APES 325 Risk Management for Firms

[Supersedes APES 325 Risk Management for Firms issued December 2017]

REVISED: September 2019

Copyright © 2019 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.

Contents

Section

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

Conformity with International Pronouncements

Appendix 1: Summary of revisions to the previous APES 325 (Issued in December 2017)

1. Scope and application

1.1 The objectives of APES 325 *Risk Management for Firms* are to specify the mandatory obligations of a Firm to:

- establish and maintain a Risk Management Framework in order to identify, assess and manage key organisational Risks;
- monitor the Firm's Risk Management Framework on an ongoing basis; and
- document the Firm's Risk Management Framework and to communicate its Risk Management policies and procedures to its Personnel.

1.2 Accounting Professional & Ethical Standards Board Limited (APESB) has revised professional standard APES 325 *Risk Management for Firms* (**the Standard**). A Risk Management Framework in compliance with this Standard was required to be established by Firms by 1 January 2013. This Standard supersedes APES 325 issued in December 2017, and Firms are required to incorporate appropriate amendments to their Risk Management Frameworks by 1 January 2020. Earlier adoption of this Standard is permitted.

1.3 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 identifies 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.

1.4 The mandatory requirements of this Standard are in **bold-type**, preceded or followed by discussion or explanations in normal type. APES 325 should be read in conjunction with other professional duties of Members in Public Practice, and any legal obligations that may apply.

1.5 Members in Public Practice conducting the operations of a Firm in Australia shall follow the mandatory requirements of APES 325.

1.6 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.

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

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

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

1.10 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 this Standard and the Code.

1.11 In this Standard, unless otherwise specified, words in the singular include the plural and vice versa, words of one gender include another gender, and words referring to persons include corporations or organisations, whether incorporated or not.

2. Definitions

Defined terms are shown in the body of the Standard in title case.

For the purpose of this Standard:

Client means an individual, firm, entity or organisation to whom or to which Professional Activities are provided by a Member in Public Practice in respect of Engagements of either a recurring or demand nature.

Code means APES 110 *Code of Ethics for Professional Accountants (including Independence Standards)*.

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 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 means a member of a Professional Body that has adopted this Standard as applicable to their membership, as defined by that Professional Body.

Member in Public Practice means a Member, irrespective of functional classification (for example, audit, tax or consulting) in a Firm that provides Professional Services. This term is also used to refer to a Firm of Members in Public Practice and means a practice entity and a participant in that 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:

(a) That is aimed at cooperation; and

(b) 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 Activity means an activity requiring accountancy or related skills undertaken by a Member, including accounting, auditing, tax, management consulting, and financial management.

Professional Bodies means Chartered Accountants Australia and New Zealand, CPA Australia and the Institute of Public Accountants.

Professional Services means Professional Activities performed for Clients.

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

Risk means the effect of uncertainty on objectives.

Risk Management means co-ordinated activities undertaken by a Firm, to direct and control the activities of the Firm with regard to Risk.

Risk Management Framework means the foundations[1] and organisational arrangements[2] 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 well as its business objectives by:

(a) Facilitating business continuity;

(b) Enabling quality and ethical Professional Services to be provided 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 procedures and should take account of the Firm's Risk appetite.

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.

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 may include:

(a) Governance Risks;

(b) Business continuity Risks (including succession planning);

(c) Business Risks;

(d) Financial Risks;

1 The foundations include the policies, objectives, mandate and commitment to manage Risk.

2 The organisational arrangements include plans, relationships, accountabilities, resources, processes and activities.

(e) Regulatory Risks;

(f) Technology Risks (including cyber security);

(g) Human resources Risks; and

(h) Stakeholder Risks.

Additional Risks specific to the Firm can be identified through the use of other relevant standards or guidance. Firms shall comply with Section 360 *Responding to Non-Compliance with Laws and Regulations* of the Code.

4.3 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.

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

4.5 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.

4.6 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.

4.7 Firms may refer to the following documents for guidance:

- *AS ISO 31000:2018 Risk Management – Guidelines* which provides useful guidance to develop a framework for Risk Management; and
- For sole practitioners and small Firms, Module 7: Risk Management and Module 8: Succession Planning in the *Guide to Practice Management for Small- and Medium-Sized Practices* issued by the Small and Medium Practices Committee 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, and that instances of non-compliance with the Firm's Risk Management policies and procedures are detected.

5.2 A Firm shall establish a process whereby instances of non-compliance with the Firm's Risk Management policies and procedures are brought to the attention of the Firm's leadership who shall take appropriate corrective action.

5.3 A Firm's Monitoring process should include the requirements for the Firm:

(a) to undertake a review of the Firm's Risk Management Framework on a regular basis; and

(b) to designate from within the Firm's leadership a person or persons with sufficient and appropriate experience and authority, the responsibility for ensuring that such regular reviews of the Firm's Risk Management Framework occurs.

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 for a Firm is a matter of judgement 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 Professional 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 a 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, the Firm's Personnel should be encouraged to communicate their views and concerns on Risk Management matters.

6.5 The documentation of a Firm's Risk Management Framework should include:

- procedures for identifying potential Risks;
- the Firm's Risk appetite;
- Risks identified;
- procedures for assessing and managing Risks;
- treatment of identified Risks;
- documentation processes;
- procedures for dealing with non-compliance;
- training of Staff in relation to Risk Management; and
- procedures for regularly reviewing the Risk Management Framework.

6.6 A Firm shall document its succession plan as part of its Risk Management Framework.

6.7 The succession plan should include specific actions that a Firm will undertake in order to enable the Firm to continue performing its professional obligations to its Clients.

6.8 A Firm shall retain all relevant documentation for a sufficient time to permit those performing the Firm's Monitoring process to evaluate its compliance with its Risk Management Framework and to comply with applicable legal or regulatory requirements for record retention.

6.9 A Firm shall document all instances of non-compliance with the Firm's Risk Management policies and procedures detected through its Monitoring process and the actions taken by the Firm's leadership in respect of those instances of non-compliance.

Conformity with International Pronouncements

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

Appendix 1

Summary of revisions to the previous APES 325 (Issued in December 2017)

APES 325 *Risk Management for Firms* originally issued in December 2011 and revised in October 2015 and December 2017. APES 325 has been revised by APESB in September 2019. A summary of the revisions is given in the table below.

Table of revisions*

Paragraph affected	How affected
1.2	Amended
1.7	Amended
2 – Introduction	Amended
2 – Definition of Code	Amended
2 – Definition of Member in Public Practice	Amended
2 – Definition of Network	Amended
2 – Definition of Professional Activity	Amended
2 – Definition of Risk Management	Amended
2 – Definition of Risk Management Framework	Amended
3.1	Amended
3.2	Amended
4.2	Amended
4.7	Amended
5.1	Amended
5.3	Amended
6.2	Amended
6.5	Amended

** Refer Technical Update 2019/7*