Risk Management for Private Health Insurers

On 27 July 2017, the Australian Prudential Regulation Authority (APRA) released the final version of Prudential Standard CPS 220 *Risk Management* (CPS 220) for Private Health Insurers (PHI). This represents the most significant change to the regulatory regime since the transition from the Private Health Insurance Administration Council (PHIAC) to APRA, with risk being the first of three phases of APRA's PHI Policy Roadmap.

The standard will apply to all PHIs from 1 April 2018.

CPS 220 is a key part of APRA's overall approach to sound risk management and extending it to the PHI sector was the logical next step in the move from PHIAC to APRA's regulatory environment.

The new standard forms the foundation of the Risk Management Framework (RMF) for all APRA-regulated financial services businesses, and therefore it is critical that PHIs fully embed the principles and practices into their operations, as there will be expectations that they are quickly up to speed and operating at the same level as other APRA regulated entities.

Speaking at the recent health insurance summit in Sydney, Peter Kohlhagen (APRA Senior Manager, Policy Development) remarked that

> *"It was natural that our first priority would be risk and risk management, because a resilient health insurer has robust processes for identifying and managing current and emerging risks to its operations and financial soundness."*

pwc

Overview of CPS 220

1. Strategy

Business plan
- Identify and assess risks in pursuing strategy
- Ensure RMF manages those risks

2. Risk governance and oversight

Board
- Establish explicit responsibilities including risk culture
- A separate Board Risk Committee (BRC) is required

Risk management function
- CRO reports direct to CEO, no dual hatting
- Adequate skills, resources, direct access to BRC

Risk management framework

Defines components of RMF, including:
- Contents of risk appetite and
- Minimum contents for policies and procedures

3. Detailed review

Annual Risk Management Declaration

Annual Review - Internal / external audit

Comprehensive independent review (three years)

Risk culture
- Key focus for APRA and an area of difficulty in demonstrating compliance
- Create culture programs / processes to measure, monitor and control

What does this mean for your organisation?

The Board has ultimate responsibility for having a RMF that is appropriate to the size, business mix and complexity of the organisation. At a minimum, the RMF must include the Risk Appetite Statement (RAS), Risk Management Strategy (RMS) and a business plan, all of which must consider the material risks of the organisation. This requires detailed policies and procedures.

CPS 220 also stipulates the need for an "operationally independent" risk management function, to be led by a CRO who must report directly to the CEO, and a compliance function. For some organisations, this will mean changes to current operational structures.

Underpinning all of these changes is a strong tone focused on risk culture. The CEO and the Board should model this tone, which should permeate the organisation and be continually monitored and measured for effectiveness.

CPS 220 has been in force for a number of years for other APRA-regulated ADIs and Life & General Insurers. PwC has been directly and indirectly involved in a number of annual and triennial comprehensive reviews across the broader Financial Services sector, as well as performing gap analyses in the lead up to implementation. Those organisations that have prepared well for the changes are seeing benefits now, with smooth and efficient comprehensive reviews.

The greatest area of challenge upon implementation has proven to be ensuring the RAS is comprehensive enough for the organisation, covering all risk categories, and demonstrating that it is embedded throughout the business. All staff, from CEO to front line, need to understand their role through a risk lens, and how the RAS impacts them. This is the first step to building the risk culture that APRA is increasingly focussed on, and are about to commence auditing and measuring.

Implementation of these new changes need to be evidenced over time to show that the RMF is operating as intended, and is effectively underpinning the risk culture. Set out on the following page is a summary of key learnings from the other Financial Services industry groups following implementation of CPS 220.

Setting your organisation up for success

Building a risk management ecosystem optimised for today's challenges requires buy-in across the organisation. Four steps that can set your organisation on the right path are discussed below.

1

Set a strong organisational tone focused on risk culture

- CEOs should ensure performance management and incentives are aligned with their risk culture goals
- Leadership team communications should foster clear and consistent messaging
- Risk should be incorporated into routine conversations and decision making.

2

Align risk management with strategy at the point of decision-making

- Having a clear view into the organisation's strategy gives the first line of defence a common vision on which to align its decisions and behaviours, positioning it to react faster to risks and disruptions
- Decision makers should embed risk management into both strategic planning and tactical execution
- Defining boundaries and natural intersections clearly across the lines of defence enables the coordination of roles and responsibilities with maximum effectiveness.

3

Implement a clearly defined risk appetite and framework across the organisation

- Define risks the company is in the business to take, risks that cannot be tolerated, which risks should be measured and monitored and which risks are associated with financial performance variances that could impede strategy achievement
- The risk appetite and framework must be clearly communicated to decision-makers.

4

Develop risk reporting that enables executive management and the Board to effectively execute their risk oversight responsibilities

- A commonly understood risk taxonomy should govern the process of aggregating, tracking, and anticipating risks, and should leverage technology and data analytics when available
- Owners should be assigned to top-tier enterprise risks and be required to provide detailed, time-bound risk action plans.

Key learnings for PHIs from other industries

Formalise informal processes. Existing good practice needs to be formally documented for compliance purposes.

Plan in advance for annual reviews, and ensure work is evenly spread and not back end loaded.

A strong RAS is a key component. Ensure it is clearly integrated into the three year business plan.

Developing a strong risk culture, including how to measure and monitor, has a long implementation timeline.

To have a deeper conversation about how this subject may affect your business, please contact your PwC engagement partner or:

Renae Cooper

Partner
Assurance
+61 (2) 8266 4761
renae.cooper@pwc.com

Katherine Martin

Director
Risk & Regulation
+61 (2) 8266 3303
katherine.martin@pwc.com

Jenn Whittaker

Director
Culture & Behaviours
+61 (2) 8266 3199
jenn.whittaker@pwc.com

Katy Waterhouse

Manager
Culture & Behaviours
+61 (2) 8266 4937
katy.b.waterhouse@pwc.com

127053608