

Proposed Principles to be addressed in APES 325 Risk Management for a Firm

Scope of the Project

The proposed APES 325 *Risk Management for a Firm* will establish the basic principles and essential procedures with respect to a Member in Public Practice's responsibilities for Risk Management for their practice.

Key Definitions

It is proposed that the Standard will include the following key definition:

Option 1

Risk Management means a process, undertaken by the Firm's Partners, management and other Personnel, applied in strategy setting and across the Firm, designed to identify potential events that may affect the Firm, and manage risk to be within its risk appetite, and to provide Reasonable Assurance regarding the achievement of the Firm objectives.

[Adapted from COSO Enterprise Risk Management – Integrated Framework (September 2004)]

Option 2

Risk Management means the systematic application of policies, procedures and practices aimed at avoiding, reducing or controlling risks.

[Adapted from CPA Australia's Risk Management Statement 1 (October 2003)]

Proposed Professional and Ethical Obligations

It is proposed that Risk Management for a Firm must be addressed from a public interest perspective and take into consideration different sizes of Firms.

In developing this Proposed Principles paper, the requirements of CPA Australia's RMS 1 *Risk Management Statement* were considered and mapped to the requirements of other APES Standards (refer attached document – *Mapping: Proposed APES 325 Risk Management, RMS 1 and other APES Standards*). Requirements not addressed in other APES Standards were considered for inclusion in this paper and where appropriate cross-references can be built into the proposed APES 325 for requirements already addressed in other APES Standards.

Fundamental Responsibilities

The proposed Standard will impose professional and ethical obligations based on the following principles and key requirements of the Code in a similar manner to other APES Standards:

- Public Interest; and
- Professional Competence and Due Care.

Coverage

The proposed Standard will contain requirements applicable to Members in Public Practice to address the following key areas:

(i) Design of a System of Risk Management

An obligation on the Firm to establish and maintain a system of Risk Management designed to:

- Be proactive in identifying and managing the Firm's risk;
- Ensure business continuity (including succession planning);
- Protect the reputation, credibility and status of the Firm; and
- Comply with relevant legal and regulatory requirements.

Guidance to acknowledge that a smaller Firm may have a less sophisticated system of Risk Management.

(ii) System of Risk Management – Policies and Procedures

To establish and maintain a system of Risk Management that includes policies and procedures, which address the following matters:

- Governance risk;
- Business continuity (including succession planning);
- Identification, assessment and responses to entity level risks;
- Identification, assessment and responses to legislative and regulatory requirements;
- Financial risk;
- People – including risks associated with recruitment/retention, accreditation/training, safety; and
- Technology risk – including computer hardware, software, communication.

(iii) Leadership Responsibilities

Responsible personnel within a Firm must establish policies and procedures designed to promote an internal culture recognising that Risk Management is essential for effective practice management in performing Professional Services of the highest quality, protecting the public interest and maintaining the reputation of the Firm.

The proposed Standard must stipulate that the Firm's chief executive officer (or equivalent) or, if appropriate, the Firm's managing board of Partners (or equivalent), assume ultimate responsibility for the Firm's system of Risk Management.

The Firm's chief executive officer or, if appropriate, the Firm's managing board of Partners shall ensure that any person or persons assigned operational responsibility for the Firm's system of Risk Management have sufficient and appropriate experience and ability, and the necessary authority to assume that responsibility.

(iv) Documentation

The proposed Standard must mandate that responsible personnel within a Firm document its policies and procedures in respect of Risk Management and to communicate them to the Firm's Personnel.

Guidance to acknowledge that a smaller Firm may have less detailed documentation.

(v) Monitoring

The proposed Standard must mandate that responsible personnel within a Firm must establish a monitoring process designed to ensure that the Risk Management policies and procedures relating to the system of Risk Management are relevant, adequate, and operating effectively.

The monitoring process shall:

- include ongoing consideration and evaluation of the Firm's system of Risk Management; and
- require responsibility for the monitoring process to be assigned to a Partner or Partners or other persons with sufficient and appropriate experience and authority in the Firm to assume that responsibility.

International Developments

The International Federation of Accountants (IFAC) Small and Medium Practices (SMP) Committee *Guide to Practice Management* is expected to be released in the second quarter of 2010. A review of the Risk Management principles and/or guidance contained in IFAC's Guide will be undertaken once it is released.