APES 325 *RISK MANAGEMENT FOR FIRMS*

A GUIDE FOR MEMBERS

AN EXPLANATION AND INTRODUCTION TO APES 325 *RISK MANAGEMENT FOR FIRMS*

Overview of the scope and application of a risk management framework

APES 325 *Risk Management for Firms* (the Standard) was issued by the Accounting Professional & Ethical Standards Board (APESB) in December 2011 and came into effect on 1 January 2013. The Standard was revised in October 2015 and took effect on 1 January 2016.

Members of CPA Australia holding a Public Practice Certificate (PPC) are required to have established a risk management framework in accordance with the Standard. It is important to note that CPA Australia has had a requirement for members to have a risk management framework in place since 1 January 2004. The requirements of APES 325 build on the framework that all CPA Australia PPC holders were already required to have.

For members in public practice outside of Australia, the provisions of APES 325 must be followed as long as local laws and/or regulations are not contravened.

> *"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." APES 325 Para 1.3*

WHAT IS RISK?

Risk is the possibility of suffering harm or loss. Risk is an indication of potential danger, be that physical, financial, emotional or professional. Risk involves the assessment of an uncertain set of circumstances or an identified hazard. In a business context, financial risk is the probability of loss, the variability of returns from an investment or the chance of non-payment of a debt.

Risk management is the process of identifying, assessing and controlling risk arising from operational factors and making decisions that balance cost with benefit. Risk management, regardless of the level of consideration, will never eliminate all risk. Risk by virtue of its nature is unpredictable. APES 325 has been issued to provide a framework for making informed decisions about risk and having plans in place to refer to when responding to the consequences of a negative risk outcome.

WHAT IS RISK APPETITE?

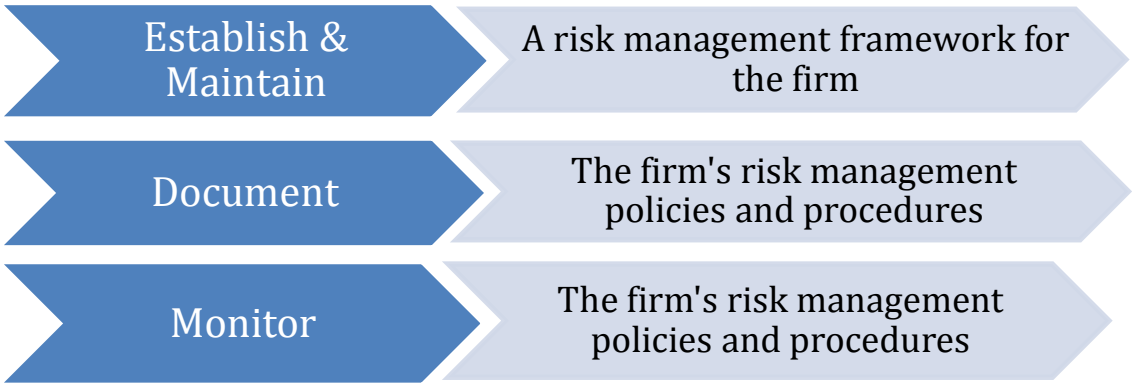
Risk appetite forms the basis on which a risk management framework is developed. Appetite for risk will vary from practitioner to practitioner and must be fully understood for the risk management strategies to be relevant. “Risk appetite is an articulation of the tolerance levels for risk that an enterprise is prepared to accept in the execution of its strategic and business objectives.”[1]

OBJECTIVES OF YOUR RISK MANAGEMENT FRAMEWORK

Practitioners are operating in a volatile and unpredictable business environment. Effective risk management is critical to reducing systematic risk and being prepared to manage uncertainty. APES 325 addresses broad business risks, it is not limited to engagement risk, or business operating risk. Disaster recovery, technological stabilisation, key business personnel plans should all be addressed within an effective risk management framework. Documenting and monitoring your risk management framework is essential in understanding how your practice can manage its obligations under the Standard as well as ensure that the business is a going concern.

CPA Australia is committed to assisting members with their practice management by providing guidance and tools to ensure risk management is embedded in the culture of your practice.

The structure of the Standard requires practitioners to:



[1] Risk Appetite: bitten off more than you can chew? PriceWaterhouseCoopers 2012 http://www.pwc.com.au/internalaudit

> *"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 services to be rendered to clients; and*
> *(c) Protecting the reputation and credibility of the Firm." APES 325 Para 3.1*

A firm's risk management framework may form part of the firm's quality control manual, the two documents being inter-related. Policies and procedures are required to be designed for both the quality control manual and the risk management framework. A policy is an over-arching philosophy or "motherhood statement" whereas a procedure is the process by which the firm executes its policy, this may include instructions or checklists.

> *"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 and should take account of the Firm's Risk appetite." APES 325 Para 3.2*

FUNDAMENTAL PRINCIPLES OF A RISK MANAGEMENT FRAMEWORK

The fundamental principles of this Standard are:

1) Firms should identify risk for their practice which is not limited to business risk or environmental risk.

    - *"Additional Risks specific to the Firm can be identified through the use of other relevant standards or guidance." APES 325 Para 4.2*

2) Risk categories referred to in the Standard may provide members with guidance but are not mandatory for members to include in their own risk management framework.

    - *"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;
        (e) Regulatory Risks;
        (f) Technology Risks
        (g) Human resources Risks; and
        (h) Stakeholder Risks." APES 325 Para 4.2

3) Principals, partners or the CEO have ultimate responsibility for the risk management framework and should be involved in its development, implementation, review and monitoring.

- *"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." APES 325 Para 4.4*

- It is more important for members to consider the risks specific to their own practice rather than arbitrarily following categories in the Standard. The categories outlines in paragraph 4.2 listed above provide members with a starting point for considering risk.

4) The Standard expects practitioners to involve their personnel in the development of a risk management framework for their firm. Their staff should be adequately qualified either professionally or by experience to provide input in risk assessment.

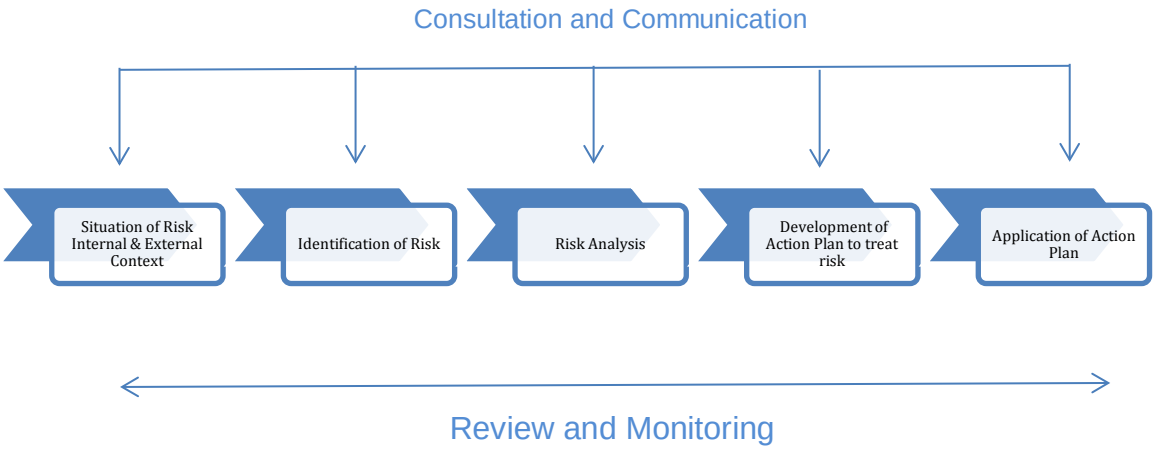
    - *"A Firm shall ensure that the Personnel assigned responsibility for establishing and maintaining its Risk Management Framework in accordance with this Standard have the necessary skills, experience, commitment and authority." APES 325 Para 4.6*

5) An interesting component of the Standard is the paragraph which requires members to consider public interest obligations within their risk management framework. This is not limited to clients who may be a public interest entity. This element of the Standard requires practitioners to assess how its practice operates in its community and the impact that the practice may have on local market conditions, for example, employment; the local economy and services to the general public.

    - *"A Firm shall establish and maintain a Risk Management Framework taking into consideration its public interest obligations." APES 325 Para 4.1*

The basic objectives of a risk management program within an organisation are to:

- provide appropriate protection of assets, financial or commercial position and business operations in order to maintain the business and its net worth
- contribute to satisfactory legal compliance, corporate governance and due diligence
- assist with quality improvement of services
- protect the reputation, credibility and status of the organisation
- enhance public and client confidence in the organization.



The most successful and useful risk management plans are those who use the collective knowledge and expertise from all individuals who are directly affected by its existence. Consultation and communication are imperative to ensuring that the risk management plan is effective in growing and sustaining the business.

Without regular review and monitoring of the risk management plan, it will be unknown if the plan is still relevant to the environment in which the business in operating. Accountants operate in a dynamic and evolving business environment – without regular review and monitoring of the risk management plan, the plan itself becomes a risk. Practitioners may come to rely on a risk management strategy that does not adequately meet the needs of the business when a risk is realised.

Situation of risk

The situation of risk identifies the scope for both external and internal identification of risks. At this stage of the process, the practitioner may consider the criteria for what constitutes risk within their practice. There may be particular or unique circumstances for the practice based on where it is operating, the type of services it provides, who the client base are, who the stakeholders are and how it delivers its products or services.

It is not possible to identify and mitigate all risks, therefore a review of known external and internal risks may assist the firm to prioritise risk. The most significant risks will be those which may impede the goals and objectives of the firm. This process should assist the practitioner to begin to categorise risk based on likelihood and consequence.

External risks are those which cannot ordinarily be controlled by an individual or small group of people. They are infrequent in occurrence yet may or may not be extraordinary events. Examples of external risk include changes to regulation, some natural disasters and economic forces.

Internal risks result from the strategic decision making process of the firm. Usually these decisions are based on both external and internal considerations and are made based on the direction, objectives and goals of the organisation.

Identification of risk

Once the context has been established, the potential risk factors or threats, and the practice's existing risk controls need to be identified.

The following checklist has been compiled as a guide only, to provide reference for members relative to identifying the risks of a practice. The checklist has been broken down in to risk categories and risk factors, members may wish to build on this checklist for the identification of risks unique to their practice environment.

Risk checklist

Risk category	Risk factor	Responsible for review	Date last reviewed & updated
Services performed	• How do you evaluate knowledge or experience requirements for both new and ongoing work? • How do you assess client expectations or intended use of reports? • Is the service provided high risk, such as assurance engagements undertaken or provided? • Can you deliver an objective report or does the client require subjective judgment?		
Contract risk	• How do you formally agree on the terms of engagement and any variation? • Do you utilise "standard terms and conditions" for all engagements? • Can your liability be capped? • How do you manage "contingency fees" or performance based remuneration? • Are you precluded from holding financial interests in the client or receiving commissions?		
Acceptance or continuance risk	• How are you formally assessing potential clients for acceptance? • Why is the client changing accountants? • Have any other professionals rejected the potential client? • Are there early signs of disputes on the fees that are proposed to service the client? • Has the client allowed sufficient time		

Acceptance or continuance risk (cont.)	for the acceptance process to be completed? • How do you evaluate retention of clients from time to time? • How do you address any conflict of interest? • How are you maintaining independence? • Are there any concerns about a client's viability, reputation, or management?		
Governance risks	• How do you develop and agree on a partnership contract? • How do you monitor independence? • How do you review your policies and procedures? • Do you have a quality control manual? When was it last reviewed and updated? • Do you have an operations manual? • How do you manage partnership disputes?		
Business continuity risks (including succession planning)	• How do you plan for succession? • How do you attract and retain key personnel? • Do you have a locum for times of illness or absence? • Do you have a disaster recovery plan? • Are you in a zone prone to natural disasters? • Do you have a practice exit strategy e.g. a plan for selling your practice/client list as a going concern?		
Business risks	• How do you secure your premises? • How do you review local market conditions? • Do you have a large percentage of clients in risk industries such as building, construction and manufacturing? • How do you market your practice? • How often do you review your fee structures? • How do you assess your competition? • Do you have a client complaint/grievance process? • How do you assess how you present your business?		

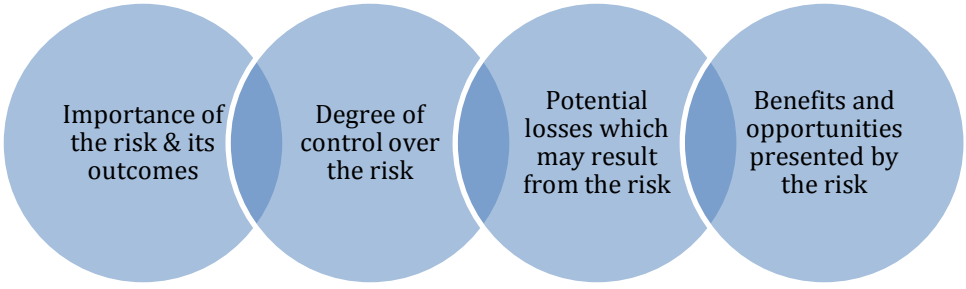
Business risks (cont.)	• How do you insure for: - Building - Contents - Infrastructure - Professional development - Key person?		
Financial risks	• What is your debt cycle/how do you monitor aging of debtors? • How do you monitor cash flow – is there enough liquid fund to meet regular outflows such as salaries, superannuation, PAYG, occupancy and finance costs? • How do you prepare and categorise a budget for the practice? • How do you assess capital resources? • How do you fund infrastructure investments? • What is your gearing ratio? • What debt covenants are in place? How do you monitor key ratios required by your financiers? • What security processes are in place to transact in cash or bank accounts?		
Regulatory risks	• How do you monitor, assess and implement changes to professional standards and legislation e.g. - APES Standards - AASB Standards - AuAS Standards - SIS Act and Regulations - ITAA - CPA Australia By-Laws - Specialist legislation such as the Bankruptcy Act for insolvency practitioners? • How do you monitor and assess the impact of changes to/or introduction of applicable legislation e.g. - Fair Work Act - Occupational Health and Safety - Australian Consumer Law - National Privacy Principles?		
Technology risks	• How do you plan for changes to infrastructure e.g. investment requirements • Do you have a help desk or a specialist available for technology		

Technology risks (cont.)	issues? How do you assess whether the specialist is appropriate? • Do you have a disaster recovery plan? • Do you have offsite back up storage for data? • How often do you back up data? • How do you secure: - Data - Physical environment - Access/password changes - Level of authority - System back up - System upgrades?		
Human resources risks	• Who are your key personnel e.g. specialist practitioners? • What due diligence is there around recruitment? • How regularly do you review HR policies? • Is there a staff feedback process? • How do you deal with staff grievances? • How do you fill staff vacancies either temporary or permanent? • What are your policies around the annual staff review process? • What are your policies around performance management?		

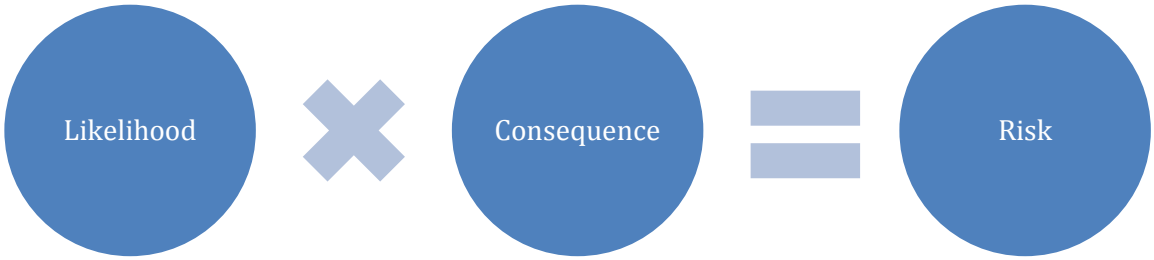
Risk analysis

A member should analyse and evaluate the practice's risks on a continuing basis.

Risk evaluation takes into account the following:



There are a number of ways in which it may be analysed and evaluated, the simplest model is to consider the likelihood of occurrence of an event and the consequences of that event.



Consult with others and use your experience to calculate the level of risk. Useful risk categories with respect to consequence and likelihood are:

Likelihood	Consequence
Very likely	Extreme
Likely	High
Probable	Moderate
Unlikely	Low

The assessment process needs to canvass amongst other matters:

- the practice's existing and anticipated areas of practice
- its composition, experience and expertise
- its management and internal control procedures
- the likelihood of being sued and the potential ambit of any claim
- assessment of new and existing clients.

The following matrix may assist member to categorise and prioritise identified risks.

Risk prioritisation matrix

CONSEQUENCES	Unlikely	Manageable	Likely	Very Likely
Extreme	High	Very High	Very High	Very High
High	Manageable	High	Very High	Very High
Moderate	Low	Manageable	High	High
Low	Low	Manageable	Manageable	High

LIKELIHOOD

Where an area of the practice is identified as posing high risk, the practice may consider:

- ✓ evaluating its ability to reduce the risk in terms of existing procedures
- ✓ adjusting or reconsider that area of practice and its development
- ✓ retraining or employing personnel to meet any staffing weaknesses
- ✓ reviewing the engagement with clients in that area of the practice
- ✓ applying risk management procedures.

Development of an action plan

Strategies need to be developed to manage the identified risks. Every practice will adopt a different approach to the development of risk management strategies based on their individual risk appetites.

Examples of strategies to manage risk are as follows:

Contingency Strategy

- A contingency strategy applies to risks of higher consequence but lower likelihood of occurrence and aims at bringing the potential consequence of the risk within acceptable confines. Simple examples of such a risk control strategy are insurance and contractual indemnities, business continuity plans, contracting some or all of the activity to another organisation or person

Preventative Strategy

- A preventive strategy applies where potential impacts are not very large but the likelihood of occurrence is high, for example client complaints. In this case, quality control assurance procedures, supervision and training would be examples of this strategy.

Monitoring Strategy

- A monitoring strategy is suited to exposures where the likelihood and consequence of risk are deemed to be relatively small. This strategy aims to ensure all "standard safeguards" are in place and working. It also requires the risk to be periodically reviewed. For example, quality checks, regular reporting, audit and performance reviews.

Mixed Strategy

- A mixed strategy corresponds to managing a risk environment that is managing potentially likely negative outcomes and outcomes of high impact or consequence which would involve a combination of strategies .

GENERAL RISK MANAGEMENT PROCEDURES

Terms of engagement

Documentation and agreed terms of engagement are essential in any practice and benefit both the member and the client.

Terms of engagement can be embodied in an engagement letter as follows:

- confirms acceptance of the appointment
- outlines the objective, scope and extent of the engagement
- highlights the extent of the member's responsibilities to the client
- defines the client's responsibilities
- manages the "client expectation gap", ensuring that the services delivered are the services expected by the client.

Confines the extent of exposure by:

- ✓ specifying limitations on the work to be undertaken
- ✓ confining the advice to the client only
- ✓ restricting use of member's name on documentation supplied to the client
- ✓ obtaining an indemnity from the client, any third party or in connection with receiverships, trust and secretarial work
- ✓ reviews on a continuing basis the scope of the engagement during the engagement period.

Reviews the form and nature of the engagement:

- where the breadth and scope of the agreed services alter or where they become more complex or detailed
- where additional services may be required by the client
- where the status or structure of the client could have changed from a partnership to a company or a trust mid-term, reviews of engagement letters should be conducted on a formalised basis and in agreement with the client
- sets the fees applicable to the engagement.

Refer to APES 305 *Terms of Engagement* for guidance.

Advise clients on risks

To avoid underwriting the client's risks, advise the client in writing of relevant dates and consequences in the event of failure by the client to act. This will transfer the risk of non-compliance back to the client to action or follow up.

Obtain adequate insurance and the control of claims once they have occurred

All members who hold a Public Practice Certificate must hold adequate and appropriate insurance to cover their professional liability. Consideration should be given to the type of services that are being performed and the exposures that this creates. Practitioners should also consider their practice structure when assessing coverage. For further information on professional indemnity insurance and professional standards legislation please refer to:

- Public Accounting Insurance page on the CPA Australia website
- Professional Standards Schemes page on the CPA Australia website.

Accurate and contemporaneous documentation

It is recommended that all advice a member or personnel provide is noted on file, by confirmation letter or report to the client. The information that should be included is:

- date
- time
- content of conversation or advice

- notation to whom it was made
- signature (if applicable).

Timeliness of action and diary systems

File notes will have the dual effect of:

- assisting with the recollection of events if there is litigation many years down the track
- being tendered in court as evidence that a conversation actually occurred (subject to authenticity of documentation being established).

Practice in areas where there is sufficient expertise

Every member is required to recognise their own limitations. Where the member forms the view that there is insufficient time, or they do not have the skill required to perform the service requested, then the matter should be referred on to a specialist.

Consultants and agents selection

Consultants and agents are required to:

- have adequate qualifications and resources
- have adequate indemnity insurance
- be independent of the member.

Client selection

A review of the practice's client mix is recommended with a view to considering:

- increasing the proportion of clients requiring lower risk advice
- the type of business conducted by the client, such as:
    - ongoing work or one-off engagement
    - the effect of the economic climate on the client's business

It is important to note that the application of such measures does not protect the member from their duty to exercise the level of skill, care and judgement appropriate to the service provided and therefore application of the highest standard at all levels is essential. Generally, the practice should consider its quality control procedures, the problems that have arisen, and how they have been dealt with in the past.

Refer to APES 110 *Code of Ethics for Professional Accountants* for guidance.

APPLICATION OF ACTION PLAN

A member needs to continuously monitor and review the strategies used to manage risk. Over time, new risks are created, existing risks are increased or decreased, risks no longer exist, the priority of risk may be questioned, the risk appetite may change or the risk treatment strategies may no longer be effective. Monitoring should comprise of:

Monitoring ensures that, as risks change, new measures are introduced to control these risks. On-going review is required to ensure that strategies remain relevant.

Record keeping

All policies and procedures should be in writing. Records should be maintained documenting the assessment process carried out, the major risks identified and the measures identified to reduce the impact of these major risks.

Failure to document policies can lead to breaches in performance because of misunderstanding or misinterpretation. A written set of policy statements supported by documented procedures provides a constant reference, a guide to action and a framework for checking that the operations are conducted in the manner intended by the member.

Conclusion

Where a practice has in place:

- a set of documented policies and procedures that reflect what the practice does
- those policies and procedures adequately address the various elements of APES 325 *Risk Management for Firms* and the mandatory requirements of other Professional Statements relevant to the practice's area of professional practice
- has a built in system of controls and checks
- has a mechanism to ensure they are kept current
- are driven by the principals of the practice who are committed to risk management and quality control

The following benefits are achieved:

- ✓ all personnel know what is required from them and how to perform
- ✓ the principal/s can determine the control and standard of service that the practice provides
- ✓ quality and consistency is promoted to clients
- ✓ communication is enhanced
- ✓ risk can be effectively managed
- ✓ there is a level of insurance that the practice is adequately managing risk.

To provide feedback on this guide please email qualityreview@cpaaustralia.com.au

CPA Australia has a range of services tailored to support public practitioners.

For further information please visit **cpaaustralia.com.au/publicpractice** or contact your local office on 1300 73 73 73.

April 2016