

2018 PwC Wealth Management Risk and Compliance Benchmarking Survey



July 2018 | In February and March 2018 we surveyed the risk and compliance functions of 71 asset and wealth management and superannuation entities (collectively referred to as the wealth management sector). Here we consider the responses, and discuss likely changes to risk and compliance practice and regulation.

Table of contents

Executive summary	2
1. Rebuilding trust	4
2. Sustainability	9
3. Technology and data as enablers.....	11
4. Accountability, incentive and consequence	17

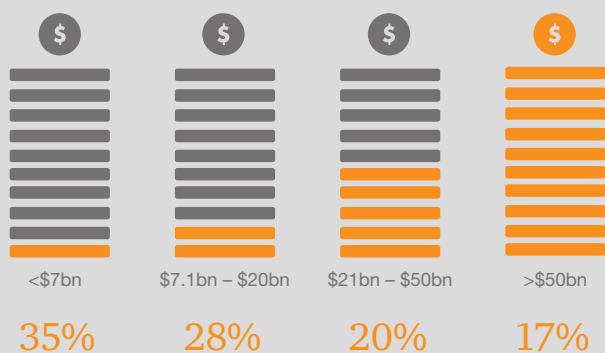
Entity type

Who participated

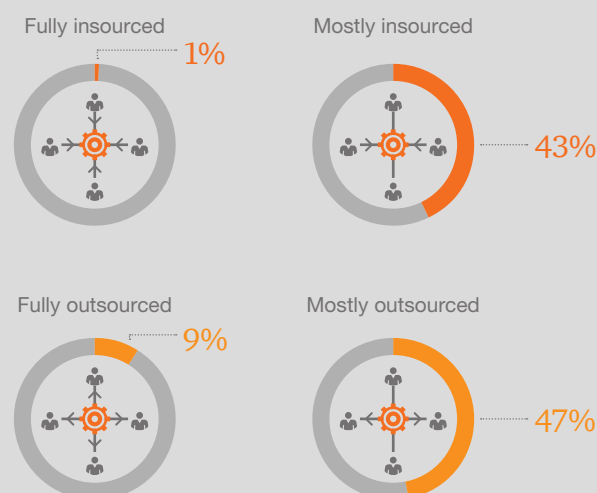


- Asset and Wealth Managers – 35
- Superannuation Fund – 28
- Other, including REITs, outsource administrators and platform providers – 8

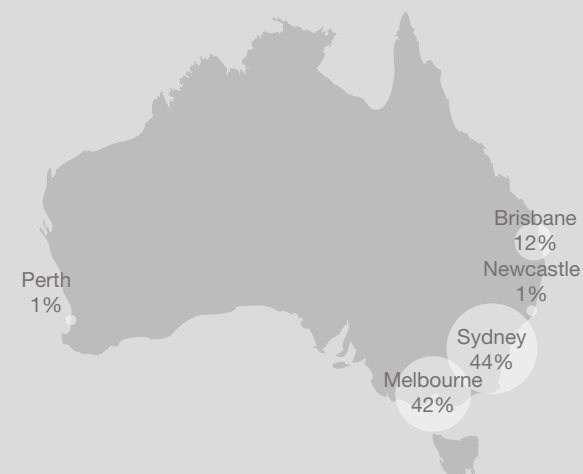
Assets under management



Operating model



Geographical location



Executive summary

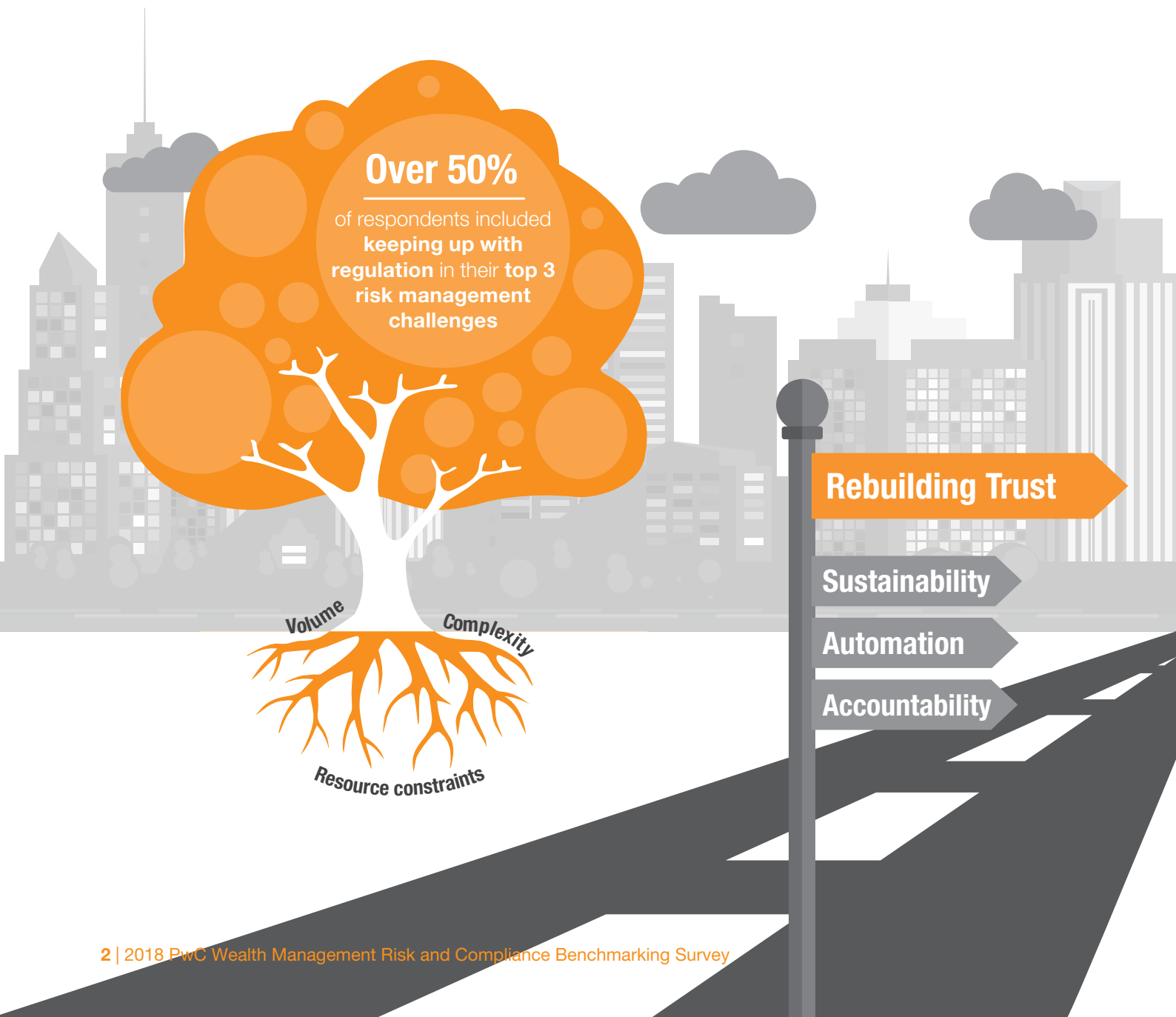
Our 11th annual survey of Australian wealth management risk and compliance functions suggests they are at a crossroads. The sector needs to regain trust: the trust of a sceptical public, and of an industry-funded regulator that is increasingly focused on enforcement.

Traditional methods to manage existing and emerging risks are not sustainable and demand for skilled people is draining an already shallow resource pool.

The automation of routine risk and compliance tasks provides a great opportunity to redeploy staff to tasks that add greater value, as well as the potential to do more with less.

Even the best tools, processes and controls can be undermined by a lack of accountability. To achieve the desired results, organisations must hold individuals to account, and offer the right incentives.

Risk and compliance functions are an important stakeholder in navigating the changing landscape and influencing the direction the Australian wealth management sector takes next.



- An unprecedented amount of activity in the first half of 2018 has unearthed issues that go to the heart of leadership, culture, conduct and risk.
- Misconduct and instances where organisations have failed to meet community expectations have been brought into focus, further eroding trust.
- The wealth management sector has to take action. Trends globally may provide an indicator of future regulation in response, however meeting community expectations goes further than reacting to legislation.
- There needs to be a fundamental change, not only what organisations do, but how they do it. Risk and compliance functions are central to driving this change.

- This step change in expectations will prompt organisations to reflect on their existing governance structures and operational processes.
- Our survey suggests the strain on risk and compliance functions continues to grow, with resources not rising in line with these increasing responsibilities and expectations.
- Risk and compliance functions will need to evolve to remain adequate and appropriate. As data and technology changes, so will the skillset of these teams.
- But they cannot do it alone. All Three Lines of Defence must take accountability.



- At the core of responding to rising expectations and rebuilding trust is how people behave. Recent examples suggest that there are few repercussions for poor outcomes.
- Organisations in our survey have made steps towards creating a more trustworthy culture. However, more needs to be done to ensure that culture is driving risk outcomes in line with risk appetite.
- As well as appropriately incentivising, organisations need to use the right tools and techniques to measure, monitor and report on culture performance indicators.
- Risk and compliance functions have to be bold enough to challenge and escalate issues and not allow a culture of collaboration to stifle their voice.

- In response to rising expectations, the wealth management sector has identified automation as an opportunity to do more with less.
- Such automation has the potential to assist with the remediation of the underlying themes at the core of failing to meet community expectations.
- Yet this potential remains largely unrealised across the sector. Our survey shows there is a lack of subject matter experts to develop and mobilise automation and a failure to agree on an organisation wide approach as the main barriers to the slow uptake of automation.
- For technology to succeed and play a role in regaining trust, data is a critical element and its quality needs to be managed proactively.

1. Rebuilding trust

Our point of view

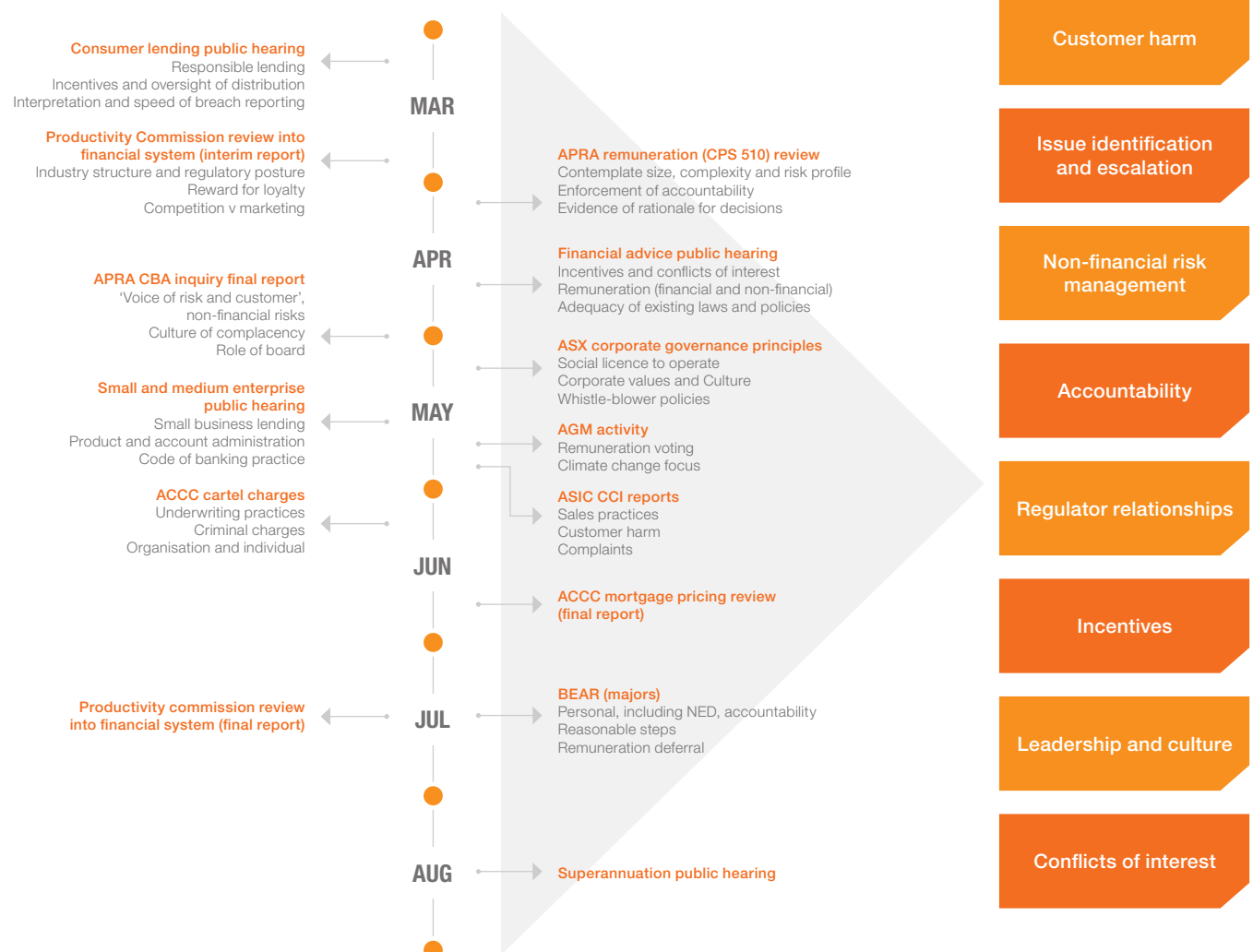
For almost a decade, the Australian financial sector has been struggling to retain the trust of its clients, the public and regulators. This erosion of trust has been deepened in the first half of 2018, with recent events shining a harsh light on poor governance and leadership.

There has to be a fundamental change in not only what organisations do, but also how they do it. This response has to go further than reacting to the regulator: it needs to satisfy community expectations, and risk and compliance functions are central to driving this change.

Step change in expectations

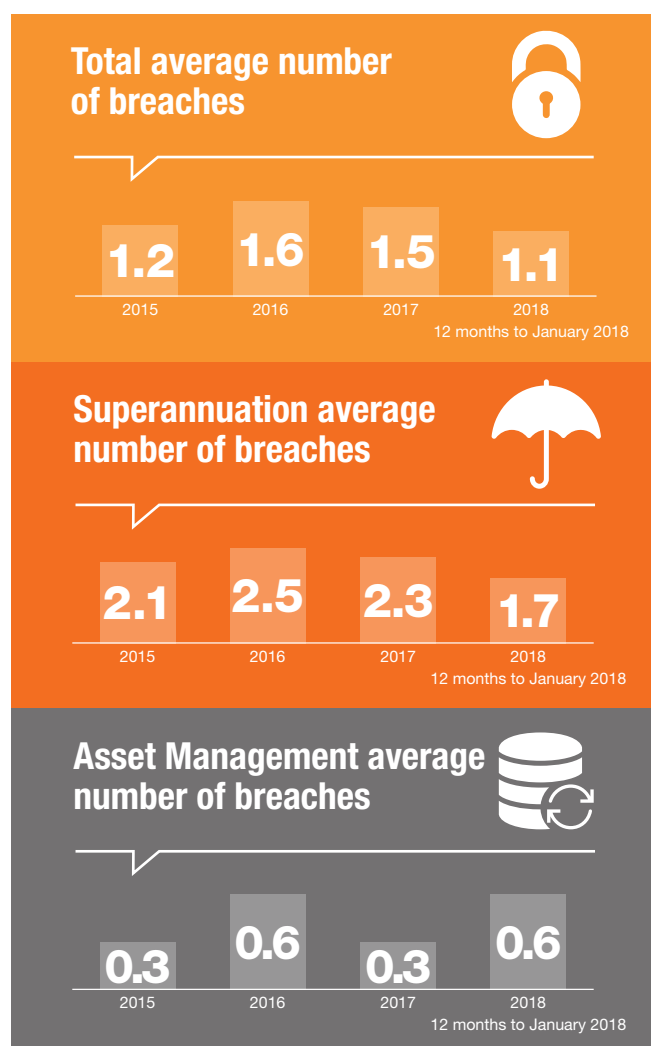
The year 2018 has seen a wave of regulation in the financial sector, intended to force organisations to act in the best interests of the community. No longer is it acceptable to simply comply with the legislation. The Royal Commission is one example of the unprecedented level of activity in the sector that is putting a spotlight on expectations, and organisations need to respond accordingly.

2018 to date



One short-term response is for line-one risk owners, when in doubt, to report incidents and breaches so that they can be understood and, if required, remedied. But our survey results suggest that this philosophy is not being followed, due perhaps to a lack of a consistent organisation-wide understanding of reporting requirements. Submissions to the Royal Commission have also led many organisations in the wealth management sector to review the way they deal with breaches, from identification to assessment and remediation.

The average number of breaches across survey participants is as follows:



However, in the last three months, anecdotally we have seen a notable increase in the number of incidents and breaches being reported to the regulators. This is a direct result of greater awareness of expectations.

The longer-term response to higher expectations cannot be the sole responsibility of risk and compliance functions. The entire wealth management sector needs to become more skilled, and to question risk owners on their understanding of what constitutes an incident and a breach.



What will the regulatory response be to changing expectations?

The Royal Commission has revealed many problems, including fees for no service, inappropriate financial advice, improper conduct by financial advisers, and a weak disciplinary regime for the financial advice profession. The volume of problems identified has brought into question the adequacy of the regulators' resources and performance. Some people have argued that ASIC and APRA already had all the regulatory powers they needed to deal with previous collapses or fraud. This raises the question of whether regulators will be more proactive in enforcement and surveillance activities in the future.

APRA has issued additional operational risk capital restrictions, and has made its first enforceable undertaking arising from poor organisational culture and conduct. We expect more such actions, especially with the closer focus on accountability resulting from the Banking Executive Accountability Regime (BEAR). However, looking overseas may provide an indicator of how local regulators may look longer term in an attempt to rebuild trust.

Is regulation elsewhere a predictor of future Australian regulation?

In June 2010 the UK government established an Independent Commission on Banking to look at structural and related non-structural reforms to the banking sector. The aim was to foster financial stability and competition in the wake of the financial crisis of 2007–08. As a result, the *Financial Services Act* replaced the previous tripartite structure of the Financial Services Authority (FSA), the Treasury and the Bank of England. The commission had found that the FSA's remit was enormous and unrealistic, that nobody knew who would be in charge in a crisis, and that the tripartite authorities needed to communicate better with each other. So the FSA was abolished, and three new bodies were created to regulate financial services, the first two in the Bank of England:

- the Financial Policy Committee (FPC) – responsible overall for financial regulation in the UK
- the Prudential Regulation Authority (PRA) – responsible for supervising the safety and soundness of individual financial firms
- the Financial Conduct Authority (FCA) – responsible for protecting consumers from sharp practices, and making sure that workers in the financial services sector comply with the rules.







If we look at regulations in Europe, the UK, Asia and the USA, we see some common themes, including conduct and culture, accountability, liquidity risk management, transparency, and conflicts of interest.

Europe has seen major changes in product governance and lifecycle obligation on designers and distributors of wealth management products.



We have observed some similar trends emerging in Australia, as a result of APRA's announced culture reviews and the implementation of the BEAR. At the moment, banks are the focus, but APRA has announced that it will eventually extend the accountability regime to all APRA-regulated entities.

Recent history shows that Australian regulation tends to follow the UK, with a lag of three to four years:

UK key regulatory risks 2013–2016		Australia key regulatory risks 2018
 Poor culture and controls continue to threaten market integrity, including conflicts of interest	➔	Conflicts of interest in vertically integrated businesses APRA culture reviews
 Large back-books may lead firms to act against their existing customers' best interests	➔	Best interest duty requirements
 Pensions, retirement income products and distribution methods may deliver poor consumer outcomes	➔	APRA's consultation package on measures to strengthen member outcomes Design and distribution obligations – product governance
 Poor culture and practice in consumer credit affordability assessments could result in unaffordable debt	➔	Royal Commission into financial services with an initial focus on home loans, car loans and credit cards
 The importance of firms' systems and controls in preventing financial crime	➔	The Anti-Money Laundering and Counter-Terrorism Financing Bill 2017 was passed effective April 2018
 Senior Manager Accountability Regime	➔	Banking Executive Accountability Regime

Data ownership and governance are central to trust

Government security policy agencies and the financial regulators are placing greater obligations on the wealth management sector to protect the privacy and security of the data they hold, including higher expectations for detective, response and recovery controls.

If a firm is to govern, manage and control data effectively, it must be able to answer the following questions:

- What data is being collected (e.g. consent to collect personal information)?
- Where is data being held (e.g. cloud, on-site, overseas)?
- How is data used and shared (e.g. sharing with third parties, using data for unintended purposes)?
- Who has access to the data (access controls, monitoring and protecting for unauthorised access)?

In their efforts to encourage competition in financial services, governments and regulators are introducing further complexities. The Revised Payment Services Directive (PSD2), open banking and data portability have all come into effect in Europe – Australia will follow.

The recommendations of the Productivity Commission's Open Banking Review included establishing an open banking regime, which would include an overarching consumer data right and the right to open banking. The aim is to bring greater competition to financial services. In May 2018 the Australian Government agreed to the recommendations, with a phased implementation from July 2019.



2/3

of respondents have a
**data management
strategy in place**



Larger organisations
more advanced
in **data
capabilities** ▶

Examples include



Comprehensive,
automated reporting



Predictive analytics

The wealth management sector has already been operating in this complex environment of portability, as member data is already transferred between different parties (the member, the institutional investor, the private investor, the fund manager, the wealth manager), with the customer being the ultimate owner of this information.

Organisations awaiting the new open banking regime will encounter further complexity in data governance and greater focus on the individual, through data privacy, ethics and protection requirements. Organisations will need to answer the following questions:

- How can our existing data governance arrangements be broadened to encompass data quality, security, privacy and use of data?
- Can we maintain the trust and security of our customers as we share their data with existing banks and third-party platforms?
- What are the security implications, reputational risks and liabilities of sharing data with other organisations in the age of open data and data portability?

Regulators are acutely aware of the heightened threat of cyber-attacks and data breaches, and understand that strong information security and governance are critical in countering such threats.



31%
of respondents had
privacy breaches during
the year to January 2018

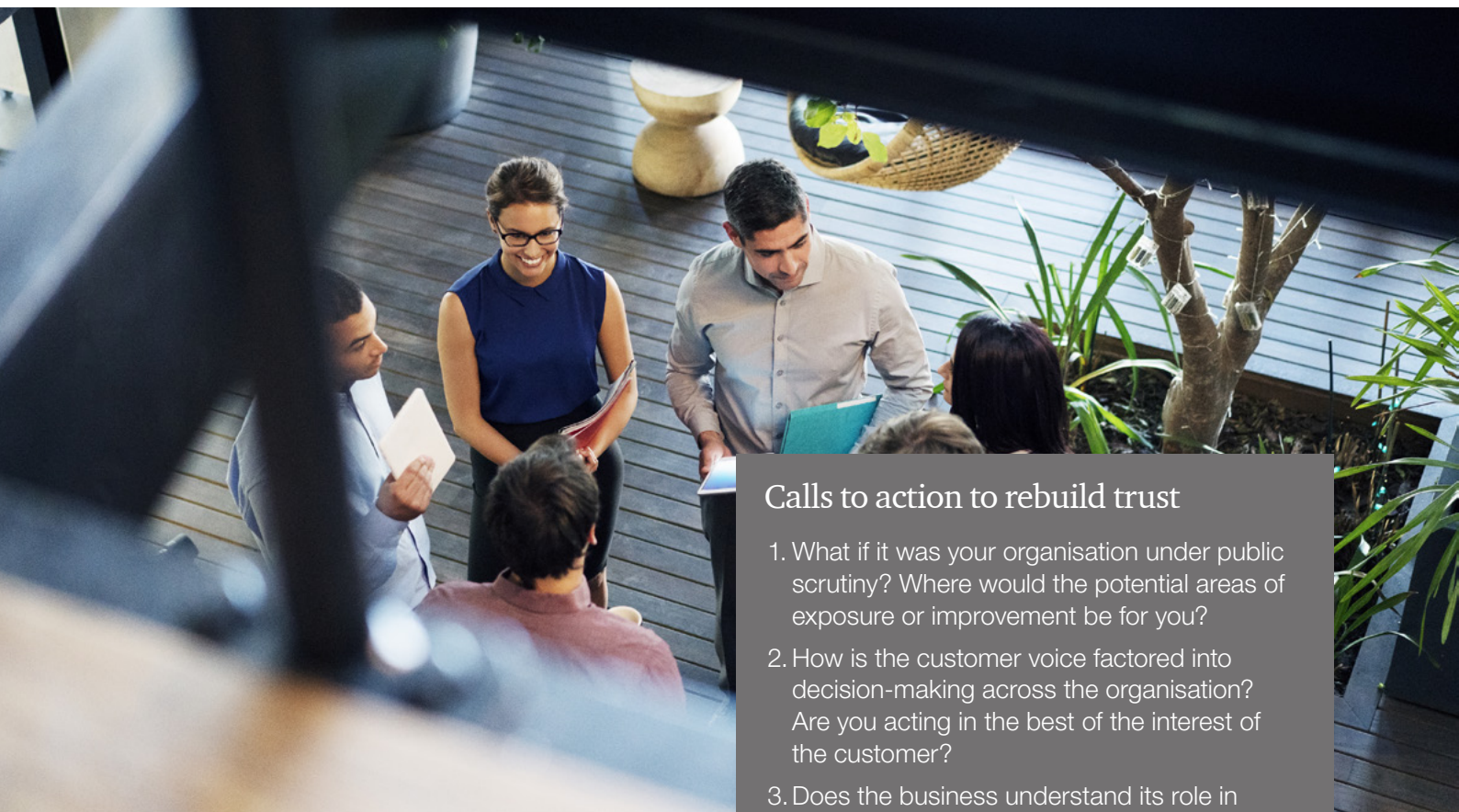
The General Data Protection Regulation, which came into effect on 25 May 2018, represents one of the highest standards of data protection in the world, and has huge consequences for the way in which organisations protect the privacy of European citizens. APRA has drafted a new minimum information security standard, CPS 234, aimed at increasing the safety of data entrusted to Australia's financial institutions.

All affected organisations will need to instruct their technology and information security teams to review how the standard fits into their existing governance arrangements, and prepare for compliance by July 2019.

32% of respondents have data
governance efforts directed by their
technology function



For many years there has been a perception that the technology department of an organisation is the 'owner' of data. And indeed, it is best placed to be the custodian of data, as it can coordinate efforts to protect and secure the organisation's data from cyberthreats. But inevitably this approach means the business as a whole, which is the ultimate producer and consumer of data, is not encouraged to 'own' its data and the risks arising from its use. Risk and compliance functions must do more to help the entire business understand and manage the full spectrum of information risks, such as data quality, data privacy and protection, and reputational risks from unethical use of data.



Calls to action to rebuild trust

1. What if it was your organisation under public scrutiny? Where would the potential areas of exposure or improvement be for you?
2. How is the customer voice factored into decision-making across the organisation? Are you acting in the best of the interest of the customer?
3. Does the business understand its role in managing the risks that everyday use of data presents?

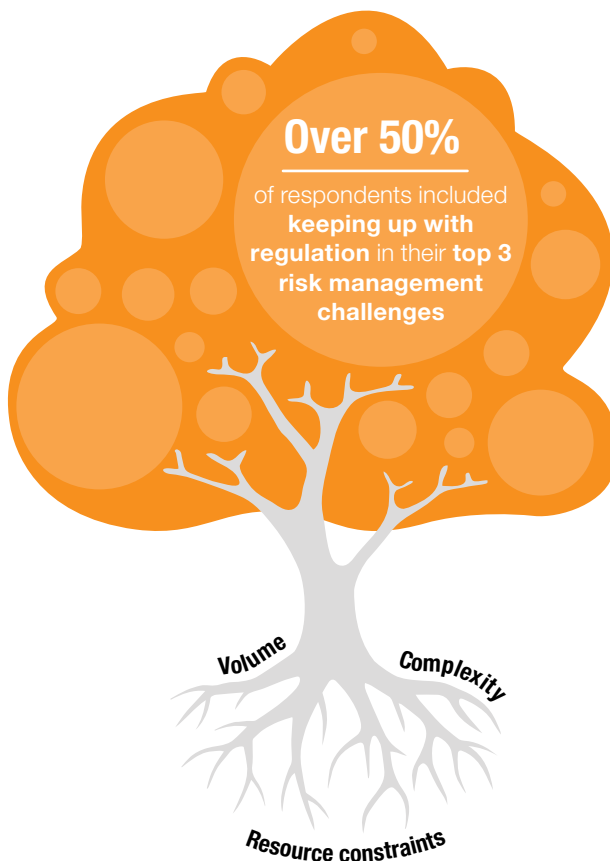
2. Sustainability

Our point of view

There is a high demand for skilled people to manage risk and compliance, but the talent pool is shallow. For this reason, organisations are at the crossroads: today's way of working is not sustainable. The skills needed for risk management and compliance are also evolving, as part of efforts to regain trust. Professionals need data management and analytics tools and skills, as well as more traditional expertise in risk management.

Regulatory burden is draining the resource pool

Risk and compliance functions are drowning in a sea of existing and proposed regulation, and scrutiny from regulators and the public will only increase with the changing expectations of 2018.



Following APRA's announcement that risk culture reviews will be performed across the industry, we expect the pressure on risk and compliance functions to continue.

Our survey results suggest that, on average, risk and compliance resources are not growing adequately even though responsibilities and expectations are.

Average full time equivalents in line 2 risk and compliance functions



A recent review highlighted the following areas of concern for APRA, and we expect to see these considered by other organisations:

- What is management's attitude to problems identified across the Three Lines of Defence?
- How proactive is management in dealing with risks?
- How insular is management when considering risk, and has it learned from past experiences and mistakes?
- Does a collaborative working environment lessen the opportunity for constructive criticism?
- Is there timely decision-making and a focus on results?
- How do I manage my ever-increasing regulatory and compliance costs?

All of these will require an organisation's risk and compliance team to work proactively with management.

Risk and compliance skills will evolve with the emergence of data



With constant regulatory change, growing volumes of data and the emergence of technologies such as RegTech and Big Data comes a demand for new skills.

If demand continues to outstrip supply in the Australian market, resource constraints will continue to be a serious impediment to meeting regulatory expectations. Salaries for specialist skills are likely to rise, and organisations will be forced to look offshore, or change the way they operate.



53%

of respondents stated that keeping up with regulatory expectations was one of their highest risk management challenges

To realise the potential of technology and data enablers, organisations will need not only expertise in regulation, compliance, financial crime and risk management, but also technical data skills. In Australia, the number of high-performing individuals with these multifaceted skills is relatively low, and 30 per cent of respondents are already feeling a strain on resources as they try to keep up with regulatory expectations.

Calls to action to grow a risk and compliance function suitable for the future

1. Is your risk and compliance function allocating adequate resources to current material risks at the same time as giving adequate thought and attention to new and emerging risks?
2. How are you educating the business on their responsibilities for managing risk and compliance?
3. Does your current risk and compliance function have the appropriate expertise to interpret output from emerging technologies? If not, do you have a plan in place to upskill existing workforce?

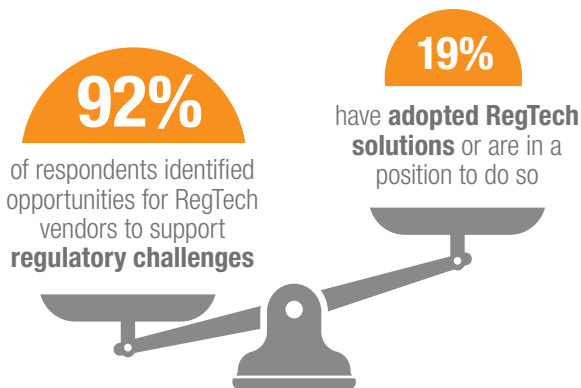
3. Technology and data as enablers

Our point of view

Rising compliance costs, along with regulators' and the industry's growing interest in automation, have created an environment in which emerging RegTech (regulatory technology) providers can assist compliance processes. Despite a growing number of external providers, risk and compliance functions should consider different options when deciding how to meet and raise operating standards.

RegTech solutions need to meet – and raise – operating standards

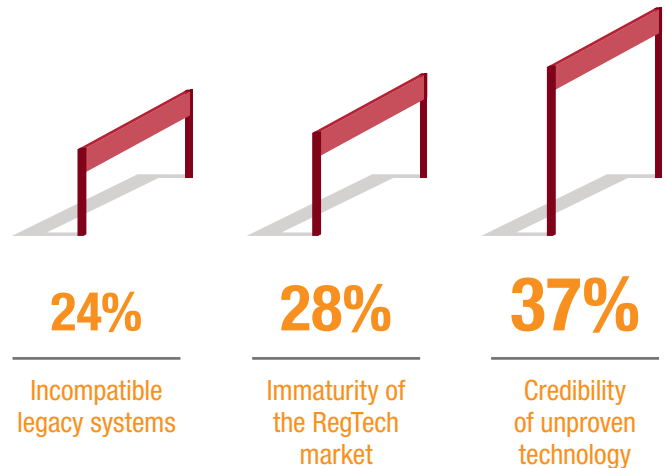
Although RegTech is the amalgamation of 'regulatory' and 'technology', it unfortunately does not mean there is now one technology to meet your regulatory needs. Rather, RegTech describes the industry that has arisen to meet regulatory and compliance needs.



Surprisingly, the early adopters in our survey are not defined by entity type, size of assets under management or operating model. This suggests that the stereotypical technology barriers of budget and size can be overcome.



Main challenges to effective adoption of RegTech

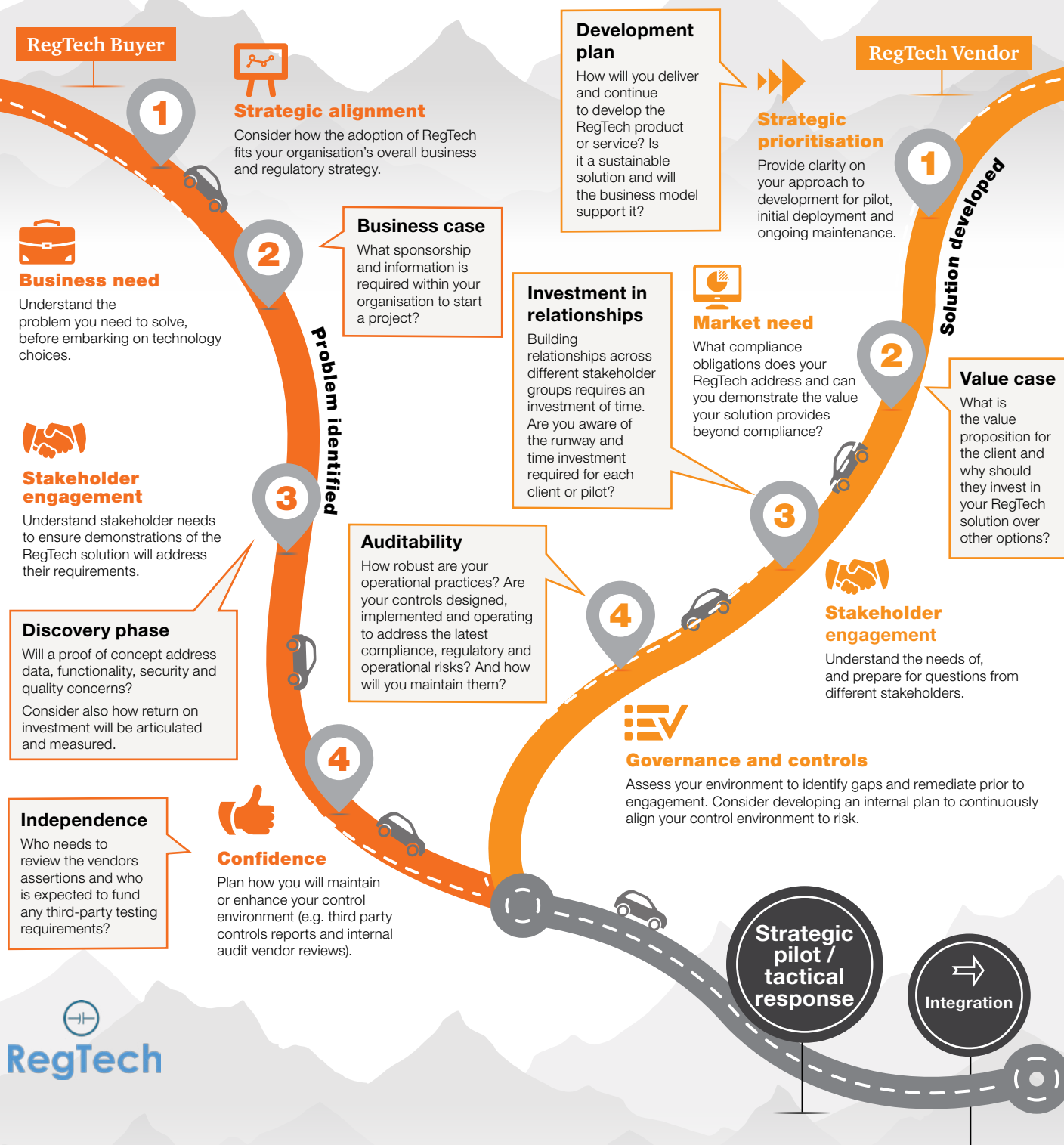


The immaturity of the RegTech market and low credibility of vendors are the highest hurdles that risk and compliance functions must overcome.

Because regulation is constantly evolving, the configurability of any RegTech solution to accommodate change should be considered a mandatory requirement by any wealth management organisation setting out on the RegTech path. It is essential in these early stages to consider how any proposed new RegTech processes or controls will fit into your organisation's overall business and regulatory strategy before making a decision. The following roadmap, developed in association with the Australian RegTech Association, helps RegTech buyers and vendors understand each other's needs as they work together to meet and raise operating standards.

Roadmap to accelerate RegTech integration

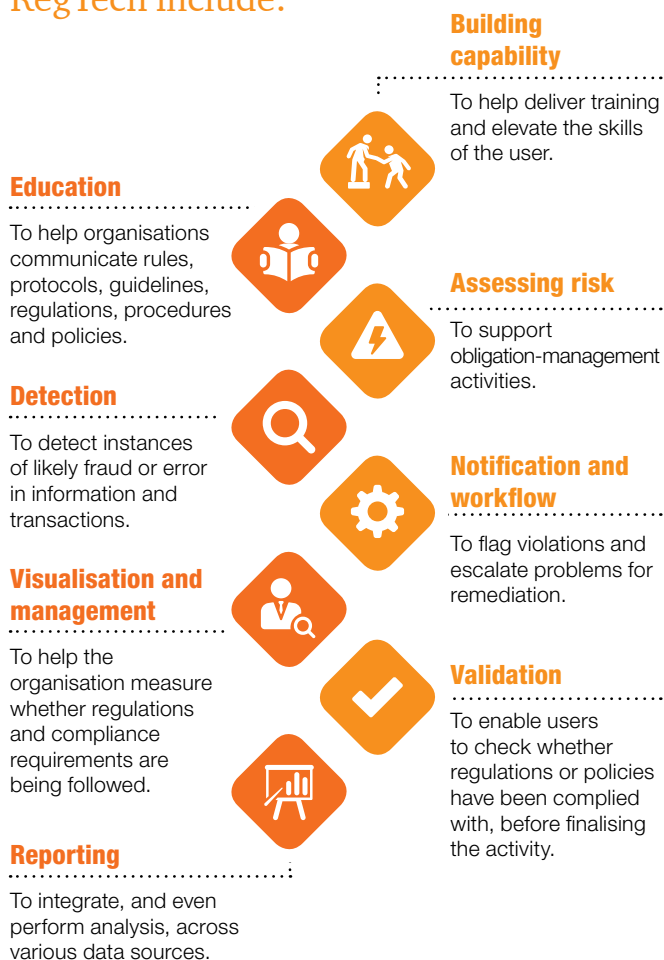
Whether you have or need a RegTech solution this roadmap provides a guide for accelerating your way to implementing RegTech.



Next steps

- Identify stakeholders in your own organisation and discuss the current state of compliance, and future requirements.
- Determine whether your current regulatory and compliance operation needs to change. If it does, set a vision and strategy.
- If RegTech is part of your vision and strategy, follow the roadmap.

Practical applications of RegTech include:

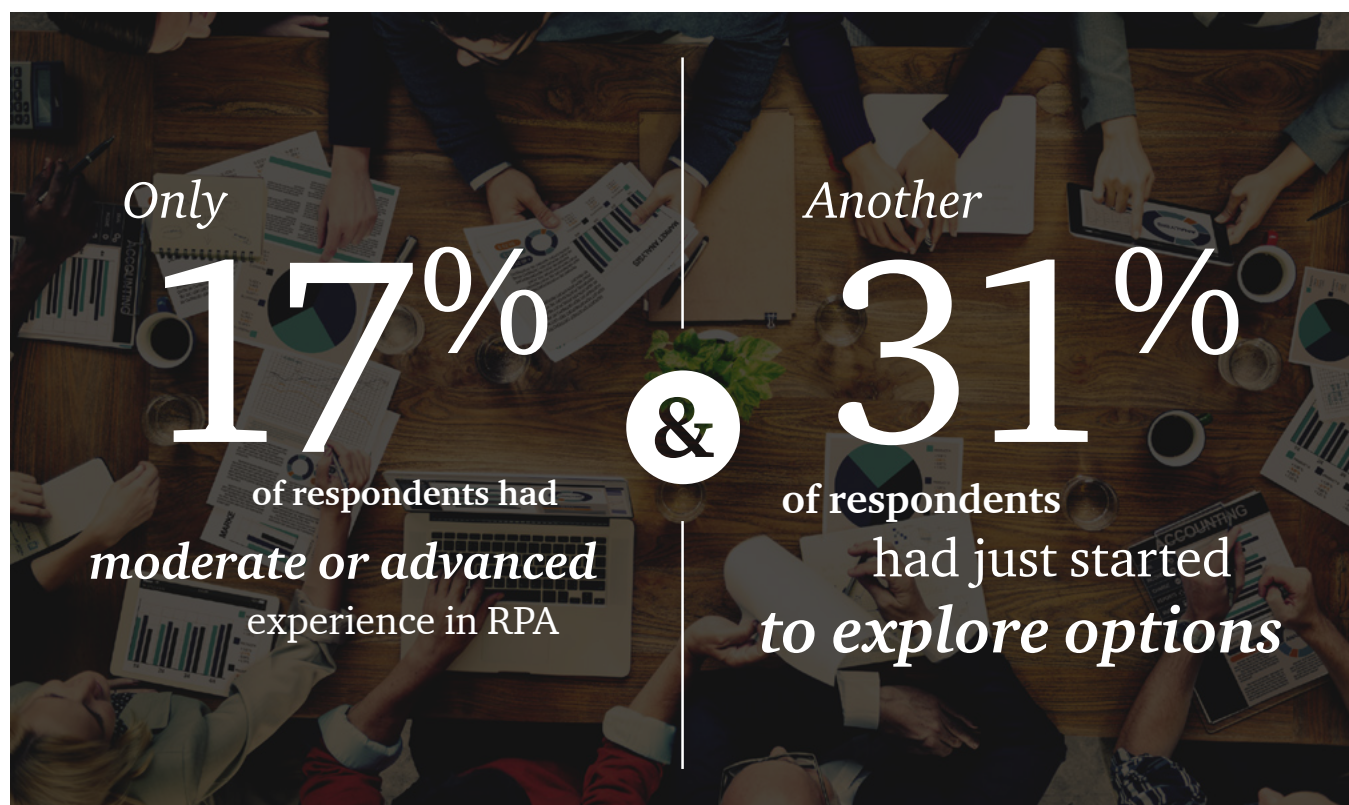


Robotic process automation (RPA): an example of the opportunities technology solutions can offer

Our survey suggests the wealth management sector lags other financial services sectors in adopting digital technology, which it has resisted for decades. This is further exacerbated by:

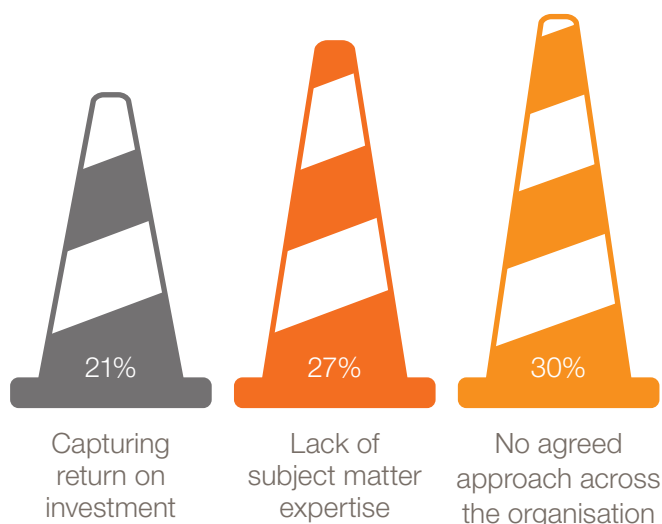
- increased regulation
- downward pressure on fees
- increased scope and complexity of asset classes and assets under management
- changing client behaviours (such as demand for more personalised advice and access to real-time analytics).

Our results illustrate the slow uptake of RPA in wealth management, in contrast to the wider financial services industry, where organisations have made the jump from exploration to execution. For example, banks for some time have been using RPA in client onboarding and diligence processes, such as anti-money laundering and Know Your Customer processes.



Many organisations in all industries are struggling to find (and keep) the subject matter expertise they need to develop their programs consistently. Although RPA is not a new concept, organisations are finding it difficult to find personnel with both a strong technical background and a sound knowledge of the organisation's business processes, who are able to build effective and sustainable solutions.

According to our survey, the main barriers to adopting RPA are:



Many respondents also highlighted a lack of understanding as a barrier to adopting RPA. Similarly, in our recent Global CEO Survey,¹ only 10 per cent of CEOs strongly agreed when asked whether they were clear on how robotics could improve their customers' experience.

What should CEOs and their leadership teams do?

In our experience, RPA is most effective when considered in conjunction with (or as an interim step towards) a range of other automation options, as part of a broader automation strategy and in alignment with the overall business strategy.

Without a doubt, RPA is a powerful tool that produces quick (and potentially significant) productivity gains. It can liberate people from time-consuming administrative tasks to focus on higher value activities.

However, we have found that organisations often stumble by looking for quick savings and solving the wrong problems. A formal strategy and roadmap will provide the rigour that is required to make automation a sustainable and transformative program. Some employees might resist automation, seeing it as a threat to their livelihoods. It takes time, effort, forethought and varying degrees of training to convince everybody, and to then use RPA effectively. When organisations underestimate these potential emotional barriers, implementation can slow down and cost more. Successful pilot projects can build momentum for other employees to embrace the change, and can increase employee buy-in.

If understood and used correctly, RPA can be applied to all areas of an organisation including risk and compliance.

RPA opportunities in risk and compliance



KYC onboarding

Data retrieval or data look up from internal and external sources to assist with the onboarding process



Investigating AML alerts

Inspecting and resolving AML alerts raised by the business



Fraud detection

Gathering and monitoring information for potential clues of suspicious activity on client's accounts



Data quality checks

Checks across multiple systems, both internal and external, to assist with integrity of investor data



Report generation

Track and report on compliance with service level agreement KPIs as part of monitoring of outsourced providers

¹ <https://www.pwc.com.au/ceo-agenda/ceo-survey/2018.html>

Rubbish data in, rubbish data out

As risk and compliance functions continue to invest in technology and consider new technologies such as RegTech, the benefits will only be as great as the quality of the available data. Many large technology projects fall at the last hurdle, when users question the information in the system, or even at the first hurdle, when the organisation finds itself obliged to spend the entire project budget on sourcing reliable, clean, structured data. For technology to succeed, data is a critical element, and its quality needs to be managed.

We typically see organisations rely on an individual's own due diligence and competence to comply with policies, standards and guidance, rather than implementing processes or system validations and controls to manage data quality. In these instances, poor quality data stagnates in systems and continues to be untrustworthy, unreliable and unable to support business decisions. The costs of fixing these problems retrospectively are very high, serving to deter executives from taking action.

To achieve their aims, risk and compliance functions need to tackle data quality head on. In our view, good data governance and data management are not about having a policy that gathers dust on the intranet, and are not just about risk management. They mean reaping the greatest possible benefits from your RegTech investment by using it to achieve your organisation's main objectives and deliver better customer outcomes.

To do this you need:

- executive sponsorship, funding, and a clear business case on how to transform data into an asset
- a vision and strategy for doing this
- a robust framework for managing data across its entire life-cycle
- policies, standards and processes
- the right people, operating model and governance structures
- a cultural change to encourage the business to take ownership of data
- enabling technologies.

The regulator is using data too

In its data strategy 2017–20, ASIC announced that it will:

- appoint a Chief Data Officer
- establish the Data and Information Governance Framework and governance forums, including the Digital Governance Board, Data Governance Council, Data Analyst Network and Data Champions Forum
- establish a data science lab
- establish data exchange frameworks with other agencies
- implement the 'One ASIC' regulatory transformation program.





More than **75%** of **superannuation funds** surveyed were **visited by a regulator** in the year to 31 January 2018

Most common APRA reviews

- Governance
- Prudential matters
- Consultation reviews
- Thematic reviews

Most common ASIC reviews

- Breach reporting
- Insurance in Super
- Member experience
- Effective disclosure



The One ASIC program will lead to a central regulatory data repository, a single integrated customer relationship management system, and a new online portal to improve communication with other parties and enable better collection of digital data.

APRA too has begun a multiyear program of work to transform the way it collects, stores, accesses and publishes data. A major component is the replacement of APRA's data-submission tool, Direct to APRA (D2A).

Over the last 12 months, ASIC and APRA have formalised common definitions across the industry, to allow for better comparability and to improve transparency of reporting from data collection. An example is the pilot data collection developed by APRA and ASIC to improve public reporting of life insurance claims performance across the industry, the results of which were released in November 2017. We expect to see more actions resulting from the pilot project and a broader look at analysis of data and transparency of reporting from recent initiatives. This includes detailed analysis and reporting of insights obtained by ASIC through breach reporting data collected over a period of time at certain organisations.

Calls to action to realise the potential of technology and data

1. Do your current risk and compliance operations meet your current and future requirement needs?
2. Do you understand the opportunities and consequences of new technologies like RPA for your organisation specifically?
3. If RegTech is a part of your strategy, do you have a clear roadmap for implementation?
4. Do you trust the quality of your data? Will it let you down when implementing new technologies?

4. Accountability, incentives and consequences

Our point of view

The public is sceptical that the Australian financial services industry will do the right thing by its clients, or by the community at large.

In response, some organisations have made steps towards creating a more trustworthy culture, yet the wealth management sector still has work to do to change and ensure that culture is driving risk outcomes in line with risk appetite.

Give individuals the right incentives, then hold them to account

The question of incentives and accountability in financial services has received a lot of attention recently. Regulators want organisations' remuneration frameworks to promote stronger risk-alignment and increased accountability. As a result, a number of regulatory reviews have been looking at incentives in the industry: the Royal Commission; the Sedgwick review into sales incentives in retail banking; ASIC's review of mortgage broker commissions; and APRA's review of remuneration practices in the financial services industry, focusing on CPS/SPS 510 Governance.

The main finding of APRA's remuneration review was that most organisations' remuneration policies and frameworks met minimum requirements, but fell short of strong governance. Although risk management is generally included in performance measures for individuals, the effectiveness of risk measures has been diminished by including them in a large pool of measures and giving them an average weighting of under 15 per cent. Further, they are not robustly applied: poor results (including poor risk behaviour) rarely leads to lower remuneration or other consequences for an individual at fault.

There have been numerous high-profile scandals in the financial services sector over the past few years. But, until very recently, individuals have not been held accountable for their poor behaviour, and few have suffered the consequences of their actions. Wayne Byres (APRA chairperson) summarised this in his April 2018 speech titled 'The Incentive to Fly Safely': "particularly at senior executive level, the carrots are large and the sticks are brittle. Not only are rewards generous, but there are seemingly few repercussions for poor outcomes". This situation has led to an erosion of trust: the public does not believe that the industry will do the right thing.

In an attempt to tackle this lack of accountability in the banking sector, and to restore trust, APRA is implementing the BEAR – a stronger responsibility and accountability framework for the most senior and influential directors and executives in authorised deposit-taking institutions (ADIs). The BEAR came into effect for the four major ADIs on 1 July 2018; one year later it will also apply to the small and medium ADIs. APRA has stated that, in the future, an accountability regime will apply to *all* APRA-regulated entities, including Superannuation Trustees, highlighting the importance of rolling out an accountability regime more broadly across financial services.

Uncover the root cause of the problem

The key to stopping bad behaviour is understanding its root cause. The Royal Commission and APRA's recent prudential inquiry into governance, culture and accountability at the Commonwealth Bank of Australia have prompted boards to pause and reflect:

- What if *your* organisation were under the microscope?
- Where would the potential areas of exposure or improvement be for you?

Consolidating records of all past inadequacies, incidents and breaches into a single repository has been confronting reading for some, and demonstrates the need for timely reporting and remediation for any incident or breach.

Many of the case studies tabled at the Royal Commission demonstrated that operational and compliance risks only received attention when they emerged fully, or after the organisation's reputation suffered. Dealing with such matters in a legalistic and reactive way is unlikely to meet community expectations.

Organisations must maintain a corporate memory despite staff turnover and other changes, so that they can identify and fix any recurring problems. Learning from incidents over previous years, so that the root cause can be understood and communicated throughout the organisation will help it learn, anticipate and adapt.

Cultural silos lead to inconsistent behaviour

In an organisation, 'culture' means the accepted ways of behaving, feeling, thinking and believing. Culture is often referred to as 'the way we do things around here'. Culture is pervasive and touches the whole organisation; everyone has a role to play in demonstrating correct behaviour. However, particular parts of a business have specific roles and responsibilities for fostering the right culture. It is important that these roles are understood and that these parts of the organisation work together consistently. Departments of human resources, compliance, risk and the front line must all encourage, foster and reward the same behaviour.

Ultimately, all these elements should complement one another, and come together to reinforce and embed the desired culture.

76% of survey respondents stated that their board has formally set expectations for the desired culture

Culture: roles and responsibilities



The **Board** is responsible for setting the desired culture for the organisation: the tone from the top and behavioural expectations. Boards are also responsible for overseeing culture. They need to know whether the culture they have is the culture they want and the community expects.



Management is responsible for implementing the culture that has been defined and set by the board. All managers also need to demonstrate correct behaviour in all they do, serving as role models to others.



The **human resources department** plays an important role in designing and implementing cultural initiatives across the organisation. It also has responsibility for personnel activities that can reinforce the culture (such as recruitment, onboarding, training, performance management and remuneration).



Risk departments are becoming increasingly involved in determining the organisation's culture. The concept of risk culture (such as through the development of a risk culture framework) is emerging. Risk departments can ensure that the organisation's culture is consistent with the organisation's agreed appetite to take on risk.



The **internal audit department** can give the board and the audit committee an operationally independent view of the organisation's culture. Although this element is still evolving, actions to date include performing stand-alone culture reviews and incorporating a cultural element into regular internal audit reviews.

Of course, in any organisation there are sub-cultures in particular areas or departments. This can be due to a range of local factors, including leadership, market, customers and environment. But where they do exist, such sub-cultures must be consistent with the desired culture set by the board.

Behaviour is increasingly being incorporated into annual performance scorecards. No longer is the focus just on *what* the employee has achieved; also assessed is *how* the employee has done this, and whether they have met behavioural expectations. Employees who demonstrate good behaviour can receive a higher performance rating, which might also lead to higher remuneration. Conversely, employees who have behaved poorly can have their remuneration cut.

Widespread outsourcing in the wealth management sector creates another hurdle to ensuring that good behaviour is consistently demonstrated and practised, not only within the organisation, but also by all outsourced providers. During the due diligence process in selecting an outsourced provider, the client should assess whether the provider's values are consistent with those of the client organisation, and whether there is a good fit. Behavioural standards need to be set and agreed between the organisation and the outsourced provider right from the start, and monitored throughout the term of the agreement.

*According to our survey,
2/3 of reportable breaches occurred
in organisations adopting a mostly
outsourced operating model*

Ways to do this include:

- sharing risk-appetite statements with outsourced providers to ensure both sides have the same expectations
- finding out what actions the outsourced provider is taking in response to regulatory reviews and public hearings in the first half of 2018
- continuously reviewing key performance indicators in service-level agreements, so they remain appropriate and allow for effective monitoring
- validating outsourced providers' processes for identifying and reporting breaches.

Using the right tools and techniques to measure culture

Because the Royal Commission and APRA's prudential inquiry into the Commonwealth Bank of Australia are both looking at organisational culture, we can expect the focus and expectations on culture to heighten. This needs to be front of mind for boards.

Under the SPS 220 Risk Management Prudential Standard, the boards of all APRA-regulated entities should form a view of their organisation's risk culture. Do not approach this as a tick-the-box exercise to meet a regulatory requirement. Rather, use it to your strategic advantage: capitalise on your cultural strengths and promptly identify and correct any behaviour that does not meet expectations.

Boards need to understand whether the culture they desire is the culture that currently prevails:

- What is the organisation doing on culture?
- How is the organisation measuring culture?
- What reporting am I receiving on culture?
- Is the data telling me what I need to know?
- Does this provide me with an understanding of the culture?



We have observed that the level of maturity in measuring and reporting culture – both in the financial services sector and elsewhere – varies between organisations.

*Only **21%** of respondents said that those charged with governance receive **periodic reporting** on culture KPIs*

This low score suggests that the wealth management sector remains immature in measuring and reporting on culture. Organisations continue to struggle with a topic that they perceive as intangible and subjective, but in fact it is possible to measure culture:

- Determine what you are measuring against
- One size does not fit all. Measures need to be fit for purpose and tailored for each organisation
- You need to measure inputs, actual behaviours, and results
- Use a combination of quantitative and qualitative measures
- Ensure there is a balance between positive/negative and predictive/lagging measures
- Less is more. Apply a small number of meaningful measures that are central to the organisation's culture
- Apply tolerances and thresholds to identify variations from expectations, so that you know when to act.

A range of tools and techniques can help you assess and measure culture. Employee-engagement surveys, KPIs and metrics are the most common (supported by the majority of survey respondents). Although these provide quantitative data, in isolation they might not get to the root cause of a cultural or systemic behavioural problem, or reveal the full picture. We recommend supplementing quantitative data with qualitative techniques.

To get a proper understanding of the culture in your organisation, you must speak to people. This might be through interviews and focus groups, which allow you to gather stories and examples, and to really dig below the surface. For example, quantitative data might suggest that there have been no whistle-blowing incidents in a given period.

This could be interpreted as a positive result, but when speaking to employees you might discover that they are not aware of the whistle-blowing channels, don't feel comfortable using them for fear of reprisal, or are not confident that any action would result – a radically different insight.

What are the different techniques that can be used?



Attracting the right people to your organisation and creating a strong culture of doing the right thing for customers will help to rebuild trust and is likely to create competitive advantage for your organisation.

Calls to action for culture to drive right outcomes

1. Do sub-cultures exist in your organisation? If so, are they consistent with the desired culture set by the Board?
2. How consistently is poor behaviour being dealt with throughout the organisation? Are there pockets where poor behaviour is managed inconsistently?
3. Does risk and compliance have adequate involvement in decision making and monitoring over agreements with and services performed by third parties?
4. Do you know where your cultural strengths are within the organisation? And if so, are you capitalising on them?
5. Are risk and compliance functions bold enough to challenge and escalate issues to management and the Board?



Contacts

Melbourne



George Sagonas

Partner
Wealth Management
+61 (3) 8603 2160
george.sagonas@pwc.com



Nicole Osborne

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



Adrian Gut

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



Owain Norman

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

Sydney



Craig Cummins

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



Stephanie Smith

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



Sarah Hofman

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



Deanna Chesler

Partner
Wealth Management
+61 (2) 8266 0003
deanna.chesler@pwc.com

Adelaide



Kim Cheater

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



Paul Collins

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



Janice Jones Smith

Director
Financial Services
+61 (8) 9238 3445
janice.jones@pwc.com

Subject Matter Experts and Publication Contributors



Pip Butt

Director
RegTech
+61 (2) 8266 0824
pip.butt@pwc.com



Katy Waterhouse

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



Jess Mufazzil

Senior Manager
Data Governance
+61 (3) 8603 1875
jess.h.mufazzil@pwc.com



Nathalie Van Nueten

Director
Robotic Process Automation (RPA)
+61 (2) 8266 3309
nathalie.a.van.nueten@pwc.com