Proposed Standard: APES 325 Risk Management for Firms

Prepared and issued by
Accounting Professional & Ethical Standards Board Limited

EXPOSURE DRAFT **XX/11**
ISSUED: [DATE]

Commenting on this Exposure Draft

Comments on this Exposure Draft should be forwarded so as to arrive by **XX XX 2011**.

Comments should be addressed to:

The Chairman
Accounting Professional & Ethical Standards Board Limited
Level 7, 600 Bourke Street
MELBOURNE VIC 3000
AUSTRALIA
E-mail: sub@apesb.org.au

A copy of all submissions will be placed on public record on the APESB website: www.apesb.org.au.

Obtaining a copy of this Exposure Draft

This Exposure Draft is available on the APESB website: www.apesb.org.au. Alternatively, any individual or organisation may obtain one printed copy of this Exposure Draft without charge until **XX XX 2011** by contacting:

Accounting Professional & Ethical Standards Board Limited
Level 7
600 Bourke Street
Melbourne Victoria 3000
Australia
E-mail: enquiries@apesb.org.au
Phone: (03) 9670 8911
Fax: (03) 9670 5611

Reasons for issuing Exposure Draft XX/11

Accounting Professional & Ethical Standards Board Limited (APESB) proposes to issue the Standard APES 325 *Risk Management for Firms* setting out mandatory requirements and guidance for Members in Public Practice.

CPA Australia has an existing risk management standard - *RMS 1 Risk Management Statement (RMS 1)* which is applicable to CPA Australia Members who are in public practice. CPA Australia has indicated to the APESB that if the APESB issues a similar standard to RMS 1then CPA Australia will withdraw RMS 1 in due course.

The Institute of Chartered Accountants in Australia also has existing guidance *N3 Risk Management Guidelines* which provides guidance to their Members in Public Practice.

Key requirements and guidance in ED XX/11

The proposed APES 325 includes mandatory requirements and guidance in respect of:

- Objective of a Risk Management Framework;
- Establishing and maintaining a Risk Management Framework for a Firm;
- Monitoring a Firm's Risk Management policies and procedures; and
- Documentation.

Proposed operative date

It is intended that this Standard will be operative from **XX XX 2011**.

Request for comments

Comments are invited on this Exposure Draft of APES 325 *Risk Management for Firms* by **XX XX 2011**. APESB would prefer that respondents express a clear overall opinion on whether the proposed Standard, as a whole, is supported and that this opinion be supplemented by detailed comments, whether supportive or critical, on any matter. APESB regards both critical and supportive comments as essential to a balanced view of the proposed Standard.

APES 325 Risk Management for Firms

Prepared and issued by
Accounting Professional & Ethical Standards Board Limited

ISSUED: [DATE]

ED XX-11 APES 325_Draft_1L_18 Apr 2011 - Clean copy

APES 325
Risk Management for Firms

(Issued XXXXXXXX 201X)

CONTENTS

1 Scope and application

1.1 Accounting Professional & Ethical Standards Board Limited (APESB) issues professional standard APES 325 *Risk Management for Firms* (**the Standard**). A Risk Management Framework in compliance with this Standard is required to be established by Firms by XX XX 2011. Earlier adoption of this Standard is permitted.

1.2 APES 325 sets the standards for Members in Public Practice and Firms to establish and maintain a Risk Management Framework at the Firm level in the provision of quality and ethical Professional Services. The mandatory requirements of this Standard are in **bold type (black lettering)**, preceded or followed by discussion or explanation in normal type (grey type). APES 325 should be read in conjunction with other professional duties of Members, and any legal obligations that may apply.

1.3 Members in Public Practice in Australia shall follow the mandatory requirements of APES 325.

1.4 Members in Public Practice practising outside of Australia shall follow the provisions of APES 325 to the extent to which they are not prevented from so doing by specific requirements of local laws and/or regulations.

1.5 Notwithstanding paragraphs 1.3 and 1.4, this Standard does not require compliance with a requirement that is not relevant in the circumstances of a smaller Firm. For example, a sole practitioner with no Staff will not have to assign the responsibility to manage the Risk Management Framework to suitable Personnel as specified in paragraph 4.4.

1.6 Members in Public Practice shall be familiar with relevant Professional Standards and guidance notes when providing Professional Services. All Members shall comply with the fundamental principles outlined in the Code.

1.7 The Standard is not intended to detract from any responsibilities which may be imposed by law or regulation.

1.8 All references to Professional Standards, guidance notes and legislation are references to those provisions as amended from time to time.

1.9 In applying the requirements outlined in APES 325, Members in Public Practice should be guided not merely by the words but also by the spirit of the Standard and the Code.

2 Definitions

For the purpose of this Standard:

Code means APES 110 *Code of Ethics for Professional Accountants*.

Engagement means an agreement, whether written or otherwise, between a Member in Public Practice and a Client relating to the provision of Professional Services by a Member in Public Practice. However, consultations with a prospective Client prior to such an agreement are not part of an Engagement.

Firm means:

(a) A sole practitioner, partnership, corporation or other entity of professional accountants;

(b) An entity that controls such parties through ownership, management or other means;

(c) An entity controlled by such parties through ownership, management or other means; or

(d) An Auditor-General's office or department.

Member in Public Practice means a Member, irrespective of functional classification (e.g. audit, tax, or consulting) in a Firm that provides Professional Services. The term is also used to refer to a Firm of Members in Public Practice and means a practice entity as defined by the applicable Professional Body.

Monitoring means a process comprising an ongoing consideration and evaluation of the Firm's Risk Management Framework designed to provide the Firm with Reasonable Assurance that its Risk Management Framework is operating effectively.

Network means a larger structure:

(i) that is aimed at cooperation; and

(ii) that is clearly aimed at profit or cost-sharing or shares common ownership, control or management, common quality control policies and procedures, common business strategy, the use of a common brand name, or a significant part of professional resources.

Partner means any individual with authority to bind the Firm with respect to the performance of a Professional Services Engagement.

Personnel means Partners and Staff.

Professional Services means services requiring accountancy or related skills performed by a Member in Public Practice including accounting, auditing, taxation, management consulting and financial management services.

Professional Standards means all standards issued by the Accounting Professional & Ethical Standards Board and all professional and ethical requirements of the applicable Professional Body.

Reasonable Assurance means in the context of this Standard a high, but not absolute, level of assurance.

Relevant Ethical Requirements means ethical requirements which ordinarily comprise Parts A and B of the Code.

Risk means the effect of uncertainty on objectives.

[Editorial note: definition from AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines]

Risk Management means coordinated activities undertaken by a Firm, including its internal culture, to direct and control the activities of the Firm with regard to Risk.

[Editorial note: adapted from AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines]

Risk Management Framework means a set of elements that provide the foundations and the Firm's arrangements for designing, implementing, Monitoring, reviewing and continually improving Risk Management throughout the Firm.

The foundations to manage risk include:

- The policies;
- objectives;
- mandate; and
- commitment.

The Firm's arrangements to manage risk include:

- plans;
- relationships;
- accountabilities;
- resources;
- processes; and
- activities.

Staff means professionals, other than Partners, including any experts the Firm employs.

3 Objective of a Risk Management Framework

3.1 An effective Risk Management Framework will assist a Firm to meet its overarching public interest obligation as well as its business objectives. A proper system of risk management will help achieve this by:

(a) facilitating business continuity;
(b) ensuring clients receive high quality services;
(c) protecting the reputation and credibility of the Firm; and
(d) meeting other public interest obligations as set out in the Code.

3.2 The Risk Management Framework consists of policies designed to achieve the objectives set out in paragraph 3.1 and the procedures necessary to implement and monitor compliance with those policies. The Risk Management Framework needs to be embedded within the Firm's overall strategic and operational policies and practices.

3.3 The requirements are designed to enable a Firm to achieve the objective stated in this Standard. The proper application of the requirements is therefore expected to provide a sufficient basis for the achievement of the objective. However, because circumstances vary widely and all such circumstances cannot be anticipated, the Firm should consider whether there are particular matters or circumstances that require the Firm to establish policies and procedures in addition to those required by this Standard to meet the stated objective.

4 Establishing and maintaining a Risk Management Framework for a Firm

4.1 A Firm shall establish and maintain a Risk Management Framework for the Firm taking into consideration the Firm's public interest obligations.

4.2 The Firm's Risk Management Framework shall include, but not be limited to, policies and procedures that identify, assess and manage the following elements:

(a) Governance risk;

(b) Business continuity (including succession planning);

(c) Business risks;

(d) Financial risks;

(e) Legislative and regulatory requirements;

(f) Potential impact of the assessed risk;

(g) Risks associated with the recruitment, retention, accreditation, training and safety of Staff; and

(h) Technology risks – including computer hardware, software, communication.

4.3 The nature and extent of the policies and procedures developed by an individual Firm to comply with this Standard will depend on various factors such as the size and operating characteristics of the Firm, and whether it is part of a Network.

4.4 A Firm shall require the Firm's chief executive officer (or equivalent) or, if appropriate, the Firm's managing board of Partners (or equivalent), to assume ultimate responsibility for the Firm's Risk Management Framework.

4.5 The Firm's leadership and the examples it sets significantly influence the internal culture of the Firm. The adoption of an appropriate internal culture by a Firm is dependent on clear, consistent and frequent actions and messages from all levels of the Firm's management that emphasise the Firm's Risk Management policies and procedures.

4.6 A Firm shall ensure that the Personnel assigned responsibility for establishing and maintaining its Risk Management Framework have the capacity to understand the entire text of this Standard, including its application and other explanatory material, to understand its objective and to apply its requirements properly.

4.7 Sole practitioners and small Firms are referred to *Module 7: Risk Management* of the *Guide to Practice Management for Small and Medium-sized Practices* issued by the Small and Medium Practice Committees of the International Federation of Accountants.

5 Monitoring a Firm's Risk Management policies and procedures

5.1 A Firm shall establish a Monitoring process designed to provide Reasonable Assurance that the Risk Management policies and procedures relating to the Risk Management Framework are relevant, adequate, and operating effectively. The Firm shall:

(a) Include an ongoing consideration and periodic evaluation of the Firm's Risk Management Framework; and

(b) Require responsibility for the Firm's Monitoring process to be assigned to suitable Personnel with sufficient and appropriate experience and authority in the Firm to assume that responsibility.

5.2 The purpose of Monitoring compliance with Risk Management policies and procedures is to provide an evaluation of:

- Whether the Risk Management Framework has been appropriately designed and effectively implemented; and
- Whether the Firm's Risk Management policies and procedures have been appropriately applied.

6 Documentation

6.1 A Firm shall document its policies and procedures in respect of Risk Management and communicate them to the Firm's Personnel.

6.2 In general, communication of Risk Management policies and procedures to Firm's Personnel includes a description of the Risk Management policies and procedures and the objectives they are designed to achieve, and the message that each individual has a personal responsibility for Risk Management and is expected to comply with these policies and procedures. Encouraging Firm's Personnel to communicate their views or concerns on Risk Management matters recognises the importance of obtaining feedback on the Firm's Risk Management Framework.

6.3 The form and content of documentation evidencing the operation of each of the elements of the Risk Management Framework is a matter of judgment and depends on a number of factors, including the following:

- The size of the Firm and the number of offices;
- The nature and complexity of the Firm's practice and the services provided.

6.4 Smaller Firms may use more informal methods in the documentation of their Risk Management Framework such as manual notes, checklists and forms.

6.5 Appropriate documentation of the Firm's Risk Management processes should include, for example:

- Risk Management Framework;
- Procedures for identifying potential risks;
- Procedures for managing risks;
- Regular review of the Risk Management Framework;
- Risks identified;
- Documentation processes; and

- Training of Staff.

6.6 A Firm shall establish policies and procedures that require retention of documentation for a period of time sufficient to permit those performing Monitoring procedures to evaluate the Firm's compliance with its Risk Management Framework, or for a longer period if required by law or regulation.

Conformity with International Pronouncements

The International Ethics Standard Board for Accountants (IESBA) has not issued a pronouncement equivalent to APES 325.