2021 PwC Insurance Risk and Compliance Benchmarking Survey

A spotlight on how risk and compliance teams are responding to regulatory changes and the COVID-19 pandemic

November 2021

pwc.com.au

Contents

About the survey

Welcome to our third Risk and Compliance Benchmarking Survey of Australian Insurers. The survey aims to give leaders of Risk and Compliance teams a view of how their peers manage risk and compliance functions, and how they are responding to regulatory changes and the COVID-19 pandemic.

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 and insights in the Risk and Compliance Benchmarking Survey to be helpful as you and the industry respond to the new and upcoming regulatory changes and increased expectations from regulators.

Who participated in the survey

18 General Insurance

10 Private Health Insurance

09 Life Insurance

Size of participant by gross premium

09 <$200m

04 $201-500m

07 $500m-1bn

09 $1-3bn

04 $3-5bn

04 >$5bn

Executive summary

At the time of our previous survey in 2019, the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry ("Royal Commission") and APRA self-assessments into governance, culture and accountability had set the path ahead for insurers and their risk and compliance functions. Prioritisation was being given to customer outcomes, supported by enhanced Board oversight and a clearly defined and understood culture.

Two years on, and whilst continuing to respond to the recommendations from the Royal Commission, insurers have also had to dynamically navigate and respond to the challenges of the COVID-19 pandemic, as well as keep up with the pace of continued regulatory changes.

In our experience, organisations that have established teams with the right capabilities, have been best placed to proactively embrace the proposed Financial Accountability Regime ("FAR") as an opportunity to articulate accountability in their 3 Lines of Defence. In addition, those insurers who have continued to actively promote risk culture have been able to both tactically respond to the challenges of the last 2 years, whilst at the same time looking ahead by developing and implementing a risk and regulatory change strategy.

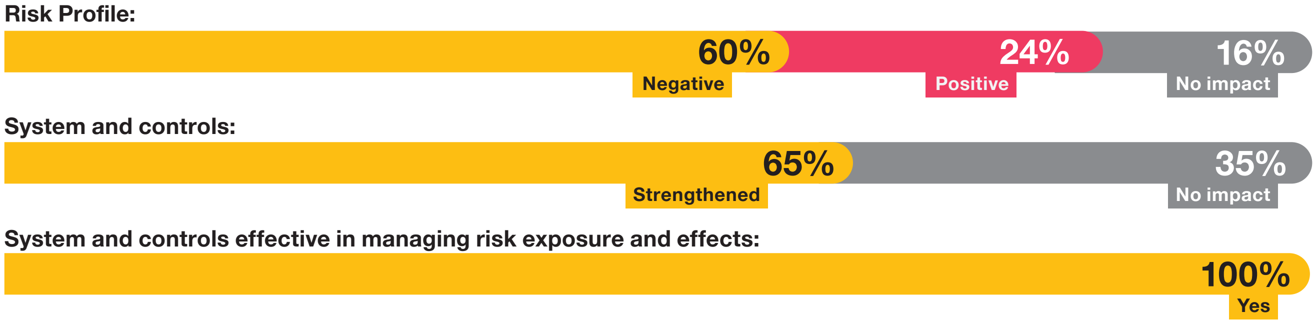
The impact of COVID-19

FY20 started like any other year, however, when the COVID-19 pandemic hit, the world we knew was turned upside down. Industries were affected quite differently by the pandemic; some prospered while others felt the pain of the economic impacts and lifestyle changes under multiple lockdowns.

The insurance industry has had significant involvement in responding to the impacts of the pandemic, with business interruption and contingency policies paying out claims. However, there has also been criticism over coverage issues, resultant legal cases, and the unknown impact of economic and claiming behaviour changes on the life and health insurance sectors.

The results of the survey indicate that, pleasingly, insurers have responded well to the pandemic both in terms of managing their risk profile, as well as strengthening systems and controls. Respondents have told us this has been achieved with minimal disruption to their business and operations. All insurers who participated in the survey have noted that their systems and controls were effective in managing the risk exposure and effects caused by COVID-19.

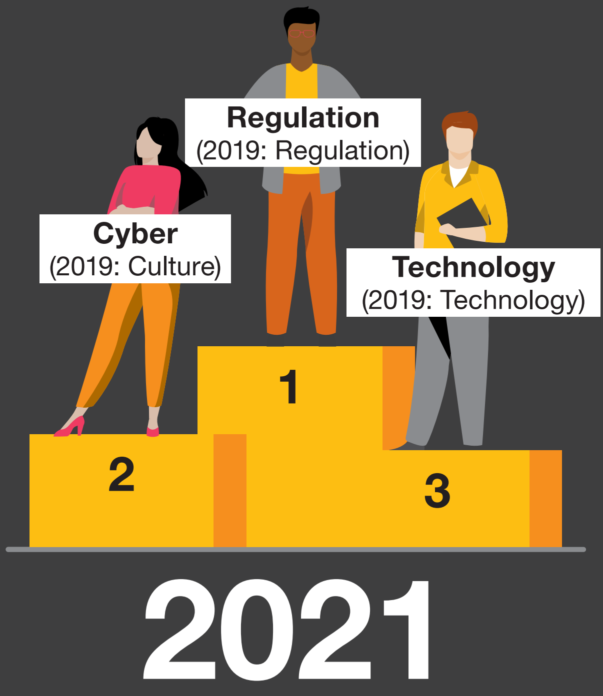
COVID-19 impact on:



Our survey indicates that

- The level of rising regulation is a concern for management, along with a general acceptance that risk and compliance teams will be required to be proactive in navigating through the challenges of the current and emerging regulatory changes.
- Insurers have been resilent to recover quickly and manage the impact of COVID-19 with minimal disruption.
- The majority of the respondents recognise that the FAR provides an opportunity to reinforce a culture of accountability and align and embed culture principles.
- Cybersecurity is an ever-increasing risk, with critical data needing to be both protected, and quality assured, in order to assist in providing valuable information for decision making. Despite the acknowledgment of this risk, one third of respondents do not currently have a formal mechanism in place to identify and manage critical data.

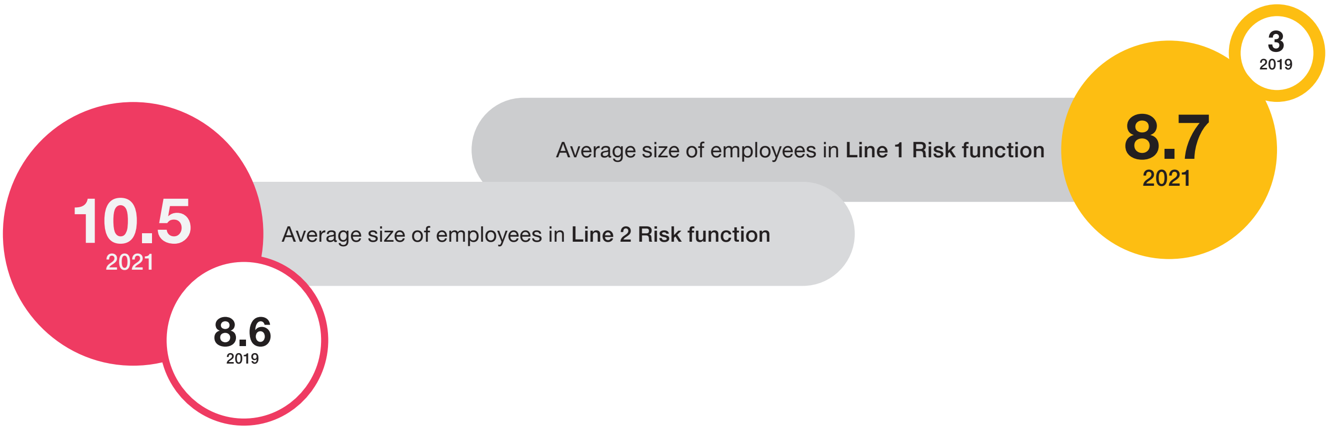
What are insurers' top three risk management challenges?



Our perspectives

- As expected, regulation remains as the number one risk management challenge for insurers, with an increasing focus across all aspects of the industry by both ASIC and APRA.
- The Federal Government is also calling for views on cybersecurity governance standards, including potential regulatory changes designed to incentivise businesses to invest in cybersecurity. Further, APRA are requesting certain insurers to conduct a risk management self-assessment exercise, as well as the recently underway tri-partite review of regulated insurers over CPS 234 *Information Security ("CPS234")*. It is clear that Cyber has now become one of the top priorities for management and Boards.
- Unsurprisingly, technology has also remained a focus area as organisations are investing and implementing Digital Transformation, Automation, Machine Learning and Artificial Intelligence technologies to support business growth and sustainability.
- Whilst not in the top three areas of risk for 2021, culture remains front of mind for both management and Boards (ranked 4th in the survey response). Risk culture has become a fundamental part of an effective risk management framework and impacts an organisation's ability to manage risk and make robust decisions.

Resourcing and capabilities



Insurers have continued to increase the capacity and capability within their risk and compliance functions as they respond to the recommendations coming from the Royal Commission, the regulatory changes that have come into effect over the last two years, and other upcoming regulatory changes.

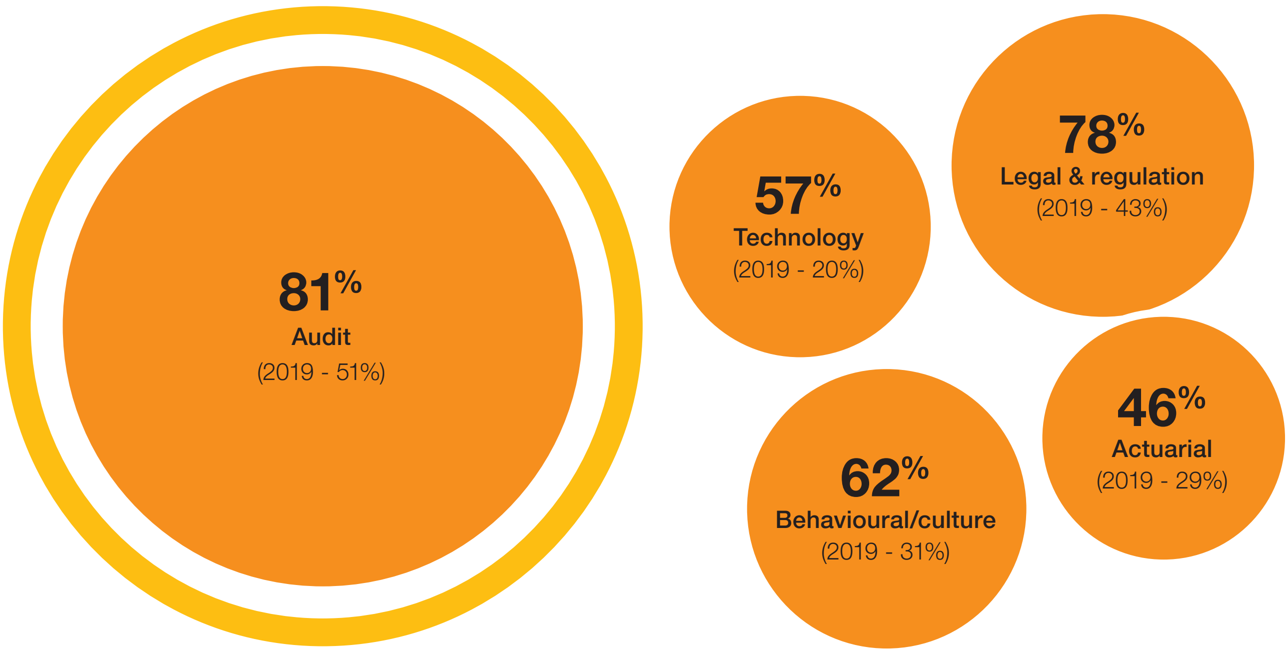
With the expected roll out of the FAR to insurance entities, and the increased emphasis on accountabilities, organisations are shifting towards a model of having more staff with risk expertise in Line 1. Our survey noted that the average size of the Line 1 risk function has increased by nearly 200%.

Our survey results also show that both Line 1 & 2 risk teams have grown not only in size but also the breadth and depth of their skillset.

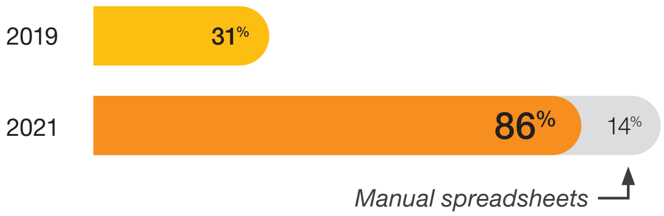
As insurers are continuing to actively promote risk culture, and the focus on cyber risk and regulatory compliance are increasing, we have seen a noticeable increase in capabilities in these areas in the risk and compliance teams.

However, securing resources will the right skill-set is challenging in the current environment where there is a shortage of skilled workforce. Risk & Compliance leaders should, where possible, maintain focus on acquiring skills that will provide the greatest positive impact in managing risk across the organisation.

Percentage of risk and compliance teams with specialist skillset



Respondents with requisite tools to manage and analyse risk and make informed decisions



In order to help complement an increase in both capacity and capability in their teams, insurers are also increasingly adopting GRC tools across the enterprise to automate and centralise risk management related activities and information.

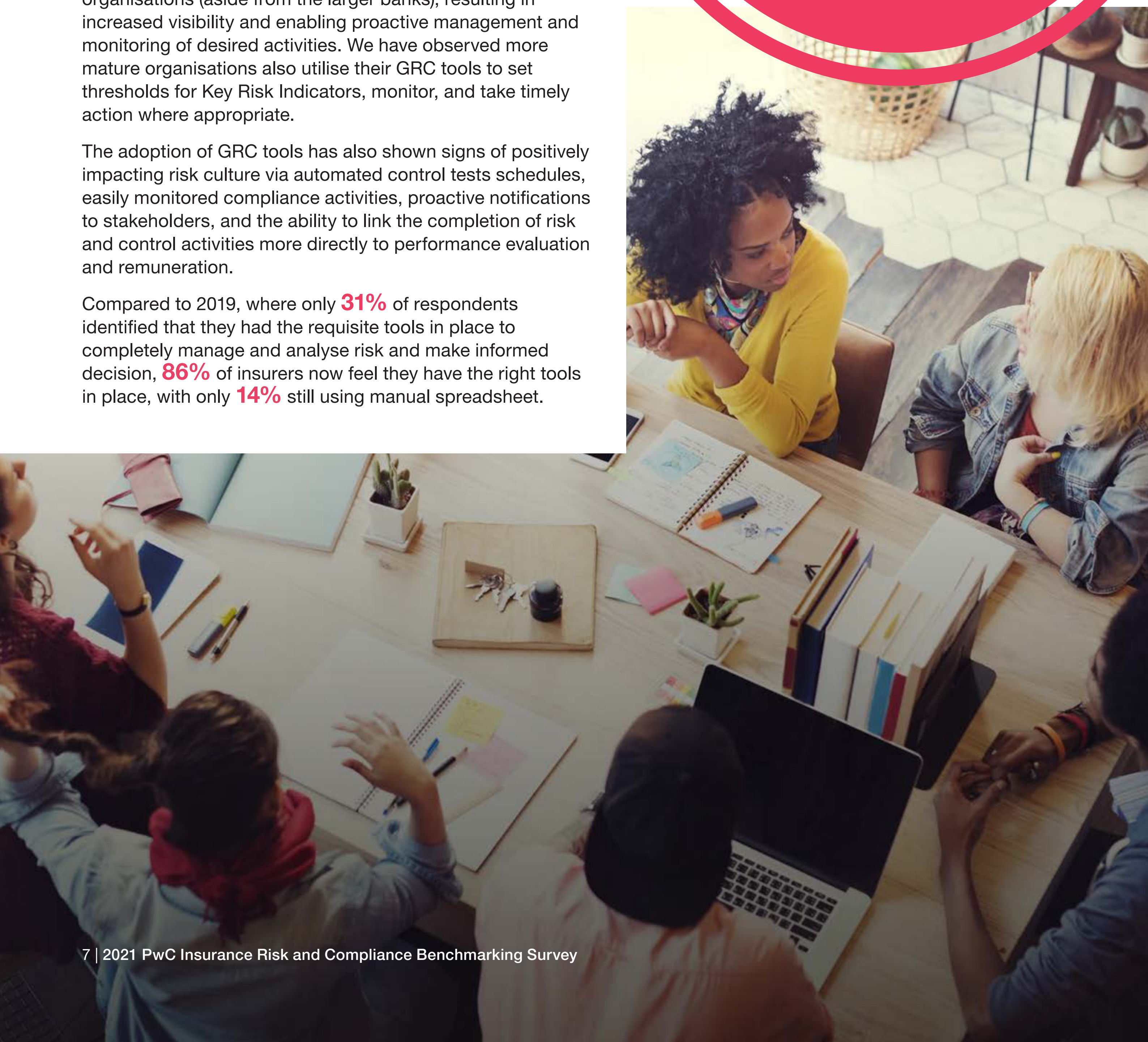
The reduction in cost of GRC solutions over the past few years has made adoption possible for a number of organisations (aside from the larger banks), resulting in increased visibility and enabling proactive management and monitoring of desired activities. We have observed more mature organisations also utilise their GRC tools to set thresholds for Key Risk Indicators, monitor, and take timely action where appropriate.

The adoption of GRC tools has also shown signs of positively impacting risk culture via automated control tests schedules, easily monitored compliance activities, proactive notifications to stakeholders, and the ability to link the completion of risk and control activities more directly to performance evaluation and remuneration.

Compared to 2019, where only **31%** of respondents identified that they had the requisite tools in place to completely manage and analyse risk and make informed decision, **86%** of insurers now feel they have the right tools in place, with only **14%** still using manual spreadsheet.

“Disparity in digital transformation efforts in financial services and insurance is often driven by the maturity and size of the organisation; while some industry leaders can afford to invest in advanced cybersecurity and privacy practices, lagging financial service firms may have more budgetary constraints.”

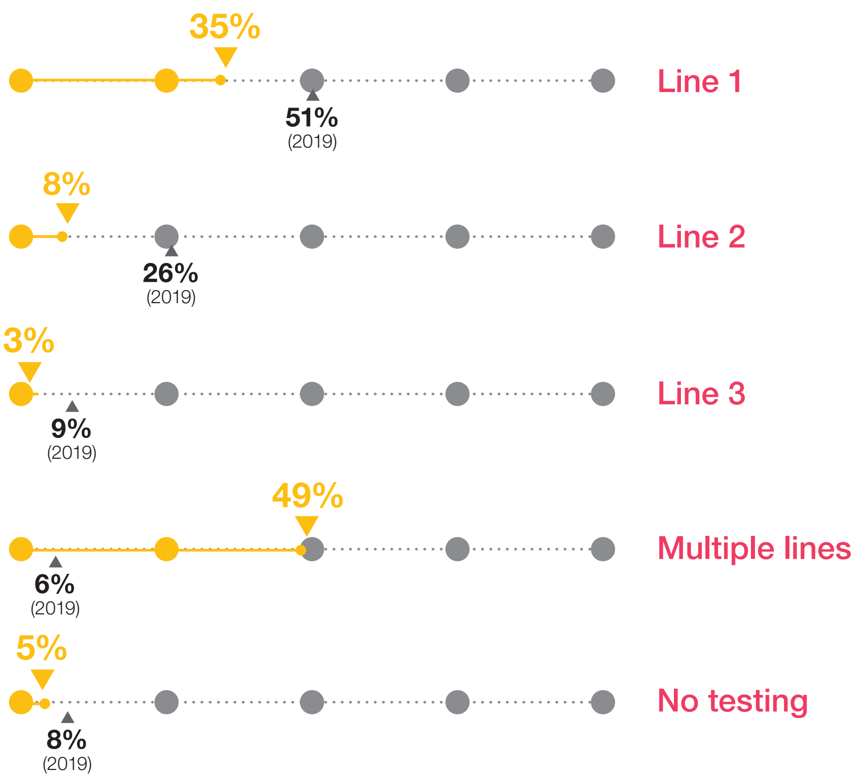
PwC Insights Forrester Report



Rigour of processes and controls

The extent to which risk and compliance obligations are mapped to controls has remained fairly consistent with 2019. The lack of progress may be attributable to COVID-19 (along with the move to a remote / hybrid working environment), as most insurers focused on ensuring the existing business processes and controls continued to operate without breakdown during the pandemic.

Responsibility for testing and monitoring of controls



The responsibility for testing and monitoring of controls has gradually shifted away from Line 1 and 2, to a broader focus across the business. Some insurers have already started to use the FAR as an opportunity to articulate who is accountable for risks, controls and associated monitoring and testing.

As we return to normalcy from COVID-19 in the near future, organisations should complement this momentum, with an investment in mapping obligations to controls before FAR formally comes into effect for insurance entities.

Governance over non-financial risks

Breaches

Average number of breaches

The average number of reportable breaches of those surveyed increased to **3.1** from **1.75** in 2019. There continues to be heightened scrutiny from regulators, and financial services entities have accepted that financial risks are not the only risks that matter.

Following the commencement of the *Financial Sector Reform (Hayne Royal Commission Response) Act 2020* on 1 January 2021, claims handling and settling services are now considered as 'financial service' under the *Corporations Act 2001* and organisations providing these services are required to hold an Australian Financial Services (AFS) License.

In December 2020, the Federal Parliament also passed legislation to strengthen the existing breach reporting regime for AFS Licensees, which is now effective for all reportable situations occurring on or after on 1 October 2021. Passage of this legislation follows the release of exposure draft legislation in early 2020 and a stakeholder consultation process. Key matters arising from the legislation are set out on this page.

1 Determine reportable situations within new timelines

Types of reportable situations are determined to be either a core obligation breach that is, or could be, significant; or additional reportable situations such as engaging in conduct constituting gross negligence or the Licensee has committed serious fraud.

A new concept of 'recklessness' has been included in the final legislation, so Licensee's must establish whether they had knowledge or a conscious awareness of a substantial risk of illegality.

Licensees are also to report to ASIC if they have commenced an investigation into a potentially reportable situation and that investigation continues for more than 30 days, in contrast with the 10 days specified in the exposure draft legislation.

2 Reportable situations in relation to other licensees

The Licensee is to report to ASIC within 30 days if the Licensee has reasonable grounds to believe that a reportable situation has arisen in relation to any other Licensee (AFSL or ACL).

3 Significance test expanded

For AFS Licensees, the breach will be significant if it is punishable on conviction by a penalty, results, or is likely to result, in material loss or damage to clients, a contravention of a civil penalty provision, or results in a breach of either sections 1041H(1) of the Act or 12DA(1) of the ASIC.

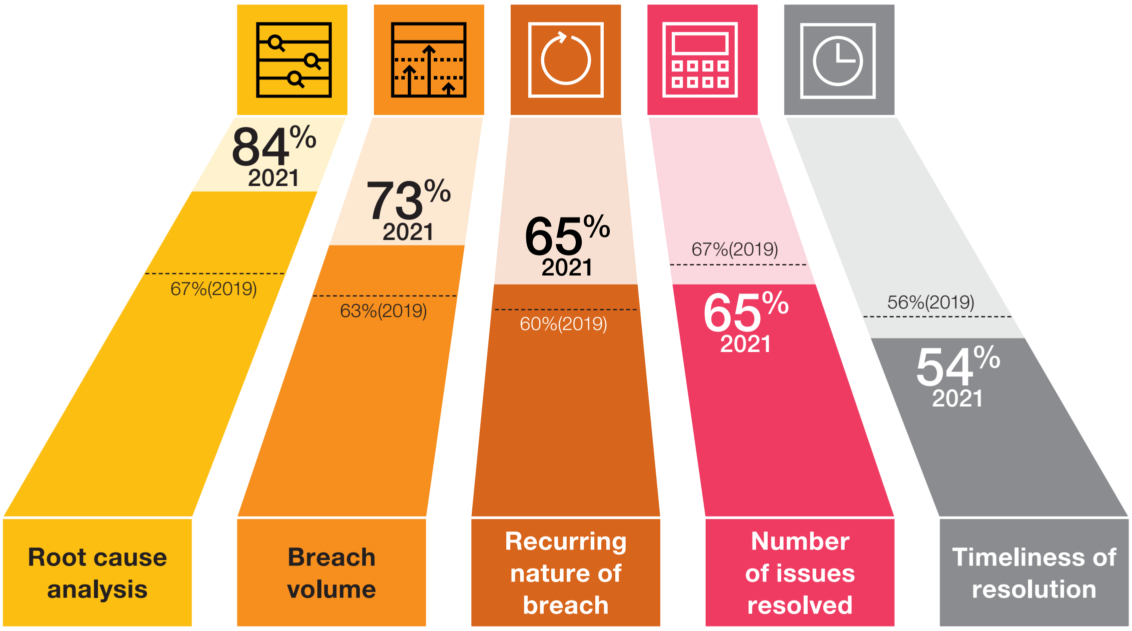
As insurers further establish responsibilities and accountabilities of the 3 Lines of Defence, the nature of trend analysis performed in relation to breaches has also evolved. **84%** of respondents are now performing root cause analysis compared to 61% in 2019, assisting insurers to limit the recurrence of similar breaches in the future.

Respondents also noted that the biggest barriers for the timely resolution of breaches remain lack of resourcing and system limitations.

Call to action

With the series of changes that have come into effect as a result of the strengthening of breach reporting regime, insurers should evaluate whether their current resource and system capabilities are appropriate to effectively manage their obligations, and make the necessary investments and enhancements.

Type of breach trend analysis performed



Complaints

Average number of complaints

681 2021

2019 685

Complaints trend analysis performed

78% 2021 VS 68% 2019

Root cause analysis

5% 2021 VS 13% 2019

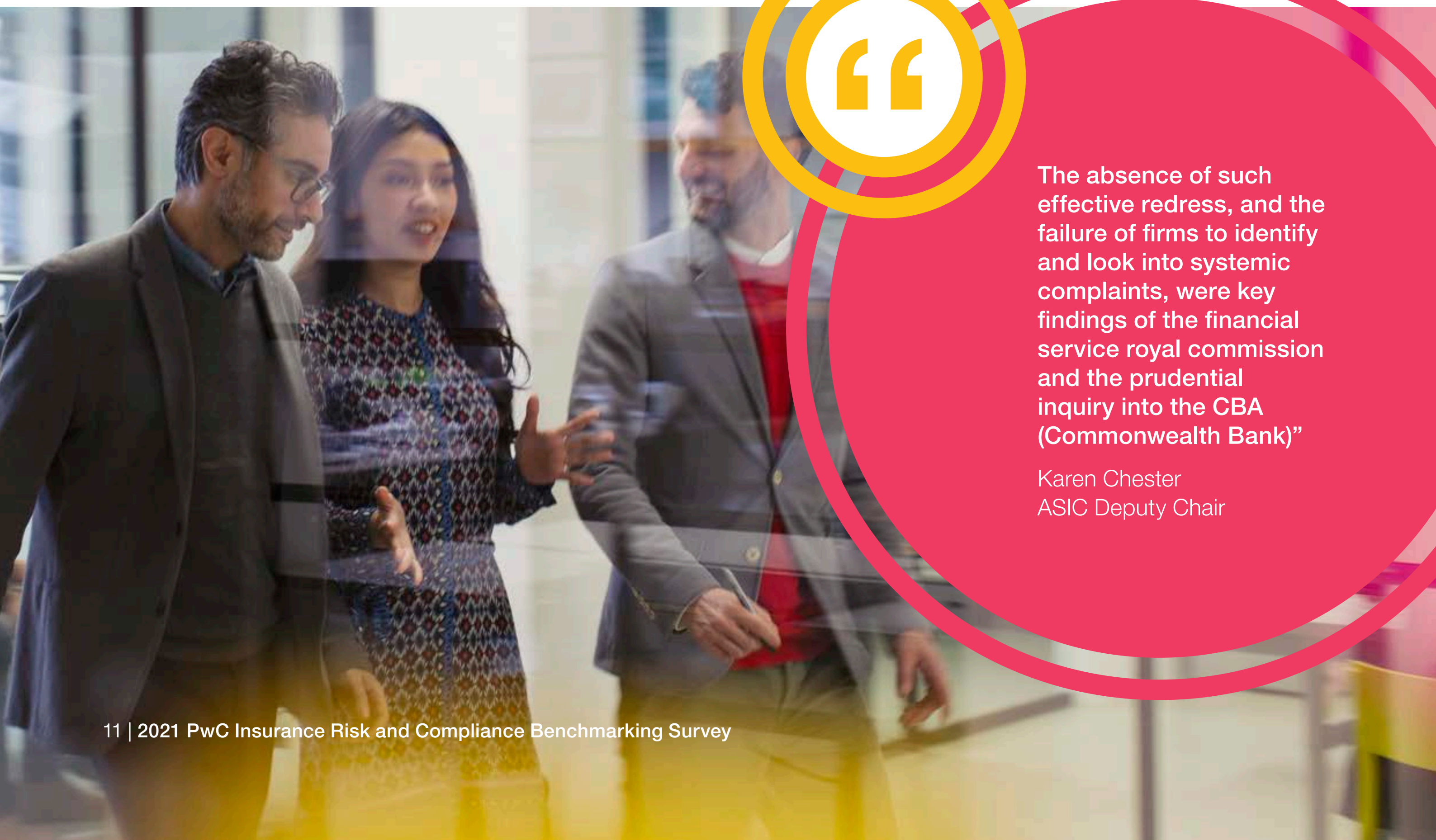
Not conducting any trend analysis

The average number of complaints received by insurers has remained broadly consistent between 2019 and 2021. Pleasingly, the majority of respondents (78%) have performed both a root cause analysis, and a trend analysis of complaints.

Timeliness remains central to effective complaint management and ensuring good consumer outcomes. A quantitative consumer research study conducted by PwC noted that the length of time taken to resolve the complaint directly impacts the complainant's view of the financial institution.

Respondents indicated that the biggest current barrier to timely resolution was again system limitations and lack of resources.

ASIC Regulatory Guide 271 *Internal Dispute Resolution* (RG 271), aims to ensure that complainants receive a final response in a timely manner by setting standards that are practical and achievable for financial institutions. The guide came into effect on 5 October 2021. For complaints received before that date, Regulatory Guide 165 *Licensing: Internal and external dispute resolution* (RG 165) applies, however this will be withdrawn on 5 October 2022.



"The absence of such effective redress, and the failure of firms to identify and look into systemic complaints, were key findings of the financial service royal commission and the prudential inquiry into the CBA (Commonwealth Bank)"

Karen Chester
ASIC Deputy Chair

Design and Distribution Obligations

Having recently come into effect on 5 October 2021, the Design and Distribution Obligations (DDO) are a fundamental shift in the way that financial products are created, monitored and provided to Australians. The design and distribution obligations are intended to help consumers obtain appropriate financial products by requiring issuers and distributors to have a consumer-centric approach to the design and distribution of products.

Issuers and distributors must implement and maintain robust and effective product governance arrangements to ensure that they comply. Product governance arrangements focus on measuring and monitoring actual consumer outcomes and are expected to be developed, implemented and reviewed. At the time of our survey, which has overlapped with implementation, **41%** of insurers were only at the identification, creation or mobilisation phase for product governance arrangements.

Some key considerations at different phases include:

Product design	Product distribution	Monitoring and review

For **product design**, a product development process that does not consider consumer outcomes will not be feasible. This includes designing a new product, as well as reviewing the design of a continuing product.

At the **product distribution** stage, product governance arrangements must include a process for effective communication between issuers and distributors.

There should be appropriate processes and controls to support "reasonable steps" which reduce the risk of distribution to consumers outside the product's target market.

For **monitoring and review**, product governance arrangements must provide an ongoing, iterative and responsive process in order to meet ongoing design and distribution obligations. An issuer should draw on information reasonably available about how consumers are using its product and the actual consumer outcomes.

41%
were only at the identification, creation or mobilisation phase.

Following implementation, the industry has been most challenged by the required data needed to comply, the reporting between the issuer and the distributor, and the interaction of DDO with financial advice. We anticipate that compliance with DDO will continue to evolve over time as data and systems mature.

Financial Accountability Regime

On 16 July 2021, Treasury released the consultation package which included the Exposure Draft and Explanatory Memorandum for the implementation of the FAR. The FAR is the government's response to recommendations made by the Royal Commission, and extends the Banking Executive Accountability Regime ("BEAR") to strengthen the responsibility and accountability of the directors and most senior and influential executives of financial institutions. The FAR follows many of the provisions of its predecessor, the BEAR, and includes both accountability and remuneration obligations.

The FAR will apply to all APRA-regulated entities, including all insurers and their Non-Operating Holding Companies ("NOHCS"). The draft FAR bill was introduced into Parliament on 28 October 2021 and is expected to be passed in the 2021 Spring Sitting. The proposed implementation date for insurers and their NOHCS is the later of 1 July 2023 or 18 months after commencement of the FAR following Royal Assent.

The FAR brings many benefits, which insurers are already beginning to realise. Of the insurers surveyed:

86% recognise that the FAR can provide greater clarity and transparency over roles, responsibilities and accountabilities

78% recognise that the FAR provides an opportunity to reinforce a culture of accountability and align and embed culture principles

A lesson learnt from implementing the BEAR is to not underestimate the complexity or time required to implement the regime. The survey indicates that insurers are beginning to undertake activities to ensure they are well prepared for FAR implementation with.

70% identified the accountable person population

41% drafted accountability statements and map

38% considered changes to their remuneration consequences framework

Calls to action

1 Consider your structure

Have you considered what FAR will mean for your organisation? Have you reviewed your entity structure and governance arrangements?

2 Reasonable steps framework

Develop a reasonable steps framework which supports Accountable Persons ("AP") in the discharge of their accountability obligations and identify gaps to remediate, through the review of key policies, processes, frameworks, charters and reporting.

3 Communicate effectively

How are you engaging and setting expectations with your key stakeholders to support FAR? How will FAR be communicated across the entity? Consider establishing a FAR project team to help obtain Executive buy-in and sponsorship.

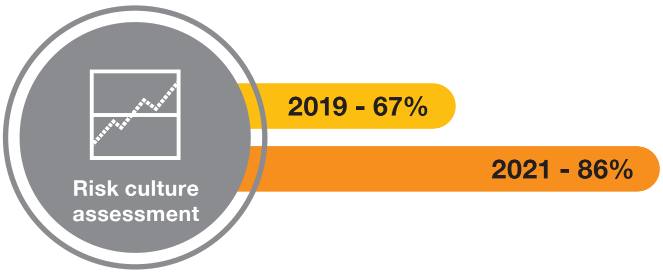
Risk culture

Risk culture is the interplay of organisational culture or the 'way we do things around here' with risk management. Risk culture is a fundamental part of an effective risk management framework and impacts an organisation's ability to manage risk and make robust decisions.

Performing a risk culture assessment

Organisations across all sectors and industries, are focusing on, and investing in, risk culture to realise strategic benefits and tackle vulnerabilities. We have seen some insurers appoint risk culture specialists (predominantly within the risk team) who are focused on uplifting the risk culture across the organisation. In conjunction with this, it is pleasing to see that **86%** of respondents have performed a risk culture assessment compared to **67%** in 2019.

Respondents that have performed a risk culture assessment

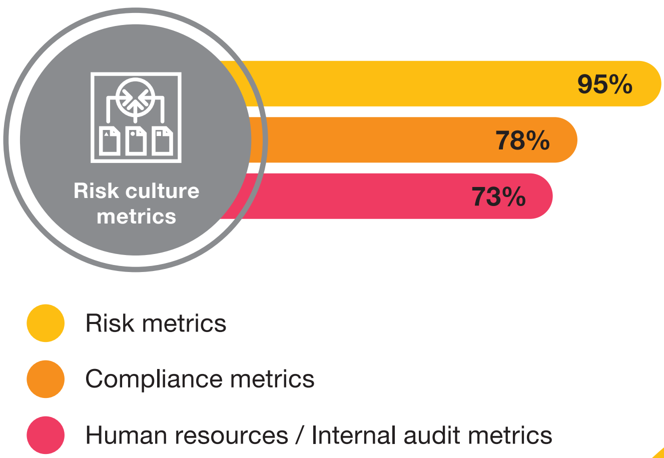


Surveys continue to be the most popular method for assessing risk culture, with **68%** of respondents either using a standalone risk culture survey, or including risk culture questions within existing employee engagement/ culture surveys. This response was broadly consistent with the 2019 and 2018 scores (**70%** and **67%** respectively).

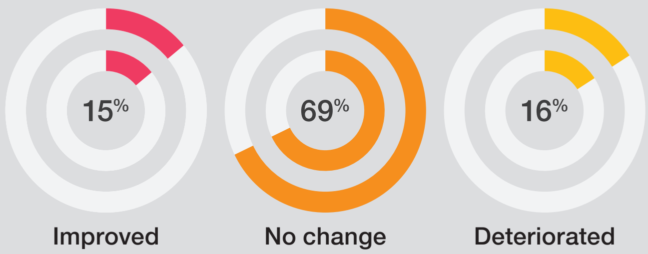
51% of respondents also noted that they utilise existing metrics/ KPIs as an input to understand their risk culture. Other methods, including the use of qualitative data gathering techniques, are also proving popular. For example behavioural observations (**43%**), interviews (**22%**) and focus groups (**27%**) respectively.

Whilst qualitative methods can be more time consuming and call for a specialist skill-set, they provide rich insights into the behavioural drivers and root causes behind the survey responses and quantitative data - an opportunity to understand both the 'what' and the 'why'.

Where respondents gather their risk culture metrics from



Impact of remote working on risk culture



The remote working environment posed a number of benefits and challenges for all insurers; changing the way we work, the risks we consider, and the potential risk culture implications.

Our work with clients has noted improvements in increased communication from leadership, more agile and nimble decision making and improved levels of trust and empowerment felt by employees. However remote working can also facilitate organisational silos, making day-to-day working more transactional which can have a detrimental effect on connectedness, collaboration and make sharing knowledge and lessons learned more difficult. We encourage insurers to lean into both these opportunities, and challenges, as future ways of working are finalised.

Defining the target risk culture

There is an increasing expectation from APRA for organisations to have a risk culture framework in place which articulates the target risk culture and subsequently demonstrates how they are measuring progress against it. **62%** of respondents have formally defined their target state, with a further **35%** planning on doing so next year.

Whilst the target risk culture needs to be bespoke for the organisation and reflective of its own circumstances (including operations, size and complexity), respondents identified the most common attributes of a strong risk culture as:

What do organisations identify as attributes of a strong risk culture?

- 86% Leadership/tone from the top
- 59% Accountability and responsibility
- 59% Speak up and escalation
- 38% Alignment of strategy with risk appetite

Measuring progress

Measuring risk culture is not easy. It is something that organisations are grappling with and approaches are evolving. Whilst metrics are commonly obtained from Risk **(96%)**, Compliance **(78%)**, HR **(73%)** and Internal Audit **(73%)**, challenges remain in the availability, applicability and quality of the metrics.

The common pitfall we see with risk culture measurement is organisations reporting on a range of 'risk culture type metrics' however it is unclear what they are measuring progress against (e.g. target risk culture). In the absence of this, and defined tolerances, it can limit the analysis and interpretation of the results, along with the ability to draw meaningful insights and conclusions to inform next steps and where intervention may be required.

More advanced approaches include developing a statistically validated measurement model with metrics identified and mapped to the target risk culture, leveraging the use of predictive analytics and artificial intelligence. Identified metrics include a combination of leading and lagging indicators, behavioural KPIs and perception, process and outcome measures. They focus on inputs, actual behaviours and behavioural outcomes.

APRA's risk culture benchmarking survey

Earlier this year, 10 general insurers participated in APRA's risk culture benchmarking survey. The survey was rolled out to all employees and consisted of approximately 40 questions covering APRA's 10 risk culture dimensions, as set out below. The participating entities received a report with their survey results, demographic insights and benchmarking comparisons against each dimension.

Risk Behaviour	Risk architecture
Leadership	Risk Culture Assessment and Board Oversight
Decision-making and Challenge	Risk Appetite and Strategy
Communication and Escalation	Risk Governance and Controls
Risk Capabilities	Responsibility and Accountability
Alignment with Purpose and Values	Performance Management and Incentives

APRA have noted that the areas with the greatest opportunity for improvement were:

- Risk governance and controls
- Decision making and challenge
- Accountability and responsibility

APRA is in the process of rolling out the survey to up to 60 more financial services institutions with general, life and private health insurers scheduled for Q1 2022.

Calls to action

- Develop a risk culture target definition and identify the supporting risk culture attributes and examples of desirable/undesirable risk behaviours.
- Develop a risk culture dashboard aligned to the target risk culture with metrics mapped to each attribute. Identity leading and lagging metrics with relevant thresholds.
- Incorporate and embed within core risk management and people processes.

Cybersecurity

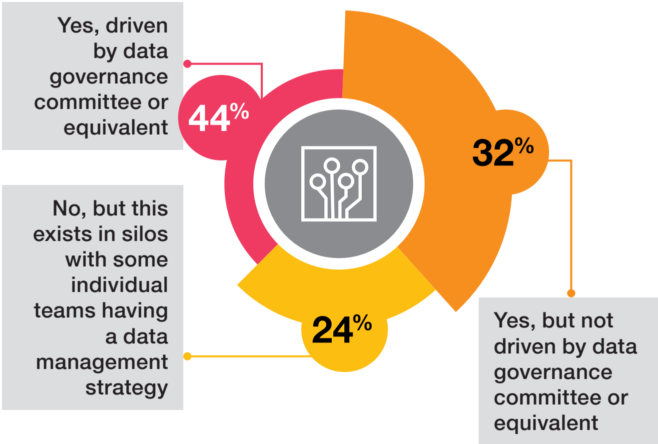
Similar to 2018, Cyber has been identified as one of the top risks for insurers in the current year survey. As a regulated entity, insurers are experiencing unprecedented scrutiny on how they govern and protect data due to the *Privacy Act*, APRA prudential standard CPS 234 and prudential practice guide CPG 235 *Data Risk Management*. This focus is set to continue with the recently launched APRA Tri-Partite reviews of CPS 234.

Additionally the Digital Transformation, Automation, Machine Learning and Artificial Intelligence technologies being pursued and adopted, are generating copious amounts of data that needs to be protected, and quality assured, in order to maximise the value of the information and insight and improve decision making.

Despite the scrutiny and focus by insurers, only **44%** of respondents currently have an enterprise-wide endorsed data management strategy driven by a Data Governance Committee or equivalent. A committee driven Enterprise-wide and endorsed data management strategy has the greatest chance of being successfully implemented. It also has the greatest chance of successfully supporting the broader business strategy.

Knowing what Information Assets to protect is foundational to information/cyber security, however survey **30%** of respondents do not have a formal mechanism in place to identify and manage critical data. Creating an information asset register that is complete and accurate requires a combination of policy, processes and technology. In addition, understanding the value of an insurer's critical data will be fundamental in creating the business case to protect it.

Enterprise-wide defined and endorsed data management strategy



"Global responses rated similarly, however a significant problem lies in the fact that cloud security and security analysts are among the roles in shortest supply. Hiring managers face tough competition in the labor market, and globally, some 3.5 million cybersecurity jobs are expected to go unfilled in 2021."

https://www.pwc.com.au/digitalpulse/digital-trust-insights-2021-the-need-for-cyber-resilience.html

https://www.csoonline.com/article/3571734/the-cybersecurity-skills-shortage-is-getting-worse.html?upd=1598452040833

https://cybersecurityventures.com/jobs/#:~:text=Over%20the%20eight%2Dyear%20period,to%20the%20MIT%20Technology%20Review.

Call to action

In order to address these challenges, insurers need to know their data, by focusing on a number of strategic questions:

- Do you know what data is being collected (registered)?
- What is the sensitivity and criticality of the data?
- Where does the data flow, including where is it stored and sent outside the organisation?
- How well governed and protected is the data, and who has access to it?

This will enable insurers to create a data strategy, and the business case, to get buy-in from across the breadth of the organisation.

ESG

Prioritising and evaluating the risk profile and materiality of the various ESG topics is crucial for companies to proactively approach ESG and embed it into, or align it with, the organisation's strategy and purpose. This is ideally complemented with appropriate Board oversight and transparent reporting.

ASIC recently undertook a surveillance exercise on climate-change related disclosure and governance practices of a cohort of large listed companies. They noted that the quality of disclosure still varies significantly with limited consistency in adoption, application and disclosure. The ASX Corporate Governance Council recently released the 4th edition of the Corporate Governance Principles and Recommendations which provides updates to principles requiring disclosure on the verification of periodic reporting, risk management strategies to include sustainability and climate change, and enhanced climate and other non-financial risk disclosure, with specific reference to the Taskforce.

"The more your company can show its purpose in delivering value to its customers, its employees, and its communities, the better able you will be to compete and deliver long-term durable profits for shareholders."

Larry Fink
Chair and CEO, BlackRock

Climate-related Financial Disclosures (TCFD).

38% of survey respondents indicated that they intend to adopt the recommendations of the TCFD, with **16%** already implementing them.

In addition to the recent announcements at the UN Climate Change Conference (COP26), regulator activities continue to increase, with a focus on transparency within capital markets. Examples include:

- APRA released its draft Prudential Practice Guide *CPG 229 - Climate Change Financial Risks* for banks, insurers and superannuation trustees on managing the financial risks associated with climate change.
- Australian Sustainable Finance Initiative (supported by APRA and ASIC) issued the Australian Sustainable Finance Roadmap in 2020, listing out 37 recommendations across different timeframes.

57% of survey respondents noted that Risk are involved in the design or operation of ESG related operational risk, such as the impact of climate change on insuranceliabilities and pricing of premiums. However, in respect of ESG matters in relation to decisions around an insurer's investment portfolio, **14%** of respondents currently say Risk have no involvement, and **54%** are only consulted if necessary.

While there is no one-size-fits-all approach, with the sharper focus by regulators, shareholders, and other key stakeholders, as companies increase their use of ESG information in decision making and reporting, Risk and Compliance will play an increasingly important role.

Risk teams' involvement will be crucial in ensuring appropriate controls exist to manage ESG risks, but understanding and helping to quantify the potential financial implications of these risks will require integration of risk management processes. Insurers therefore need to go beyond the current regulatory minimum. Only those companies which take a holistic approach – starting with their own strategy – will be able to stand out from the competition, manage emerging risks and pioneer new business areas.

Calls to action

The most immediate call for action is a combination of heightened regulatory requirements, risk awareness, and demand for data and transparency to enable the management and disclosure of ESG factors. As companies re-evaluate what they report publicly, formal non-financial disclosures are starting to augment or replace non-binding frameworks.

Investors/stakeholders are asking for greater transparency – in many cases, asking for much more than is required by financial reporting standards.

At a minimum, there is an expectation of insurers to demonstrate better linkage between the ESG disclosures, and the discussion on judgements and sensitivities in the financial statements. For example:

- How does the sensitivity analysis included in the ESG report link to the sensitivities presented in the financial statements?
- If nothing is presented regarding how management has assessed climate risk in the financial statements, is this consistent with the Operating & Financial review/ presentation of ESG report that considers these risks in detail?

Contacts

Sydney

Rod Balding
Partner
+61 2 8266 1324
rodney.balding@pwc.com

Renae Cooper
Partner
+61 2 8266 6471
renae.cooper@pwc.com

Scott Fergusson
Partner
+61 2 8266 7857
scott.k.fergusson@pwc.com

Scott Hadfield
Partner
+61 2 8266 1977
scott.hadfield@pwc.com

Voula Papageorgiou
Partner
+61 2 8266 7802
voula.papageorgiou@pwc.com

Chris Verhaeghe
Partner
+61 2 8266 8368
christopher.verhaeghe@pwc.com

Melbourne

Chris Braithwaite
Partner
+61 3 8603 1557
chris.braithwaite@pwc.com

Morven Fulton
Partner
+61 3 8603 3641
morven.fulton@pwc.com

Britt Hawkins
Partner
+61 3 8603 2785
britt.hawkins@pwc.com

Subject Matter Experts

Bernadette Howlett
National Insurance Leader
+61 2 8266 4720
bernadette.howlett@pwc.com

Sarah Hofman
Partner, Financial Services Regulation
+61 2 8266 2231
sarah.hofman@pwc.com

Nicola Costello
Partner, Digtal Trust and Cybersecurity
+61 2 8266 0733
nicola.costello@pwc.com

Craig Sydney
Partner, Digtal Trust and Cybersecurity
+61 2 8266 4938
craig.sydney@pwc.com

Katy Waterhouse
Director, Risk Culture and FAR
+61 2 8266 4937
katy.b.waterhouse@pwc.com

Claudia Warwar
Director, Digtal Trust and Cybersecurity
+61 411 258 375
claudia.warwar@pwc.com

pwc.com.au

127084310