporting roles but should not assume line responsibility for managing specific risks or for the effectiveness of controls.
- Both internal and external assurance providers, such as those concerned with health, safety, the environment, quality, operational effectiveness, or financial accounting, play an important role in monitoring and evaluating the effectiveness of the internal control system and

[2] The International Organization for Standardization (ISO)'s *Standard 31000:2009—Risk Management* (discussed in Appendix B) uses the term "risk criteria" to indicate the terms of reference against which the significance of a risk is evaluated. Other guidelines use the terms "risk appetite" and "risk tolerance." However, as these terms are not clearly defined, this guidance uses the term "limits for risk taking."

conveying—independent of management—re-assurance to the governing body. However, they should not assume responsibility for managing specific risks or for the effectiveness of controls.

B.2 The governing body could have an audit or risk management subcommittee, to which it could entrust some of its primary oversight tasks with respect to internal control. However, the governing body as a whole should retain overall responsibility for overseeing risk management and internal control.

B.3 In some organizations, separate risk management functions exist. The risk officer function should enable broad risk management and internal control awareness across the organization, rather than an enforcer of compliance. Risk officers can strengthen the risk management and control competence of governing bodies, management, and employees, but should never take over risk management and internal control responsibilities from line managers.

B.4 As risks should have "owners," controls should also be owned by someone who is responsible for their operation. The control owner or operator would normally be the person who executes the control on a day-to-day basis and can be someone other than the risk owner.[3] The organization should explicitly designate and communicate the various risk and control owners.

B.5 The professional accountant in business, with his or her specific training and mindset, is in a good position to support management in determining, as well as implementing and monitoring, the various roles and responsibilities with respect to internal control. Professional accountants may also serve as risk officers in organizations.

What other internal control responsibilities/actions should be expected from the governing body and management?

C. Poor "tone at the top" is a significant factor in organizational failures.

PRINCIPLE C—Fostering a Motivational Culture

The governing body and 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.

C.1 The governing body and management should fully acknowledge the importance of the "tone at the top," the culture, and the ethical framework of the organization, all of which are essential to an effective internal control system. The governing body and management alike need to lead by example with respect to good governance, risk management, and internal control. For example, if senior management appears unconcerned with risk management and internal control, then employees down the line will be more inclined to feel that appropriate management of risk through effective controls is not a priority.

C.2 Another important element of leadership is to ensure that the values of the organization with respect to governance, risk management, and internal control are communicated from the top as

[3] This does not affect the overall responsibility of the risk owner for the proper modification of that risk and, thus, for the design, implementation, application, monitoring, and evaluation of the corresponding controls.

key values of the organization. This concept needs to be part of a broader culture of responsibility within an organization.

C.3 A code of conduct can support and enable the desired types of employee behavior and point out the consequences of violating the principles of its code of conduct or ethics. In addition to having a code, management should continually reinforce its principles in word and deed, with training programs, model behavior, and by taking appropriate actions in response to violations.

C.4 Effective "tone at the top" includes the creation of clear roles and responsibilities with respect to governance, risk management, and internal control, as well as assigning these topics high priority at regular governing body, management, and employee meetings. Other examples are a "hands-on" approach in the operation of controls, effective whistle-blowing procedures, and appropriate follow-up on control weaknesses or failures.

C.5 The provision of sufficient resources to carry out internal control is also an important part of setting the right tone.

C.6 Professional accountants in business in senior positions within the organization can create awareness among their colleagues regarding the importance of governance, risk management, and internal control.

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

D. Recognizing positive performance can have a huge impact on strengthening internal control. 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 D—Linking to Individual Performance

The governing body and 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 assigned internal control objectives.

D.1 The crucial importance of internal control to sustainable organizational success cannot be overemphasized. Achieving the organization's objectives and maintaining effective controls are inextricably linked. Sustainable success is based on people who create opportunities and properly control their business. This should, therefore, be explicitly recognized in the organization's process of performance assessment. Managers should also be held explicitly accountable for being in control, for example, by issuing in control statements or letters of representation.

D.2 This is supported by the view that emerged from the UK Financial Reporting Council's *Review of the Turnbull Guidance on Internal Control—Evidence Paper*, which states 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."

D.3 The organization should also ensure that those who are responsible for each risk are maintaining those risks within established limits for risk taking, as they may be inclined to choose their own risk limits over those of the organization.

D.4 Professional accountants in business can support their organization in incorporating information on control objectives and control performance into the various organizational and personal or team performance management systems.

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

E. There is a risk that people with assigned internal control responsibilities might not have sufficient knowledge, experience, skills, or time to adequately fulfill those responsibilities. This can seriously weaken and even jeopardize the effectiveness of the internal control system, which can in turn damage an organization.

PRINCIPLE E—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.

E.1 Competence in this respect means:

- having sufficient understanding of how changes in the organization's objectives, external and internal environment, strategy, activities, processes, and systems affect its exposure to risk;
- knowing how risks can be treated with appropriate controls, in line with the organization's risk management strategy and policies on internal control;
- knowing the principles of the segregation of duties to ensure that incompatible duties are properly segregated, so that no individual has total control over a transaction;
- being able to implement and apply controls, monitor their effectiveness, and deal with any insufficiently covered risks, as well as with possible control weaknesses or failures;
- having sufficient capabilities available to evaluate and improve individual controls; and
- being able to execute or review the evaluation and improvement of the organization's internal control system.

E.2 While professional accountants in business can support the organization as coaches and provide on-the-job training on risk management and internal control, they need senior-level management sponsorship and financial support to serve in these roles. With this sponsorship, professional accountants in business can help enhance the level of internal control competence within the organization.

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

F. Often, organizations implement internal controls without adequate assessment of the external and internal environment, as well as their objectives, activities, processes, or systems that are sources of risk.

PRINCIPLE F—Responding to Risk

Controls should always be designed, implemented, and applied as a response to specific risks and their causes and consequences.

F.1 Controls are a means to an end—the effective management of risks, enabling the organization to achieve its objectives. Before designing, implementing, applying, or assessing a control, the first question should be what risk or combination of risks the control is supposed to modify.

F.2 Organizations should mandate that all strategic and operational decision making is supported by risk management and the subsequent implementation of appropriate controls. All important deviations from the intended outcome need to be assessed.

F.3 Organizations should be aware that various risks can create an aggregated effect of uncertainty on the achievement of their objectives. Therefore, risks should be assessed and controls designed taking common causes and synergies into account, including escalation and domino consequences. For example, a flood can create a domino effect, 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 business failure.

F.4 Appropriate controls should be put in place to modify risk so that the level becomes acceptable. Important considerations for adequate selection, implementation, and operation of controls include:

- the characteristics (causes, consequences, and their likelihoods) of the corresponding risks;
- the organization's limits for risk taking;
- the various types of controls, for example, managerial or transactional controls, preventive or detective controls, and manual or automated controls;[4]
- the suitability of the mix of controls, taking into account the organization's size, structure, and culture;
- the costs compared with the benefits of more or different controls; and
- the continuous changes that can make existing controls ineffective or obsolete and drive the need for periodic assessment of controls (see Principle H, *Monitoring and Evaluating*).

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

F.5 Depending on the type and level of risk and based on, among other things, the internal control considerations mentioned above, organizations can decide:

- to avoid a certain risk by not starting or terminating the activity that gives rise to the risk;
- to take on additional risk in pursuit of higher reward by engaging in riskier activities or lowering the level of internal control;
- to control a risk by removing the source, changing the likelihood, or changing the nature, magnitude, or duration of the consequences;
- to share a risk by insuring against the risk, which is also considered a control; or
- to accept a risk by doing nothing apart from monitoring the changes in risk.

These decisions should be made explicitly and consciously.

4 Automated controls can be beneficial as they allow clear allocation of responsibilities and consistent operation of the control. That is, once an automated control is correctly implemented, it works each and every time.

F.6 Controls should be cost-effective in a broad sense—the overall benefits, taking into account economic, environmental, and social considerations, regulation, and the organization's limits for risk taking, should be larger than the costs, and the greater the difference, the more cost-effective the control. The consequence of this principle is that internal control can, therefore, only provide reasonable assurance that an organization meets its control objectives. It should be recognized, though, 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.

F.7 The balance between risks and related controls is continually changing in a dynamic environment and controls should be continually reevaluated and re-optimized. Risk reassessment 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 or the level of controls applied. Additionally, external developments may affect risk, which, in turn, may necessitate changes in internal controls.

F.8 The effort to design, 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, overly stringent control requirements can paralyze the organization: internal control becomes a goal in itself.

F.9 Professional accountants in business can support their organization by designing controls to be 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?

G. In many organizations, the internal control system exists in written instructions and procedures, but these may not be sufficiently adopted or followed 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 within the organization to make sure that the internal control principles are fully understood and correctly applied by all.

G.1 Internal controls can only work effectively when they, together with the risks they are supposed to modify, are clearly understood by those involved. Therefore, controls should not be documented and communicated in isolation but integrated through formal and informal channels into the elements of the management system in which they are intended to operate, including the related objectives, activities, processes, systems, risks, and responsibilities.

G.2 Proper documentation and communication are vital for effective internal control. When documenting and communicating controls, attention should be paid to the usability and understandability of the various policies, procedures, etc. The use of plain language supports effective internal control. This language should meet professional and technical standards but also be understandable for non-professionals in this area, such as line managers and process owners.

G.3 Documentation is only the beginning; risk management and internal control should also be embedded into the way people work. Therefore, management should ensure, through active communication and discussion, 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 risk management and internal control is to actively engage people, through training and team meetings, in the treatment of the risks they "own" and the development, implementation, operation, and evaluation of the related controls. This is especially important when people change roles—the risk profile, the relevant limits for risk taking, the controls in place, and the residual risk should be fully passed on to incoming staff.

G.4 Changes in the internal control system should be reflected in updated documentation and additional communications. This requires identifying, documenting, and communicating who makes the decisions; assigning responsibility for various processes; and determining how changes in the internal control system are to be approved, implemented, and monitored. It is crucial to test the design of newly implemented and documented controls, followed by monitoring their operating effectiveness.

G.5 The common use of online systems both facilitates and challenges the effective documentation, communication, and monitoring of internal control. This reality must be considered in ensuring effective dissemination and use of the organization's internal control policies and procedures, including updates.

G.6 Professional accountants in business are frequently engaged in the improvement of documentation and communication of internal control systems. In addition, a professional accountant in business can support the organization, for example, by organizing internal control training sessions and establishing an understandable, common internal control language that meets professional and technical standards.

How should internal control be monitored and evaluated?

H. The organization should become aware that a problem with either an individual control or the internal control 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

Both individual controls as well as the internal control system as a whole should be regularly monitored and evaluated. Identification of unacceptably high levels of risk, control failures, or events that are outside the limits for risk taking can be a sign that an individual control or the internal control system is ineffective and needs to be improved.

H.1 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 effective, but it should also be evaluated in the context of how the overall internal control system is intended to work. Conversely, an effective internal control system should be able to detect and remediate, in a timely manner, individual controls that have become deficient or redundant. Therefore, both the individual controls (see H.2) and the overall internal control system

(see H.3) should be regularly monitored and evaluated in conjunction with each other. This completes the "Plan-Do-Check-Act Cycle" with respect to internal control.[5]

H.2 Monitoring, evaluation, and improvement of individual controls

H.2.1 Individual controls that have previously been proven to be effective can weaken over time, fail, or become redundant. Required controls could also be non-existent. Possible causes for control weaknesses or failures include:

- constant changes in the organization, its objectives, its actions, and its environment can shift the nature or level of risk and render existing controls ineffective or no longer appropriate, even if they still appear to operate well;
- the risk analysis is no longer correct and therefore the basis for the control is no longer valid;
- controls were not appropriately designed for the related risk (a design flaw) or implemented incorrectly;
- a control is not being properly executed (an operational flaw), for example, because of:
  - a lack of control resources;
  - assigned management or employees have changed and are insufficiently aware of their control responsibilities;
  - a lack of knowledge or competence with regard to the operation of the control;
  - complacency or lack of oversight; or
  - acceptance of unsubstantiated third-party assurance.

Even after remediation of deficient controls, the residual risk can still be outside the organization's limits for risk taking, which might necessitate the implementation of additional or different controls. For example, hacking of corporate and government computer systems has become much more sophisticated, and, therefore, what was good internal control practice only a year or two ago may be inadequate today.

H.2.2 Poorly designed or implemented controls are a major source of risk and the design of controls themselves, as well as their implementation, should be subjected to risk assessment. In particular where the controls are in the form of written instructions or a procedure, then a suitable form of risk assessment should be used to test and optimize the controls and the process whereby they are implemented through training and communications.[6]

H.2.3 When should the monitoring and evaluation of individual controls occur? 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. Monitoring should include the investigation of

[5] The "Plan-Do-Check-Act Cycle," also called the Deming Cycle, is an iterative, four-step management process typically used in organizations for the control and continuous improvement of processes and products. For more information, see International Organization for Standardization's website.

[6] For example, through the use of a hazard and operability study (HAZOP), which is a structured assessment of a planned or existing control procedure in order to identify and evaluate weaknesses or deficiencies.

events and other incidents to determine how controls have performed and how they could be improved. Existing controls are also to be evaluated as part of every risk assessment and reassessment.

H.2.4 Who is responsible for monitoring and evaluation of individual controls?

- Firstly, those directly involved in the execution of the control activity should check the effective operation of the control as part of their control routine (i.e., self-control).
- Next are the managers who "own" the underlying risk and are responsible for the continued suitability and effective operation of the related controls. Ongoing monitoring, for example via their supervision of those involved in the execution of the control activity, is usually an effective practice as it is performed close to the operation of the control and relatively early in the process (as compared to separate evaluations that tend to be performed less frequently). Additionally, this reinforces the message that controls are an integral part of their responsibilities.
- In addition, independent monitoring and evaluation, for example, via internal and external audit, could provide additional, and more objective, assurance on maintaining the effectiveness of individual controls, for example as part of monitoring and evaluation of the internal control system (see H.3).

H.2.5 How should monitoring of individual controls be executed? Monitoring and evaluation of the effectiveness of applicable controls should be part of an individual's job responsibilities. In general, monitoring and evaluation should be performed by persons who are sufficiently competent. It is best if controls are allocated to designated individuals; the "control owners" (see Principle B, *Determining Roles and Responsibilities*). Management should also communicate methods for employees and others to report deficiencies in or breaches of established controls as part of the overall governance system.

H.2.6 When monitoring and evaluating individual controls, professional accountants can help their organization establish ongoing monitoring systems and recognize the value of direct evidence of effectiveness, such as error rates, customer complaints, and numbers and amounts of unmatched cash items. In fact, these are among the best sources of information on control failure.

H.2.7 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 ensuring that it will not happen again, all of which should be part of the continuous-improvement cycle;
- decommissioning outdated controls—while making sure that they are truly obsolete—to keep the internal control system effective;
- properly documenting the corrections of the 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.

H.3 Monitoring and evaluation of the internal control system

H.3.1 Even where internal control systems were previously effective, over time they can deteriorate and 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 guidelines—are in place and functioning well, for example, in accordance with this guidance.

H.3.2 Organizations need a structured process to ensure that the internal control system is being thoroughly evaluated on a timely basis.

H.3.3 When should internal control system monitoring occur? The actual timing should at least be dependent on the pace of internal and external change. For example, monitoring can take place periodically in tandem with the yearly business planning and evaluation cycle, or when there are indications of reduced effectiveness, such as several failures of individual controls.

H.3.4 Who should monitor the internal control system? The governing body, possibly supported by the audit committee, should ensure that the internal control system is periodically monitored and evaluated. The actual assessment can be executed by the organization's management. A staff person who is sufficiently independent from those responsible for the system, such as the internal auditor, could provide additional assurance on the effectiveness and cost efficiency of the internal control system.

H.3.5 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 risks associated with achieving objectives for these areas. 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.

H.3.6 Actions arising from the evaluation of the internal control system should include combining the results of the previous "Plan-Do-Check-Act 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 its limits for risk taking.

H.3.7 An integral part of the monitoring and evaluation of the internal control system is reporting the results and status of corrective action plans to the governing body to enable them to discharge their responsibilities.

How should the organization report on internal control performance?

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

PRINCIPLE I—Providing for Transparency and Accountability

The governing body, together with management, should periodically report to stakeholders the organization's risk profile as well as the structure and factual performance of the organization's internal

control system.

I.1 Organizations should transparently report on the structure and performance of their governance, risk management, and internal control system in their various reports to internal and external stakeholders, such as through their periodic accountability reports or on the organization's website.

I.2 However, organizations should not only report on 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 system works; and what has been done to remediate any control failures or weaknesses. A better understanding as to how an organization manages its risks creates trust and the necessary reassurance to its stakeholders.

I.3 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. A large portion of the information that is relevant for managerial decision making is also relevant for external stakeholders. However, competitive and confidentiality issues should be taken into account. Establishing open communication with stakeholders about the organization's governance, risk management, and internal control is instrumental in this respect.

I.4 Organizations should develop a mechanism to incorporate relevant feedback from the various stakeholders into their internal control system.

Appendix A: Definitions

Internal control: IFAC recognizes that the term "internal control" can have multiple meanings, including:

- A system or process: the entirety of an organization's internal control system, i.e., an organization's internal control system.
- An activity or measure: the actual measure to treat risks and to effectuate internal control, i.e., individual controls.
- A state or outcome: the outcome of the internal control system or process, i.e., an organization achieving or sustaining appropriate or effective internal control.

These three meanings are further defined below.

Internal control system or process: based on the definition used by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the International Auditing and Assurance Standards Board defines internal control as, "the process designed, implemented, and maintained by those charged with governance, management, and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations."

An enriched and broadened definition of internal control, taking into account some of the suggestions of IFAC's *Global Survey on Risk Management and Internal Control* (2011), would be: Internal control is an integrated part of an organization's governance system and risk management, which is understood, effected, and actively monitored by the organization's governing body, management, and other personnel, to take advantage of opportunities and to counter the threats, in line with risk management strategy and policies on internal control set by the governing body to achieve an organization's objectives through, among other things:

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

Internal control activity or measure: activities performed to treat risks and effectuate internal control. Examples of actual control activities include managerial controls, such as executing the "Plan-Do-Check-Act Cycle," or transaction controls, such as verifications, reconciliations, authorizations, physical controls, and supervisory controls that oversee transaction controls. Internal control as an activity or measure is sometimes simply referred to as "control."

Internal control as a state or outcome: an organization is "in control," when it has achieved its internal control objectives.

Internal control objective: desired level of internal control, achieved by treating the risks an organization faces in accordance with its risk management strategy and policies on internal control, while achieving the organization's objectives.

Risk: ISO *Standard 31000:2009—Risk Management* (see Appendix B) defines risk as "the effect of uncertainty on objectives," which can be positive or negative.

Risk management: ISO *Standard 31000:2009—Risk Management* defines risk management as, "coordinated activities to direct and control an organization with regard to risk."

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.[7] This definition reflects both the performance and conformance aspects of governance.

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.

Governing body: the person(s) or body (e.g., a board of directors) with primary responsibility for overseeing the strategic direction of the organization and 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, remuneration, and ethics committees. 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.

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 internal factors defined by the officers, shareholders, or constitution of an organization, as well as external forces, such as consumer groups, clients, and regulators.

Performance: policies and procedures that focus on opportunities and risks, strategy, value creation, and resource utilization, and 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.

Useful information: if information is to be useful, it must be relevant and faithfully represent what it purports to represent. The usefulness of information is enhanced if it is comparable, verifiable, timely and understandable. This is aligned with the definition of useful financial information in the *Conceptual Framework for Financial Reporting* (International Accounting Standards Board, 2010).

Tone at the top: the words and deeds of an organization's governing body and senior management that determine its values, culture, and the behavior and actions of individuals; also defined as "leading by example" or "walking the talk."

---

7 *Board Briefing on IT Governance, 2nd Edition* (IT Governance Institute, 2003)

Appendix B: Resources

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* (IFAC, 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.
- *Internal Control from a Risk-Based Perspective* (IFAC, 2007) includes ten senior-level professional accountants in business who share their experiences and views on establishing effective internal control systems.
- *Global Survey on Risk Management and Internal Control—Results, Analysis, and Proposed Next Steps* (IFAC, 2011) contains over 600 responses from around the globe and provides an analysis of survey results and summarizes respondents' recommendations for the next steps in this area.
- The IGPG *Evaluating and Improving Governance in Organizations* (IFAC, 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.
- *Integrating the Business Reporting Supply Chain* (IFAC, 2011) features 25 prominent business leaders provide their recommendations on what should be done to effectively improve governance (including risk management and internal control), 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* (IFAC, 2011) outlines the diverse roles of professional accountants in business and the many ways they serve their employers and the public interest.
- *Enterprise Risk Management—Integrated Framework* (COSO, 2004) expands on internal control and provides key principles and concepts on the broader subject of enterprise risk management. A summary can be downloaded at the COSO website at www.coso.org.
- COSO is also set to release its revised *Internal Control—Integrated Framework* and companion documents in early 2013. Visit the COSO website for further information.
- *Standard 31000:2009—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.
- *HB158: Delivering Assurance Based on ISO 31000:2009 Risk Management—Principles and Guidelines* (Standards Australia, Standards New Zealand, and the Institute of Internal Auditors—Australia, 2010) describes how to develop a risk-based assurance strategy and program, plan an assurance engagement, report the assurance program, and design controls.

- On March 1, 2010, the *King Code of Governance for South Africa* (King III) came into effect. The code recommends companies maintain effective governance, risk management, and internal control system.
- IDW Accounting Standard IDW RS FAIT 1 *Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie* (*Principles of Proper Booking When Applying Information Technology*] (Institut der Wirtschaftsprüfer, 2002) is Germany's generally recognized standard on internal control over financial reporting.
- *Managing Opportunities and Risks* (Certified Management Accountants Association of Canada, 2012) explores ways to use the risk management process to exploit opportunities, drive organizational innovation, and generate short- and long-term profits.
- *Rules for Risk Management: Culture, Behaviour and the Role of Accountants* (Association of Chartered Certified Accountants, 2012) examines members' views of integrated risk management and the role that accountants play, both in terms of the role that they play now and the extent to which their expertise could be used in more effectively managing risk in the future.
- *Basic Standard for Enterprise Internal Control* (Chinese Ministry of Finance, Chinese National Audit Office, China Securities Regulatory Commission, China Banking Regulatory Commission, and China Insurance Regulatory Commission, 2008) applies to all companies listed on the Shanghai and Shenzhen stock exchanges. Large, non-listed and listed medium-sized Chinese companies will also be encouraged to adopt its provisions. More information on the Chinese-language document is available in English from KPMG and *China Briefing*.
- *Internal Control: Guidance to Directors* (UK Financial Reporting Council, 2005), also known as the Turnbull guidance, sets out best practice on internal control for UK listed companies, and assists them in applying the UK Corporate Governance Code.
- COBIT®, developed and issued by ISACA, is a business framework for the governance and management of enterprise IT that allows managers to bridge the gap between control requirements, technical issues, and business risk.
- *A Framework for Board Oversight of Risk* (Canadian Institute of Chartered Accountants, 2012) provides a practical approach to risk oversight designed specifically for boards of directors, including a framework, methodology, and toolsets.

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

Exposure Drafts, Consultation Papers, and other IFAC publications are published by, and copyright of, IFAC.

IFAC does not accept responsibility for loss caused to any person who acts or refrains from acting in reliance on the material in this publication, whether such loss is caused by negligence or otherwise.

The IFAC logo, 'International Federation of Accountants', and 'IFAC' are trademarks and service marks of IFAC.

Copyright © June 2012 by the International Federation of Accountants (IFAC). All rights reserved. Permission is granted to make copies of this work provided that such copies are for use in academic classrooms or for personal use and are not sold or disseminated and provided that each copy bears the following credit line: *"Copyright © June 2011 by the International Federation of Accountants (IFAC). All rights reserved. Used with permission of IFAC. Contact permissions@ifac.org for permission to reproduce, store or transmit this document."* Otherwise, written permission from IFAC is required to reproduce, store, transmit, or make other similar uses of this document, except as permitted by law. Contact permissions@ifac.org.

ISBN: 978-1-60815-123-3

Published by: International Federation of Accountants

529 Fifth Avenue, 6th Floor, New York, NY 10017
T + 1 (212) 286-9344 **F** +1 (212) 286-9570
www.ifac.org