AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY
1 Martin Place (Level 12), Sydney, NSW, 2000
GPO Box 9836, Sydney, NSW, 2001

T 02 9210 3000 | W www.apra.gov.au

4 July 2017

TO: ALL PRIVATE HEALTH INSURERS (PHIs)

RISK MANAGEMENT – THEMATIC REVIEW OBSERVATIONS

In September 2015, APRA commenced a thematic review program on the risk management arrangements and practices in each of the 33 private health insurers that made up the private health insurance industry (this number has now increased to 37). The program ran for 20 months and concluded in May 2017.

The program was undertaken in the context of supervision of the industry transferring from the Private Health Insurance Administration Council to APRA in July 2015, and under the auspices of APRA's strategic objective to apply particular supervisory attention to the quality of governance, risk culture and risk management in regulated institutions throughout 2014-18.

This letter shares some high-level observations from the thematic review, whilst noting that the key challenges facing PHIs with respect to their risk management arrangements include:

- Forming a view of the risk culture and taking steps to address any desired changes
- Ensuring the operational structure of the insurer facilitates effective risk management
- Aligning their risk management practices with their risk register and not the other way round
- Assessing and managing the risks to their strategic and business objectives
- Establishing a Chief Risk Officer role with appropriate reporting lines and obtaining an adequately skilled and independent person to fill the role

Attachment 1 provides more detailed observations and common recommendations against the assessment framework that formed the basis of the review. These are attributed to the industry as a whole due to their prevalence within the majority of individual insurers. Whilst they do provide insight into the risk management arrangements within the industry, they do not speak to the specific arrangements of individual health insurers.

Questions on the issues outlined in this letter should be directed to your supervisory team.

Yours sincerely,

Louis Serret
Acting Executive General Manager
Specialised Institutions Division

ATTACHMENT 1:
INDUSTRY OBSERVATIONS AND RECOMMENDATIONS

Risk Governance

Risk governance focuses on the functioning and effectiveness of the internal and independent governance arrangements of a regulated institution. It encapsulates not only the role, responsibilities and functioning of the board in relation to risk governance and an institution's risk management framework but also other internal or independent functions in place to assess the adequacy of, and adherence to, operational controls and risk management policies and procedures independent of management.

The review focused on two key elements of risk governance:

1. The extent to which the Board drives and engages with risk management; and

2. The Risk Management Framework.

The Board drives and engages with risk management

Most boards of private health insurers considered that risk management was an important aspect of their deliberations and discussions during board meetings. The review observed that whilst this was the case, the formal use of risk management processes and risk data by boards was not widespread. For example, there was limited evidence of formal risk assessments supporting business proposals nor detailed analysis of both the intended and unintended consequences of decisions being asked of a board.

Common Recommendation

- That the Board require from management an analysis of the risks to and consequences of business and project proposals, to inform a view and stimulate Board discussion on the likelihood of success and the ability to manage the intended and unintended consequences, of the proposal.

The governance arrangements of all insurers included the establishment of a board committee framework to assist the board in governing risk and overseeing key functional areas. A board audit committee and in many cases a board risk committee was in place to oversee the risk management framework and adequacy of internal control. Whilst these structural arrangements are fundamental to the governance of an insurer, their ability to effectively oversee risk and control is heavily influenced by the information being sought and subsequently provided. The review observed that while there was a range of 'risk' reporting to committees, such reports were often based on performance results which, by definition, look to the past. There were few examples of regular and robust enquiry as to the operational effectiveness of the risk management framework.

In addition to the recommendations below, APRA is of the view that there is an opportunity for all PHIs to more effectively use internal audit (Third Line of Defence) as a source of assurance that the risk management framework is being effectively applied both at an organisational level and in respect of specific audit engagements.

Common Recommendations

- That the Board require from management more regular and robust risk reports that include reliable information on past and current risk levels, trend of the current risk level, effectiveness of the control framework and any issues being experience in the management of the risk.

- That the Board supplement the oversight of the risk management framework with independent reviews of the appropriateness, effectiveness and adequacy of the risk management framework.

The Risk Management Framework

All insurers had in place to some degree, a risk management framework that detailed the principles and processes for applying risk management across the organisation. In most cases, the formalization of this framework was based on the risk assessment process defined in the ISO 31000 Risk Management Standard. Many insurers were also looking to apply the Three Lines of Defence model of business assurance as part of their risk management framework. Notwithstanding these arrangements, the review concluded that there was generally poor integration of risk management into the business management arrangements of insurers. This was apparent from the misalignment between material risk and the organisational structure, limited use of risk based planning, a single consequence matrix and a lack of risk reports from the First Line of Defence.

Common Recommendation

- Establish an Enterprise-wide Risk Management Framework that reflects and informs the structure of the organisation and links strategic/business/operational objectives.

Internal control was appropriately viewed by most insurers, as the framework of policies, procedures and practices within the organisation that produced conformance and delivered results. An observation from the review was that the environment in which this framework operated did not explicitly inform the approach to internal control. APRA was keen to encourage insurers to formally think about, define, assess and improve the internal control environment in order to enhance the overall performance of internal control within their organisations.

Common Recommendation

- Formalise an internal control framework and leverage existing processes to assess and improve the performance of the internal control environment.

Operational Risk Management

Operational risk is focused on internal processes, people and systems, and external events. The application of risk management is fundamental to ensuring the adequacy and ongoing performance of internal processes, people and systems, as well as the response to and management of external events.

The review focused on two key elements of operational risk management:

1. The effectiveness of risk management processes; and

2. The establishment and maintenance of effective control frameworks.

Risk Management Processes

Most insurers have adopted the ISO 31000 Risk Management Standard as the basis for their risk assessment processes. During the review however, it became apparent that there was significant variation in the quality of the risk assessment processes being conducted, with only a few examples of effective risk analysis that produced robust risk management data. This was evident through the absence of risk assessment reports, a lack of specificity in defining objective, poorly framed risks, inadequate consideration of cause and consequence, and little if any stakeholder engagement.

Common Recommendation

- Review and improve the risk assessment processes and frame risks in a way that maximises the effectiveness of risk analysis and control development.

Under the Three Lines of Defence Model of Business Assurance, the Second Line of Defence plays a pivotal role in supporting the establishment and maintenance of effective risk management processes. This role includes the provision of specialist risk management advice, support and training throughout an organisation. It is the provision of specialist risk management support which enables the production of quality risk assessments and risk data that underpins the performance of the risk governance and operational risk management arrangements. The review observed significant variance in the capability of the role across the industry, with only a few insurers having adequate performance by their Second Line of Defence.

Common Recommendation

- Improve the risk management capability in the Second Line of Defence to support effective risk assessments against business objectives at all levels of the organisation.

Effective control frameworks

The Three Lines of Defence Model of Business Assurance is predicated on the provision of assurance by front line functions (First Line of Defence) that their business objectives are being and will continue to be achieved, because risks to the achievement of those objectives are being adequately controlled. Such assurance can only be provided if thorough risk assessments have been undertaken against business objectives and control frameworks are being monitored. This is the integration of risk management into the business management system. Whilst many insurers recognised and adopted the Three Lines of Defence Model, in practical terms there was little evidence during the review, of this type of assurance being provided by First Line of Defence functions. Although many insurers had a strong compliance culture with an active compliance framework, reporting regimes such as monthly risk and control attestations by managers, did not appear to be founded on robust risk assessments and diligent monitoring of control frameworks.

Common Recommendation

- Maximise the assurance of business control from business units in the First Line of Defence by requiring managers to review and report on the effectiveness of control frameworks for individual risks to their business objectives.

Project Management, Business Continuity and Outsourcing

The control frameworks established by insurers for these three business functions were reviewed as part of the thematic review program. The review again observed significant variation in the approach to and control of, these functions.

For example the strength of the control framework supporting project management ranged from non-existent to very strong. Similarly, the review observed some very detailed and effective business continuity arrangements against some comparatively immature and weak approaches.

With respect to outsourcing, there appeared to be very little outsourcing of material business activity by the industry besides the widespread outsourcing of claims processing capability and hospital contracting arrangements, by the smaller 'end of town'. Any outsourcing arrangements were generally supported by an Outsourcing Policy, which in the main detailed a due diligence process to be followed but failed to enshrine the requirement for a service provider to demonstrate their ability to deliver the required services through a risk assessment and control plan.

Common Recommendations

- Enhance project management planning by incorporating controls required to manage both project management and project objective risks, into the project plan.
- Improve the preparedness to manage a business disruption event and develop an approach to business resilience that considers Emergency Response, Business Continuity and Disaster Recovery.
- Ensure proposals to outsource material business activities include an assessment of the risks to the delivery of the material business activity.

Conclusion

The thematic review of the risk management arrangements across the private health insurance industry gave APRA an opportunity to assist insurers to improve their Risk Governance and Operational Risk Management arrangements. The reviews also supported the developing regulatory relationship between APRA supervisors and each of the PHIs. APRA acknowledges the time and effort of the Boards and Management of each insurer in accommodating the reviews undertaken.

PHIs, as a general observation, are committed to applying risk management within their governance and management arrangements. Whilst such commitment is a prerequisite to the successful implementation of risk management, the industry needs to recognise that risk management, as a governance and business management discipline, requires formal structure and process, and must be integrated into the business management arrangements if it is to achieve the benefits that are available. APRA remains concerned that complacency may be creeping into the industry due to perceptions of adequacy with the current arrangements.

The recommendations from the reviews are designed to assist insurers with their risk management 'journey' and obtain more tangible and reliable outcomes from their risk management investment. APRA is also looking for assurance that improvements to both the Risk Governance and Operational Risk Management arrangements are being achieved through the implementation of the recommendations.

Overall the industry is reasonably placed to meet future requirements of APRA in respect of risk management. Such requirements will be designed to increase the performance of the governance and management arrangements within individual insurers by mandating policies, procedures and practices (controls) to ensure that risks are being effectively managed.

Going forward, APRA will continue to focus on the risk management arrangements within individual PHIs through monitoring progress with the review recommendations as well as assessing other key enablers of effective risk management such as Risk Culture, the Three Lines of Defence Model of Business Assurance and the implementation of the CPS 220 Risk Management Standard.