Appendix A

Guide for Commentators

The aim of this International Good Practice Guidance (IGPG) is to establish a benchmark for good practice in maintaining effective internal control, and in particular, to help professional accountants in business (PAIB) 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?

a. No, the title Evaluating and Improving Internal Control in Organizations is misleading. It conveys this IGPG as a comprehensive evaluation guide.

According to sections 1.4 and 2.4, this IGPG complements existing IC frameworks. Section 3.2 states this IGPG aims at helping PAIBs to evaluate and improve internal control systems by highlighting **only those areas (with their related control principles) where practical application of internal control framework often fails or could be improved in organizations.**

PAIB should make it very clear that this is NOT a comprehensive guide. We recommend reinforcing this by make the following changes:

3.2 "These principles are not meant to be a comprehensive set of principles formulated to design and implement a system of internal control…but to facilitate evaluating and improving existing internal control system…"

The title should clearly convey that the principles presented do not constitute a complete set. We propose the following alternative titles for consideration:

- Focus Areas for Evaluating and Improving Internal Control in Organizations
- Watch List for Evaluating and Improving Internal Control in Organizations
- Common Deficiencies/Weaknesses/Challenges/Improvement Opportunities in Implementing Internal Control System
- Supplemental Guidance for Evaluating and Improving Existing Internal Control Systems
- Guidance for Complementing Internal Control Frameworks

b. The term internal control fits in the context of this IGPG.

2. Are the Internal Control definitions in Appendix A suitable for this guidance? Can or should they be further clarified? **(See track changes for recommendations)**

As defined in Appendix A., internal control is an integrated part of an organization's governance and risk management system, which is effected, understood, executed, and actively ~~followed~~ monitored by the organization's governing body, management, and other personnel, to ~~exploit~~ take advantage of opportunities and to manage the risks within the risk tolerances established by the governing body in achieving the organization's objectives through:

a) executing effective and efficient ~~strategic and operational~~ processes;

b) providing reliable information ~~to internal and external users~~ for timely and ~~effective~~ informed decision making;

c) ensuring conformance with applicable laws and regulations, as well as with the organization's own policies, procedures, and guidelines;

d) safeguarding the organization's resources against loss, fraud, misuse, and damage and;

e) safeguarding the availability, confidentiality, and integrity of the organization's information ~~systems~~, including IT systems.

The scope of internal control covers objectives, plans, information, policies, procedures, processes, systems, activities, functions, projects, initiatives, and endeavors of all types at all levels of a company, as well as "tone at the top" and other intangibles that influence the organizational culture.

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?

This question contradicts the purpose of the IGPG. According to 2.4, this IGPG is not an internal control framework; it should be used to complement other control frameworks. Since this IGPG only focuses on those areas where internal control is often applied incorrectly in organizations, by design this is not intended to provide comprehensive coverage of all the fundamental areas for evaluating and improving internal control. The areas are included if practical application fails.

If the intention is to provide comprehensive coverage of all fundamental areas for evaluating and improving internal control, a better approach would be to use or refer to an authoritative framework such as Turnbull, Coco or COSO, as the basis and link the specific areas where practical application of internal control framework often fails or could be improved in organizations.

The Guidance

4. Is the application guidance for each principle adequate to guide good practice?

The application guidance for each principle is adequate. We recommend making the following changes to clarify and enhance the IGPG; the proposed changes are underlined. Most of the changes are self-explanatory. Where appropriate, we included reasons for the suggested changes in parentheses.

3.2 B. "… (including governing body… management at all levels, employees, internal and external auditors…" (Employees are critical to the organization).

3.2 H. Add: "The organization should recognize and consider the residual risk after taking control into account..."

"Identification of unmanaged significant risks…or previously undetected conditions …" (Use condition instead of errors, to include all types of exceptions)

4.1 The answer does not address the question regarding scope of internal control. The question and the answer do not align well with Principle A and its application guidance.

4.1 A.1 "… Risk should not (rather than cannot) be taken ..." (We believe this is the intent).

4.1 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…in that risk management focuses on the identification …"

"Internal controls are risk controls, and once this is properly understood, one of the greatest barriers to integration will be removed." (The original text does not recognize that there are many other barriers to integration, gaining a proper understanding is only one of the barriers).

4.1 A.3 "…it can result in an enterprise-wide governance, risk management, and control system …"

"…Integrates and aligns activities…related to objective setting, planning …"

4.1 A.4 "…ensuring that operational controls exist and (instead of or) are functioning as intended …"

4.1 A.5 "Are risks only managed …, or is consideration also given …" (It has already been established that consideration should be given, therefore the question should focus on execution).

4.2 The answer does not address the question. The question was on responsibility; the answer was on authority.

4.2 B.1 Second bullet, "Management should design….appropriate for the risk strategy and internal control policies …"

Third bullet," Each person within the organization…should be held accountable for understanding the risks and the rationale of internal control activities, executing the controls as designed, and managing specific risks within his or her span of authority." (Not understanding the risks and the reasons for the controls are root causes for control breakdowns).

4.4 "There is a risk that people with assigned internal control responsibilities might not have sufficient …" (It is better than might have insufficient).

4.4 D.1 Add: Knowledgeable about the principles of the segregation of duties to ensure incompatible duties are properly segregated so that, no individual has total control over a transaction.

Being able to monitor and execute changes related to objectives, strategies, policies and procedures, processes and systems, reassess the associated risks and develop appropriate risk controls and responses for the changes. (Change is a key risk that needs to be managed).

4.4 D2. While professional accountants 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 their financial support to serve in these roles. With this sponsorship they can help enhance…

4.5 E.2 "Another important element...with respect to governance, risk management and internal control…"

Add: More important than just having a code, management should continually reinforce its principles in word and deed, with training programs, and by taking appropriate actions in response to violations.

4.5 E.3 "Good "tone-at-the-top" …with respect to governance, risk management and internal control… management and employee meetings." (Messages and directives need to reach the employee).

4.5 E.4 "…the importance of governance, risk management and internal controls."

4.6 F.1 "…When designing, implementing, operating or assessing internal controls, the first question should be what are the risks to the business objective? The next question is how are these risks managed? Finally, are the risk management techniques (including controls) well-designed, and are they operating effectively?" (The original text implies that we first identify the control and then, ask which risk(s) each control mitigates. This approach will not identify missing controls.)

4.6 F.5 Replace too much attention on control by overly stringent control requirements. (we believe this is the intent).

4.6 F.6 The concept addressed in this section is critical. Internal controls are not the only method of responding to risk. This concept should be addressed earlier and more prominently in the IGPG.

Remove (by doing nothing); accepting the risk is making a decision.

4.6 F.7 "…taking into account – reputational, economic…the payment of even a small bribe can cause very serious reputational damages to any organization. "

4.6 F.8 "Finally, external developments that change the risk factors or levels may …"

4.7 G.4 "and determining how changes in the internal control system are to be approved, implemented and monitored."

4.7 G.5 "This reality must be considered in ensuring effective dissemination of the organization's internal control policies and procedures..."

4.8 H2.1 Change design fault to flaw and operational fault to flaw.

4.8 H2.2 These possible causes should be combined under 4.8 H.2.1.

4.8 H2.3 "When should the monitoring of controls occur? " (Change was made to clarify the original text, "When should monitoring controls be done?" In this case monitoring can be interpreted as an adjective instead of a verb).

4.8 H2.4 Recommend linking assurance to The Three Lines of Defense Model.

Add: The Three Lines of Defense Model is often used to communicate the roles played by management, business-enabling functions, and internal audit in providing assurance on internal controls. The First Line of Defense is operations management and employees. The Second Line of Defense is centralized business-enabling functions with specialized skills, such as Risk Management, Internal Controls, Legal and Regulatory Compliance, Quality, and Security. The Third Line of Defense is Internal Audit. Internal Audit provides independent and objective assurance on the effectiveness of governance, risk management and control practices including the effectiveness of management's and business-enabling functions' monitoring control.

4.8 H2.7 "…such as error rates, customer complaints, and numbers and amount of unmatched cash items. In fact this is one of the best sources of information for control failures." (The original text was "risks that occur frequently," control failures seem a better fit).

4.8 H2.8 Add two bullets:

"Determining whether the risks which the control is intended to address are still relevant."

"Determining whether the control is still appropriate for the current risks."

(These two steps are important to ensure risk and controls are assessed against current condition).

4.8 H3.3 Switch the sentences to read: "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 revision of strategy, or when there are implications of reduced effectiveness, such as several failures of individual controls." (Improve the flow).

4.8 H3.4 "The actual assessment can be accomplished through an integrated approach among the organization's management, finance, and internal audit function"

4.8 H3.5 "… The internal control system….evaluated against risk management strategy, internal control policies and an acceptable internal control framework…"

4.8 H3.6 "Actions arising from the evaluation should include combining the results of the previous cycle with new input." (It is not clear what the previous cycle refers to).

4.8 H3.7 "An integral part of the … is reporting the results and status of corrective action plans to the governing body to enable them to discharge their responsibilities."

4.9 I3 "…Establishing open communication…organization's governance, risk management and internal control…"

5. Are there other resources on internal control that should be considered for inclusion in the appendices?

We recommend adding the following:

- Other key internal control models such as Coco and Turnbull.
- The King III Report on Corporate Governance.
- Financial Reporting Council Internal Control – Guidance for Directors on the Combined Code UK.

Other Issues

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

We believe there is benefit to issuing an integrated IGPG on governance, risk management and internal control. As noted in section 1.2, internal control is a subset of risk management, which in turn is a subset of governance. The need to have an integrated guidance was highlighted by respondents to IFAC's *Global Survey on Risk Management and Internal Control* (2011).

As noted in section 2.3, the IFAC's *Global Survey on Risk Management and Internal Control* (2011) 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 the 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.

Additional Comments

We offer the following comments and suggested changes for consideration.

- There are several references to internal control being an integral part of risk management. We recommend adding governance to be consistent with the diagram in section 1.2.

- The IGPG advocates having PAIBs serve as consultants, coaches, and trainers on internal controls for the organization. For example, 4.3 C.3 indicated that "The professional accountants in business should ensure that information on control objectives and control performance is incorporated into various organizational and personal and/or team performance management systems." Additional statements in sections 4.1 A5, 4.2 B1 & B4, 4.4 D2 and 4.7 G6 similarly encourage PAIBs to take a leading role in internal control matters throughout all aspects of an organization.

  However, PAIBs typically have accounting related credentials and experience, and are usually assigned to the Accounting function. For PAIBs to operate as encouraged in the IGPG, they need to have broader competencies than many, or most, PAIBs may have. PAIBs should be cautioned to ensure they have these competencies and will need sponsorship from senior management to promote internal controls and assist management in evaluating and improving internal controls outside their function.

  PAIBs should collaborate with internal audit on internal control related matters. Internal audit is an independent, objective assurance and consulting activity. Evaluating and improving the effectiveness of risk management, control, and governance processes in the organization is its core mission. Internal audit reports to the Audit Committee or other governing body; it has a broad mandate and Board sponsorship.

- The term "occurring risks" is an odd term; it can be replaced by "risks" throughout the IGPG.

Presentation

- In section 4, recommend moving the numbers (e.g., 4.1, 4.2, 4.3, etc.) associated with the answers to the questions.

- Appendix A. Definition

  The format for presenting the definitions is inconsistent. For the first two, Internal Control and Risk Management, the definitions start on a separate line. From Governance through Stakeholder Value, the definitions start on the same line, making them appear to be part of the definition of Risk Management.

Other Suggested Changes

See underlined text for suggested addition or changes.

1.1 Exploit has a negative connotation in some countries and we recommend changing to "take advantage of".

1.2 Internal control is an integral part of …, to be consistent with various definitions of risk management and governance system.

Recommend adding the concept of monitoring which is a key role of the governing body.

1.4 Combine 1.4 and 2.4 to eliminate the duplication.

2.2 "…in some financial institutions – governance, risk management and internal control…Moving forward……are impacted by many interdependent variables."

Appendix A. Definitions (The original text is Internal Control Definition and we recommend removing Internal Control to make it less prescriptive).

- Governance Definition. We recommend using definition in the King III Report on Corporate Governance; it is more current.

- We recommend changing conformance to: "Compliance with laws…policies, procedures, guidelines and contractual agreements…"

- Performance - the definition refers to policies and procedures. Recommend changing to something along the line of "Ability to take advantage of opportunities and risks, execute strategy, create value and achieve objectives."