Driving better outcomes

Empowering Risk and Compliance functions to help deliver strategic outcomes

In late 2019, we surveyed Risk and Compliance functions of Australian asset managers and superannuation entities (collectively referred to as the Wealth Management sector). Here we discuss how Risk and Compliance functions can drive change beyond the short term and proactively deliver better customer outcomes.

www.pwc.com.au

Survey by numbers

2019 Biggest risk management challenges

#1 Regulation
2018 - Regulation

#2 Third party oversight
2018 - Third party oversight

#3 Risk management culture
2018 - Preparing for cyber attacks

Top priority initiatives following APRA Prudential Inquiry and Royal Commission

46% Impact self-assessment of the Royal Commission report

42% Strengthening of accountability

42% Self-assessment against the APRA CBA report

40% Investment into risk and compliance functions

Deep dive exercise to assess and understand culture

50%	25%	25%
Have performed	Intend to in the next 12 months	Have not performed

Regtech readiness

14% Not ready at all

25% Unclear on strategy alignment

29% Starting conversations

14% Ready and aligned

18% Using Regtech solutions

Top driver for implementing a data management program

67% Information security/privacy

64% Data governance

64% Data quality

2019 Barriers to Regtech adoption

42% Immaturity of regtech market

32% Uncertainty over regulations

21% Legacy system

2018

Credibility of unproven technology **37%**

Immaturity of regtech market **28%**

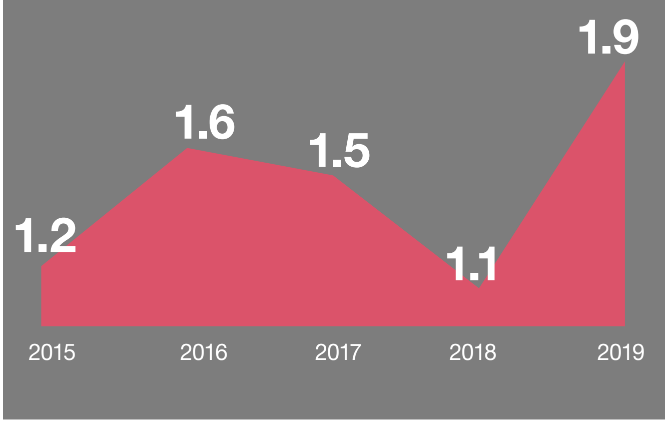
Incompatible legacy system **24%**

90% Use business attestations to form part of risk management framework

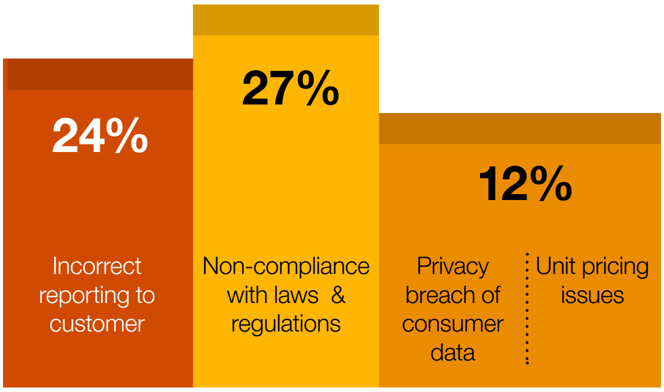
10% Have risk and compliance obligations fully mapped to controls tested

3/4 of respondents validate controls at key service providers

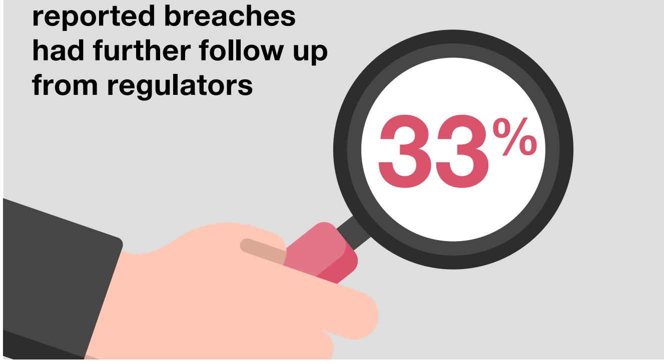
Average number of reportable breaches



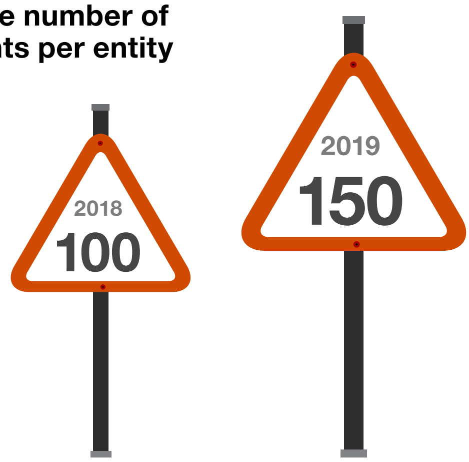
Nature of top 3 reportable breaches



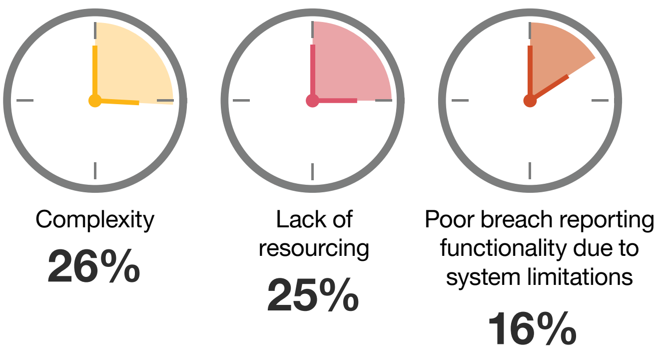
1/3 of those who reported breaches had further follow up from regulators



Average number of incidents per entity

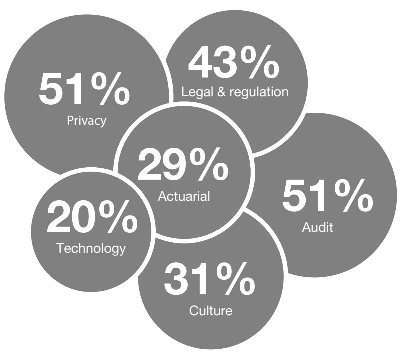


Barriers to timely resolution of incidents & breaches & complaints

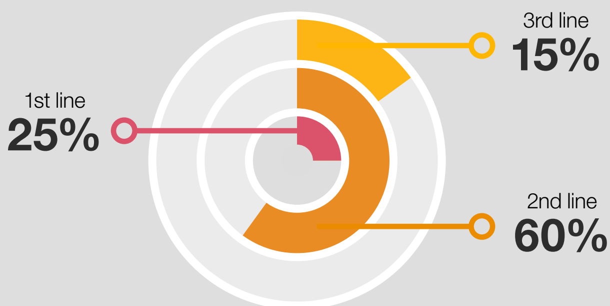


Types of breach analysis performed

Percentage of risk and compliance teams with specialist skills



Who is responsible for testing of controls in relation to risk & compliance



Executive summary

Nearly a year on from the conclusion of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (the Royal Commission), our 12th annual survey of Risk and Compliance functions across the Wealth Management sector has indicated the aftershocks are still being felt.

Consumer trust levels remain low, regulators are becoming better resourced and customer centricity is front of mind. There is heightened reputational risk for those who act inappropriately at a time when brand is seen as a key differentiator for growing the business and driving sustainability.

Our survey shows the expected reaction to the events of 2018 have continued during 2019. As a result, prioritisation of changes to sustainably drive better customer outcomes has been difficult. Action is needed to:

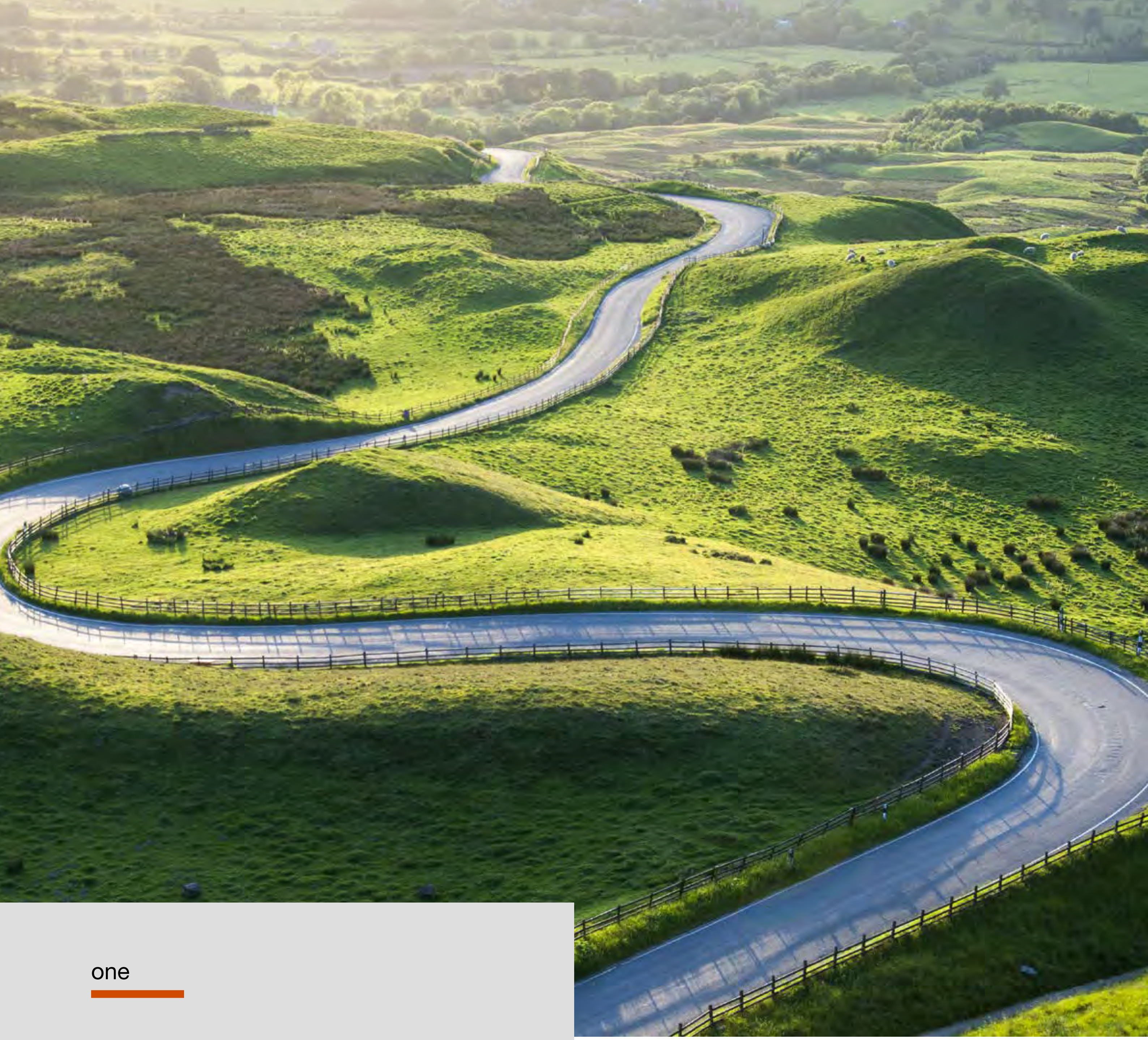
1. own and harness the culture of the organisation;
2. establish strong foundations to manage data well and be able to embrace the speed of technological change; and
3. strengthen accountability through clear identification and allocation of risk responsibility.

The immediate remediation response has required a significant shift in the mindset for Risk and Compliance teams, leading to:

1. greater transparency;
2. increased interaction with key stakeholders with the customer front of mind;
3. a rethink of the existing 3 Lines of Accountability (defence) across the business; and
4. higher quality and more insightful information.

Strategic changes will take time to embed but do provide organisations with an opportunity to move beyond a short-term riposte to a longer lasting response which better protects customers and enhances organisational value.

Three strategic choices the Wealth Management Industry have in 2020 and beyond



one

Own your culture, or be owned by it

The fallout from the Royal Commission has highlighted the consequences of getting organisational culture wrong.

“Failings of organisational culture, governance arrangements and remuneration systems lie at the heart of much of the misconduct examined in this commission”[1]

1 Commissioner Hayne Final Report, February 2019

Regulatory authorities continue to call out 'risk culture' as an area for improvement. APRA's Information Paper on companies' self-assessments[2] reported the culture component as the 'weakest', 'poorly executed', and that culture was a 'root-cause' of risk issues.

The current environment presents an opportunity for organisations that can convert culture into a strategic asset, that is aligned to business outcomes and the operating model of the organisation, to deliver those outcomes.

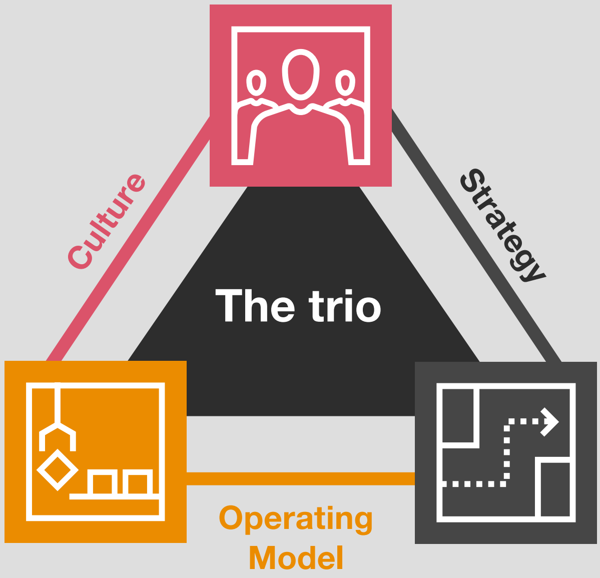
- Customers are demanding a better experience; a differentiated and tailored proposition can retain and win business.
- Regulatory authorities and the community expect more from financial institutions, closing the trust gap requires meaningful and demonstrable behaviour change.
- Within superannuation ongoing consolidation and growth of funds presents an opportunity to realign culture to support better outcomes in the future.

This does not automatically mean that your current culture should be uprooted and reestablished from the ground up. Culture doesn't change very often or very fast. It has its strengths and flaws in different circumstances. Understanding and harnessing the inherent positives of your culture can be a way of allowing good pockets of behaviour to spread organically throughout the organisation.

Half of respondents have taken action to assess and understand their current culture, with a further 25% intending to do so in the next 12 months. Of the respondents that had performed a deep dive, consistent takeaways included the importance of openness when things go wrong, clearer roles and responsibilities across the 3 Lines of Accountability (defence) and alignment from the board downwards.

The culture agenda should be shaped from the very top but a leadership team cannot influence it by acting solely from its base of positional power. Identification of the informal leaders within the organisation can help reinforce the few critical behaviours.

2 APRA Information Paper Self-assessments of governance, accountability and culture, October 2019



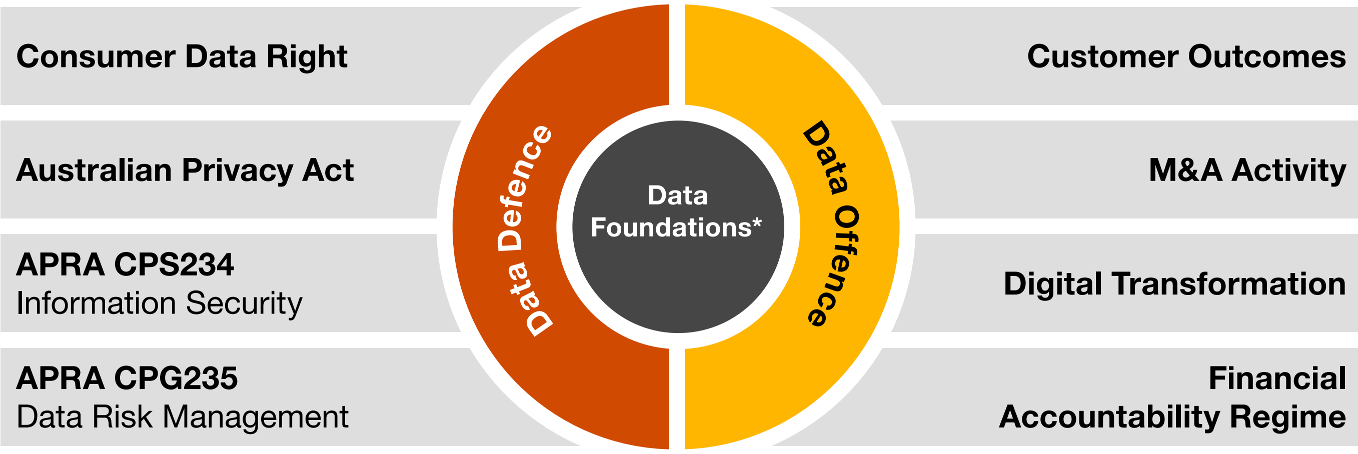
Calls to actions

- Are you setting your culture agenda to align to your strategic agenda? Have you linked it to business outcomes?
- What are your critical few behaviours and how do you reinforce those?
- Use both formal and informal levers. How do you motivate those individuals who intuitively understand the culture and its sources of emotional energy?

two

Data done well

Articulating the vision, objectives and the need to leverage and safeguard data is the starting point to doing data well. Data can be viewed from a defensive perspective, in response to rising regulatory expectations. It can also be seen as an offensive asset to support delivering customer outcomes and broader digital transformation. Either way, strong data foundations are needed. Data outlives people, processes and systems.



* Data Foundations include having an Enterprise Data Strategy, Business Case, Roadmap & Plan and Data Governance Function.

Strong foundations stem from establishing a dedicated program of work to deliver a formalised and systematic approach to managing data. Half of survey respondents had defined their Data Management Strategy and communicated it to organisational stakeholders. The other half of respondents had this as a top data management priority. Other top priorities included designing data architecture, implementing policy standards and tackling legacy environment challenges.

Being able to define the outcomes of the data management program and align it to the broader business strategy will help the development of a business case and future plan of action.

Survey participants sighted information security/privacy as the top business driver to improve how data is managed. Investment in compiling appropriate internal and external data will increase as the use of data becomes more mainstream and visible to a wider group of stakeholders. APRA's recently published data heatmap assessing the performance of MySuper products is one example of how the regulators plan to access accurate and timely data to monitor effectively the safety and stability of the Wealth Management sector.

In our 2018 Wealth Management Risk and Compliance Benchmarking survey, the automation of routine risk and compliance tasks was seen as one way of doing more with less. This need for assistance from technology has intensified, with 73% of Australian CEOs in our most recent CEO Survey[3] identifying speed of technology change as an obstacle to growth.

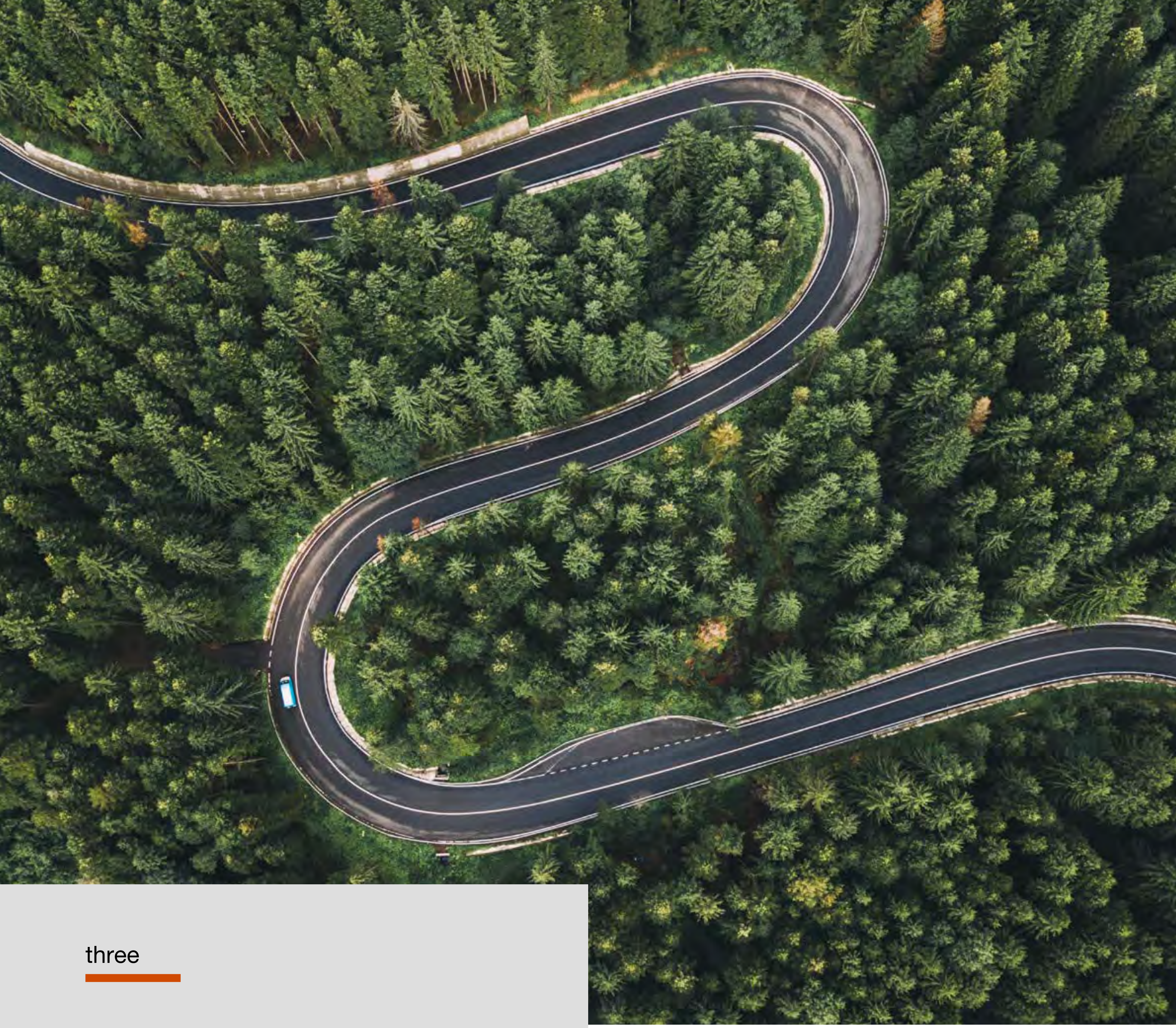
There has been an upward trend in readiness and adoption of RegTech solutions in the 2019 responses. We expect this to keep rising into the future, with a further 29% of respondents starting conversations this year. Only 14% of respondents ranked their organisation as not ready at all.

The main challenges to effective adoption of RegTech remain consistent with the 2018 responses, the uncertainty over regulation replacing credibility of unproven technology the only change in the top 3. This is surprising given regulators positivity towards the use of RegTech to enhance an organisation's response to increasing customer and regulatory expectations.

3 PwC's 23rd CEO Survey 2020: Australian findings

Calls to actions

- Have you identified your data dependencies across the organisation, both internally and externally?
- How confident are you with the quality and completeness of your data to correctly inform business decisions and manage risk?
- For new regulatory requirements, have you assessed the ability of current systems and quality of data to meet the new/updated regulatory requirements and importantly, the interplay of requirements across the various regulations?



three

Clear accountability supported by a 'trust and verify' mindset

The community expects the financial services industry to do the right thing and for individuals to be personally accountable when they don’t. A legislative accountability regime will be applicable to asset managers and superannuation, however the Wealth Management industry should not be waiting for this to become effective to take action.

Half of survey respondents called out strengthening accountability as a top priority initiative for 2020. This presents an opportunity to drive improvements in how they govern themselves, which could lead to faster and more confident decision making in the longer term.

Considering who your accountable persons population could be and simplifying the landscape they are responsible for will provide clarity initially. Organisational context will then shape choices on intent, ownership and coverage.

Business attestations is an established way in which those accountable confirm key controls that mitigate risks they are responsible for are designed and operating effectively. 90% of those surveyed use them to form part of their Risk Management Framework.

What is less mature is the verification behind such attestations. Only 10% of respondents have risk and compliance obligations fully mapped to controls which are tested. Risk owners need to understand what assurances support such attestations so that they themselves are satisfied that risks have been appropriately managed. This approach supports good risk governance and broader community expectations.

One of the toughest scenarios when implementing clarity in accountability includes the oversight of third parties. Appropriately managing and monitoring service providers was in the top 3 risk management challenges for two thirds of those surveyed. This "show me, don't just tell me" mindset still applies. Independent validation of key service provider controls, either by your organisation or an independent third party, was how 2 out of 3 respondents were managing this risk.

CPS 234 Information Security is just one example of the complexity third parties can present when addressing the current and emerging risk management and compliance needs of organisations. Those accountable should have a good knowledge of third party relationships in place and awareness of how they are managing your information and the criticality/sensitivity of this information.

Calls to actions

- Have you considered what the Financial Accountability Regime will mean for your organisation? Experience from implementing the Banking Executive Accountability Regime amongst even small ADIs suggests the effort should not be underestimated.
- Have you considered who your accountable person population could be? This could be beyond the Directors and Executive level.
- Have you considered who is giving assurance as to the design and operating effectiveness of key controls that mitigate risks that you are responsible for?
- How are you engaging and setting expectations with your key stakeholders to support your accountability regime?

Four tactical responses by the Wealth Management Industry in 2019

one

Transparency

Not surprisingly, our survey shows a 75% increase year on year in the average number of reportable breaches amongst respondents.

Following the completion of the Royal Commission, there has been a surge in the volume of breaches reported and voluntary reporting of incidents and near misses - a sign that organisations are digging deeper to identify incidents and breaches and report them in response to heightened expectations.

Reflection: Remain vigilant when it comes to considering incidents, breaches and complaints. Are you asking should we, rather than could we?

It is evident that organisations are spending more time analysing events, capturing information and generally being more prudent when considering if a matter is an incident or a reportable breach.

However more can be done by organisations to ensure timely issue identification, assessment and reporting. A significant number of survey participants cited resourcing and system limitations resulting in poor data capture as major barriers to more timely issue resolutions - in the current environment this explanation is no longer acceptable and action needs to be taken.

Reflection: Invest in systems, resources and relationships with key third parties to ensure timely issue identification, assessment and reporting to regulators

Similar to the increase in breach reporting, the newly formed Australian Financial Complaints Authority (AFCA) has reported that it has handled more complaints in 2019 than the combined number of complaints handled by its three predecessor organisations - the Financial Ombudsman Service, the Credit and Investments Ombudsman and the Superannuation Complaints Tribunal in 2018. This may be an indication of customers being more engaged, which is an interesting trend.

Uplifting internal complaints handling capabilities will help create positive complaint management cultures that welcome complaints and focus on fair and timely consumer outcomes. RG 165 Licensing: Internal and external dispute provides a framework for this.

The two leading challenges amongst survey participants in meeting the proposed RG 165 are capturing of social media complaints (45% of respondents) and evidencing customer satisfaction (25% of respondents), again indicating a lack of resources and system sophistication.

When it comes to analysing breaches, incidents and complaints, root cause analysis was the number one method utilised amongst survey participants. This was a positive response, particularly in the light of APRA's recommendations for organisations to conduct such analysis as discussed in their prudential report into governance, culture and accountability at the Commonwealth Bank of Australia.[4]

4 https://www.apra.gov.au/news-and-publications/apra-releases-cba-prudential-inquiry-final-report-and-accepts-enforceable

two

Greater stakeholder engagement with the member front of mind

We have seen a significant shift in regulator oversight and engagement with organisations, with close to 50% of respondents having a visit or review performed by a regulator during the period. In most cases, these visits/reviews were performed by APRA and ASIC.

Survey respondents ranked regulation as the biggest risk management challenge for a 5th year in a row in 2019. Respondents cited volume, complexity, resource constraints and clarity of regulation as the top four challenges in keeping up with the expectations of the regulator.

This year alone, we have seen the release of over 30 regulatory changes as well as a number of guides for the Wealth Management industry to sign up to and self regulate.

There has also been an increase in the involvement of industry bodies to lobby for clarity and practicality of regulatory standards, guidance and education as well as the setting of realistic timelines.

Many organisations have started to undertake readiness assessments ahead of regulatory deadlines to ensure they identify and action any regulatory obligation gaps.

Reflection: Establish separate project management office function/focus groups to ensure successful implementation of regulatory requirements by due dates

Where a project management office is deployed, consider costs, resources and formalisation of governance, controls and documentation required when moved into business as usual

For example, a RG 132 Funds management: Compliance and oversight gap assessment was performed by the majority of survey respondents and more than two thirds of those amended their compliance plans and used the guidance as an opportunity to uplift their compliance frameworks and systems. The common gaps identified by respondents through their self assessments and independently conducted reviews included:

- The need for monitoring and assessment of effectiveness of the compliance plan controls across Line 1 and Line 2 and how this is described in the compliance plans
- Inclusion of group level and scheme-level compliance risks and controls in the compliance plan, including risks across areas such as inadequate resources, investment strategy, market and valuation risk as well as some emerging risks such as cyber, whistleblowing and ethics/conduct
- Removal of numerous compliance procedures and statements (as opposed to controls) in the compliance plans
- Inclusion of cyber resilience plans and health checks in the compliance plans.

Reflection: Pre-implementation reviews can help identify mistakes before they perpetuate

three

Risk and compliance accountability across the organisation

Many entities are revisiting the structure of their Risk and Compliance functions as part of a broader exercise of how risk and compliance accountability should be structured across the organisation.

Having the right talent mix is essential in building an effective 3 Lines of Accountability (defence) model and to establish a strong risk culture across the organisation.

It is clear that the capabilities needed for risk and compliance roles are no longer the same as they were years ago. Organisations are lifting their risk management capability and this is evident from the survey responses. Although auditing skills are prevalent in nearly all of those working in a Line 2 role, 1 in 3 now have Cyber expertise and nearly half have Behavioural Culture skills.

Throwing more resources to respond to the current risk and compliance landscape doesn't seem to be the solution. Despite Risk and Compliance functions of those surveyed increasing in headcount year on year for the last couple of years, 39% of respondents expressed "resource constraints" as one of the top challenges when it comes to keeping up with regulatory expectations.

This may be attributed to blurring of the 1st and 2nd lines. This has restricted Line 2 to do their intended role which is providing oversight to the business and taking responsibility for establishing policies and procedures for risk management and compliance.

Of those surveyed, there is still a heavy reliance on Line 2 to perform the majority of testing of controls. In a mature 3 Lines of Accountability (defence), Line 1 is responsible for identifying, owning and managing the risk. There is some independent testing from the Risk and Compliance functions, but in a monitoring capacity only.

Reflection: Vendor oversight and management is required to understand trends in incidents and breaches and connect the dots

36% of respondents also indicated that their compliance obligations are partially mapped to controls and tested to a limited extent.

Not having a nexus between compliance obligations to controls that are subjected to a routine oversight/testing program, means that there may be unidentified exposure outside of the organisation's risk appetite.

This, coupled with the lack of Line 1 Risk and Compliance business partnering roles, could be an indicator that the current model is no longer suitable for the organisation.

Reflection: Equip everyone to be risk alert and root cause focused

For a more effective approach to meeting community expectations, a holistic lens to risk management and compliance should be applied across the organisation. For example, core risk management and compliance activities should be established as part of day-to-day activities in the business.

For those survey respondents with established Business Partners embedded into Line 1 functions, the majority of testing of controls is performed by Line 1 itself.

four

Is more better?

Our survey results indicate that board delegated committees are receiving and are expected to read and understand significant volumes of information. Whilst reporting may be comprehensive, it is not concise and appears to be overly complex and detailed, requiring significant manual preparation and collation and reliance on key individuals to produce the final products.

Reporting to committees and boards can sometimes be voluminous and lack focus. Whilst this may be manageable in the short term, in the current environment of regulator and public scrutiny, there is a risk of 'over–reporting' and defending of decisions where quantity is mistaken for quality. This poses the threat of excessive reporting to committee members who then need to focus on the detail of operational matters covered in the papers, rather than spending time providing strategic oversight and leadership to the business.

Reflection: Separate educational content from decision making content in reporting papers to help committees and boards answer the "so what?"

Committees should work with management and revisit what information they need to satisfy their obligations and to perform their duties in order to streamline risk reporting, noting that does not necessarily mean cutting out information.

Contacts

Melbourne

George Sagonas

Partner
+61 3 8603 2160
george.sagonas@pwc.com

Sean Hill

Partner
+61 3 8603 2358
sean.d.hill@pwc.com

Nicole Oborne

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

Adrian Gut

Director
+61 3 8603 6417
adrian.gut@pwc.com

Owain Norman

Senior Manager
+61 3 8603 0458
owain.a.norman@pwc.com

Sydney

Craig Cummins

Partner
+61 2 8266 7937
craig.cummins@pwc.com

Stephanie Smith

Partner
+61 2 8266 3680
stephanie.smith@pwc.com

Sarah Hofman

Partner
+61 2 8266 2231
sarah.hofman@pwc.com

Deanna Chesler

Partner
+61 2 8266 0003
deanna.chesler@pwc.com

Brisbane

Paul Collins

Partner
+61 7 3257 8558
paul.d.collins@pwc.com

Subject Matter Experts

Michelle Kam

Partner, Culture
+61 2 8266 1299
michelle.kam@pwc.com

Jon Benson

Partner, Data
+61 3 8603 1669
jon.benson@pwc.com