

A spotlight on how risk and compliance functions are supporting insurance organisations build trust | July 2018

Insurance Risk and Compliance Benchmarking Survey







Contents

About the survey	5
Executive summary	6
Maturity of risk and compliance functions	8
Technology and data	16
Culture and conduct	20





About the survey

Welcome to our Insurance Risk and Compliance Benchmarking Survey – PwC’s first annual survey of Risk and Compliance executives from Australia’s leading insurers. The survey aims to give Risk and Compliance function leaders a view of how their peers structure and staff their organisations, and how they are responding to significantly heightened expectations from customers and regulators.

We received responses to our survey from executives of 37 different organisations across general, life and private health insurers, with gross premium ranging from below \$200m to over \$5bn.

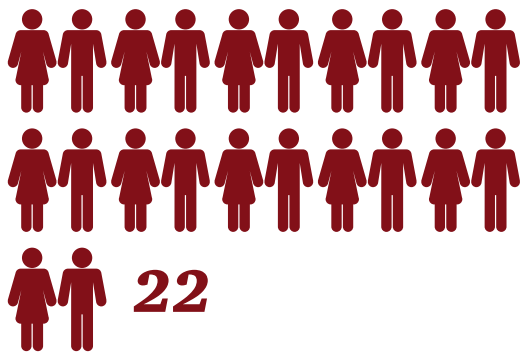
We express our sincere thanks to those who participated in the survey.

We hope you find the information in this report to be insightful and valuable as the industry responds to the increasing expectations of consumers and regulators, and in doing so re-builds trust.

Who participated in the survey.

Entity type

General Insurance



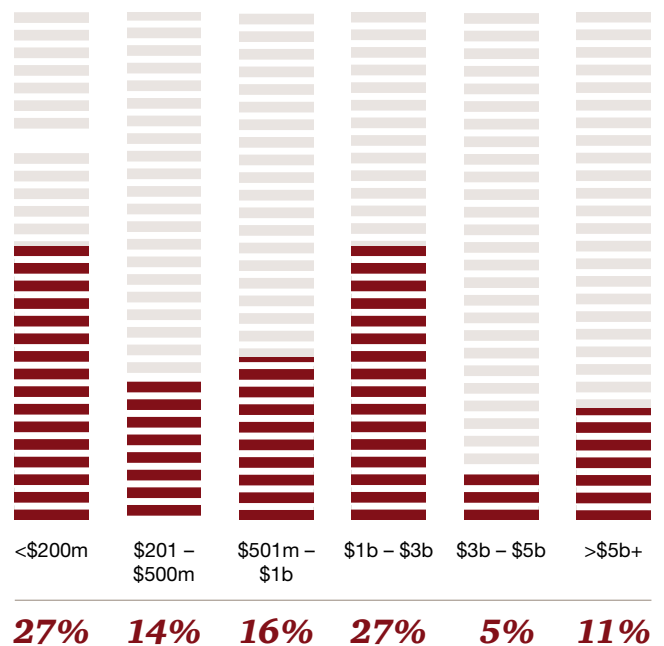
Private Health Insurance



Life Insurance



Gross premium written



Executive summary



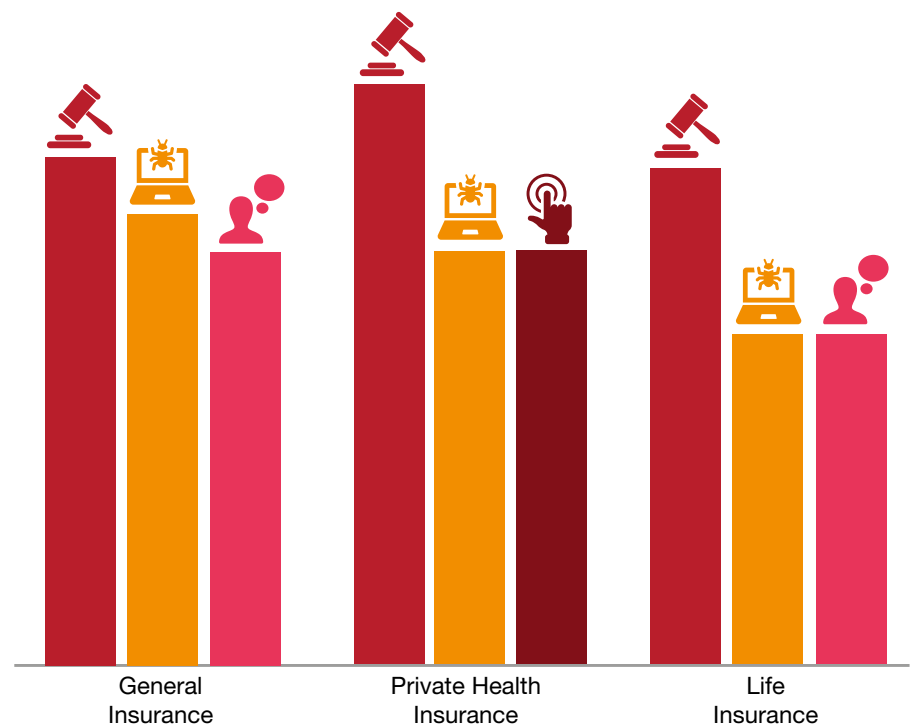
The first half of 2018 has seen some of the most significant questions being asked of the governance and leadership of financial institutions in Australian corporate history.

The Royal Commission has dramatically highlighted increased public expectations of the sector, and APRA's recent report of its Prudential Inquiry into the Commonwealth Bank of Australia (CBA) is causing organisations to fundamentally reassess their risk governance, in particular how well they are managing non-financial risks.

These developments are against a backdrop of continued focus in the insurance industry on matters relating to trust; for example, the establishment of the Life Insurance Code of Practice, ASIC's focus on add-on general insurance products, and the ACCC's recent prioritisation of consumer issues in Private Health Insurance.

Insurers have a profound impact on society, but they currently have a significant challenge to build engagement with, and trust of, their consumer base. It is clear that the role played by risk and compliance professionals in supporting insurance companies navigate the complex external environment has never been more important.

What are your top three risk management challenges?



 Regulation

 Cyberattack

 Culture

 Use of technology

Maturity of risk and compliance functions

There is a general acknowledgement that more should be done to further embed fundamental structures and risk management practices within insurance organisations. Insurers see opportunities for enhancing clarity and accountability of roles, including modifications to the three lines of defence model and refinement of internal reporting lines. With this ongoing focus, we anticipate increased demand for IT, actuarial and conduct specialist skills in second line roles to reflect the challenges insurers are currently facing.



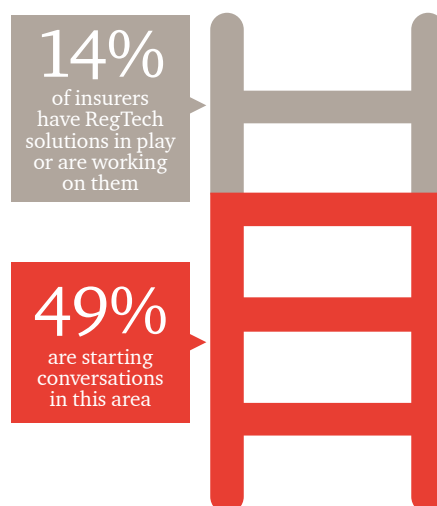
Our report highlights that respondents are generally not confident that compliance obligations have been well documented and mapped to relevant controls. There is also an opportunity for more consistent use, and validation, of business attestations, and enhanced reporting to Risk Committees of information relating to non-financial risks.



Technology and data

Insurers are increasingly looking at how to leverage technology to drive more effective risk management and compliance monitoring, with a number of organisations still reliant on spreadsheets.

Our survey also indicated that insurers are looking to engage with RegTech; however, given the change management that is required to implement such solutions, it is important to consider how the adoption of RegTech fits your organisation's overall business and regulatory strategy.



More broadly, insurers are looking to change how business is conducted and InsurTech is starting to drive innovation and collaboration. Whilst technology can open up new opportunities, the increased level of personal data insurers are collecting is increasing risk. Consequently, it has never been more important to have an effective data management framework in place, with a clear understanding of, and focus on, critical data.

Culture and conduct

Heightened regulator focus and reports of behavioural failings have driven an increased attention on culture. Most insurers have defined their desired culture, however in our experience there are opportunities to increase the extent to which defined culture aligns with broader strategic objectives, risk appetite, values and behaviours.

Insurers are also currently grappling with how to effectively measure culture, and how to make their culture work for them. Culture frameworks have been best adopted where organisations have implemented an enterprise-wide approach that links culture and behaviour to outcomes; with the most appropriate measures to reflect progress regularly monitored.

Recently, the industry has experienced the rise of the Chief Customer Officer, with over a third of organisations surveyed having such a role. We have also seen organisations assigning a 'voice of the customer' role in key executive meetings. We see such roles increasing, and being further formalised, in the near term. We anticipate insurers will draw stronger links between performance, remuneration and risk outcomes, and will adopt a stricter approach to consequence management.

Maturity of risk and compliance functions

How well are risk and compliance functions set up to support organisations in a climate of increasing public expectations?

Three lines of defence (3LoD)

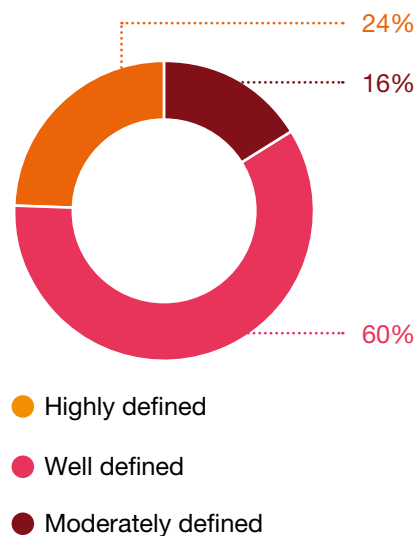
A well-defined, consistently understood, and fully embedded 3LoD model provides the bedrock to a robust risk management framework.

However, in our experience, there are a number of challenges in effectively implementing such a model, including:

- roles and responsibilities in the first line are not clearly documented and well understood,
- lack of consequence management at an individual level to support accountability,
- blurring between lines, where overlaps or gaps are not identified, and
- lack of communication and coordination between lines, resulting in each line working in silos.

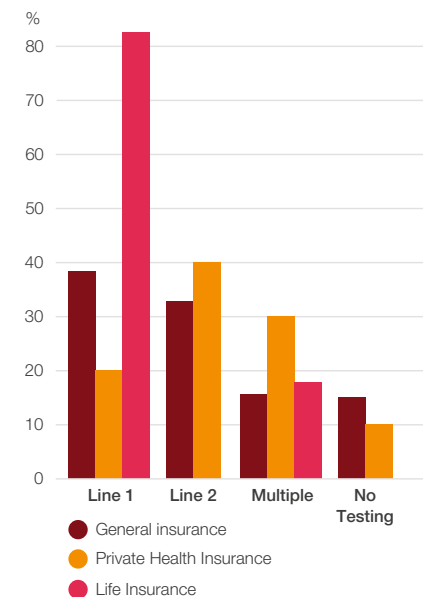
24% of respondents indicated the 3LoD within their organisations are highly defined, with all lines having a strong understanding of roles and responsibilities. Most of the respondents consider their 3LoD are well defined, but with some overlap.

How defined is the organisation's three lines of defence?



41% of respondents indicated the responsibility for testing of controls is assigned to Line 1. This gives the Risk and Compliance teams within Line 2 the opportunity to monitor and challenge at a higher level.

Responsibility for testing controls



In a mature environment, greater responsibility for risk activities in the front line should lead to faster risk-event recovery and stronger risk cultures. This is dependent on sufficient oversight, challenge and support from Line 2.



There is no 'one size fits all' 3LoD model, and organisations should consider what is most effective for their size, complexity and stage of maturity. What is most important, is that there is absolute clarity of roles and accountability, both in design and in consistent practice, throughout the organisation.

46% of respondents indicated the Head of Compliance currently reports to the Chief Risk Officer, **24%** to the Chief Executive Officer and **20%** to the Head of Legal, highlighting the range of reporting structures currently in place in relation to compliance.

Given recent developments, some insurers are considering how to elevate the authority and stature of compliance, and the Head of Compliance in particular. Regulators have recently suggested the elevation of the stature of compliance functions could be achieved by appointing the Head of Compliance as a member of the Executive Committee and/or the Non-Financial Risk Committee.

“Compliance functions globally have more recently been focused not just on evaluating whether an activity or product is allowed under regulation (‘can we?’) but critically, whether they should engage in such an activity or product in the first place (‘should we?’)”

APRA CBA report

70% of respondents have separate chairs for Audit and Risk Committees. Larger insurers, with annual gross premium written above \$500 million, are more likely to have separate chairs for Audit and Risk Committees.

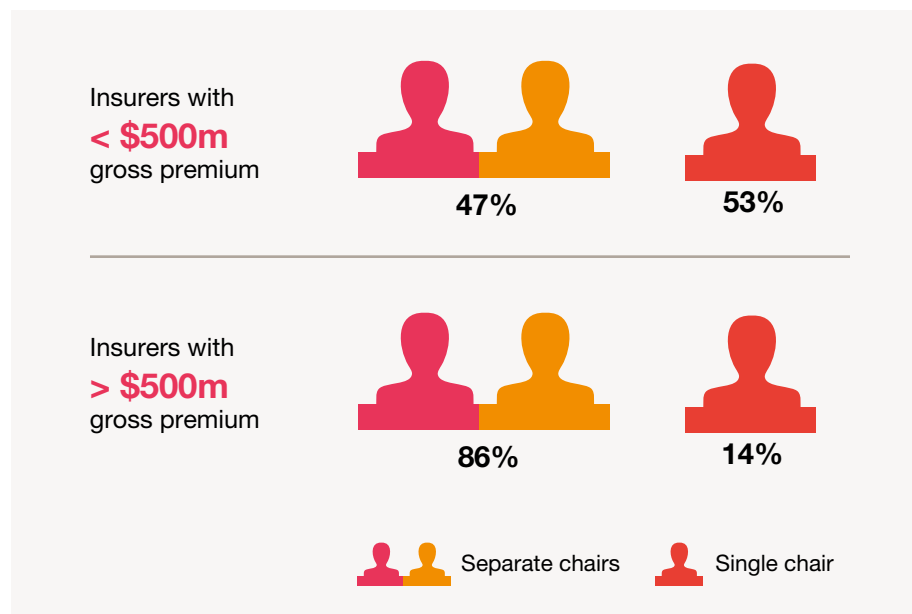
We anticipate more insurers will move to a model of having separate chairs of Audit and Risk Committees to further facilitate focus and accountability.



Calls to action

1. Is your current 3LoD model designed and operating in the most effective way to meet the needs of the organisation? Could more be done to enhance clarity and accountability?
2. Does the stature of your compliance function need to be elevated to assist in a more rigorous and strategic management of compliance risk?

Separate or single chair(s) for Audit and Risk Committees

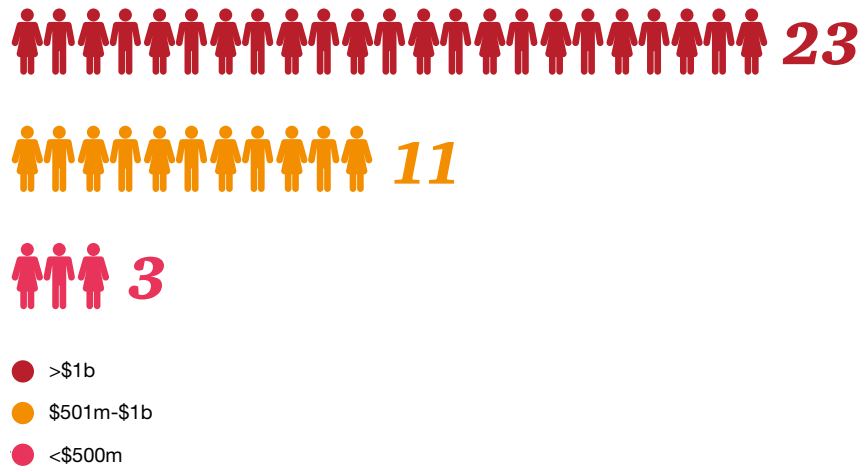


Team size and skillsets

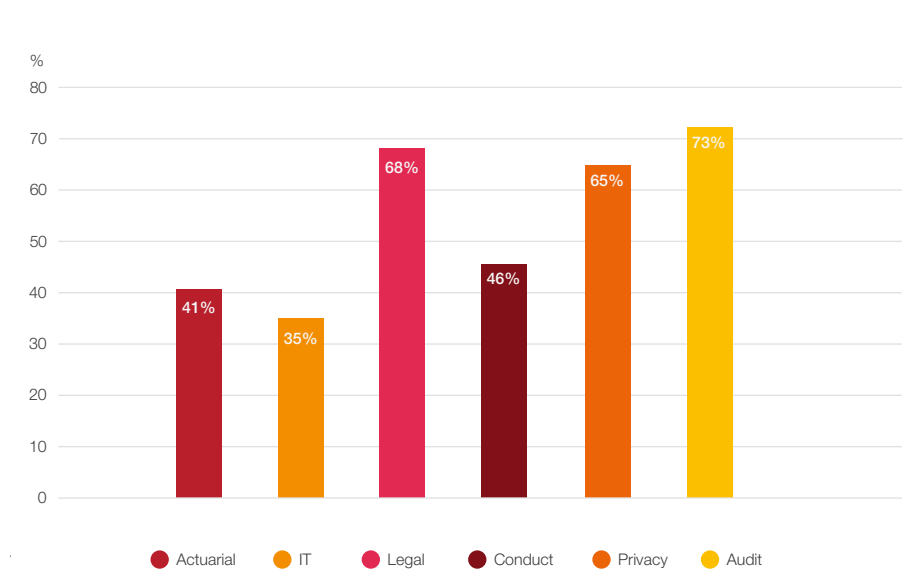
With the spotlight increasingly on risk and compliance functions, we anticipate organisations re-assessing both capacity and skill set of their risk and compliance teams in the near future.

The average size of local risk and compliance teams surveyed currently ranges from 3 to 23, with an average of 11 per organisation. We expect this to increase in the near future as organisations look to strengthen these functions in response to heightened regulatory and public expectations. We also anticipate companies will reassess the skill base in these teams, and forecast an increased demand for employees with expertise in conduct, given the environment of increased customer expectations. This in turn could also lead to a call for greater actuarial expertise as organisations look to challenge the appropriateness of product design. Given the concerns insurers rightly have in respect of cyber risk, we further anticipate an increase in IT expertise in risk and compliance teams.

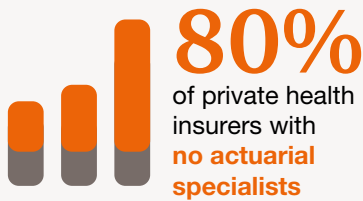
Average number of risk and compliance employees by company size



Percentage of risk and compliance teams with the following specialist skills



In their risk and compliance teams, there are:



Call to action

1. Is the size and specialist capability of your risk and compliance functions appropriately aligned to the organisation's risks, and the need to respond to increasing regulator and public expectations?

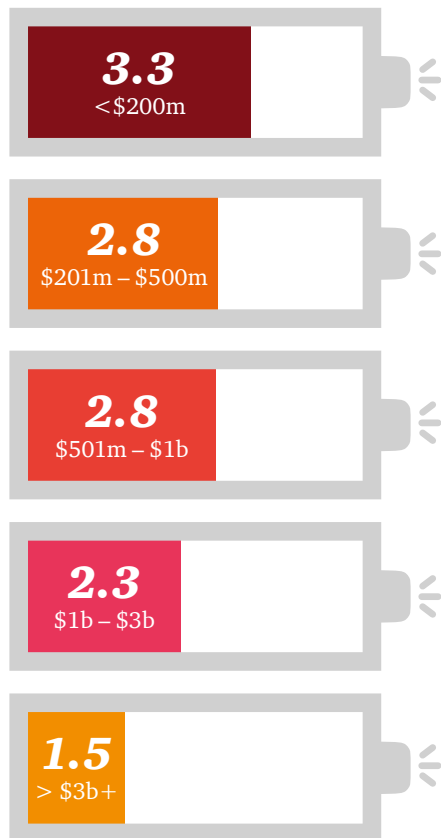
How risks are identified and managed

The survey results identified an opportunity for a number of insurers to have their compliance obligations more robustly documented, mapped to controls, and monitored through the effective use of business attestations.

The mapping of obligations to controls, which are routinely tested, forms the fundamental basis of mitigating risk of non-compliance. It helps clearly define roles and responsibilities and provides a robust basis for business attestations.

Insurers rated the extent to which their obligations are currently mapped to tested controls at an average of **2.5 out of 5** (with 5 being fully mapped and tested).

Extent to which risk and compliance obligations are mapped to controls and tested (by company size).

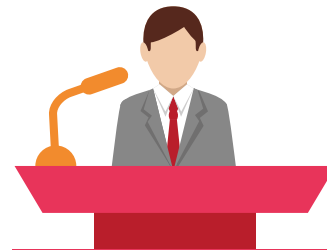
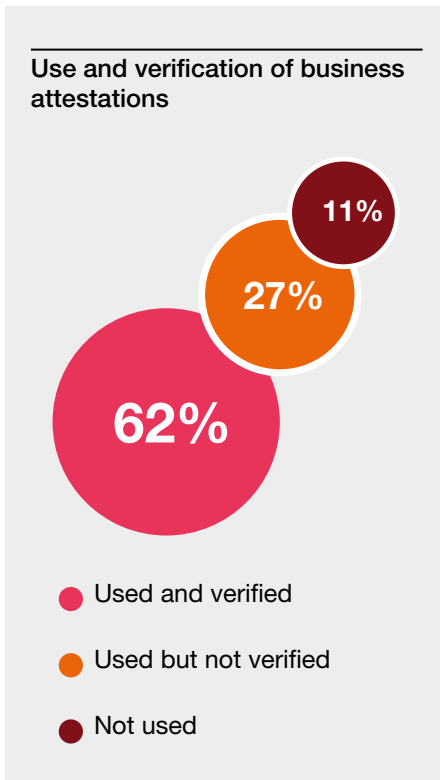


The rating decreases as organisations get larger, possibly reflecting increased complexity.

Business attestations are also an important mechanism to focus the minds of senior management in relation to risk and compliance. Independent verification of such attestations helps to assess whether there is sufficient basis for attestation sign off.

11% of insurers indicated no attestations were used in the business, while **27%** of insurers use attestations but no verification of the integrity is performed.

Periodic testing of business attestations should be performed to help avoid the process becoming a formality.



Calls to action

1. Do you have a plan in place to address gaps in mapping of regulatory and compliance obligations?
2. How effectively is your control program providing you assurance that controls over these obligations are operating as designed?



How risks are monitored and reported

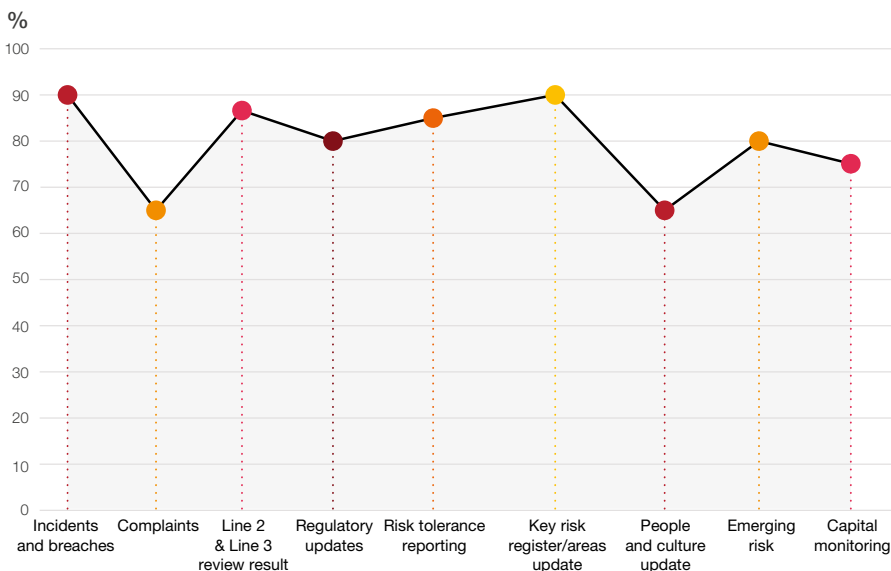
While areas reported to Risk Committees are more likely to be closely monitored and managed, our survey indicated that People and Culture and Complaints are the least frequently reported areas surveyed.

With the current environment and regulatory expectation, we anticipate Risk Committees seeking more robust reporting of these areas.

“Board members interviewed referenced an increasing philosophy of ‘don’t tell me, show me’ to ensure that the trust placed in management teams is verified.”

APRA CBA report

Topics reported to Risk Committees



More than

80%

of insurers surveyed have presented the outcome of a reverse stress test to the Board



On average, insurers have presented

13

different capital scenarios to Boards over the past 3 years.



Calls to action

1. Does the organisation effectively capture the voice of external customers?
2. Does the organisation regularly report non-financial risk information to Risk Committees?

Breaches, incidents and complaints

Breaches

What constitutes a reportable breach is judgemental. The average number of reportable breaches of those surveyed (1.5 for the year ended 31 December 2017) is low compared to the average number of non-reportable breaches of 110. We anticipate the number of reportable breaches increasing this year, particularly following the Royal Commission.

In the current climate, we also see organisations adopting a more conservative approach to assessing whether a breach is reportable or not, and if in doubt, reporting.

One of the challenges identified through the survey was the inconsistency within organisations of the expectations, and definitions, regarding incidents and breaches. It is therefore critical that risk and compliance teams properly educate the front line to embed a consistent understanding of reporting requirements.



Breaches trend analysis

76% of survey respondents performed trend analysis. **86%** of these respondents said that they have benefited from the analysis with a reduction in similar incidents and breaches, as well as with earlier identification of breaches.

While the majority of respondents are analysing root causes and breach volume trends, only **41%** are analysing timeliness of breach resolution.

We expect organisations will perform more trend analysis over timeliness of reporting and issue resolution in the future, as this helps promote accountability.

Type of breach trend analysis performed

Root cause analysis

65%

Increase/decrease over the last month/year

57%

Recurring nature of a breach/issue

46%

Number of issues resolved

46%

Timeliness of resolution

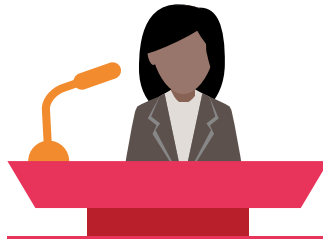
41%

Complaints

The largest drivers of complaints across insurers are claims rejection and poor customer service.

As for breaches, it is important that complaints trends are analysed to assess and remediate root causes, with better practice to also report the results to the Risk Committee.

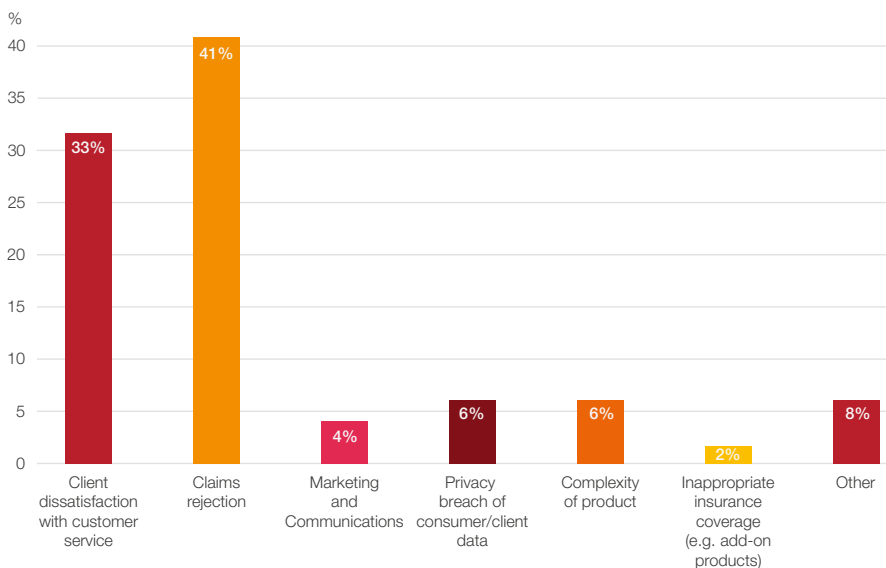
The Australian Financial Complaints Authority (AFCA) will replace the Financial Ombudsman Service (FOS) from 1 November 2018. Organisations need to consider the impact of the change, engage in conversations with the new authority, and make necessary changes to procedures and disclosures to customers.



Calls to action

1. Do you have documented definitions of breaches and incidents? Are such definitions clearly and consistently understood by the business?
2. How effectively are you using breach and complaint data in identifying and resolving issues in a timely manner?

Nature of complaints





Technology and data

RegTech solutions

Many risk and compliance teams are currently reliant on less sophisticated tools such as spreadsheets. By strategically developing technology and data capabilities, organisations can enhance the effectiveness of their risk and compliance processes.

41%

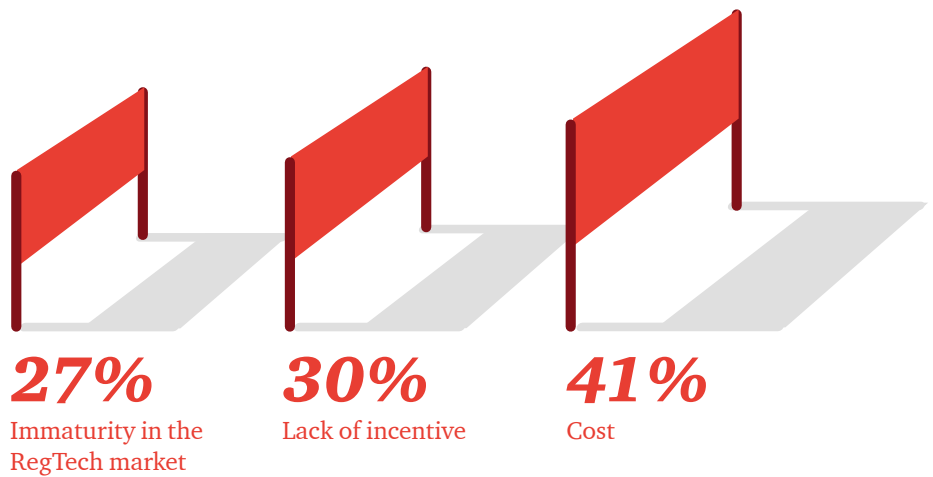
of respondents feel they do not currently have the requisite tools to effectively manage risk and compliance processes.

It is clear from our survey that insurers' interest in new technology is growing. This, combined with the growing expectations of regulators and increasing compliance costs, has created an environment where current compliance processes are ripe for disruption by emerging RegTech providers. While there is a growing number of external providers in this space, there are a number of matters to consider before embarking on your RegTech journey.

The evolving regulatory landscape means the configurability of RegTech solutions for changing regulations should be a key consideration for insurance organisations when embarking on the RegTech path. It is essential in these early stages to consider how the adoption of RegTech fits your organisation's overall business and regulatory strategy.

Our survey indicated the current cost, lack of incentives and immaturity of the RegTech market are the major hurdles external providers need to overcome. We have developed a roadmap in association with the RegTech Association to help RegTech buyers and vendors understand each other's needs as they work together.

Main challenges to the effective adoption of RegTech cited by respondents.



14%

of insurers have RegTech solutions in play or are working on them

49%

are starting conversations in this area

Roadmap to accelerate RegTech integration

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



RegTech is the amalgamation of 'regulation' and 'technology'

Unfortunately, that does not mean there is currently a 'one-stop shop' technology to meet all your regulatory needs.

Management of critical data

Having an enterprise-wide defined and endorsed data management strategy is the bedrock of data management and governance.

Insurers currently face a significant risk of loss of sensitive information, and this risk is only likely to increase as they look to collect more data.

Damage could be caused in a wide number of ways; theft or ransom of sensitive customer data (such as personal, medical, or financial information – described as “gold” on the black market and “dark web”), the corruption of insurers’ databases, and the theft of intellectual property. The ensuing potential for reputational damage is large.

Consequently, having an effective data management framework in place has never been more critical.

Our survey highlighted there are currently some organisations without a data management strategy and others where such a strategy only exist in silos.



Key areas of focus for effective data management



Building an inventory of critical data (crown jewels)



Harmonising the meaning of ‘critical data’ across applications and repositories



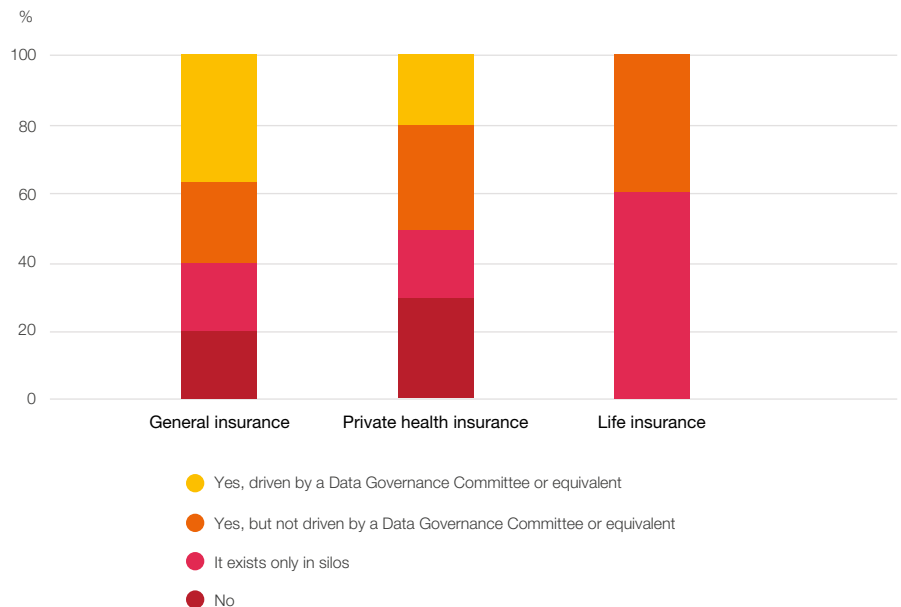
Establishing effective, preventative data quality control processes (business rules, authorisations, etc.)



Calls to action

1. How well do plans to adopt RegTech fit in with your broader business and regulatory strategy?
2. If your organisation does not have a data management strategy with critical information clearly defined, do you have a plan in place to address this?

Use of a enterprise-wide defined and endorsed Data Management Strategy





Culture and conduct

Culture

How do organisations define an appropriate culture, aligned to strategy and risk appetite, and then measure culture against this desired state?

'Culture' is the pattern of behaving, valuing, feeling, thinking and believing in an organisation. Heightened regulator focus and reports of organisations' behavioural failings have driven increased attention on 'culture' in a range of industries, including insurance.

This is reflected in our survey which indicated that, in nearly all organisations, Boards have either set a formal expectation regarding culture, or are expecting to do so in the near future.

In our experience, whilst there might often be general agreement on desired culture, there are frequently missed opportunities to increase the extent to which this aligns with broader strategic objectives, risk appetite, values, and behaviours.

Our survey identified that the majority of respondents (two-thirds) currently rely on operational mechanisms to manage culture (e.g., development of codes of conduct, conduct training delivered to all staff, etc.). One third reported using more mature mechanisms to manage their culture, including incorporating data analytics and KPIs. However, this is still a step below more advanced, predictive approaches that provide opportunity for deep insight, early detection of potential issues, and which can be used to facilitate a strategic and proactive response to culture management. Organisations acknowledge they still have a way to go in terms of culture management, with the significant majority of respondents rating this area as 'qualitative'.



Calls to action

1. Has your organisation defined its desired culture and the associated and specific behaviours that it aspires to? How clearly is this communicated and understood by employees at all levels?
2. Are there any risks to be aware of with regard to populations that act on behalf of, but are not employed by, the organisation (e.g. third parties) and may therefore not receive the same expectations (e.g., thorough induction, training, or tone from the top) of the desired culture?
3. How clear is the alignment between the desired culture, broader strategic objectives, and the organisation's risk appetite? Do these demonstrate a high degree of congruence or is there potential for confusion around what behaviours and outcomes are most valued?

Is there a formal expectation set by the Board regarding desired culture for the organisation?

70%

of Boards have set a formal expectation of desired culture.

24%

expect to do so in the next 6-12 months.

Why is this important?

Culture, and understanding what drives people to take risks within organisations, is complex. Attitudes towards taking and dealing with risk are heavily influenced by the dominant values of teams, as well as by individual behaviours and the behaviours of direct and informal leaders in the organisation.

Add to this the self-sustaining and enduring nature of culture, high-pressure decision environments, and the general complexity of today's world of work, it is clear that a multi-pronged approach to managing culture and behavioural risk is required. There is no silver bullet but an opportunity does exist to manage culture more proactively.

Part and parcel of managing culture is measurement – or, rather, measurement of the key indicators and factors that drive progress towards the desired state. As organisations increase their focus on measurement and reporting, there is a need to consider how fit-for-purpose measures can be used to develop insights, drive progress on initiatives, and inform strategic decisions. Interestingly, the survey identified a reliance on fairly traditional measurement methods such as surveys, employee profiling, and customer satisfaction. Whilst these reflect sensible individual measures, in our experience, there are several methodological considerations that need to be established.

Whilst it is important to understand an organisation's dominant cultural traits, because these can act as derailers or a strength to leverage, the brunt of the focus should be placed on understanding what critical few actions will most effectively drive progress towards the aspirational state.

The question emerges, to what extent do Boards and Executives put in place expectations around culture management and measurement that actually drives meaningful insight and action? In our experience, many organisations have yet to 'make their culture work for them' through an effective enterprise-wide approach that links culture and behaviour to outcomes through a consistent framework that also informs the most appropriate measures to reflect progress.



Calls to action

1. Do the selected measures provide a balance of lead and lag indicators? Or is there a stronger focus on lag indicators because these are more readily available and more easily interpretable?
2. Is there tracking of both historical and current state data to monitor trends over time? How is this presented and discussed to inform decisions around next steps?
3. What is the process for interpretation and insight? Are measures triangulated or interpreted in isolation? Is there a reliance on narrowly-sourced data points to interpolate/generalise insights?
4. How are measures selected for inclusion/reporting? Is there clarity on how each measure specifically drives the desired culture and behaviour? Or are measures simply reported because they are measured?

How are insurers currently measuring culture?



Employee survey/feedback



Employee profile – turnover, training record, performance



Breaches (including timeliness of resolution)



Customer satisfaction



Independent assessment

Conduct

The recent spotlight on conduct across the financial services industry is a call to action to urgently regain customers' confidence and trust.

Companies could consider whether this is merely an increased burden or whether this presents an opportunity to engage more closely with customers and drive a strategic advantage.

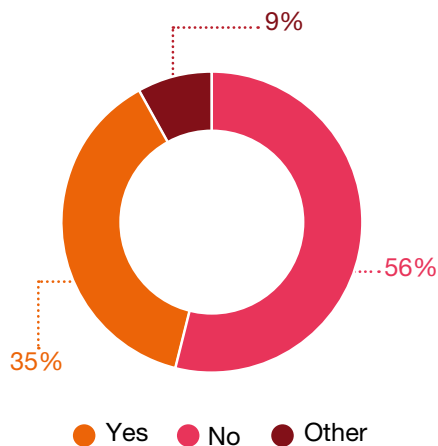
In light of this, organisations should reassess how the voice of the customer is being heard in key decisions, and to what extent conduct is being effectively measured. Organisations could also reflect on whether conduct risk is clearly defined and sufficiently elevated within the risk management framework.

“A formal Conduct Risk Strategy should be designed to embed the ‘should we?’ question into key decision-making processes.”

APRA CBA report

35% of respondents currently have a Chief Customer Officer or similar role within the organisation.

Do you have a Chief Customer Officer?




We have also seen organisations starting to use executives rotating a ‘voice of the customer’ role within key meetings, helping to bring in an ‘external perspective’ to discussions.


46% of respondents indicate that conduct is measured within the organisation. Most others plan to adopt conduct measures in the next two years.

Top 3 conduct performance metrics

The top 3 key performance metrics that are currently used for measuring conduct by insurers relate to:

 Complaints

 Monitoring/testing sales practices

 Breaches and timeliness of resolution

Whilst these measures are useful to understand how the organisation may be performing as it relates to conduct, they are typically lag measures, which reflect matters that have already occurred.

To be on the front foot, organisations could consider developing insight and analysis about pressures that create behavioural risk, that in turn may result in conduct failures.

For example, many known predictors of misconduct relate to the team environment. This is often assessed using qualitative observations, with some organisations using capability assessment activities or 360 feedback to gather data, for example on how leaders manage errors (do they blame, or use as a coaching opportunity?) and how well they model ethical behaviour.



Calls to action

1. Have you considered whether conduct risk is sufficiently elevated within your risk registers, and in reporting to the Board?
2. Have you considered including a Chief Customer Officer within your executive team, or rotating the role of the ‘voice of the customer’ in key executive meetings?

Remuneration

How is remuneration being used to support desired culture and conduct outcomes?

Remuneration is never far from the headlines for financial service companies, and regulators are pushing for strong risk alignment and increased accountability. As a result, a number of regulatory reviews have been looking at incentives in the industry.

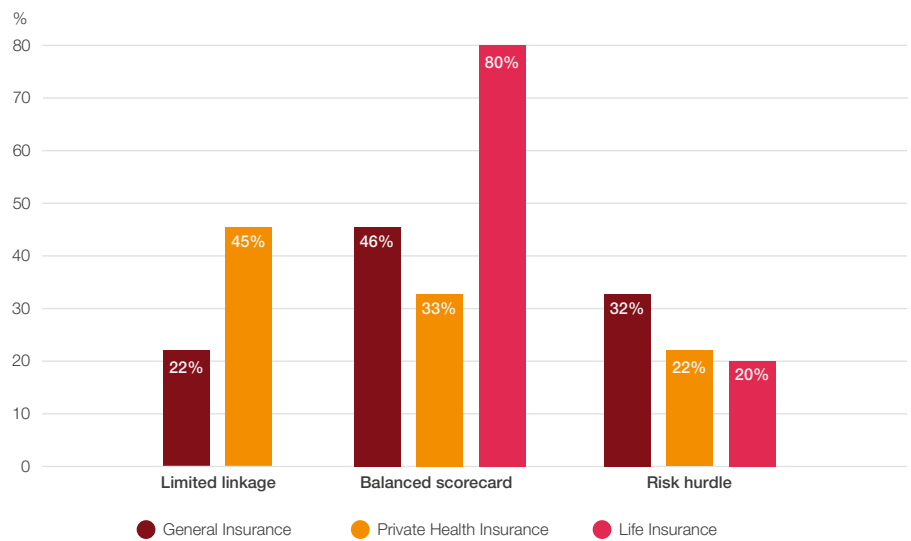
The main finding of APRA’s recent remuneration review was that most organisations’ remuneration policies and frameworks met minimum requirements, but fell short of strong governance. Although risk management is generally included in performance measures for individuals, the effectiveness of risk measures were diminished by including them in a large pool of measures and giving them an average weighting of under 15 per cent.

Further, APRA reinforced that incentives are not robustly applied: poor results (including poor risk behaviour) rarely lead to lower remuneration or other consequences for an individual at fault.

“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.”

Wayne Byres, APRA chairperson, April 2018

Extent to which remuneration is linked to risk objectives and metrics



41% of insurers surveyed incorporated risk as one of the performance measures in determining overall bonus through a balanced scorecard approach. The average weighting given to risk management related metrics among these insurers was 18%. This is slightly more encouraging than APRA’s finding in its review.

27% of insurers surveyed adopted a “gateway” approach where a hurdle is created for risk metrics which must be met for a performance bonus to be awarded. This is also close to the APRA review result where 25% of APRA sampled institutions utilised this approach.



Calls to action

1. Do remuneration structures in place appropriately reflect the Board’s risk appetite of the balance between shareholder return and customer expectations?
2. Is your organisation robustly applying its remuneration policy in relation to poor risk behaviour?



Contacts

Sydney Insurance Contacts

Rod Balding

Partner

T: +61 2 8266 1324
E: rodney.balding@pwc.com

Renae Cooper

Partner

T: +61 2 8266 6471
E: renae.cooper@pwc.com

Scott Fergusson

Partner

T: +61 2 8266 7857
E: scott.k.fergusson@pwc.com

Scott Hadfield

Partner

T: +61 2 8266 1977
E: scott.hadfield@pwc.com

Voula Papageorgiou

Partner

T: +61 2 8266 7802
E: voula.papageorgiou@pwc.com

Chris Verhaeghe

Partner

T: +61 2 8266 8368
E: christopher.verhaeghe@au.pwc.com

Melbourne Insurance Contacts

Chris Braithwaite

Partner

T: +61 3 8603 1557
E: chris.braithwaite@pwc.com

Morven Fulton

Partner

T: +61 3 8603 3641
E: morven.fulton@pwc.com

Britt Hawkins

Partner

T: +61 3 8603 2785
E: britt.hawkins@pwc.com

Stewart Paterson

Director

T: +61 3 8603 1056
E: stewart.paterson@pwc.com

Subject Matter Experts

Pip Butt

Director, Assurance Innovation Leader

T: +61 2 8266 0824
E: pip.butt@pwc.com

Sarah Hofman

Partner, Financial Services Regulation

T: +61 2 8266 2231
E: sarah.hofman@pwc.com

Caroline McCombe

Partner, Risk Consulting

T: +61 2 8266 2767
E: caroline.mccombe@pwc.com

Jenn Whittaker

Director, Culture

T: +61 2 8266 3119
E: jenn.whittaker@pwc.com

pwc.com.au

© 2018 PricewaterhouseCoopers. All rights reserved.

PwC refers to the Australia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

Liability limited by a scheme approved under Professional Standards Legislation.

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au.

WLT127062737