2022 PwC Superannuation and Asset Management Risk and Compliance Benchmarking Survey

As part of our 14th annual survey we surveyed over 30 Australian Superannuation and Asset Management entities. The survey focused on three key areas impacting the sector - regulatory change, ESG and data risk management - and this publication summarises the resulting themes and challenges posed as well as providing calls to action in response.

www.pwc.com.au

Executive Summary

In the year that has passed since our last survey, the landscape within which the Superannuation and Asset Management sector operates continues to grow in complexity, with regulatory and public accountability on the rise across many operational facets.

The three key areas for consideration highlighted in this year's survey are:

1 **Regulatory change - increasing expectations and accountability**

Key regulatory implementations (ASIC's Design and Distribution Obligations, Internal Dispute Resolution, Breach Reporting and APRA's Superannuation Data Transformation Program) have occupied the industry taking significant time of risk and compliance functions and creating unprecedented levels of data for organisations to manage and report. Many organisation across the industry are still refining business as usual controls to meet their additional regulatory obligations.

2 **Environment, Social and Governance (ESG) - expectations on the rise**

Overseas regulatory developments in ESG have sharpened the focus and expectations of industry stakeholders domestically and highlighted for the sector that integrating ESG into your business strategy and operations is now a question of when, not if. A key element of success in integrating ESG into the decision-making of the superannuation and asset management industry centres around the ability of an organisation to influence the actions and business decisions of their investee companies in a meaningful way.

3 **Data Risk Management - an emerging landscape**

Key to a strong data risk management framework is the ability to assess criticality and sensitivity of data holdings, enabling delivery against legislative and regulatory obligations and ensuring the framework supports operational resilience.

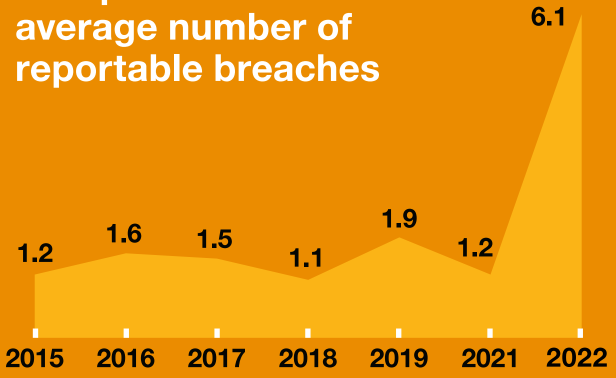
These recently introduced reforms, including the focus on ESG, are all aimed at achieving better member/investor outcomes. For organisations to meet this objective, they require better data to execute on their obligations more effectively.

We hope you enjoy reading this publication and that it provides some perspectives for further discussion and consideration within your organisation.

Survey by numbers

Over 30 survey participants across the Superannuation and Asset Management sector

Comparison of average number of reportable breaches

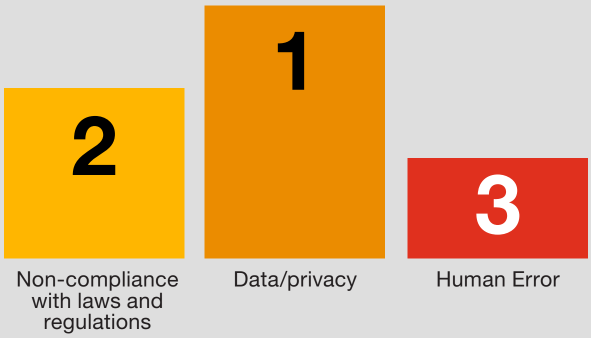


60% of participants offer ESG or Green products

On average **16%** of investor enquiries related to ESG

240% increase in complaints recorded post implementation of RG 271 *Internal Dispute Resolution*

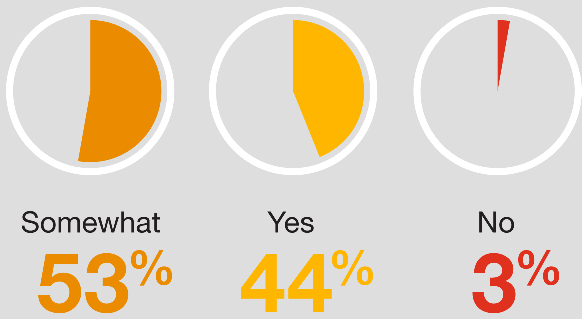
Nature of top 3 reportable breaches by volume



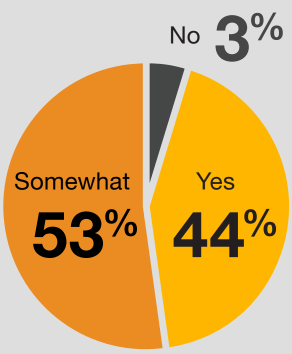
44% of participants experienced challenges meeting the new timeframe requirements of RG 271 *Internal Dispute Resolution*

30% of respondents do not report any metrics/items to the Board relating to DDO

Does your organisation have formal data risk management controls in place?



Percentage of Enterprise Risk Management frameworks which include and assess a taxonomy of Enterprise data risks



83% of survey participants have appointed an Executive owner for the implementation and effectiveness of data risk management

Regulatory change - increasing expectations & accountability

Last year's publication recommended a call to action that organisations treat regulatory change as a strategic opportunity to clarify responsibilities, improve accountability, connect with customers and improve operational processes.

We also recommended that organisations ensure future ongoing processes, controls and monitoring are developed and documented by internal implementation working groups, including accountability for each, to enable a smooth transition to business as usual.

Our engagements with organisations across the industry this year have indicated that for a number of entities, the timeline to implement significant regulatory change initiatives was condensed to a few months with a number of initiatives only implemented post the effective date of October 2021.

The introduction of the Financial Accountability Regime (FAR) will increase public scrutiny and accountability for those defined as Accountable Persons under the legislation. This means the need to continue to clarify responsibilities, improve accountabilities and embed new controls in BAU, remains a key strategic opportunity for organisations this year.

As ASIC's Product Design and Distribution Obligations (DDO), RG 271 *Internal dispute resolution*, RG 78 *Breach reporting by AFS licensees and credit licensees* and APRA's updated reporting as part of its Superannuation Data Transformation Program were only effective since late 2021, our experience is that many organisations are still in the process of formalising their controls to address the key requirements. In most instances, the controls have been implemented, however many controls are still being formalised and embedded. This is particularly the case for DDO which is a new legislation, whereas with RG 271 and RG 78 the focus has been predominantly on tightening the process to reduce the reporting timeframes and refining governance and reporting processes to manage the increase in the volume of breach reporting and complaints. As predicted in last year's survey, there has been a notable increase in what would have previously been considered insignificant incidents being reported, for example breaches impacting one member such as member statements not being sent or a unit pricing breach significantly lower than under the previous Financial Services Council industry guidance of 30 basis points. Our survey results have also highlighted that there has been a material uplift in the capturing of complaints following the introduction of RG 271. This increase leads to an increase in reputation risk for organisations and an impact on member/investor experience if not appropriately managed and responded to.

Though most funds met deadlines for APRA's new reporting forms and the recent introduction of the Retirement Income Covenant (from 1 July 2022), the relatively short period to implementation has meant in the case of reporting forms, a number of manual processes were used which will need to be automated, improved and documented going forward. The similarly short period to implement the Retirement Income Covenant means that though many funds have set their strategies for retirement, there will need to be further steps to implement and evolve these over the next twelve months.

We have also observed that the incorporation of Cyber Resilience and Business Continuity into Managed Investment Scheme (MIS) compliance plans continues to be an area of challenge for organisations, particularly the inclusion of appropriate obligations and controls and the level at which these are documented in the plans. ASIC has indicated they expect these to be limited to the key governance, monitoring and reporting controls in line with RG132.128 - RG132.130 *Funds management: Compliance and oversight*. For entities regulated by APRA there are obviously different expectations as outlined in CPS 234 *Information Security*, however, as superannuation trustees assess their compliance with the Prudential Standard they will inevitably look through to their service providers, which in many cases includes asset managers.

In light of the increased focus by both ASIC and APRA on superannuation and asset management entities, now is an opportune time for management to consider any learnings from recent regulatory change initiatives such as timeliness and accountability across Line 1 and Line 2 and to develop guidelines for upcoming regulations that outlines key milestones, stakeholder involvement and activities for delivery - particularly in light of the fact that the new remuneration standard CPS 511 *Remuneration* which comes into effect as early as 1 January 2023 for Significant Financial Institutions and the FAR is still expected to be implemented despite the change of Federal Government. As a key action arising out of the Hayne Royal Commission we do not expect the draft legislation to come off the table.

Calls to action

- Consider any learnings from recent regulatory change initiatives such as pre implementation testing, timeliness and ownership across Line 1 and Line 2
- Assess the formalisation of newly implemented key controls to determine whether these are adequately documented, including cyber controls in MIS compliance plans, and evidenced and there is appropriate governance oversight and reporting in place
- Keep the foundational principles of DDO and FAR at the forefront in the decision making process of your organisation
- Consider how you are handling incidents, breaches and complaints from a technology perspective - with so much data available are you making best use of the data to identify and report trends, root causes and themes?

Environment, Social and Governance (ESG) - expectations on the rise

ESG (Environmental, Social and Governance) considerations continue to be a key area of focus for Australian superannuation and asset management entities with organisations navigating through what ESG means for their investment strategy and engagement with their members/investors. Regulatory focus on ESG in the industry has heightened with the U.S. Securities and Exchange Commission (SEC) recently publishing proposed rules that cover, among other things, Registered Funds with names including ESG terms (Green, Sustainable etc.) to have 80% of underlying assets invested in a way that aligns with the fund's name. The proposed rules are aimed at protecting investors against misrepresentations of what a fund invests in based on its name - that is, protection against greenwashing. The SEC also released a proposed ESG disclosure rule[1] which would categorise funds into one of three categories; Integration funds, ESG-Focused funds and Impact funds with a sliding scale of disclosures required depending on categorisation.

Further, the Portfolio Holdings Disclosure regulations, which were effective 31 December 2021, will continue to bring ESG to the fore for superannuation trustees.

[1] https://www.sec.gov/rules/proposed/2022/33-11068.pdf

Consistency of public ESG commitments and actual activities is critical

Locally, in June 2022, ASIC issued an information sheet on greenwashing titled "How to avoid greenwashing when offering or promoting sustainability-related products" which highlighted a number of examples of disclosures to avoid - including using vague terminology, misleading headline claims and failure to disclose how and when sustainability targets will be met. With 60% of our survey respondents noting that their organisation's response to ESG has been to launch products specifically around ESG, the way products are described as well as the integration of ESG factors in the investment decision making process should be a key focus for organisations.

It is critical that companies begin to demonstrate consistency between public commitments and internal activities to manage and measure progress.

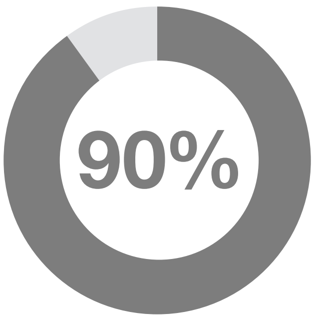
Of the survey respondents that have made a commitment to decarbonise their portfolios, 22% are measuring carbon intensity across all of their investments while 33% are measuring a subset of their portfolios. This potential gap between commitments and measurement will present challenges for those organisations unable to demonstrate progress to investors.

Influencing investee companies

A key element of success in integrating ESG into the decision-making of the superannuation and asset management industry centres around the ability of an organisation to influence the actions and business decisions of their investee companies in a meaningful way. With only 56% of respondents saying that they have the appropriate level of influence over an investee, organisations should challenge themselves on their engagement strategy with their portfolio and identify how best to use their team's time and resources to have the greatest impact. Some managers have taken an approach of focussing on a singular key ESG issue such as climate risk and engage with all of their investee companies on that basis, whereas other managers have taken a risk based approach and targeted investments in their portfolio which they believe have the greatest customer influence, for example the removal of tobacco or weaponry exposure. With the limited ability to influence investees noted in the survey, it raises the question around what actual levers exist to make the necessary changes to an investee and do organisations risk backing themselves into a corner unable to live up to the statements they have made to members and investors?

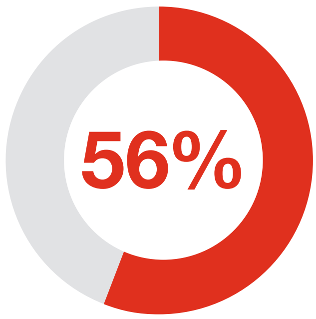
ESG - a key focus for all stakeholders

of investor queries are related to ESG topics



of survey participants feel that they have the right ESG skills versus a recent AICD survey which found less than 20% of boards had formal climate training[2]

of organisations offer ESG or Green products



of organisations can influence actions of their investee companies

[2] https://www.aicd.com.au/risk-management/framework/climate/climate-governance-study-risk-and-opportunity-insights-from-australian-directors.html

With 90% of respondents saying that they have the right skills when it comes to ESG, it shows that there has been significant upskilling in the market over the last few years. However, with the metric noted above regarding influence over investee companies, which although may be attributable to an organisation's size, some of these initiatives have yet to turn into action.

Future disclosure and regulation

From a reporting perspective, the Internationally Sustainability Standards Board (ISSB) has released their first two exposure drafts which provide an indication of their expectations for reporting in the future, the ISSB is planning to have the final standards issued by the end of 2022. The first standard (S1), which covers General Sustainability-related Disclosures, provides a framework as to how sustainability disclosures should be considered and reported whereas the second standard (S2) is specific to the area of climate. One of the appendices released (volume B15) as a part of S2 includes specific metrics for disclosures for asset management entities. Organisations should review the draft metrics and assess their readiness and begin to identify where gaps exist against these metrics. The ISSB has indicated that topics beyond climate will be released in future.

The ESG landscape from an investor, market and regulatory perspective continues to evolve and it is expected that the fast rate of change seen in the last year will continue - the Asset Management regulations coming out of the European Union will be in effect from January 2023, while the UK has released fund manager disclosure obligations with more to come, and the SEC will likely finalise their own reporting obligations for corporate entities. These changes will place additional obligations on fund managers themselves, as well as create more free-flow of ESG information that Superannuation Funds and Asset Managers will be able to use for their own reporting purposes.

Calls to action

- Assess your investment products and related disclosures against ASIC's information sheet on greenwashing
- Evaluate the effectiveness of your engagement with investee companies on ESG to date and determine if any refinements are required
- Assess completeness and accuracy of data that will be required under ISSB reporting requirements
- Where public ESG commitments have been made consider how these align with actual business practices and whether you have the processes and controls in place to deliver on these commitments

Data Risk Management - an emerging landsape

As countries all over the world adjust to the volatile and uncertain environment that we now operate in, there has never been a more important time for superannuation and asset management entities to ensure that the right people have access to the right data of the right quality at the right time to achieve their strategic, operational resilience, and member obligations.

Data risk management is fast becoming a boardroom and audit committee conversation with regulators increasing their focus on ensuring appropriate controls are in place for regulatory and market facing reporting, privacy and security management, and digital resilience.

Data is increasingly seen by regulators also as a tool for good, and expectations of the use of data to promote member outcomes, design customer oriented products and monitor for issues, have increased.

As the superannuation and asset management sector seeks to respond to these evolving threats and challenges, they are developing an increased understanding of the need for a systematic approach to baselining their data risk profile, and bringing data risks within appetite.

This need is further emphasised by the fact that privacy breaches were the most common breach type for survey respondents.

In PwC's experience, we have observed that data risks can manifest across a number of dimensions.

With proactive focus, organisation's can reduce risk and improve business performance and value.

Data Threats

- Inaccurate and untimely executive and operational reporting
- Data regulation breaches and cyber attacks
- Excessive spend resulting in 'point solutions' and untrusted data silos
- Disrupted transformation projects due to legacy data challenges
- Double handling and manual errors resulting in quantifiable costs

Defence | **Data Risk Management and Governance** | **Offence**

Data Risks Management Objectives

- Improved agility and oversight
- Protecting privacy, operational resilience and regulatory trust
- Increased ROI on data spend
- De-risking digital / Data-centric transformation
- Reducing inefficiency and waste

Maturity of the Superannuation and Asset Management sector

Our survey results highlight that while awareness of data risks is on the rise, formality of approach is on the whole somewhat immature:

76% of respondents have appointed an Executive with accountability for data risk management framework and controls implementation

83% of respondents are assessing the design and operating effectiveness of data controls in relation to data risks

46% of respondents have fully implemented data risk and/or data governance frameworks

36% of respondents have formally assessed and incorporated an Enterprise data risks taxonomy within their enterprise risk management framework and implemented assurance mechanisms

The survey results highlight that whilst the majority of the industry have an elevated appreciation of the importance of data risk management, significant focus is required to embed strategic risk management practices across the 3 lines of defence.

In the absence of a formal data risk management framework, organisations are exposed to:

1. Not having a clear understanding of the data sensitivity, criticality of their data holdings and exposures to mismanagement, both within the organisation and at third party service providers
2. Inability to deliver on legislative obligations
3. Inadvertently overlooking key data threats that could adversely impact operational resilience, financial performance, and reputation

Calls to action

- Appoint an executive owner to take accountability and drive ownership of data
- Catalogue and prioritise data holdings based on criticality and consider governance measures over data held by third party service providers
- Assess control adequacy to ensure critical data is secure, protected, and fit-for-purpose
- Proactively remediate data and control deficiencies identified

Contacts

Risk and Compliance

Deanna Chesler
Partner

deanna.chesler@pwc.com

Adrian Gut
Partner

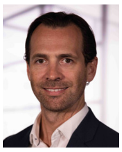
adrian.gut@pwc.com

Environment, Social and Governance

Diane Winnard
Partner

dianne.e.winnard@pwc.com

Data Risk Management



Jon Benson
Partner

jon.benson@pwc.com

WLTD0312083