sunsuper

Risk **Governance Self-Assessment**

Table of contents

Purpose and objective of the self-assessment

The purpose of the self-assessment was to review the embedment and effectiveness of governance, culture and accountability within Sunsuper's risk governance practices.

The central objective was to identify changes to improve how we operate.

Development of a roadmap of activity to achieve a 'target state' is the primary outcome. This roadmap will directly influence the future state of business operations. The Board will monitor progress of activities.

Methodology

The self-assessment followed a staged approach:

1. Review of artefacts and previous assurance and review activities, including particular insights derived from extensive preparation for the Royal Commission into Financial Services;
2. Targeted Board and Executive Leadership Group (ELG[1]) surveys and analysis;
3. Board and Executive Leadership Team (ELT[2]) review of the APRA CBA Prudential Inquiry Report and identification of similar themes/issues; and
4. Group sessions with the Board and ELG exploring focus areas identified through (2 and 3).

We identified focus areas through the survey activity by considering:

- Results that appeared skewed (either positively or negatively);
- Results where materially divergent views were exhibited; and
- Questions supported by a significant number of comments.

KPMG were engaged to provide independent challenge over the design of the self-assessment. This engagement involved an 'insights briefing' to the Board and ELT on the themes within APRA's CBA Inquiry Report and their applicability to the broader financial services sector.

Management were responsible for analysing insights from the survey activity, identifying focus areas for further deeper dive sessions and developing and agreeing with the Board the roadmap of improvement activity.

KPMG facilitated focus group sessions to test hypotheses formed through survey activity and seek additional feedback from the Board and ELG.

A Board sub-Committee supervised the self-assessment process and provided input and insight.

[1] The ELG comprises the CEO, Executive General Managers (EGMs) and 'Heads of' business units (HOs).
[2] The ELT comprises the CEO and Executive General Managers (EGMs)

Other review activity

An important element to the self-assessment was the critical assessment of recently completed review and assurance activity in relevant areas to test and challenge where this work should inform the reflection.

Key activities informing this self-assessment include:

- Board Performance Assessment 2018 (conducted with the assistance of the AICD)
- Independent Governance Review 2017 (conducted by Cameron Ralph Khoury)
- Macquarie University Risk Culture Study 2018
- Risk Management Framework Comprehensive Review 2017 (conducted by KPMG)

Role of the Board

Scope of review

This element of review had regard to the overall governance structures in place within Sunsuper at both Board and Committee level, the operation of Management (Executive) Committees and the interaction and reporting between these.

We considered reflections and observations from the AICD Board Performance Assessment and the independent review of the organisational governance framework.

The depth of these reviews supported meaningful insights identified through this self-assessment process.

There was particular focus on:

- the Board's interaction with the organisation;
- the degree of challenge from the Board to Management;
- the degree of self-challenge exhibited by Management;
- perceptions on the 'sense of urgency' where issues or risks are identified or trending; and
- the effectiveness of information flow and reporting mechanisms.

Strengths

- The Board model is a strong positive contributor to promote challenge and rigour.
- A formalised structure of Management (Executive) Committees exists to promote open communication, effective decision making and cross-functional accountability.
- A healthy level of candour is inherent within Board interactions and their interactions with Management - this is constructive and there is a mindfulness that challenge is thoughtful so as not to engender defensiveness.
- Close oversight of audit findings and open issues and risks is evident by the Board and relevant Committees with clear and open challenge exhibited, and timely closure of open issues.
- Senior leaders and those with regular Board interactions conveyed a high level of confidence that they understand the Board's expectations on management of risk, risk tolerance and risk appetite, expected standards of behaviour and issue and risk escalation.
- Where direct communication from the Board to the business had occurred in the past, this was well received and embraced.

Opportunities for improvement

- The Board agreed that more regular and direct communication to the business would be beneficial. The Board recognised this needs to preserve clarity in the role of the CEO.
- The Board will continue to reiterate to Management the importance of cascading key messages.
- Risk reporting can be more consistent with more focus on quantitative risk assessment and escalation of risks before they become issues.
- More defined ownership over enterprise risks will better embed accountability and ensure clarity on decision-making and ownership of risk outcomes.
- Management can more meaningfully apply the risk framework objectively and consistently so that escalation of risks, trends and issues is appropriate.
- A formal assessment of the current Audit, Compliance and Risk Management Committee (ACRMC) will be undertaken to inform future structure and composition (including an assessment of the benefits and disadvantages from constituting a stand-alone Risk Committee).

Risk management and compliance

Scope of review

This element of review considered how the risk management and compliance function operates. This included the degree of understanding and embedment of the three lines of defence and the understanding of core concepts and their useful application in practice.

We reviewed how Line 2 operates as a 'challenge function' and the capacity and capability of risk and compliance resources (Line 2 and Line 1).

There was specific focus on managing risk in change – particularly in light of the growth trajectory of the business and the portfolio of change projects that are in-flight (and to come).

A review of foundation elements of the risk framework assessed how well these:

- support risk in practice and meaningfully guide the business through decision making, and risk and issue identification and escalation; and
- promote root cause analysis and 'lessons learned' to reinforce continuous improvement.

A review of Board and Committee reporting identified how effective this is for the Trustee to remain appraised of the enterprise risk profile, emerging risks and trends and keeping informed of issues arising.

Areas of particular focus included:

- how well the ELG can articulate the Board's standards for managing risk;
- framework adequacy, effectiveness and embedment;
- the culture of compliance and effectiveness of this outside of pure regulatory adherence;
- resourcing, capacity and capability within the risk and compliance function;
- change management and integration of Line 2 in the risk in change process; and
- the degree of embedment of 'lessons learned' in assessing successes as well as failures both within the organisation and critical evaluation of external events or issues.

Strengths

- A strong risk aware culture is evident and there is a universal articulation of the concept of risk management as 'everybody's business'.
- A strong consensus view is that there is a 'high standard' of expectation of risk management from the Board.
- Management is particularly strong on acknowledging the role of risk management as integral to decision making.
- The risk and compliance function is well regarded by the business and considered to have a strong 'ethical compass'.
- Management Committees such as the Compliance and Risk Management Committee are positive enablers and important forums for collaboration and discussion of arising issues.

Opportunities for improvement

- A consensus view emerged that the pace of growth within the fund has outrun the risk response (risk resourcing and control review and improvement).
- There are capacity and capability gaps within the risk and compliance function. Whilst short term resources have been appointed as an interim measure, increased investment in this function is a priority. A structural review will consider the additional specialised risk capabilities required, with areas such as investment and advice a focus. This additional capability will complement existing specialised capability in areas such as technology.
- Improvement in Line 1 knowledge, skills and understanding of core risk and control concepts, expectations and assurance methods will increase effectiveness.
- Training and awareness of core risk and compliance concepts and practical guidance and tools can be improved.
- Better mechanisms for improving the 'rolling up' of risks is needed. A more comprehensive enterprise view of the risk profile will address any ambiguity of Executive ownership of risks.
- More frequent collective review and recalibration of the enterprise risk profile will improve awareness and involvement in managing these.
- Conduct risk must be expressly articulated organisationally and be integrated into the risk management framework to promote the importance of "how we do business" to support success

Issue identification and escalation

Scope of review

This element of review considered the decision making processes in place that promote the identification of issues, how these are escalated and how remediation decisions are made, progressed and tracked.

We assessed documented policies and the linkage of escalation processes to the risk management framework and overall system of delegation.

We sought Board and Management's views on how well this is working in practice and any areas of misalignment in views were explored and unearthed.

We actively considered the role of complaints including the line of sight to complaints trends and to 'outlier' or egregious complaints that might be symptomatic of emerging or systemic issues not otherwise apparent through trend analysis.

We undertook an exploration of cultural considerations and evaluated the degree of willingness and openness to raise and discuss issues.

We considered how potentially systemic weaknesses are identified and assessed, by considering emerging trends and issues.

We also considered the insights gained from participating in the Macquarie University Risk Culture Study.

Strengths

- A strongly member focussed culture and 'mono-line' business model promotes a genuine desire and willingness to support identification, escalation and remediation of risks and issues.
- Executive and Management Committees are key forums through which cross-functional discussion, exploration and escalation of issues occurs.
- The Board Audit, Compliance and Risk Management Committee (ACRMC) drives a sense of urgency and exercises regular and appropriate oversight of actions to address risks and issues.
- Where matters of particular concern are identified, the ACRMC ensures oversight is established between scheduled ACRMC meetings
- The ACRMC receives Internal Audit and External Audit reports directly and in full – these are not 'filtered'. There is full transparency and opportunity to explore all audit outcomes, irrespective of rating or perceived 'severity'.
- The ACRMC meets separately with Internal Audit and External Audit without management present at each meeting. The CRO attends each ACRMC meeting without other management present.
- There has been active and deliberate elevation of risk focus at Board level and increased referral of issues from the ACRMC to the Board and relevant Committees to ensure oversight is rigorous.
- The Board expressed a strong degree of confidence in the CRO and his ability to ensure line of sight to key issues.
- A specific Portfolio Risk and Issue Management Framework exists. This directly aligns to the enterprise Risk Management Framework and articulates how Enterprise Change captures, manages and reports risks and issues (including escalation).

Opportunities for improvement

- The Board expressed some concern that unidentified issues may exist, more than it was concerned about full disclosure or willingness to address issues transparently. There was a sense of inadequate recognition that 'unknown unknowns' may exist.
- Board skills and expertise in technology needs more depth to support their effective challenge in this area.
- Management should ensure that representations to the Board are appropriately balanced as some Board members perceive that there may be 'overly positive' messaging in certain circumstances.
- There needs to be more focus on timeliness of escalation of incidents, issues and concerns. There is inconsistency in the perception of effectiveness of issue and risk escalation with the ELT viewing this more favourably than the HOs.
- Greater consistency in how identification and escalation of issues / risk occurs requires attention including:
    - process improvement to align understanding of issue / risk identification at all levels;
    - better communication on outcomes where risks or issues are escalated to ensure staff are kept informed of Executive decisions and to further embed risk awareness culturally; and
    - HOs need greater line of sight about issues escalated to the Board.
- The Board identified room for improvement in the quality and depth of risk reporting noting that Management had been responsive to Board feedback and there is an ongoing program of improvement.
- The governance, risk and compliance (GRC) IT platform needs improvement or replacement to add greater functionality, including better trend analysis, risk hierarchies and improved quality of reporting
- Investment in quality training will reinforce the role of Line 1 in risk management, reporting and analysing risk events and the escalation of issues. A focus on embedment of training concepts and follow up is necessary to effect meaningful change.
- Regular discussion of risk and risk management practices by Management will model required behaviours. Team meetings should feature risk issues as a prominent and early agenda item.
- Member complaints can support early issue identification and business process improvement. The Board wants to understand the complaints processes better and the insights gained from member complaints.
- The Management Breach Working Group is an existing forum for discussion of incidents and for airing and examination of issues. This group requires additional focus to ensure it functions optimally and that the right stakeholders attend.

Financial objectives and prioritisation

Scope of review

Through survey activity and focus group discussion, we explored the degree of 'balance' within decision-making with a focus on:

- how investment (time, resources and financial funding) decisions are made;
- how these decisions are made in the context of change; and
- how financial objectives and non-financial objectives are considered and compared in these decisions.

Strengths

- The strongly 'member focussed' culture was again identified a key driver of ensuring appropriate balance within decision-making.
- The Management Strategic Investment Committee (SIC) is a strength in the overall governance of risk in change, with the CRO as Chair ensuring a structurally embedded opportunity for the 'voice of risk' in the process.
- There is embedment of risk management within project governance and a prioritisation methodology involving a 'challenge' session from HOs to promote a balanced approach.
- Filtering of projects and prioritisation is subject to SIC approval ensuring Executive challenge and accountability.
- The process supports critical risk projects, but can benefit from review to ensure impartiality in the assessment of activities without a direct financial or revenue impact.
- There is acknowledgement that emphasis on return on investment is important for ensuring member value. This creates challenges when comparing projects delivering less tangible (especially, non-financial) benefits such as compliance and risk mitigation initiatives

Opportunities for improvement

- There are inconsistent views as to how well we achieve this balance in practice across the organisation.
- Board members noted that when reviewing and approving projects, it is not always clear what the benefits are, particularly where benefits to members varies across member cohorts and business cases can be better quantified with more meaningful data over consistent time horizons.
- There is opportunity to further embed the risk appetite statement as a tangible tool in decision-making and promote balance through a varied risk lens.
- The business needs clearer communication about prioritisation decisions and the trade-offs inherent in these decisions.
- There is acknowledgement that decisions need a clear cost / benefit analysis to be embedded but there is an opportunity for more analysis on member outcomes.
- There is overreliance on cultural drivers to achieve a balanced outcome where both financial and non-financial risks are appropriately considered. However, this may not support consistently good outcomes and improvements to the supporting frameworks are necessary for this to become enduring.

Accountability and remuneration

Scope of review

We undertook a review of the accountability framework with particular focus on:

- how well the roles and responsibilities in the management of risk and governance of decision-making are defined;
- the degree to which a collegiate and consultative environment may inhibit constructive challenge or promote 'over consulting';
- the degree to which the Board exhibits constructive challenge to Management;
- the degree to which remuneration arrangements support both individual and collective accountability for risk outcomes; and
- any discrepancy in perceptions of the Board, Executive Management and the HOs as to how well accountability and remuneration frameworks operate in practice.

Strengths

- There is a favourable view of the widespread adoption of the RACI model[3] as a tool to minimise ambiguity and allow regular calibration of ownership of tasks through a structured process.
- There is a constructive culture of the Board challenging Management to embed accountability for issues and risk management.
- The lack of a federated structure that constrained CBA and a mono-line and uncomplicated business structure within Sunsuper is conducive to clearer ownership and accountability.
- There is close proximity of Executive Management to operations and to members resulting in greater engagement and more transparency of the impacts of decisions, including in relation to risks and issues.

Opportunities for improvement

- The RACI model, whilst effective, is inconsistently applied. There is potential to over focus on the decision-making aspect of the 'A' element rather than accountability for decisions or outcomes over the medium to longer term.
- The variable short-term reward program for the majority of staff does not have any performance measurement criteria relating to risk or compliance. There is a requirement to meet Essential Requirements Gate obligations that currently includes risk and compliance training and meeting assurance obligations. These measures and obligations are currently being enhanced and strengthened and will be effective 1 January 2019.
- No system of incentive deferral exists for the majority of staff and there is no clawback in the reward scheme. Reductions where some requirements are only 'partially met' do not go far enough.
- Behavioural gates that currently exist do not go far enough and have not resulted in meaningful consequences, nor do they reward good risk management behaviours.

[3] The RACI model identifies roles and responsibilities
Responsible: person who performs an activity or does the work.
Accountable: person who is ultimately accountable and has Yes/No/Veto.
Consulted: person that needs to feedback and contribute to the activity.
Informed: person that needs to know of the decision or action.

- Management and the Board are addressing shortcomings in remuneration practices as they intersect with risk management practices. This will include further review of the Essential Requirements Gate and a review of how the Nominations and Remuneration Committee (NRC) and the ACRMC interact in influencing remuneration decisions.

Culture and leadership

Scope of review

We gave consideration as to how the Sunsuper culture operates as an informal system to shape desired risk governance behaviours and the degree of embedment within and across the organisation.

Particular regard was paid to assessing whether the "chronic ease" observed by APRA within the CBA was observable and whether indicators of "complacency and reactivity" presented.

We formed a critical view of how the central Sunsuper value of 'Customer First' manifests in practice and translates to observable outcomes. We challenged stakeholders to cite examples based on their first-hand experience.

Views were sought on how well the Board and Management 'walk the talk' in role modelling expected behaviour and the consistency of this across the organisation.

We focussed on how well the balance of empowerment and challenge was experienced by stakeholders to uncover any discrepancies needing exploration.

Strengths

- There is unanimous agreement that the culture of the fund is strongly member focused. Perception of members' interests as paramount to day-to-day operations and strategic investment decisions is strong.
- There is also strong sentiment that decisions made are always with members' interests in mind.
- There is consistent and frequent messaging from the CEO to guard against hubris and complacency.
- The Board has a shared consciousness of the importance of guarding against success leading to complacency and that such complacency masks underlying vulnerabilities.
- A key value of 'candour' supports a culture of respectful challenge and of speaking up.
- Executive meetings allow time for reflection and debate of issues and discussion of risks and issues. The ELT rated the willingness to raise and discuss issues (within their own and other areas of responsibility) strongly.
- There is a consistent and aligned view at ELT that the collaborative and collegiate environment is equally a strength and an area of potential risk. Maintaining the right 'tension' is important – this self-awareness is a strong precursor for good outcomes.
- Structured leadership training is in place with investment in promoting a consistent style of leadership 'the Sunsuper way' centred on strong accountability and commercial acumen.

Opportunities for improvement

- The remuneration framework needs change to better reward good risk behaviour.
- Implementation of a better defined and enforced 'Essential Gate' and overhaul of attributes supporting behavioural aspects of remuneration reviews have been progressed. There is more work needed to implement initiatives where Management have more 'skin in the game' and to promote accountability with meaningful remuneration consequences (both positive and negative).
- There is some evidence of an over-reliance on good intent and a strong culture to drive meaningful member focussed outcomes
- Greater use of objective data in decision-making will lead to more confidence that sound member outcomes will result.
- Additional focused investment in data analysis to is needed to test that initiatives and decisions have promoted members' best interests.
- Whilst not systemic, pockets exist where the response to challenge is defensive rather than open and receptive. This may be indicative of a weakening risk culture and should be addressed.
- As a result, management are not fully confident that no culture blind spots exist. Guarding against hubris and complacency needs to permeate through the organisation more deeply and consciously.
- There was some disparity in the views of the ELT and HOs about the embedment of the culture of constructive challenge to avoid group think.
- A more active integration of the "should we" question can be embedded into key frameworks and forums to elevate this as a conscious rather than inherent consideration

Conclusion

This self-assessment has provided a timely opportunity to pause and deeply reflect. It has allowed us to identify how we can become a more resilient organisation and protect the strong culture that we have built and value so deeply.

Through the activities and initiatives planned, we aim to deliver enduring change.

We strongly believe in the significant benefits that increased scale delivers to our members' individual and collective interests. Our challenge, and our commitment, is to maintain the right balance between pursuing growth (and realising scale benefits) whilst always prioritising the interests of our members.

Driving deeper embedment of the 'Customer First' ethos requires that we focus on achieving a healthy, constructive tension of the twin pillars of growth and guardianship. We have recognised that we cannot rely on our culture to support this in isolation of strong frameworks and unambiguous intent.

The roadmap of activities has been designed with this in mind.

Strong, cohesive and effective leadership is needed to champion this change, to protect and build on our strengths and to guard against self-imposed bureaucracy and 'process over substance'. Leadership will key to delivering on this intent and is central to driving meaningful improvement.

The actions we will implement represent change for our business and our people. Clear, effective and timely communication will be an important element to successfully delivering on these changes.

Growing the safe way for the benefit of our members will continue to be our focus.