

Potential Black Letter Paragraphs

1. A Firm shall establish and maintain a system of risk management designed to:
 - (a) Be proactive in identifying and managing risk;
 - (b) Ensure business continuity;
 - (c) Facilitate the development and implementation of strategy and business decision making;
 - (d) Protect the reputation, credibility and status of the organisation and the profession;
 - (e) Enhance public and client confidence in the organisation;
 - (f) Comply with relevant legal and regulatory requirements.

Elements of a system of risk management

2. A Firm shall establish and maintain a system of risk management that includes policies and procedures including, but not limited to:
 - (a) Governance risk;
 - (b) Business continuity;
 - (c) Identification, assessment and responses to business risks;
 - (d) Identification, assessment and responses to engagement risks;
 - (e) Identification, assessment and responses to legislative and regulatory requirements;
 - (f) Identification, assessment and responses to performance risk;
 - (g) Financial risk;
 - (h) People – including risks associated with recruitment/retention, accreditation/training, safety;
 - (i) Technology risk – including computer hardware, software, communication;
3. A Firm shall document its policies and procedures in respect of risk management and communicate them to the Firm's Personnel.

Leadership responsibilities for risk management within a Firm

4. A Firm shall establish policies and procedures designed to promote an internal culture recognising that effective risk management is essential for effective practice management, in providing Professional Services of the highest quality, protecting the public interest and the maintaining the reputation of the Firm. Such policies and procedures 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 system of risk management.
5. A Firm shall establish a risk management framework and supporting risk management plan with policies and procedures that any person or persons assigned operational responsibility for the Firm's system of risk management by the Firm's chief executive officer or managing board of Partners has sufficient and appropriate experience and ability, and the necessary authority, to assume that responsibility.

APES 325 Risk Management Project

Monitoring

6. A Firm shall establish an annual 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. This process shall:
- (a) Include an ongoing consideration and evaluation of the Firm's system of risk management; and
 - (b) 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.

Documentation of the system of risk management

7. A Firm shall establish policies and procedures requiring appropriate documentation to provide evidence of the operation of each element of its system of risk management.
8. A Firm shall establish policies and procedures that require retention of risk management documentation for a period of time sufficient to permit those performing Monitoring procedures to evaluate the Firm's compliance with its system of risk management, or for a longer period if required by law or regulation.

Potential Commentary/Guidance Paragraphs

In relation to the Objective of the Standard:

- C1. The objective of this Standard is to establish basic principles and essential procedures relating to risk management and to provide guidance regarding a Member in Public Practice's responsibilities on certain matters relating to minimising business and operational risks to the Firm.
- C2. 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.

In relation to Communication/Documentation:

- C3. 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 system of risk management.
- C4. The form and content of documentation evidencing the operation of each of the elements of the system of risk management 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 organisation.
- C5. Appropriate documentation relating to documenting the risk management system and Monitoring should include, for example:
- Risk management framework (including an initial approval and amendment process);
 - Procedures for identifying potential risks;
 - Procedures for minimizing or eliminating risks;
 - Review processes from the point of view of risk management;

APES 325 Risk Management Project

- Financial delegation processes and procedures;
- Documentation process;
- Training of staff.

In relation to Elements of a system of risk management:

C6. At a minimum, a risk management policy should identify, analyse and evaluate the following areas of risk:

- Business risks;
- Firm's quality control;
- Staff and security control;