A spotlight on how risk and compliance has contibuted to building trust across the Australian Wealth Management sector over the past decade

2017 Risk and Compliance Benchmarking Survey

10th Annual Survey | August 2017 | *This marks the tenth anniversary of our annual look at what is shaping the Risk and Compliance landscape in Australia. PwC surveyed 52 Australian-based Superannuation Funds and Asset and Wealth Managers. We also interviewed numerous executive and non-executive directors and compliance committee members to bring an additional perspective to this year's survey.*

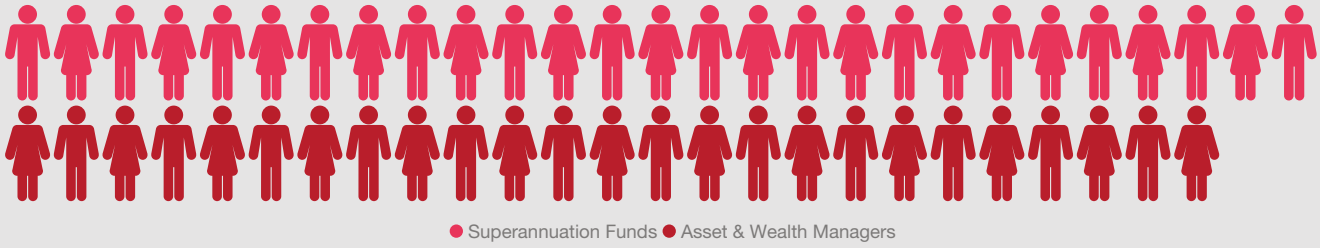
pwc

www.pwc.com.au

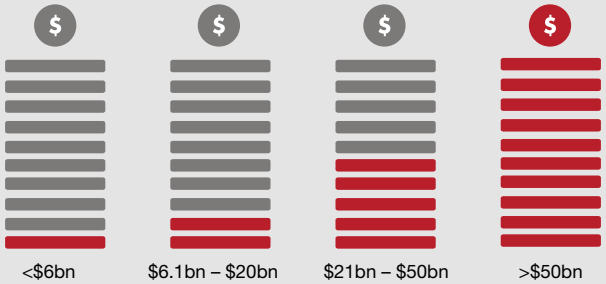
Table of contents

Who participated

Entity type



Assets under management



33% 29% 25% 13%

Geographical location

Executive summary

There have been significant changes in the Wealth Management sector since the *Superannuation Industry (Supervision) Act and Managed Investment Act* were introduced in the 1990s. Today the sector is the custodian of one of the largest pools of savings in the world, in an ever changing landscape that presents new opportunities and challenges.

With this comes greater scrutiny, both from regulators and the public, which has intensified since the financial crisis almost a decade ago. Over the years, this survey has highlighted the challenge that the industry has been tasked with, of trying to keep pace with rapidly changing regulations, while simultaneously trying to deliver value for customers and members, including reducing operating costs. This year is no different. We continue to see significant new regulatory requirements being imposed on the industry to provide greater protection and transparency for customers and members.

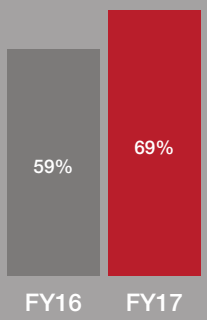
75% Ranked keeping up with regulatory expectations of risk management practices in their top three risk management challenges.

40% of CEOs were concerned that the rapidly changing regulatory environment is increasing the risk of their organisation not complying with relevant laws and regulations.[1]

Our recent PwC/Financial Services Council Chief Executive Officers (CEO) Survey[1] also highlighted that the majority of financial services CEOs believe that the burden of regulation is increasing, and are concerned about the cost of compliance. More worryingly, they are not convinced that current regulations are actually providing the value that customers and members seek, or supporting efforts to earn customers and members' trust. It's increasingly clear that industry and regulators need to find other ways to achieve closer collaboration, leading to regulation that adds real value, meets the needs of customers and members, and supports rather than hinders good business, innovation and growth.

1/3 respondents believe the current Australian regulatory model restricts their competitiveness globally.

Over the last decade, we have observed an increasing trend toward industry adopting a heavily outsourced operating model. The challenges this presents has been magnified in recent years due to the volume of data being generated and the increasing expectations to adequately monitor service providers. Further understanding who has access to your data has never been more important, with cyber attacks now part of business as usual.



10% increase year on year in the number of respondents having an enterprise wide data management strategy.

[1] PwC/Financial Services Council Chief Executive Officers (CEO) Survey July 2017
[2] PwC's Risk in Review 2017: Managing risk from the front line for greater resiliency and growth

Culture and conduct have always been a key driver of conduct, however it has received increased scrutiny in recent years. There has also been a trend toward using data to more effectively monitor culture and conduct. It is clearly important that the 'right people do the right things at the right time', yet our survey suggests measuring culture is still in its infancy for many. Tools to measure culture in the future will combine and analyse current data points and allow organisations to predict behaviours before they happen.

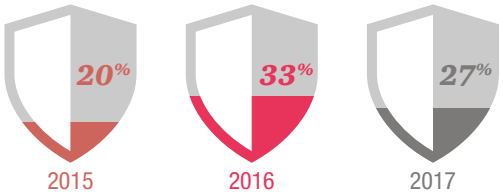
of respondents include risk related objectives and metrics in annual performance reviews.

What constitutes a reportable breach has been debated since our first survey in 2008. This could explain the lack of any clear trend in the number of breaches and incidents throughout the ten years of survey responses.

37%

of respondents do not have policies in place to comply with the new mandatory data breach notification requirements.

27% of respondents indicated the three lines as defence model to manage risk within their organisations are highly defined.



The effectiveness of the three lines of defence model has been discussed in recent surveys. Today, there is greater emphasis on the first line of the business owning and managing risk and compliance, with the Risk and Compliance function playing a greater monitoring role. This view is consistent with our 2017 PwC Global Risk in Review Survey,[2] which concludes that shifting risk decision-making to the front line drives higher revenues, faster risk-event recovery and stronger risk cultures.

Risk and Compliance functions

81% centralised

19% decentralised

With a significant pipeline of new regulatory reforms ahead of us, it is critical for organisations to look beyond traditional approaches to managing risk and compliance. Further, we should continue to remind ourselves of the important role risk and compliance plays in delivering better outcomes for customers and members. We hope this survey, and the discussions and debate which follow help contribute to enhancing trust in the sector.

Using FinTech to meet changing customer needs is seen as the number one opportunity for over 70% of respondents.

Impact of regulation

Our point of view

The Wealth Management sector has largely met regulatory challenges to date, but the real question is whether the sector is resilient enough to withstand the constant 'start, stop, deferral' approach to regulatory change, and continue to thrive?

- Over the years regulators have in addition to mandated compliance also imposed a principles and risk based focus. Consequently their engagement has moved from traditional annual visits to constant dialogue in the form of visits, thematic assessments, desktop and deep dive reviews.
- In the last five years we have seen key industry changes driven by regulation that has resulted in significant shocks to organisations which have continued to be compliance driven.
- The introduction of Superannuation Prudential Standards was a significant turning point for organisations to embed a risk led thought process in all decisions.
- Going forward we expect to see this risk led thought process having more of an impact on organisations' strategy and decision making.
- We see data playing a key role in the future outlook of regulatory supervision since the adoption of the increased reporting obligations, providing regulators with a constant stream of data points to enable greater analysis and organisational profiling.
- Organisations cannot afford to be complacent – policy uncertainty and constant regulatory change is contributing to an erosion of trust and the opportunity to drive value added service offerings to benefit members and customers.

Throughout the years...

From the introduction of the *Superannuation Industry (Supervision) Act* in 1993 and the *Managed Investment Act* in 1998, the Wealth Management sector has subsequently seen a steady stream of regulatory change, which shows no sign of abating in the short-term.

2001-2003

- The *Corporations Act 2001* and Australian financial services licence *(AFSL)* requirements released
- Government reviews effectiveness of the *Managed Investment Act* recommending the development of standards relating to qualifications and experience of compliance committee members

2004-2008

- Introduction of *Registrable Superannuation Entity Licensees (RSE Licencees)* concept requires trustees to demonstrate to APRA that they have adequate resources, risk management systems and skills
- *Anti-Money Laundering and Counter-Terrorism Financing Act 2008* introduces the need to identify and monitor customers, maintain a compliance program, report suspicious matters and cash transactions and file annual compliance reports

2012-2013

- The introduction of APRA Prudential Standards
- Significant increase in APRA reporting obligations (from 900 to 4,500 plus data points)

2014-2015

- Introduction of StrongerSuper reforms including MySuper licensing regimes and SuperStream
- The Federal Government released its response to the 2014 *Financial System Inquiry,* setting out an agenda for improving Australia's financial system including measures to ensure the Superannuation system is competitive, financial advice standards are lifted and financial regulator accountability and capability is enhanced

2016-2017

- AUSTRAC published first money laundering and terrorism financing Superannuation sector risk assessment
- ASIC releases a number of new regulatory guides, including RG 97 *Disclosing fees and costs in PDSs and periodic statements* and RG 259 *Risk management systems of responsible entities*
- Introduction of *Attribution managed investment trust (AMIT)* tax regime for registered schemes
- The Senate passes the *Privacy Amendment (Notifiable Data Breaches) Bill 2016* introducing a mandatory data breach reporting regime for the first time from 2017
- Government releases consultation draft legislation aiming to improve accountability and member outcomes in Superannuation

Regulator interactions

Over the 10 years of this survey, regulators have moved from annual on site focused reviews (predominantly APRA) to a regime of constant dialogue, monitoring and thematic reviews from multiple regulators. Once upon a time the regulator's dialogue was with risk and compliance personnel, but now it has evolved to include the board and/or senior management (including internal audit).

The larger Superannuation Funds (AUM $21bn plus) stood out amongst the respondents for having regular interactions with a host of regulators (APRA, ASIC, ATO and AUSTRAC). Interactions with the Privacy Commissioner were periodic for larger Superannuation Funds, but were still more frequent than for other survey participants.

Regulator	Nature of interactions
APRA	• Larger Superannuation Funds reported frequent engagement and an open relationship with APRA, whereas small (AUM < $6bn) and mid-Supernnuation (AUM $6bn – $20bn) Funds cited having periodic interaction • Interactions were predominantly through industry forums and roundtable discussions.
ASIC	• When it came to ASIC, again, it was the larger institutions (both Superannuation Funds and Asset Managers) who have regular interactions with the regulator, contrasting with others who reported ad hoc dealings. • Survey participants noted an increase in engagement with ASIC through industry forums and roundtable discussions.

The nature of regulator interactions varies, with APRA being the most active at industry forums and round table discussions.

Readiness for regulatory change

The pace of regulatory change continues and shows no sign of slowing in the short term.

RG 259

The release of **RG 259 *Risk management systems of responsible entities,*** while not introducing new requirements, does for the first time provide guidance regarding expectations of compliance with the requirements of the *Corporations Act 2001*. In releasing the new regulatory guide ASIC has stated that there is no transitional period and while they will take a facilitative approach until March 2018, it is a signal that the bar is being raised on responsible entities to a level previously expected by APRA of RSE Licencees.

In response to RG 259, the majority of asset managers identified the following areas where they will have to update their risk management frameworks:

1. designing and performing stress testing and scenario analysis on at least an annual basis;
2. creating or documenting risk registers, risk appetites and/or risk tolerances; and
3. documentation of the risk management system in place.

2016-17 Federal Budget

In response to the recent changes to Superannuation announced in the **2016-17 Federal Budget**, a significant majority of Superannuation Funds feel ready to respond. While the introduction of a Superannuation savings scheme for first home buyers brings implementation costs to RSEs, it generally is seen as an opportunity to interact with a younger demographic earlier in their working life.

VIEW FROM THE TOP

So much of the Boards and committees focus is on risk and compliance. Driving strategy is getting less focus as a result."

Risk and Compliance Committee Member of a large platform provider

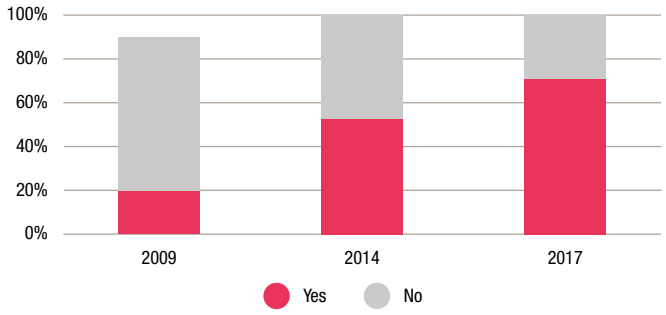
APRA visits made up over 50% of all visits/reviews to survey participants. Unsurprisingly this correlated with Superannuation Funds reporting 78% of all regulator reviews conducted during the year.

Did a regulator visit or conduct a review in 2017?

Visits/reviews by regulator

Over the years we have seen an upward trend in regulator visits amongst survey participants, which is to be expected given the trend in regulation and increased focus on the Wealth Management sector. This is a trend we expect to continue with the heightened focus on investor protection.

Trend in regulator visits



Over the years we have also seen a shift in how survey participants characterise their relationship with regulators.

2009

70% described regulator relationship as neutral

2011

42% described regulator relationship as positive

2017

50% described having a regulator relationship that involves regular and open dialogue

Resourcing

As regulatory change continues, 56% of respondents have increased their resourcing in the last 12 months in response, either through recruiting full time resources (33%), recruiting contractors (23%) or reallocating existing resources from other areas of the organisation (44%).

Australian regulatory model and global competiveness

There was an acknowledgement amongst the majority of respondents that Australia's regulatory model makes it an attractive place to invest due to:

- A high focus on member protection and disclosure;
- Positive interaction with regulators;
- Australia's capital adequacy requirements; and
- A flexible, principle approach backed by regulatory action where required.

VIEW FROM THE TOP

"Broadly, the Australian regulatory model has served members well whilst acknowledging it could also be improved. Internationally it is well regarded; expect overseas frameworks to adopt features of our model over time."

Non-Executive Director and Compliance Committee Member of a global fund manager

However there are further opportunities to improve regulation in the sector:

- Regulators need to provide clearer guidance on expectations when introducing new regulation (e.g. expectations of RG 97 has been difficult for the industry to digest); and
- The volume of regulatory change requires significant resources, time and money and creates uncertainty which impacts strategic planning. It draws away from business as usual and there needs to be greater alignment to global regulator expectations.

1/3 respondents

believe the current Australian regulatory model restricts their competitiveness globally.

How will an industry funded regulator impact your organisation?

We are gradually seeing the recommendations made in the Financial System Inquiry flow through into regulation. Monitoring compliance with these new regulations requires a well-funded and resourced regulator.

From 1 July 2017, the Federal Government has introduced the operation of an industry funded model for ASIC. Similarly to APRA, this user pays model will recover ASIC's regulatory costs though annual levies and fees-for-service and is seen as a critical component of the Government's plan to improve consumer outcomes in the financial system.

The introduction of the proposed regulations has also created uncertainty, with the mechanisms that will be used to calculate the levies payable by each class of regulated entity not yet finalised.

Consolidation of Superannuation Funds present new risks

Economies of scale and an outcomes driven focus is challenging the business models of Superannuation Funds. As a result, we have seen increased merger activity and alliances amongst funds and this will only continue as the regulator pushes for a more efficient and outcomes driven Superannuation system. Recent draft legislation may give the regulator extra powers to challenge Boards on a member best interest test, rather than just on a scale test.

When considering a merger and/or alliance partner, there are a wide array of areas that need to be worked through. Risk and Compliance functions will play an important role throughout and their responsibilities may include:

- Assessing the risk profile of the fund/organisation;
- Development of the governance framework and protocols;
- Overseeing the transfer of member data;
- Contributing to the member communication strategies; and
- Assisting with the assessment of outsourced service provider capabilities and selection of preferred provider.

VIEW FROM THE TOP

"APRA is pushing for Superannuation Fund consolidation. The vertically integrated model of the banks is being dismantled, will the large Superfunds be the vertically integrated model of the future?"

Risk and Compliance Committee Member of a large fund manager

Calls to action

1. Organisations need to take ownership of their risk appetite and apply this when interpreting the principles based expectations of regulators.
2. Organisations need to consider that the challenges to implement the policy pipeline will have implications for many years to come. This includes federal budget changes, defining the objective of Superannuation, efficiency and competitiveness reforms, transparency disclosures and the evolution of retirement products.

Data management, cyber security and outsourcing

Our point of view

- Organisations within the Wealth Management sector have historically adopted a simple outsourced model, traditionally led by custody, administration and accounting services.
- Over time, the drive to maximise customer focused opportunities and advances in technology has led to a complex outsourcing ecosystem which presents different types of risk.
- Superannuation Prudential Standards have set principles for organisations to monitor material outsourcing arrangements. The focus on materiality means organisations may not apply the same consideration and rigour to all outsourcing arrangements. This could lead to the risk of not adequately managing and monitoring risk exposures associated with other outsource arrangements (e.g. FinTech and Cloud providers). These providers may not meet the definition of material business activity but may be more inherently risky and could have reputational implications.
- The spotlight on protecting sensitive information continues to rise and will only increase in intensity in the coming years. As a result, there will be more pressure on organisations to take ownership and be accountable for data management.
- The frequency and severity of cyber attacks has many organisations considering cyber insurance.

Throughout the years...

2009

- 82% of respondents outsource Custody, 50% Administration and 40% Accounting Services
- Monitoring of outsourcing not appropriate given the extent of services outsourced in a Managed Investment Scheme structure, 1 in 5 do not review SLAs on an annual basis

2012

- 90% now outsource Custody, 65% Administration and 52% Investment Management
- Only 35% monitor External Service Providers frequently

2013

- Introduction of outsourcing Prudential Standard

2015

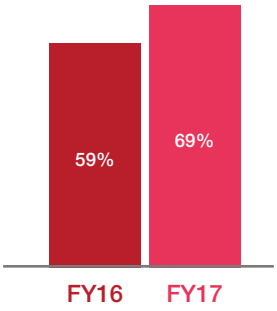
- Office of Australian Information Commissioner announces intention to introduce mandatory data breach reporting
- Preparing for cyber attacks targeted against the privacy of consumer/member data consistently in top 3 biggest risk challenges
- 95% of respondents rated their Board's oversight of privacy & cyber security risks as weak, or sufficient but needing improvement

2016

- Only 59% of respondents have an enterprise wide response to data management
- 49% have increased cyber security budgets compared to 2015
- 65% have performed a cyber security and privacy risk assessment and gap analysis, up from 38% in 2015
- Site visits remain the most effective mechanism to monitor performance of External Service Providers

Data management

The governance of data has continued to be a priority for the Wealth Management sector, with 69% of respondents having in place an enterprise wide defined and endorsed data management strategy. This is an increase from 59% last year. However, just under half of survey respondents have established a separate, formal Data Governance Committee with representatives from both the business and technology to drive the implementation of the data management strategy.



10%

increase year on year in the number of respondents having an enterprise wide data management strategy.

Increasingly, we are seeing the Wealth Management sector view data governance as more than just a compliance activity. Pressures from the threat of new FinTech competitors and intermediaries, as well as the recommendations in the Productivity Commission's recent report on data availability and use may translate into an open data regime in Australia. Add to this the building momentum to derive new member/unitholder or operational insights from data, the governance of data can be a strategic enabler.

Leading organisations have already recognised the opportunities and are driving a convergence of sorts around data quality, protection and privacy – that is, a more coordinated approach to managing the risks and opportunities arising from the increased sharing and usage of data.

The focus on data has raised other considerations for organisations, particularly with respect to data accessibility, sharing and usage. These considerations are a new dimension in the trust equation, particularly for organisations with retail customers in the Wealth Management sector.

This will continue to evolve as a greater variety and volume of data is transmitted realtime in higher velocity to customers and to and from third parties.

Given the increase in the creation, storage and transmission of data – it is interesting to note that just over a third (37%) of survey respondents do not have policies in place to comply with the new mandatory data breach notification requirements.

37%

of respondents do not have policies in place to comply with the new mandatory data breach notification requirements.

Superannuation Funds in particular hold a significant amount of confidential data about their members and often employ third parties to hold or manage this data.

In response, organisations need to be alive to the following key questions:

- *Are you aware of all the places that your confidential or critical data resides?*
- *What checks and balances are in place to make sure that third party service providers handle your data with care and quickly report/escalate any data breaches to you so that they can be handled appropriately?*

However, whilst the world is evolving in relation to data, many organisations in the Wealth Management sector are still struggling with the basics of data management (ie. what data is critical, who owns it and what does good quality mean)?

There appears to be a recognition amongst survey respondents how critical data management is, with 25% of organisations stating they had a partially developed mechanism or that they plan to formalise it in the next three months.

> Identity has been at the heart of almost every [data] breach in the past two years"[3]

Richard Kneeley, PwC US Managing Director, Cyber security and Privacy

Cyber security

With the emergence of data becoming one of the sector's key assets, it then logically follows that 52% of participants identified preparing for cyber attacks against the privacy of consumer data and confidential information as one of the top three risks. This finding is consistent with that of the 2017 PwC CEO Survey which reported that 59% of Asset and Wealth Management CEOs are concerned about cyber threats.[4]

VIEW FROM THE TOP

Boards must recognise this risk and understand the challenges cyber security poses on their Funds. The pace of change will continue to increase rapidly. Systems that were fit for purpose in the past will no longer be capable in this new environment and will need to change in a more competitive market place to have innovation and technology right."

Compliance Committee Member of a global fund manager

[3] Toward new possibilities in threat management: Key findings from the Global State of Information Security Survey 2017
[4] 20th CEO Survey/Key findings in the Asset and Wealth Management industry/February 2017

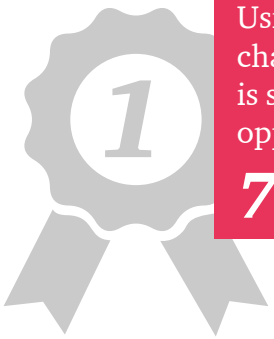
VIEW FROM THE TOP

As 'Fintechs' emerge, the level of member engagement will change. New technologies will foster greater member engagement and they will need to be prepared for that and evolve with it."

Risk and Compliance Committee Member of a large platform provider

Using digital to improve member engagement

Digital platforms provide new opportunities to engage with customers and members. Understanding the needs of customers and members and tailoring a product to meet these needs to gain a competitive advantage will be achieved through deeper, more real time engagement.



Using FinTech to meet changing customer needs is seen as the number one opportunity for over **70%** of respondents

In addition, the opportunity of digital engagement brings with it responsibility. PwC's 2017 CEO Survey[4] indicated that CEOs see cyber security breaches as the biggest threat to building trust. However they appear far less concerned about cyber threats than their peers in banking and insurance.

[4] 20th CEO Survey/Key findings in the Asset and Wealth Management industry/February 2017

Outsourcing

The focus on protecting consumer and organisation owned data and confidentiality from the threat of cyber attack, coupled with the fact approximately half of survey respondents maintain data offshore, it is more critical than ever that the Wealth Management sector effectively oversees third parties and their handling of data.

46%

of respondents have a formal mechanism in place to identify and manage "critical data"

50%

of respondents maintain data offshore

Calls to action

1. Organisations should understand, prioritise and categorise their supplier base using a risk based approach.
2. When it comes to data management, Boards should be asking themselves the following questions:
   - how effective is their cyber security strategy at addressing the risks the business faces?
   - what is the organisation's comprehensive strategy for addressing data security and is it effective?
   - does the strategy include innovative technologies to monitor, identify and respond to cyber threats or incidents?
3. Cyber insurance is a new and evolving area, therefore it is important that companies thoroughly understand their policies – what's covered, and more importantly, what isn't. Boards will want to understand the company's policy and how the insurance market is changing, particularly as underwriters become more sophisticated.

Culture and conduct

Our point of view

Culture has always been the driver of conduct, however it has received increased scrutiny following the Global Financial Crisis (GFC) and has been a growing theme year on year since our 2011 survey.

- Culture can be the root cause of misconduct – it's about identifying the warning signs and taking action in order to protect consumer confidence.
- We are seeing more executives and directors starting to appreciate the value that understanding behaviours and factors that lead to behaviours can make.
- Culture is often seen as too intangible to evaluate and track. But by assessing the levers that influence it and the behaviour and outcomes it generates, it's possible to develop a clear and quantifiable assessment. This assessment can provide a clear indication of whether employees understand what is expected, whether they're translating this into their day-to-day activities, and whether recognition and other reinforcing mechanisms appropriately support this. This assessment can then form the basis for clearly targeted interventions that go beyond vague talk of cultural change.
- Culture indicators to focus on include tone from the top, accountability, effective communications and alignment of recruitment and reward to the values of the organisation.

Throughout the years...

2011

- Following the GFC, regulators increase scrutiny on role of directors in delivering effective corporate responsibility following actions taken of directors of failed companies
- Greater ownership of risk at Asset Manager's senior management level results in strengthening of the three lines of defence model

2014

- APRA's 220 Prudential Standards come into play, Risk and Compliance functions seen as playing significant role in articulating current state, identifying ideal state and monitoring actual state of culture
- Surveys predominantly used to assess current state of culture

2015

- 75% ranked creating a culture that supports organisation-wide risk in their top three risk management challenges
- Culture seen as an important tool to influence conduct, promote desired behaviours and identify the more pervasive problems organisations face in response to stakeholder expectations

2016

- 60% ranked creating a culture that supports organisation-wide risk in their top three risk management challenges
- 98% believed they had a culture that encourages escalation of business risks to senior leadership

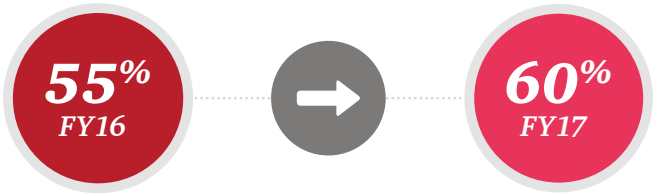
Culture and conduct: A recurring theme

Culture and conduct has emerged as a recurring theme in the benchmarking survey as the sector responds to increased regulator expectations.

Risk and performance

There continues to be a clear acknowledgement of the importance of creating an environment where the right people take the right action at the right time. The design and implementation of risk management frameworks and policies are important to enable the management and consistency to the organisations risk exposure.

Larger Superannuation Funds indicated risk related objectives form a part of annual performance reviews, having a strong impact on performance ratings and recognition. Larger Asset Managers responses varied in comparison, with only 50% focusing on risk impacting performance. This was even less prevalent in smaller sized organisations across both Superannuation and Asset Management, with only a handful making the linkage between risk and recognition.



of respondents include risk related objectives and metrics in annual performance reviews.

Measuring culture

Progress has been made in terms of setting principles and defining, at a high level, the mechanisms for measurement and requirements for reporting.

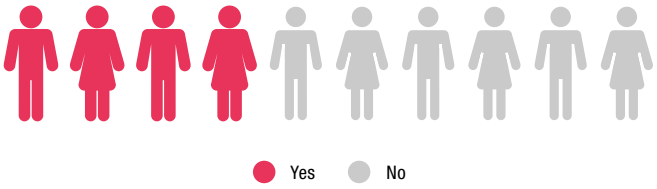
The next step is to assess culture against these principles and determine the specific actions required to achieve the desired state.

> "I can't stress this enough. Reward staff to behave as you would want them to. Act as you would want them to act."
>
> Ian Lauchlin, Deputy Chairman, APRA Macquarie University Financial Risk Day, Sydney 13 March 2015

Overall, 40% of respondents are currently measuring culture and conduct across their organisation. Larger Superannuation Funds and Asset Managers are leading way, with two thirds of respondents already doing this.

Of the 60% currently not measuring culture and conduct, over half plan to implement measurement tools within two years.

Do you currently measure culture and conduct?



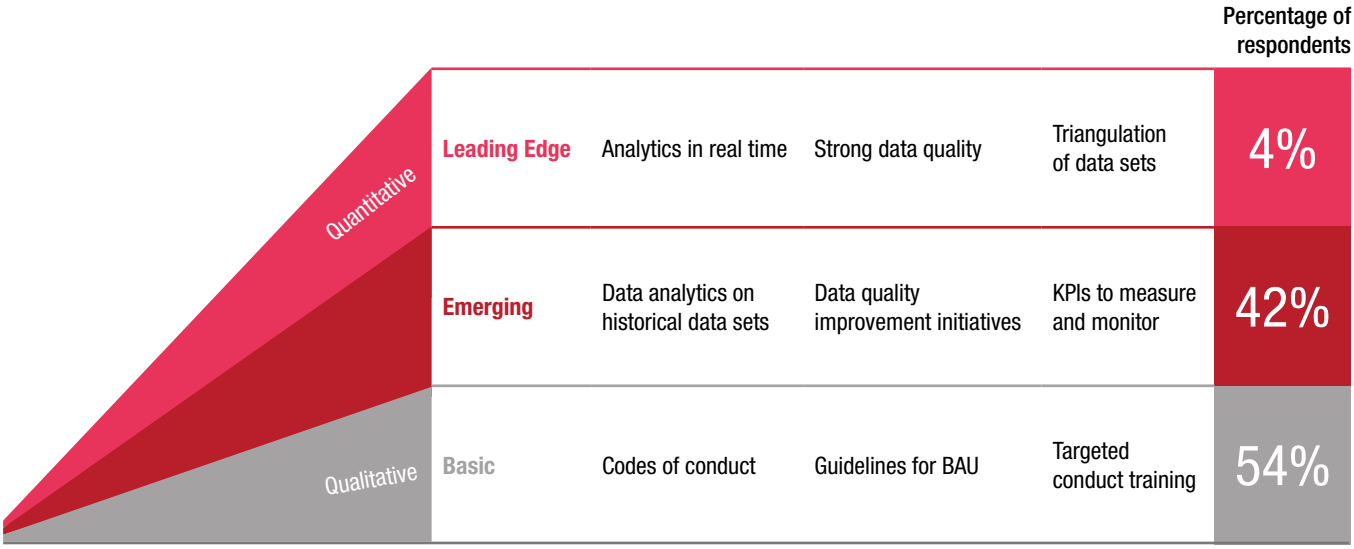
The most frequent means for measuring culture was by performing surveys of staff to determine behaviour in particular scenarios. Although this may raise awareness of what the desired behaviour is, it does not mean that employees will act in that manner consistently.

Through the use of the data, organisations can understand how employees are actually behaving. Techniques such as analysing data points from key systems that employees use in their day to day job as well as from ancillary functions (e.g. email) provide greater transparency.

Undesirable behaviour can be identified on a real time basis and its impact managed. Further, an organisation can understand if there are root causes and use these to predict future behaviour to eliminate undesirable behaviour before it occurs.

Only 4% of respondents considered themselves to be leading edge when it came to the use of data to manage culture and conduct.

Continuum of Culture and Conduct measurement



Reporting

More than 60% of participants indicated that culture and conduct monitoring and measurement outcomes are not reported to the relevant committees responsible for risk management. Only 12% indicated that it's a standing meeting agenda item.

Reporting on culture and conduct to those who are setting the tone from the top is important to ensure that there is alignment between expectations and the organisations culture.

Calls to action

When setting a vision for culture, organisaitons should ask themselves the following questions:

1. Do Boards and senior management foster a strong culture and trust their employees to behave as expected? Does your culture convey what your organisation stands for?
2. Does your organisation have a clear and compelling vision and set of values, and is what is expected as a result understood within the organisation?
3. What elements of our culture do we want to reinforce and what would we like to change?
4. To what extent is our leadership living up to our values and how is this demonstrated?
5. To what extent is staff behaviour aligned with our vision and how is this monitored?
6. How effective are rewards, performance management and other reinforcing mechanisms in supporting our desired culture and behaviour?
7. Does HR have a seat at the table when culture and resource risks are discussed at Audit and Risk committees and Board meetings?

Breaches, incidents and complaints

Our point of view

- The setting of expectations and definition of breaches and incidents is not consistent amongst organisations and can get even more complicated in an outsourced model.
- Definitions of breaches and incidents are not always articulated in Key Performance Indicators and Service Level Agreements.
- The link between breaches, incidents and remuneration is not strong – organisations rarely incentivise employees to raise breaches and incidents.
- Complaints, incidents and breaches relating to the misuse or handling of data are trending upwards.
- Incidents of data breaches have been siloed and isolated to date, but the introduction of the new mandatory data breach notification regime means the regulator now has stringent reporting requirements.
- The channels for lodging complaints have changed – once the domain of letters and phone calls which organisations could largely manage the contagion risk of, complaints are now real-time and out in the public via social media.

Throughout the years...

2009

- Definitions and clarifications of what is a 'breach' is inconsistent across the sector
- Most common breaches are inaccurate calculation of fees and expenses and unit pricing errors
- Fund performance tops complaints type, direct result of market volatility following the GFC

2010

- ASIC and APRA sign a memorandum of understanding setting out a framework covering cooperation, information sharing and regulatory and policy development

2012

- Average number of breaches per respondent fall, 1.4 in 2011 to 0.6 in 2012
- 2/3rds of respondents conduct breach trend analysis
- Complaint handling continues to improve in traditional mediums however only a few monitor social media for customer feedback

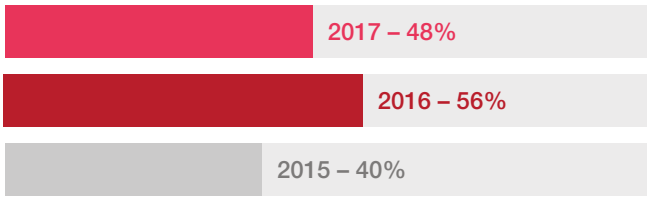
2014

- Sector still not clear on what constitutes a reportable breach
- Over half of the 1,300 breaches identified are as a result of a control failure by external service providers
- 42% monitor social media for complaints, up from 23% in 2012
- ASIC introduces concept of significant breaches and associated reporting requirements.

2016

- Over half of respondents report a breach to either ASIC, APRA, AUSTRAC or the Privacy Commissioner during the year
- Average number of breaches per respondent is 1.6 up from 1.2 in 2015
- 38% increase in detected information security incidents
- Types of complaints consistent for the last couple of years, most frequent are: poor customer service, products fees and account maintenance issues

The percentage of respondents that had a reportable breach to a regulator for the year ended 31 March 2017 has declined to 48%.



Breaches

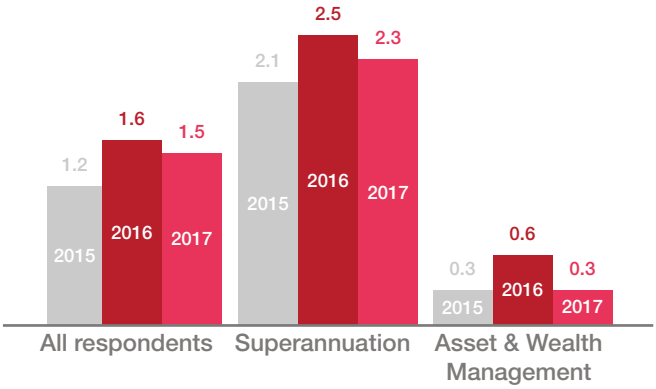
Confusion as to what constitutes a reportable breach has persisted since our first survey in 2008. This inconsistency could explain the lack of a clear trend in the number of breaches and incidents throughout the 10 years of survey responses.

Our survey results across all respondents show the average number of reportable breaches to the regulator was 1.5 per year, slightly down from the average of 1.6 in 2016.

The main drivers of reportable breaches across all respondents included non-compliance with the law and licencing requirements, and unit pricing issues.

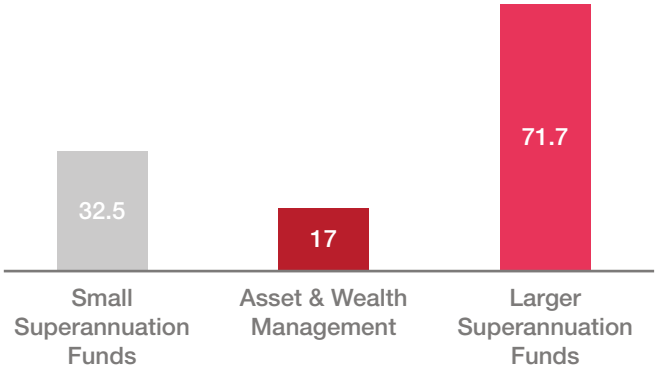
The average number of non-reportable breaches was also down, 32 in the current year compared to 40 in 2016.

1.5 The average number of reportable breaches per respondent for the year ended 31 March 2017.



The majority of non-reportable breaches were as a result of incorrect reporting to members/unitholders and privacy breaches.

The average number of non-reportable breaches per respondent for the year ended 31 March 2017.



On average larger Superannuation Funds had the most non-reportable breaches per respondent. This may indicate that they have greater resources and are more closely monitoring their operations.

Breach analysis

85% conduct root cause analysis over their incidents and breaches. Out of these, over half said that this analysis has resulted in a reduction of similar incidents and breaches as well as earlier identification and resolution of these issues.

Government focus on increasing transparency and accountability

Breach reporting continues to be an area of focus for both the regulators as well as the government. On 11 April 2017, the Government released a paper on *'Self-reporting of contraventions by financial services and credit licensees'* by the ASIC Enforcement Review Taskforce. The proposals outlined in this paper aim to improve transparency and accountability in the financial services sector by broadening and strengthening the obligations on licensees. The Taskforce will provide its recommendations to Government by the end of 2017. The proposed reforms are aimed at:

Reducing ambiguity whether breach is significant and must be reported + Enhancing accountability + Introducing penalties for non-reporting + Requiring ASIC to publish breach reports data + Introducing equivalent reporting regime for credit licensee = Proposed reforms

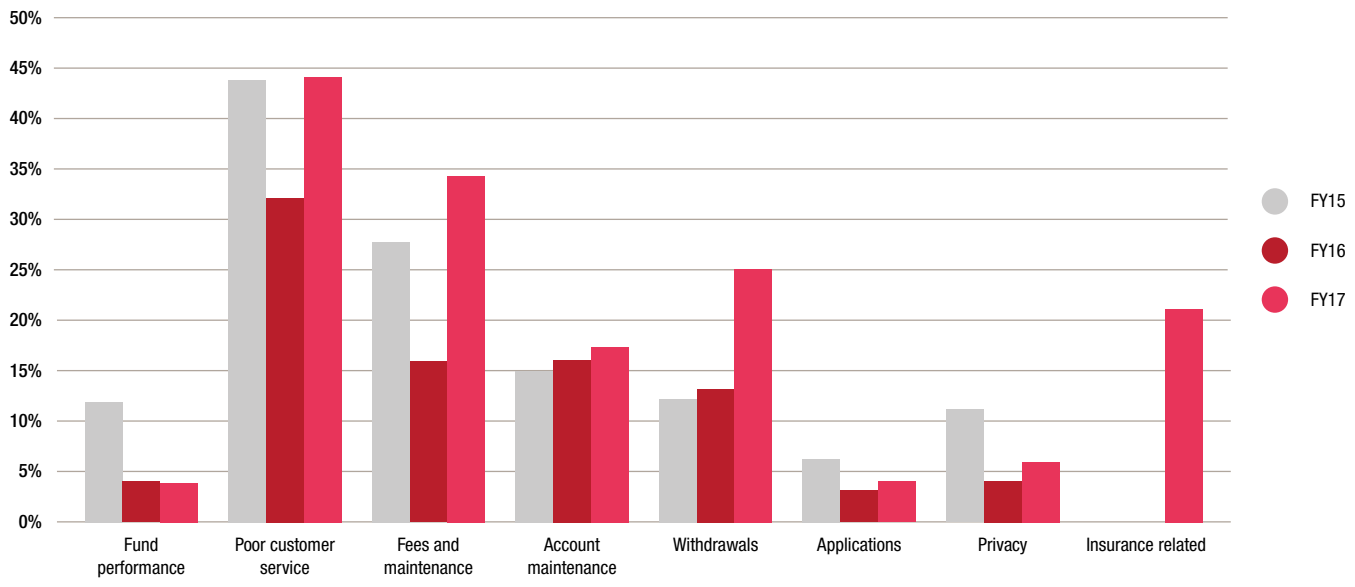
AUSTRAC is also in the process of consulting with the Superannuation industry with respect to greater transparency in reporting fraud incidents and near misses.

Complaints

The three largest drivers of complaints are dissatisfaction with customer service, fees and maintenance and issues relating to withdrawals. This remains broadly consistent with the prior year. Our survey results also indicate that respondents are also grappling with complaints surrounding insurance related matters as a significant area of focus. With the introduction of the insurance in Super working group and the governments ongoing interest in whether insurance in Super is still viable and the structure around product design for MySuper members, insurance in Super will continue to be an area of public scrutiny and risk and compliance focus.

Traditionally, complaints have been communicated directly between member to Fund avenues (e.g. phone, mail). However, over time complaints have been more broadly communicated via mainstream digital channels, including social media, which reaches out to other stakeholders real time. This change has impacted processes, resources and the level of effort needed by the business and risk and compliance functions. This will continue to be a challenge.

Nature of Complaints



VIEW FROM THE TOP

Regulatory change is a constant. Committee members need to be on top of it and understand how well prepared management is."

Non-Executive Director and Compliance Committee Member of a global fund manager

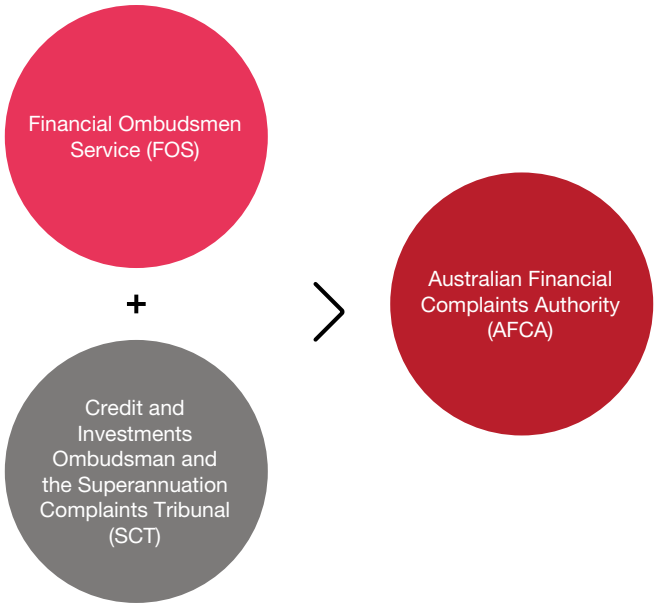
Will RG 97 lead to an increase in complaints?

We continue to see the implementation of RG 97 *Fees and costs disclosures in product disclosure statements and periodic statements* impacting the organisations. Respondents have indicated a range of readiness, with only 50% feeling adequately prepared for the new requirements.

The ASIC deadline for updating product disclosure statements (PDSs) is 30 September 2017. Overall, there is an expectation that the disclosed fees and costs for many funds and Superannuation options will increase under RG 97.

This could confuse members as fees and costs appear to have increase albeit in substance nothing has changed.

Given the complexity associated with the adoption and interpretation of RG 97 the communications to all stakeholders becomes extremely critical. Those that have early adopted have developed communication strategies (call centre scripts, website disclosure, written material) in anticipation of the response to the release of the data.



Improving outcomes for investors

Following the governments review of the Australia's External Dispute Resolution (EDR) and complaints framework for the financial system in 2016, the EDR released its final report in April 2017. Its main recommendation was to establish a new single EDR body for all financial disputes (including Superannuation disputes). The rationale for a central EDR body is to aid in achieving comparable outcomes for customers and members with similar complaints, improve the efficiency of disputes involving firms that are members of different schemes and eliminate duplicative costs for the sector and for the regulator.

AFCA will operate in place of the Financial Ombudsman Service, the Credit and Investments Ombudsman, and the Superannuation Complaints Tribunal from 1 July 2018.

Calls to action

1. Organisation should document their definition of breaches and incidents and ensure they are included in Key Performance Indicators and Service Level Agreements.
2. The new mandatory data breach notification regime comes into effect in 2018 – organisations should ensure they have policies in place to comply.
3. Does your organisation have a policy in place to respond to complaints on social media? How is the marketing team engaging with compliance to ensure complaints are escalated and appropriately considered?
4. RG 97 comes into effect in PDSs from 30 September 2017 and given the complexity involved the communications to all stakeholders (media releases, script for call centres, board communications etc.) becomes extremely critical. Organisations should have a communication plan in place.

Evolution of risk and compliance functions

Throughout the years...

2009

- Compliance functions of MIS respond to the GFC by increasing workload for a reducing compliance team and moving to risk based monitoring of compliance plans
- Tenures of committee members not defined in over half of respondents
- Drop in compliance resources has increased the reliance placed on the business to own and monitor compliance
- 93% have a centralised Compliance function

2011

- War for talent escalates following the GFC, retention of skilled resources seen as competitive advantage in pursuit of market growth
- Greater ownership of risk at the senior management level results in a strengthening three lines of defence model

2012

- Filling compliance roles becomes easier, with 20% expressing difficulty to fill vacant roles. Down from a 1/3rd in 2011
- Splitting time and resources between business as usual and understanding and planning for new reform is a common challenge

2014

- 62% required to up-skill or recruit for new skills and capabilities as a result of the regulatory change agenda
- 44% note maintaining the quantity, skills and capability of risk and compliance resources as a key challenge faced by the Risk and Compliance functions
- Of those responsible for risk and compliance, 45% wear multiple hats in their role
- 87% have a centralised Compliance function, up from 80% in 2012

2016

- Of those responsible for risk and compliance, 65% have a pure stand-alone role and do not double hat responsibilities across risk and compliance
- 33% have a highly defined three lines of defence model to manage risk, up from 20% in 2015

The risk and compliance function of the future

Given everything we have seen in the last 10 years and the expectation of more regulatory change, what does the risk and compliance function of the future look like?

Just adding more resources or rolling out more tools will not work and is not sustainable. Organisaitons will need to have the right people, the right culture and the right behaviour in order to build trust and thrive.

27% of respondents indicated the three lines as defence model to manage risk within their organisations are highly defined.

Contacts

Melbourne

George Sagonas

Partner
Superannuation and Asset Management
+61 (3) 8603 2160
george.sagonas@pwc.com

Nicole Oborne

Partner
Superannuation
+61 (3) 8603 2914
nicole.oborne@pwc.com

Symon Dawson

Principal
Risk & Regulation Consulting
+61 (3) 8603 0067
symon.b.dawson@pwc.com

Adrian Gut

Director
Asset Management
+61 (3) 8603 6417
adrian.gut@pwc.com

Owain Norman

Senior Manager
Asset Management
+61 (3) 8603 0458
owain.a.norman@pwc.com

Sydney

Craig Cummins

Partner
National Superannuation Leader
+61 (2) 8266 7937
craig.cummins@pwc.com

Stephanie Smith

Partner
Asset Management Leader
+61 (2) 8266 3680
stephanie.smith@pwc.com

Sarah Hofman

Partner
Financial Services Regulation
+61 (2) 8266 2231
sarah.hofman@pwc.com

Emma Grogan

Partner
People and Organisation
+61 (2) 8266 2420
emma.grogan@pwc.com

Deanna Chesler

Director
Asset Management
+61 (2) 8266 0003
deanna.chesler@pwc.com

Adelaide

Kim Cheater

Partner
Financial Services
+61 (8) 8218 7407
kim.cheater@pwc.com

Brisbane

Paul Collins

Director
Financial Services
+61 (7) 3257 8558
paul.d.collins@pwc.com

127051706