

# APES 325 Risk Management for Firms

Prepared and issued by  
Accounting Professional & Ethical Standards Board Limited

ISSUED: November 2011

Copyright © 2011 Accounting Professional & Ethical Standards Board Limited (“APESB”). All rights reserved. Apart from fair dealing for the purpose of study, research, criticism and review as permitted by the Copyright Act 1968, no part of these materials may be reproduced, modified, or reused or redistributed for any commercial purpose, or distributed to a third party for any such purpose, without the prior written permission of APESB.

Any permitted reproduction including fair dealing must acknowledge APESB as the source of any such material reproduced and any reproduction made of the material must include a copy of this original notice.

**APES 325**  
**Risk Management for Firms**

(Issued November 2011)

**CONTENTS**

---

	<b>Paragraphs</b>
Scope and application	1
Definitions	2
Objectives of a Risk Management Framework	3
Establishing and maintaining a Risk Management Framework for a Firm	4
Monitoring a Firm's Risk Management policies and procedures	5
Documentation	6
<i>Conformity with International Pronouncements</i>	

---

## 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 1 January 2013. Earlier adoption of this Standard is permitted.
- 1.2 APES 325 sets the standards for Members in Public Practice to establish and maintain a Risk Management Framework in their Firms in respect of the provision of quality and ethical Professional Services. Members have a responsibility, whether as owner, partner or employee, to ensure that the Firm implements the requirements of the Standard. The level of responsibility will depend on the position held by each Member in the Firm, but as a minimum all Members should participate in the Firm achieving the objectives of the Standard. The Standard adopts the Firm as the overarching entity which must implement the requirements of the Standard, but it is the Firm's Members in Public Practice who have responsibility to ensure this occurs.
- 1.3 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 in Public Practice, and any legal obligations that may apply.
- 1.4 **Members in Public Practice conducting the operations of a Firm in Australia shall follow the mandatory requirements of APES 325.**
- 1.5 **Members in Public Practice conducting the operations of a Firm outside 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.**
- 1.6 **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 ongoing consideration and evaluation of the Firm's Risk Management Framework designed to provide reasonable confidence that the Firm's 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.

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

**Risk** means the effect of uncertainty on objectives.

**Risk Management** means coordinated activities undertaken by a Firm, to direct and control the activities of the Firm with regard to Risk.

**Risk Management Framework** means the foundations<sup>1</sup> and organisational arrangements<sup>2</sup> for designing, implementing, Monitoring, reviewing and continually improving Risk Management throughout the Firm.

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

### 3 Objectives of a Risk Management Framework

- 3.1 An effective Risk Management Framework should assist a Firm to meet its overarching public interest obligations as set out in the Code as well as its business objectives by:
- (a) Facilitating business continuity;
  - (b) Enabling quality and ethical services to be rendered to clients; and
  - (c) Protecting the reputation and credibility of the Firm.
- 3.2 The Risk Management Framework should consist of policies designed to achieve the objectives set out in paragraph 3.1 and procedures necessary to implement and monitor compliance with those policies. The Risk Management Framework should be an integral part of the Firm's overall strategic and operational policies and practices.
- 3.3 A Firm's quality control policies and procedures, developed in accordance with APES 320 *Quality Control for Firms*, should be embedded within the Risk Management Framework. This will facilitate a Firm complying with this standard and APES 320 and ensure consistency within the Firm's policies and procedures.

---

<sup>1</sup> The foundations include the policy, objectives, mandate and commitment to manage Risk.

<sup>2</sup> The organisational arrangements include plans, relationships, accountabilities, resources, processes and activities.

- 3.4 The requirements of the Standard are designed to enable a Firm to achieve the objectives stated in paragraph 3.1. The proper application of the requirements is therefore expected to provide a sufficient basis for the achievement of the objectives. 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 objectives.

## **4 Establishing and maintaining a Risk Management Framework for a Firm**

- 4.1 **A Firm shall establish and maintain a Risk Management Framework taking into consideration its public interest obligations. The Firm shall periodically evaluate the design and effectiveness of the Risk Management Framework.**
- 4.2 **The Firm's Risk Management Framework shall include policies and procedures that identify, assess and manage key organisational risks which include but are not limited to:**
- (a) Governance risks;**
  - (b) Business continuity risks (including succession planning);**
  - (c) Business risks;**
  - (d) Financial risks;**
  - (e) Regulatory risks;**
  - (f) Technology risks**
  - (g) Human resources risks; and**
  - (h) Stakeholder risks.**
- 4.3 The Firm should consider whether the risks identified in paragraph 4.2 are applicable and include policies and procedures as relevant. Additional risks specific to the Firm may be identified by reference to other risk standards such as *AS/NZS ISO 31000:2009 Risk Management - Principles and guidelines*.
- 4.4 The nature and extent of the policies and procedures developed by a 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.
- 4.5 **The Firm's leadership shall be responsible for the Firm's Risk Management Framework. The Firm's chief executive officer (or equivalent) or, if appropriate, the Firm's managing board of Partners (or equivalent), shall assume ultimate responsibility for the Firm's Risk Management Framework.**
- 4.6 The Firm's leadership and the examples it sets significantly influence the culture of the Firm. The adoption of an appropriate culture by a Firm is dependent on clear, consistent and frequent actions and messages from all levels within the Firm that emphasise the Firm's Risk Management policies and procedures.
- 4.7 **A Firm shall ensure that the Personnel assigned responsibility for establishing and maintaining its Risk Management Framework in accordance with this Standard have the necessary skills, experience, commitment and authority.**
- 4.8 Firms may refer to *AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines* which provides useful guidance to develop a framework for Risk Management. For guidance 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 confidence that the Risk Management policies and procedures relating to the Risk Management Framework are relevant, adequate, and operating effectively.**
- 5.2 A Firm's Monitoring process should identify whether there are any instances of non-compliance with the Firm's Risk Management policies and procedures thereby enabling the Firm's leadership to take appropriate action.
- 5.3 A Firm's Monitoring process should include the following:
- (a) A requirement for the Firm to undertake a review of the Firm's Risk Management Framework on a regular basis; and
  - (b) The Firm to designate from within the Firm's leadership a person or persons with sufficient and appropriate experience and authority the responsibility for ensuring such regular review of the Firm's Risk Management Framework.

## **6 Documentation**

- 6.1 A Firm shall document its Risk Management Framework.**
- 6.2 The form and content of documentation of the Risk Management Framework is a matter of judgment and depends on a number of factors, including:
- The number of Personnel and offices of the Firm; and
  - The nature and complexity of the Firm's practice and the services provided.
- 6.3 A Firm shall document its Risk Management policies and procedures and communicate them to the Firm's Personnel.**
- 6.4 Communication of Risk Management policies and procedures to Firm's Personnel should include a description of the policies and procedures, the objectives they are designed to achieve, and a message that each individual has a personal responsibility for Risk Management and is required to comply with the policies and procedures. In recognition of the importance of obtaining feedback on the Firm's Risk Management Framework and policies and procedures, Firm Personnel should be encouraged to communicate their views and concerns on Risk Management matters.
- 6.5 The documentation of the Firm's Risk Management Framework should include:
- Procedures for identifying potential risks;
  - Risks identified;
  - Procedures for assessing and managing risks;
  - Treatment of identified risks;
  - Documentation processes;
  - Training of Staff in relation to Risk Management.; and
  - Procedures for regularly reviewing the Risk Management Framework.
- 6.6 A Firm shall retain all relevant documentation for a sufficient time to permit those performing the Firm's Monitoring function to evaluate its compliance with its Risk Management Framework and to comply with applicable legal or regulatory requirements for record retention.**

### ***Conformity with International Pronouncements***

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