



### **Risk Management Prudential Standards - CPS 220 and SPS 220**

The regulator expects an institution to operate within its risk appetite and that its board has a view of how the institution's culture supports its risk management framework. Boards are therefore responsible to identify any necessary changes to culture, and ensure the institution takes steps to address them.

The reality is that a strong and positive organisational culture cannot be regulated into existence. To avoid a 'tick-the-box' mentality, APRA has not provided guidance or outlined specific initiatives it expects to see implemented. Rather, the regulator seeks to identify and encourage better practices across the industry.

APRA's Information paper on Risk Culture (October, 2016) profiled a number of approaches that have been piloted or adopted by regulated entities. Since that time, our perspective is that industry has not done enough to understand how their cultures support good risk outcomes.

A large number of organisations appear to have an over-reliance on simplified techniques, such as a handful of 'risk culture' questions in existing culture or engagement surveys, benchmarking or KPI dashboards. These relatively unsophisticated techniques can entrench an institutional blindness to the specific culture-related vulnerabilities that could undermine good risk outcomes.

It is worth noting that APRA has conducted assessments across a number of regulated entities with techniques that are varied and much more sophisticated than those adopted by many industry participants. We believe APRA is effectively role modelling 'what good looks like'.

As Helen Rowell, Deputy Chair APRA announced when tabling the Superannuation Governance in 2017: What does 'good' look like? report



The reality is that a strong and positive organisational culture cannot be regulated into existence. To avoid a 'tick-the-box' mentality APRA has not provided guidance or outlined specific initiatives it expects to see implemented. Rather, the regulator seeks to identify and encourage better practices across the industry.

"Good governance is not just about complying with a prudential standard, or following a code. It is about continually striving to improve practices and ensure the trustee itself, as well as its business operations, remain fit for the future."

APRA has invested heavily in new expertise, including organisational psychology, to support its program of work. While larger institutions may have the requisite scale to invest in similar capabilities, this is not an easy option for smaller industry participants across mutual banking, superannuation funds and many insurers.

### **Superannuation funds**

The superannuation industry is increasingly in the crosshairs of Australian regulators, to ensure they have a view on risk culture and that the appropriate tone is being set from the top. At the same time there is heightened public, regulator and government interest in the performance of trustees and their ability to meet the best interests of members including:

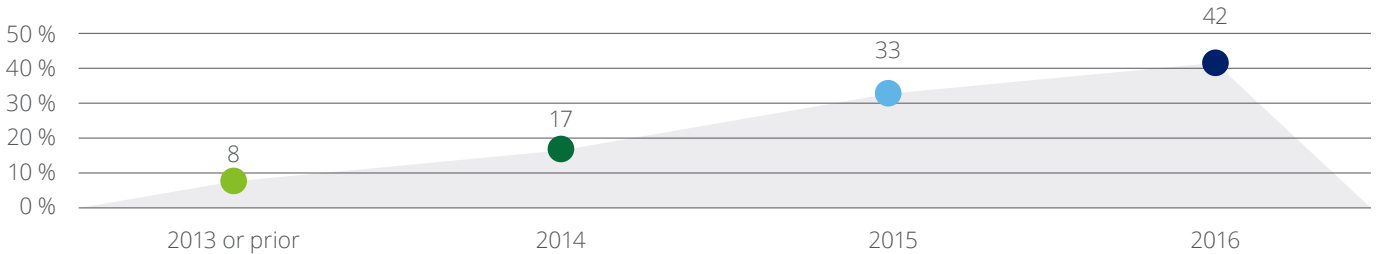
- The recent government proposed 'member outcomes test'
- Conduct in superannuation
- The role of insurance in superannuation
- APRA's information paper assessing Risk Culture across the financial services sector in October 2016.

### **Industry Snapshot**

To get a better handle on what 'good looks like' we undertook a survey of the superannuation industry focusing on the different approaches adopted for understanding risk culture. With response from 20 superannuation funds we asked how many and how often organisations undertook assessment programs; how the organisation defined risk culture; what techniques they used when assessing risk culture; how important and accountable senior management is for risk culture; and the facility to incorporate member feedback into changes to member products.

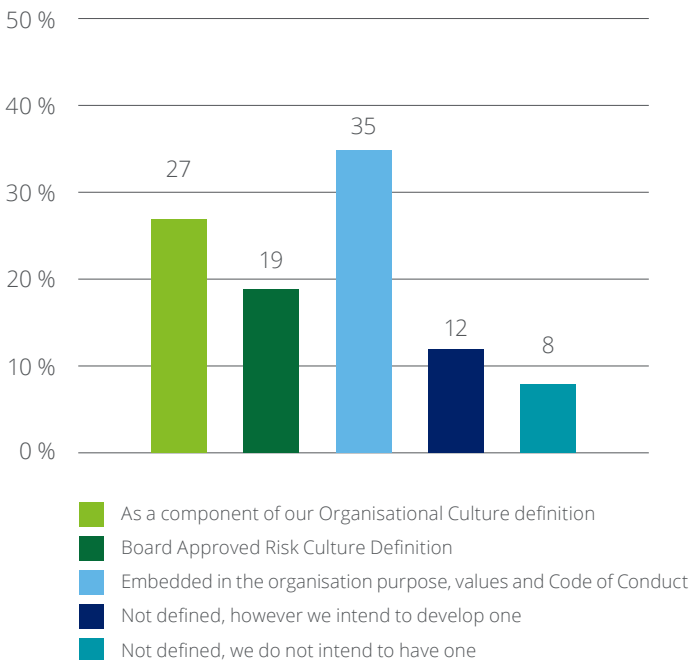
### When did your organisation commence regular risk culture assessments?

While the prudential standard SPS220 has been in place since 2013, most of the surveyed funds have only recently started risk culture assessments.



### How has your organisation defined risk culture?

The majority of surveyed funds (62%) have defined risk culture as either part of organisational culture or have embedded it in the organisation's Purpose, Values and Code of Conduct. While the prudential standards focus on 'risk culture', it is important to recognise that risk culture is simply a lens on culture. Embedding good risk practices as part of the organisation's culture maximises the benefit of reinforcing these practices through already established mechanisms such as performance management, leadership development and incentives.

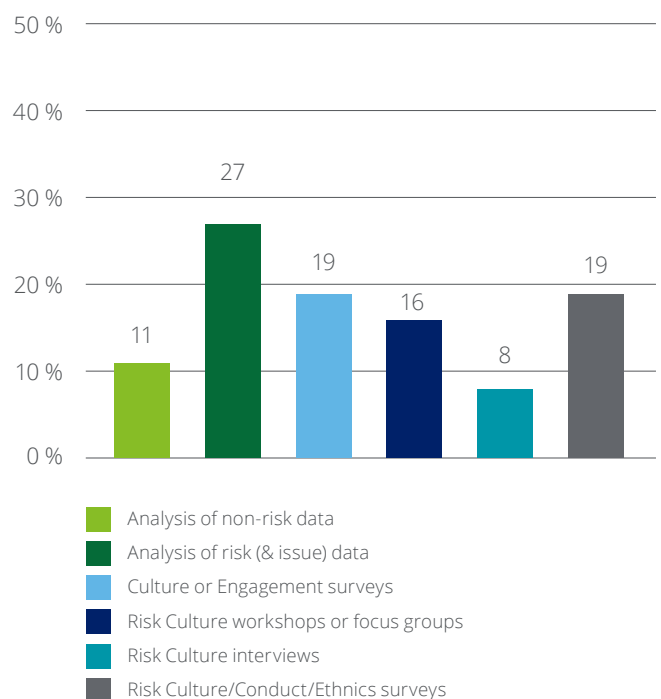


### Assessment techniques

63% of respondents indicated they have an approach for measuring and understanding risk culture. 55% of funds have performed their risk culture assessments in house with their most prevalent techniques:

- Analysis of risk data (27%)
- Culture / engagement surveys (19%)
- Risk Culture / conduct / ethics surveys (19%)

Data analytics and simple surveys are useful techniques to understand where there may be culture-related vulnerabilities, however their utility in helping organisations understand the underlying drivers - the 'why' - to determine the most appropriate actions is low. Organisations often end up treating the symptoms of culture - instead of the reasons why people think and behave the way they do.



## When looking at accountability and importance of risk culture

Some 32% of respondents said they aren't confident that all senior leaders and board members understand the risk culture of their organisation, and almost half (48%) of respondents believe that risk management is valued less in their organisation than investment performance or member returns.

More than a fifth (21%) of the organisations surveyed either intend to, or recently merged with another superannuation fund or business. So the lack of confidence, or focus on risk culture, is a concern when needing to consider the culture implications of such a big organisational undertaking.

## Member impacts

When asked how member feedback is incorporated into the product's design, it was predominantly through focus groups, surveys, product feedback and complaints.

Also 76% of organisations have policies or processes in place to identify where changes to the operation of a fund might have an unfair impact on particular classes of members. And of concern is the statistic that 37% of organisations don't have processes in place that allow member feedback about the fund to be incorporated in to the product's design.

## Risk Culture principles

Based on these insights, we designed a number of leading practices that superannuation funds should consider:

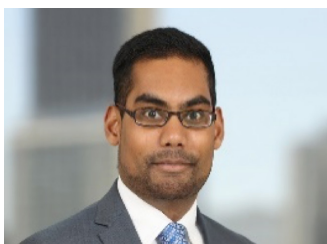
1. The board and executive set the cultural tone for the organisation
2. An organisation's culture (and risk culture) is defined through purpose and values (aspiration) and the code of conduct (minimum standards)
3. Risk and HR teams play distinct and yet critical roles in helping leaders to understand and positively influence how staff understand, think about, and act in relation to risk
4. Multiple techniques and sources of insight should be triangulated to understand how organisational culture supports good risk outcomes (mirroring what APRA is role modelling to industry)
5. Organisations must focus on the drivers of behaviour, or else well-intentioned actions that only target symptoms (e.g. communications, training) may drive potentially damaging attitudes or behaviour under the radar.

A strong risk culture starts from within. And when the culture is right, it will permeate throughout the organisation and customers will see and experience the difference.



**Grant MacKinnon** leads Deloitte's global Risk Culture Centre of Expertise. His work centres on the identification and redress of culture-related vulnerabilities or organisational 'design flaws' that result in unsustainable risk exposure or undesirable outcomes. He advises organisations from around the world across a broad range of industries. Grant's expertise is grounded in a deep understanding of system dynamics and operations research built up over a number of years within large and complex global organisations.

**+61 2 9322 3693** [gmackinnon@deloitte.com.au](mailto:gmackinnon@deloitte.com.au)



**Nicholas Rozario** is a Director of Superannuation & Wealth in the Assurance & Advisory Practice in Deloitte. He has 13 years of diverse experience across the financial services sector within professional services and the financial services industry. He has worked with leading financial institutions in Australia and the UK, with a strong focus on the risk, controls and compliance aspects of banking, superannuation and wealth management operations. Nicholas delivers internal and external audit services to Australian superannuation entities and asset managers, and assesses risk management and control frameworks. He implements policies and procedures relating to Stronger Super, including, operational risk reserves and APRA Prudential Standards.

**+61 2 8260 4468** [nirozario@deloitte.com.au](mailto:nirozario@deloitte.com.au)

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/au/about](http://www.deloitte.com/au/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

### About Deloitte

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's approximately 244,000 professionals are committed to becoming the standard of excellence.

### About Deloitte Australia

In Australia, the member firm is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 7,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at [www.deloitte.com.au](http://www.deloitte.com.au).

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Touche Tohmatsu Limited.

© 2017 Deloitte Touche Tohmatsu.

M CBD\_City\_11/17\_055227