Practice Guideline 6B Actuarial Advice Regarding Risk Management

June 2023

Contents

Contents

1. Introduction

1.1. Application

This Practice Guideline (PG) has been prepared to assist Members working in the general insurance, life insurance, health insurance (collectively 'insurance' or 'insurers') and superannuation industries, and whose work includes:

1. Identification, assessment, and management of an institution's risks for an Enterprise Risk Management (ERM) Program.
2. Advising on Risk Management Frameworks (RMFs) for Australian Prudential Regulation Authority (APRA) regulated institutions under relevant Prudential Standards issued by APRA, which are summarised in Section 2.

This PG provides guidance on managing conflicts of interest that might arise in connection with the above activities.

The PG also applies to Members who support another Member carrying on work in the above areas in accordance with this PG, as relevant to their contribution to the Services.

Unless otherwise specified, 'institutions' refers collectively to insurers and superannuation fund trustees.

The PG is intended to assist Members by identifying matters they should consider when providing advice on their institutions' RMFs and to assist those Members who perform Chief Risk Officer or equivalent senior risk management roles in effectively discharging their duties. It is intended to assist Members on risk management practice areas including risk identification, risk controls and risk assessments.

Risk measurement components of the RMF, including Target Capital are addressed in PG 6A (Target Capital). In the case of insurers, Members should consider PG 6A and PG 6B in conjunction to ensure a holistic approach on providing advice on RMFs. PG 6A does not apply to superannuation fund trustees.

1.2. About this Practice Guideline

This PG was prepared by the Institute's Risk Management Practice Committee (RMPC) and supersedes and builds on the previous Information Note - Actuarial Advice on Risk Management Frameworks (August 2019) that focused principally on insurers.

This PG also reflects the approach in Sections 2.3 and 2.4 of International Standard of Actuarial Practice 6 - Enterprise Risk Management Programs and IAIS Insurance Core Principles (IASP 6) issued by the International Actuarial Association in December 2018. This PG:

a. has been prepared in accordance with the Institute's Policy for Developing Professional Practice Documents; and

b. is to be applied in the context of the Institute's Code of Conduct ("Code").

This PG is not mandatory. Even so, if this PG covers the Services a Member provides, then the Member should consider explaining any significant departure from this PG to the Principal and record that explanation.

All work performed under this Practice Guideline, whether by the Member providing advice or by a Member supporting the Member providing advice, is designated as an Applicable Service. As such, the Member's attention is directed towards PG 1 (General Actuarial Practice). In the case of a Member supporting the Member providing advice, Practice Guideline 1 applies as relevant to their contribution to the Services.

1.3. Relationship to PG 1

Compliance with PG 1 is a pre-requisite to compliance with this PG. References in PG 1 to 'the applicable Professional Practice Document (PPD)" or "all applicable PPDs" should be interpreted as applying equally to this PG 6B, as appropriate.

1.4. Other Relevant Documents

This PG must be applied in the context of the relevant legislation, regulation, and accounting standards prevailing at the time of application. If there is a conflict in wording, then the legislation, regulation and accounting standards take precedence over this PG.

In this context, legislation, regulation, and accounting standards include laws, regulations, prudential standards, subordinate standards, rules issued by government authorities and standards issued by professional bodies which have the force of law. Also included are relevant modifications or substitutions of these. Similarly, a reference to a PS or PG includes any modification or replacement of that PS or PG.
Apart from the Code or a PS, from legislation or from regulatory standards, no other document, advice, or consultation can be taken to modify or interpret the requirements of this PG.

This PG does not constitute legal advice. Any interpretation or commentary within this PG regarding specific legislative or regulatory requirements reflects the expectations of the Institute but does not guarantee compliance under applicable legislation or regulations. Accordingly, Members should seek clarification from the relevant regulator and/or seek legal advice in the event they are unsure or require specific guidance regarding their legal or regulatory obligations.

1.5. Defined Terms

This PG uses various capitalised terms whose precise meaning is defined in the Glossary of General Defined Terms Used in Practice Guidelines, or in the Code.

1.6. Commencement Date

This PG is effective for relevant Services provided on or after 1 July 2023.

2. Applicable Regulations

2.1. Relevant Regulations

Australian regulations and associated guidance which may be relevant to advice on Risk Management Frameworks for APRA regulated institutions include the following APRA Prudential Standards and the associated Prudential Practice Guides, as applicable:

- CPS 220 (Risk Management) (effective 1 July 2019) ("CPS 220").
- CPS 320 (Actuarial and Related Matters) (effective 1 July 2019) ("CPS 320").
- GPS 110, LPS 110 and HPS 110 (Capital Adequacy) (effective from 1 July 2019, 1 January 2013 and 26 June 2015, respectively) ("GPS 110", "LPS 110" and "HPS 110", respectively); and
- SPS 220 (Risk Management) (effective 1 January 2020) ("SPS 220").

2.2 RMF Definitions in CPS 220 and SPS 220

CPS 220 and SPS 220 include the following similar definitions of the Risk Management Framework:

- **CPS 220**
  "The risk management framework is the totality of systems, structures, policies, processes and people within an institution that identify, measure, evaluate, monitor, report and control or mitigate all internal and external sources of material risk. Material risks are those that could have a material impact, both financial and non-financial on the institution or on the interests of depositors and/or policyholders."

- **SPS 220**
  "The risk management framework is the totality of systems, structures, policies, processes and people within an RSE licensee's business operations that identify,

assess, manage, mitigate and monitor all internal and external sources of inherent risk that could have a material impact on the RSE licensee's business operations or the interests of beneficiaries (material risks)."

2.3. Specific Paragraphs of CPS 220 and SPS 220

Paragraph 26 of CPS 220 and Paragraph 12 of SPS 220 describe the Material Risks applicable to insurers and superannuation trustees (RSE licensees), respectively.

Under Paragraph 47 of CPS 220, the independent comprehensive review of the RMF must, at a minimum, assess whether:

- the RMF is implemented and effective;
- it remains appropriate, considering the current strategic and business plan and business operations;
- it remains consistent with the Board's risk appetite;
- it is supported by adequate resources; and
- the RMS adequately documents the key elements of the RMF that give effect to the strategy for managing risks.

Under Paragraph 29 of SPS 220, the independent comprehensive review of the RMF must, at a minimum include review of:

- whether the risk management framework remains appropriate for the RSE licensee's business operations;
- the specific resources utilised, at a minimum, to undertake the risk management activities required by the Prudential Standard and whether those activities are supported by adequate resources;
- the risk appetite statement;
- the RMS to ensure that it accurately documents the RSE licensee's RMF and the RSE licensee's strategy for managing risk;
- all risk management policies and procedures; and
- all risk management and internal control systems.

2.4. Financial Condition Reports for Australian Insurers under CPS 320

In preparing a Financial Condition Report (FCR) for an insurer and assessing the financial condition under CPS 320, an insurer's Appointed Actuary must make general observations on the overall RMF with a focus on financial risks, and how these risks are managed by the insurer. Members should apply the principles articulated in this PG when making these observations.

3. Identification, Assessment and Management of Institution Risks for an ERM Program

3.1 Risk Identification

3.1.1 A Member who is responsible for, or significantly involved in, identifying institution risks should consider factors including, but not limited to, the following:

1. The strategic objectives and business plan of the institution.
2. The circumstances of the institution including its size, business mix, complexity, and the markets where it operates.
3. The processes for collecting information and whether the staff have adequate qualifications, training, and experience to understand and identify the risks.
4. Whether the risk identification process is sufficient to identify current and emerging risks that are reasonably foreseeable, relevant, and material including risks that directly or indirectly impact the financial condition and other objectives of the institution (e.g., reputational risk).
5. The time frame over which the risks may emerge and may impact the institution.
6. The risks that may arise from reasonably foreseeable changes in the business of the institution (operations, markets, products) and from business conduct.
7. Whether underlying risks within financial structures that have limited transparency have been sufficiently identified (e.g., off-balance sheet exposures, complex asset, or reinsurance structures).
8. Whether the reasonably foreseeable causes of institution risks and their consequences have been sufficiently identified.
9. Risks arising or increasing because of risk management activities (e.g., credit risk arising from the transfer of risk).
10. The impact of non-financial risks including those relating to information security and cyber, technology, suppliers and outsourcing, business continuity and other operational risks.
11. The impact of Environmental, Social and Governance (ESG) risks on the institution.
12. The impact that an institution's culture, governance structure and remuneration systems may have on the ability and willingness of the management and staff to identify and manage risks, and whether culture, governance structure or remuneration generates, magnifies, or mitigates risks; and
13. Input regarding the identification of risks from management, other knowledgeable persons within the institution, other subject matter experts and regulators.

3.1.2 A Member who is responsible for, or significantly involved in, assessing the probability and impact of the institution's risks should consider factors including, but not limited to the:

1. Qualitative assessment of risks in addition to, or instead of, assessing them quantitatively.
2. Risk correlations, risk aggregations and tail risks (e.g., catastrophe and pandemic risks, and complex outsourcing risks).
3. Appropriateness of the risk modelling, stress testing, reverse stress testing and scenario testing techniques used.[1]
4. Extent to which the risk models that measure the probability and impact of risks provide results that are consistent with information expressed by market prices for the risks concerned or related risks.
5. Consistency among the various valuation methodologies underlying the ERM program.
6. Operation and effectiveness of the processes and mechanisms used to address risk control and risk mitigation.
7. Appropriateness of the assumptions regarding future actions taken by management and by external parties, considering prior experiences in the industry with similar actions.
8. Input regarding probability and impact from management, other knowledgeable persons within the institution, other subject matter experts and regulators.
9. Consistency of risk assessments over time.

3.2. Risk Controls

A Member who is responsible for, or significantly involved in, implementing, or maintaining risk management controls, mitigation, monitoring or communication and reporting of the institution's risks should consider factors including, but not limited to:

1. The institution's risk management policies and risk appetite and tolerance statements.
2. The relationship between the institution's financial strength and risk profile, and the institution's risk management system.
3. Any significant inconsistency in the evaluation of the institution's risk tolerances

[1] PG 6A (Target Capital Life, General and Health Insurance) addresses ERM programs for insurers that often involve stress testing, scenario testing and other modelling techniques. PG 5 (Insurer Enterprise Risk Models) provides helpful guidance on these subjects. Members applying this PG may find PG 6A and PG 5 to be valuable resources. PG 6A does not apply to superannuation fund trustees.

and risk limits.

4. The extent to which the results of the risk models used to measure the economic costs and benefits of risk mitigation are consistent with information expressed by market prices for the risks concerned or related risks.
5. The operation and effectiveness of the processes and mechanisms used to address risk control and risk mitigation. These mechanisms include processes and controls for compliance, fraud, and counter terrorism/money laundering risks.
6. The appropriateness of the assumptions regarding future actions taken by management and by external parties, considering prior experiences in the industry with similar actions.
7. The culture within the institution to commit to, and implement, risk mitigation actions when needed.
8. The impact of reasonably foreseeable future adverse circumstances on the availability and effectiveness of future risk mitigation practices.
9. The existence and effectiveness of feedback loops in the risk management process.
10. How the nature and relative importance of risks may change over time.

3.3. Risk Assessment

A Member who is responsible for, or significantly involved in, performing an aggregate risk assessment of the institution should consider, in addition to the elements addressed in Section 3.2. above, factors including, but not limited to:

1. The financial strength, risk profile, business management, governance structure and risk environment of the institution.
2. Whether the risk management processes align with the institution's objectives and strategy, regarding aggregate risk taking and regarding each major risk category, as reflected by the risk appetite, risk tolerance and risk limits.
3. The interdependence of risks relating to the institution's assets and liabilities, noting that correlation of risks between different asset classes, products and business lines may not be linear, and may change under stressed conditions.
4. The way in which the institution's capital models relate to and connect with its risk appetite and risk limits. Risk and capital management processes should inform one another and there should be clear linkages between them.
5. Off-balance sheet exposures that may revert to the institution in times of difficulty; and
6. Diversification benefits that result from aggregation of risks.

3.4 Considerations for Groups

If the institution is part of a group, the Member should consider factors including, but not limited to, the following:

1. The risks and benefits of belonging to a group structure, recognising potential limits on fungibility of capital and on transfer of assets between separate legal entities.
2. Foreseeable changes in the group structure which could impact the capital and solvency of the institution and its ability to continue in business.
3. Risk modelling, stress testing, reverse stress testing and scenario testing, should include changes in the group structure and in the support that is received from other members of the group.[2]
4. Assumptions that may be suitable for an individual institution may not be suitable when it is part of a larger group.
5. Imposition of risk management controls and tolerance limits by group management.
6. Differences in legal and regulatory requirements between jurisdictions.
7. Contagion effect of adverse circumstances in other members of the group which could impact the capital and solvency of the institution; and
8. The appropriateness of adopting group policies and functions.

3.5. Reviews and Governance

A Member who is responsible for, or significantly involved in, developing, implementing, maintaining, or reviewing an ERM framework should consider factors including, but not limited to, the following:

1. The engagement of the Executives and the Board in assessing, setting, monitoring, and reviewing the institution's risk appetite and risk profile, and whether the interests of policyholders and other relevant stakeholders are considered appropriately within those processes.
2. The adequacy of the risk management resources and capabilities within the institution for the current and expected risk profile and risk management strategies.
3. The quality, extent and effectiveness of independence, challenge and monitoring reflected in the framework.

[2] PG6A (Target Capital Life, General and Health Insurance) addresses ERM programs for insurers that often involve stress testing, scenario testing and other modelling techniques. PG5 (Insurer Enterprise Risk Models) provides helpful guidance on these subjects. Members applying this PG may find PG6A and PG5 to be valuable resources. PG 6A does not apply to superannuation fund trustees.

4. The extent and results of recent reviews and audits of control effectiveness, and management's response to the findings.
5. The management of potential conflicts of interest. Policies and supporting processes should be in place, well understood and adhered to, and be subject to regular independent assurance.
6. The extent of use of risk management and risk assessments in the decision-making practices of the institution.
7. The effectiveness of risk communication channels within the institution, including risk escalation processes, and with its regulators.
8. The effectiveness and timeliness of the reporting of, and response to, incidences and breaches related to the operation of the ERM framework within the institution.
9. The operational quality and effectiveness of key ERM framework related policies, processes and mechanisms, including, but not limited to, outsourcing management, business continuity management (including pandemic response management), whistle blowing policies, fraud and privacy risk management, model risk management and business conduct risk management.
10. The extent to which the ERM framework is adaptive to changes to the institution and to its environment.
11. The extent to which the ERM framework complies with regulatory requirements and guidelines applicable to it.
12. The adequacy of the insurer's ICAAP, Capital Management Policy or Own Risk and Solvency Assessment (ORSA) if applicable; and
13. Contingency or Recovery plans to restore the institution's financial strength and viability in severe adverse circumstances.

4. Considerations in Advising on Risk Management Frameworks for APRA Regulated Institutions under CPS 220 and SPS 220

4.1. Assessing the Suitability, Adequacy and Effectiveness of an Institution's RMF

The relevant risk management Prudential Standards and Prudential Practice Guides provide a benchmark, and mandatory considerations in certain cases, for the key components of an RMF. The Member should check that the RMF is compliant with the applicable Prudential Standards.

In reaching their review findings, Members should also consider, but not be limited to, the following areas:

1. Risk management processes, documentation, and systems

- The institution's Risk Management Strategy (RMS) and related policies need to meet any relevant CPS 220 or SPS 220 requirements.
- An institution's risk management policies should be subject to regular review, implemented, and adhered to, across the business.
- The processes, procedures, documentation, and systems should support the operation of the RMF, including those used to identify, assess, mitigate, and monitor all internal and external risks.

2. Risk Management culture and capability, and level of staff engagement

- How do staff perceive and interact with the RMF, how does the institution respond to "bad news" and are post-implementation reviews used when new processes or change management programs are implemented?
- Is the ownership of risks clear and are governance frameworks understood and operating effectively, clearly reflecting the most recent organisation, relevant roles and responsibilities and ensuring an appropriate level of independent oversight, challenge, and assurance?
- The risk management function's structure and reporting lines should reflect the activities required and performed, and the function should have the skills, authority and level of independence needed.
- If a "three lines of defence" (3LOD) approach is in place, the Member should consider if this is operating effectively to create a segregation of duties between those actively managing risk and those responsible for independent oversight, challenge and assurance to Executives and the Board.

3. Risk management reviews

The Member should consider the following in relation to risk management reviews, issues, or events:

- The findings of internal or external reviews (for example, audit reviews, regular or ad-hoc reviews) and the "root causes" and outcomes of any material incidents that have arisen. Details of any "near misses" and any mitigating actions or new controls put in place to prevent a reoccurrence.
- Action items that have been identified in the previous risk management review by the Member and/or internal or external reviews of the RMF or its components, to ensure these have been addressed in a timely manner.
- Key risk management issues that have emerged since the last review, noting that for an insurer, many of these will need to be reviewed in any event, as part of the insurer's Financial Condition Report (FCR).
- The approach the institution takes to considering risk events that have impacted other relevant Institutions. As a test of the RMF, the Member should consider any publicly reported major risk incidents that have occurred to other

relevant Institutions, including what controls are in place to prevent or mitigate such incidents, if the same set of circumstances were to occur within their institution.

In the case where the Member has not had suitable access to enable a review of the RMF or has been unable to access suitably skilled people to review aspects of the Framework, they should document the potential limitations in respect of their findings and may need to consider their ability to continue with the engagement.

4.2. Forming an Objective Opinion on an Institution's RMF

As part of the review, a Member should form an objective opinion on an institution's RMF and outline the process adopted in making such conclusions.

It is recognised that the findings of a review of an institution's RMF by a Member is likely to contain areas of judgment. This judgment should be reasonably formed, supportable, clearly articulated and documented.

The Member may conclude that an institution's RMF is materially inadequate, unsuitable and/or not 'fit for purpose'. Such a view will necessarily be based on judgment and is not a simple conclusion.

Alternatively, the Member may conclude that part of the RMF is adequate, whilst some components have weaknesses that should be addressed. However, risks do not function in isolation, and control deficiencies in one area may suggest control weaknesses in other areas, or a heightened level of risk in one, or more, parts of the institution. The Member should form a holistic view of the suitability and adequacy of the institution's RMF, and the institution's risk assessment and control environment are important elements in forming such a view.

A way to assess the extent of this risk awareness and efficiency and effectiveness of managing risks would be to consider how well risks have been identified, assessed/quantified, reported, and managed. For example:

1. How clearly can the Board articulate the key risks the institution faces?
2. How well have any "warning signals" or "alarm bells" of events in the institution been communicated?
3. How rapidly were these escalated and addressed?
4. Has the process for reporting and managing new risks been effective?
5. How frequently, or materially, have instances arisen where risks have fallen outside the risk appetite or tolerance levels?
6. Does the institution have adequate risk management resources considering its size and the complexity of its risk profile? If not, are there concrete plans for uplift?
7. How well have risks or incidents been documented and reported?

8. Have there been material control failures during the year and in what risk areas?
9. Have the follow up remedial actions been implemented adequately, and any insights been actioned?
10. How frequently and by what method have the risks been assessed?
11. How frequently and using what approaches have the risks been quantified? Are there any material gaps in the institution's ICAAP/ORSA if applicable or Financial and Business Recovery Plans? How were these identified and communicated? What are the plans to resolve the gaps?

Even if no material issues have arisen during the year, the Member should consider the institution's ability to effectively respond to emerging risks and those seen in other relevant Institutions.

If the Member begins to form the opinion that the institution's RMF is materially inadequate or unsuitable, it would normally be appropriate to raise questions with the individuals accountable for the areas of inadequacy and include the Chief Risk Officer, at the earliest opportunity, to reduce any potential misunderstanding, to provide context, and to ensure that the institution has the ability to respond in a timely and appropriate manner. There may be situations where the Member disagrees with management, in which case it may be appropriate to document management's view in the review documentation.

If the Member does conclude that there are material inadequacies, then particular care will be needed to effectively communicate these within the institution (refer Section 4.3). Members may find it useful to seek advice, or a second opinion, from a senior actuary or other specialist, especially if their views may prove controversial in the institution. Although accountability for any areas of concern may lie with other people, and ultimately with the Board, the Member is encouraged to play an appropriate role in facilitating improvements to the institution's RMF. For example, it may be appropriate to support the institution in developing an action plan and monitoring its implementation.

4.3. Communicating the Member's Findings of the Review of the RMF

In communicating findings within the institution and to the Board, the Member should:

1. Briefly outline the process and diligence used to support their conclusions. This can be addressed by outlining the process adopted in conducting the review of the RMF, noting the considerations outlined in Section 4.2, as well as any potential limitations on the opinions provided.
2. Ensure that the documentation on the process used to support their findings does not detract from the results of the review, the conclusions reached, or any recommended improvements, by considering the needs of the audience and not providing excessive detail. Where appropriate, further detail on the process

adopted and the results of the review should be disclosed in an appendix or recorded in the Member's working papers.

3. Provide an update on items and recommended improvements raised in previous internal and external reviews and any audit items.
4. Demonstrate an understanding of new items that have emerged since the previous review, where appropriate cross-referencing these items with relevant parts of the previous review reports.
5. Highlight areas where improvements have been made or where deteriorations have occurred since the previous review, and improvements that are recommended for the future; and
6. Identify and document any barriers that have impeded the Member in conducting the review and the resulting limitations on the findings.

It is important that the scope of the Member's findings is well defined and understood. For the avoidance of doubt, and to avoid misunderstanding, any limitations on the scope of the review and the opinion provided should be included in the communication or report.

5. Managing Conflicts of Interest

There is a potential for conflicts to arise for a Member. The presence of a conflict may depend on how a Member has been involved in prior activities that are subsequently related to a later activity. This may involve multiple occasions of involvement with a product, business process or other activity for the institution. A conflict may also be perceived by an independent person outside the institution.

Examples of potential conflict could include involvement in:

- Product development/pricing and the subsequent valuation of those product liabilities;
- Advising on benefit design, reserving and/or investment decisions for superannuation funds;
- Recommending reinsurance structures and/or asset-liability structures and subsequent capital requirement assessments; or
- The design/ implementation of the RMF and subsequent review of the suitability and adequacy of the institution's RMF. For example, the Member may have a role in the oversight of risk across the institution and/or as a Chief Risk Officer.

In these examples, the potential conflict may be managed via:

- Making appropriate disclosure of the conflict and any resulting limitations on any findings; and

- Seeking, or placing reliance on, other independent reviews of the RMF such as those by internal audit and/or external reviews.

However, if the Member feels their exposure or interaction with the institution's RMS limits their ability to perform a review, provide an opinion, or recommend improvements on the RMF or on the risk identification, controls, and assessment, they should seek to ensure alternative and suitably skilled people are made available to undertake the work.

If the situation involves a conflict of interest, Members must manage any such conflict of interest in accordance with the Code.

End of Practice Guideline 6B