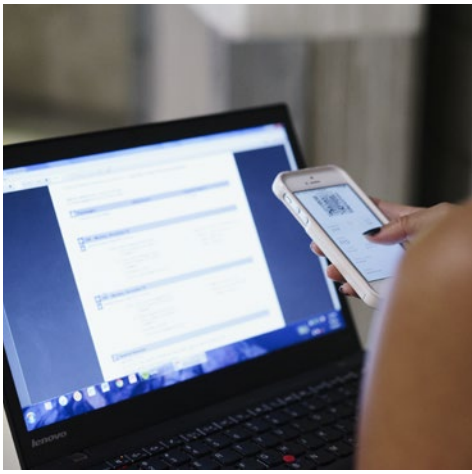
2016 Risk and Compliance Benchmarking Survey | August 2016 | *The Risk and Compliance landscape in Australia continues to experience rapid change, presenting both opportunities and challenges. Building on the themes we identified in our 2015 publication called 'The Emergence of New Threats', throughout this paper we highlight the insights gained from our latest Risk and Compliance survey as well as PwC perspectives on industry trends that will shape risk and compliance in Asset and Wealth Management and Superannuation (collectively referred to as the Wealth Management sector) in the future.*

Are you ready to manage risk and compliance in a digital world?

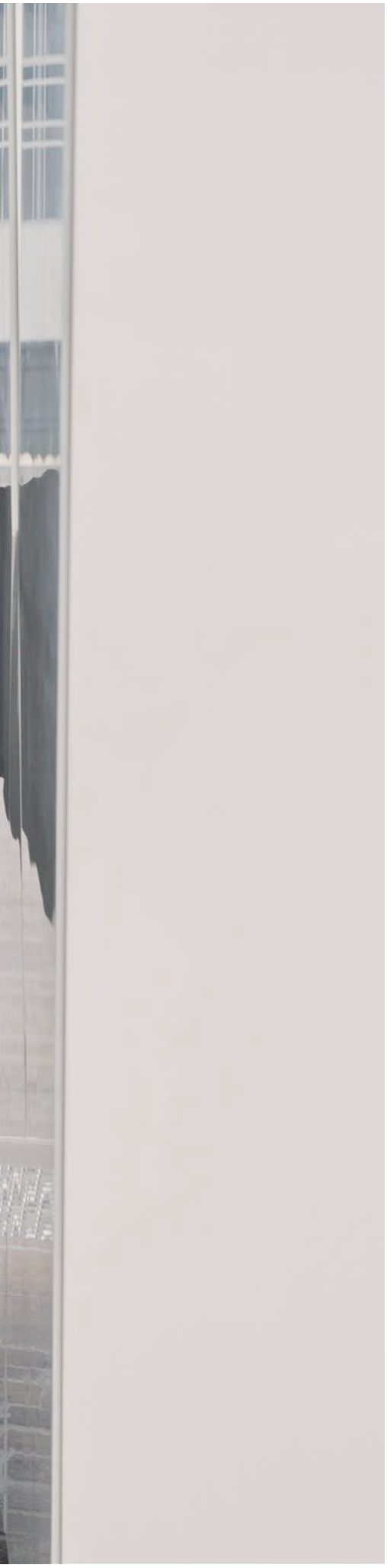


pwc

pwc.com.au

About the survey

PwC surveyed 55 Australian-based organisations across the Wealth Management sector in May and June 2016 using a combination of structured questions and open text responses. The size of those surveyed ranged from organisations with less than 20 total employees managing below $500 million in assets to 200+ total employees with up to $100 billion under management. We express our sincere thanks for those who participated in this survey.



Contents

Executive summary

We are pleased to share the perspectives we have gained in our 9th Annual Risk and Compliance Benchmarking Survey entitled *"Are you ready to manage risk and compliance in a digital world?"*.

Digital innovation is not new to the Australian financial services industry. Its scale and depth however is impacting all stakeholders. Whether it is the need for effective analysis of the growing volume of data being generated, the ongoing and increased threat of cybercrime or the prominent rise of the use of cloud technology, innovation is changing the way in which products are designed and services are delivered to customers and members.

Our report is split into three sections:

Current risk trends facing the Wealth Management sector

The pace of innovation in the Australian financial services industry is unprecedented and the Wealth Management sector is operating in a rapidly changing landscape. Organisations continually need to keep abreast at a minimum. Technology is at the centre of this and with it comes different risks and, if managed well, could translate into differentiating opportunities. In our report we discuss the following current risk trends facing the sector:

- **Enterprise-wide data management** – With more information and choices available to customers and members than ever before, most, if not all, in the Wealth Management sector are looking to adopt enterprise-wide data management capabilities. Formalised data management addresses not only adherence to industry and regulatory compliance[1] but also drives operational cost efficiencies and foundations for enhanced insights to support the organisation's digital strategy.
- **Continued rise of cyber security risk** – It is no wonder that cyber security continues to be one of the most significant risk categories that the Wealth Management sector is grappling with, as technological change continues to disrupt how organisations compete and create value in ways that often alter operating models.
- **Supplier risk management** – Outsourcing of functions continue to be prevalent in the Wealth Management sector. As innovation evolves, organisations are forming non-traditional alliances with different types of suppliers (e.g. use of cloud technology, gateway providers). There is a need for organisations to understand their supplier operations across a number of axis, especially when handling critical data.

The three biggest risk management challenges are...

Creating a **culture** that supports organisation-wide risk

Appropriately managing and monitoring **third party outsourced service providers**

Preparing for **cyber attacks** targeted against the privacy of consumer/member data and confidential information

In 2015, these were...

Operationalising policies and procedures that have been introduced to address increasing regulation

Managing **reputational risk**

Preparing for **cyber attacks** targeted against the privacy of consumer/member data and confidential information

[1]As laid out by *Prudential Practice Guide: CPG 235 – Managing Data Risk*, September 2013.

The burden of significant change exposes gaps in business as usual

There has been an uplift in the number of organisations reporting breaches across the Wealth Management sector compared to last year. We explore the reasons behind this rise:

- **Increasing reportable breaches a sign of the times** – The rise in reportable breaches can be attributed in part to the increasing burden placed on the Wealth Management sector to adjust to the fast-paced environment they operate in. This has drawn resources away from business as usual compliance.

The role of culture in risk and compliance

The use of culture to influence conduct, promote desired behaviours and identify the more pervasive problems organisations face is one way in which the Wealth Management sector is responding to stakeholder expectations. Our survey suggests there is a range of maturities within the Wealth Management sector when it comes to the following:

- **The culture dimension** – Government, Boards, Senior Management and regulators all acknowledge the impact creating the right culture has on identifying and managing risks. More organisations are using technology to monitor, reward and reinforce behaviours to align with the organisation's values.
- **Responsibility and accountability** – During this period of advanced innovation, it is encouraging to see that Boards and Senior Management are increasingly appreciating the value a clearly defined Three Lines of Defence/ Assurance model can have on managing current risks and identifying emerging risks.

George Sagonas
Partner, Assurance

Findings

Who participated...

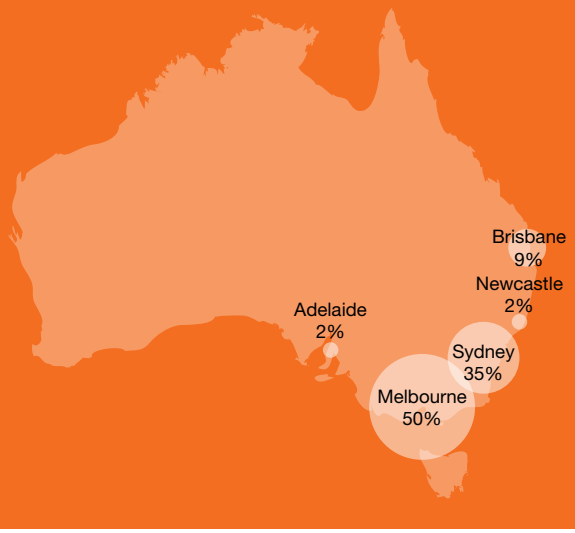
Entity type

● Superannuation Funds ● Asset & Wealth Managers

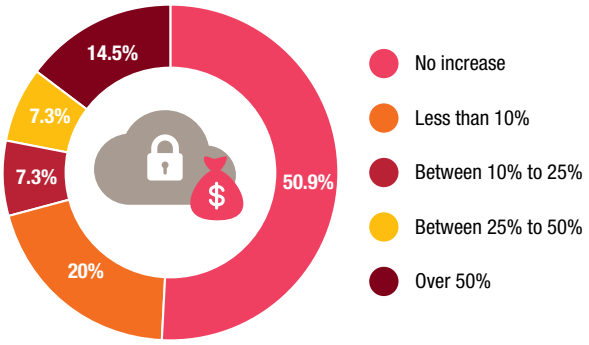
Assets under management

28% *37%* *22%* *13%*

Geographical location



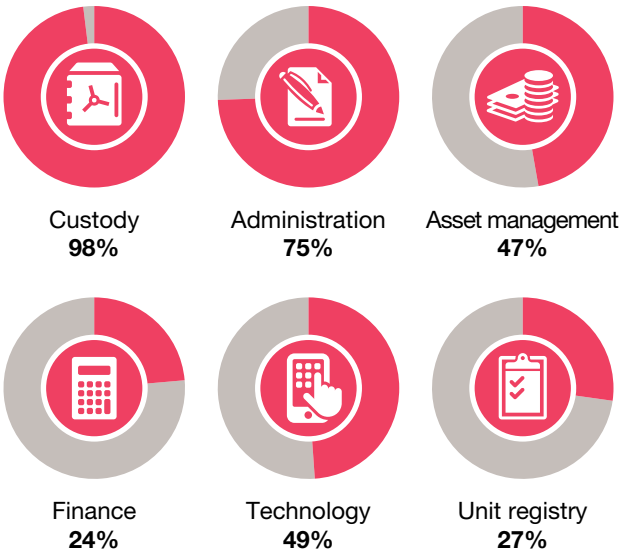
How much has your cyber security budget increased for FY16?



Site visits were ranked as the most effective way for monitoring external service providers.

76% of organisations ***test a range of scenarios*** as part of their disaster recovery framework.

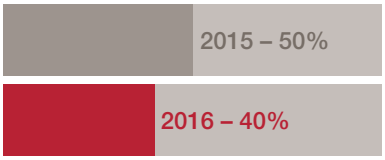
Percentage of respondents that outsource the following functions



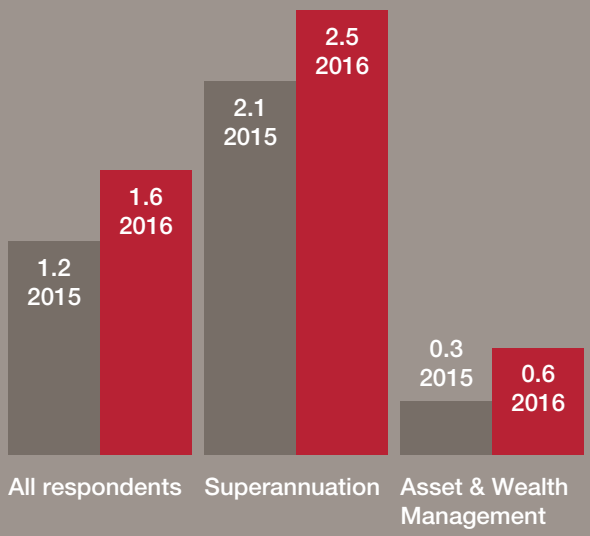
65% have performed a ***cyber security and privacy risk assessment*** and gap analysis.

58% *of respondents described their relationship with the applicable regulators as involving **regular** or **frequent and open** dialogue.*

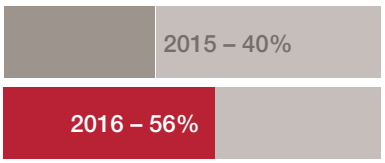
40% of the non reportable breaches disclosed by respondents resulted from service provider control failures.



1.6 The average number of reportable breaches per respondent for the year ended 31 March 2016.



*The percentage of respondents that had a reportable breach to either **ASIC, APRA, AUSTRAC** or the **Privacy Commissioner** for the year ended 31 March 2016 has grown to 56%.*

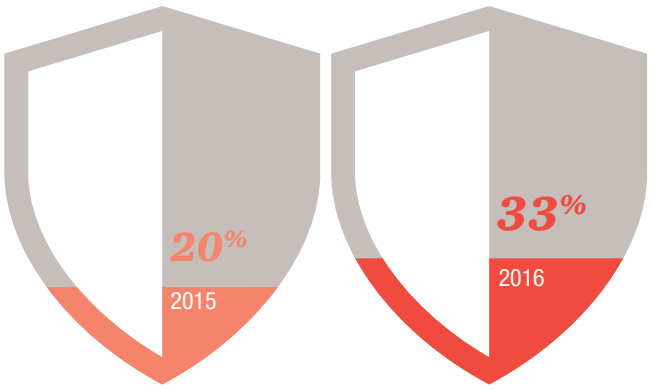


60% ranked creating a ***culture that supports organisation-wide risk*** in their top three risk management challenges.

91% *of organisations have **internal** Risk and Compliance functions*

55% of all employees are required to fulfil risk-related objectives or metrics as part of their annual goals.

33% of respondents indicated the three lines of defence model to manage risk within their organisations are highly defined.



*only **47%** of organisations have all the requisite tools available to completely analyse risk and make well-informed decisions.*

Current risk trends facing the Wealth Management sector

Enterprise-wide data management

How can strategic decisions be made without robust and mature data management?

Without effective governance, overall data management doesn't exist.

Data strategy: putting the puzzle pieces together

Organisations use data every day to achieve overall strategic goals. Governance around enterprise-wide data management is critical and risk and compliance can support the digital strategy in achieving these goals.

The initial focus of those in the Wealth Management sector is to better manage their data to meet regulatory requirements and secondly achieving a better customer/member experience, including cost reduction, process efficiencies and other operational insights.

As more focus is placed on achievement of the latter goals for data, establishing a robust data management strategy that is aligned with the organisation's strategic goals has become essential to obtaining stakeholder buy-in and driving the data management program forward to full maturity.

The increase in respondents with defined and endorsed data strategies demonstrates the focus in recent years of executive sponsorship, support and funding. As data management programs continue to mature, the corresponding data strategies will continue to become more stabilised.

A significant amount of respondents still continue to manage data in silos and on a tactical (reactive) basis. As data tends to be shared and utilised across the organisation, stakeholder buy-in and support increases significantly when data management exists as an enterprise function. The key is to involve the entire business (including IT), as full operational governance is lowest when data ownership resides only with technology teams.

83%

of respondents have implemented a data strategy of some sort

59% – Enterprise-wide

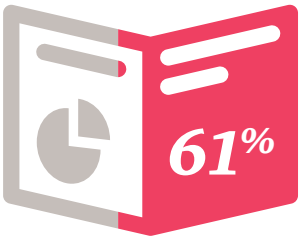
24% – Siloed within the organisation

Data governance: enforcement of policies and standards

In line with APRA expectations, data management should not be conducted in an ad hoc and fragmented manner. Organisations should adopt a systematic and formalised approach to data management, including the implementation of a hierarchy of policies, standards, guidelines, procedures and other documentation to support business processes.[2]

The implementation and enforcement of data management policies and standards indicate that within an organisation:

- Data management responsibilities have been established and assigned
- Data programs have owners (i.e. Chief Data Officer) and governance infrastructure
- Data management teams are becoming official functions with defined processes and have executive support
- Organisations are becoming serious about their data management capabilities



of respondents have documented and implemented data policies and standards to guide operational procedures and have assigned ownership to enforce these documents

Challenges to achieving good data management and governance

Implementing enterprise-wide data management and governance programs has proven to be a tough challenge for most in the Wealth Management sector especially when functional departments operate in silos.

The most common hurdles we see the sector facing are:

- Building an inventory of critical data, which takes time and requires significant coordinated efforts.
- Harmonising the meaning of data across hundreds of applications and repositories, which can prove to be a daunting challenge.
- Establishing effective, preventative data quality control processes (business rules, authorisations, etc.). Tactical "find" and "fix" is still the prevailing approach for data reconciliation.

Whilst the 2016 survey results reveal that there has been an uptake in the number of respondents implementing data management mechanisms over their critical data, 30 per cent of respondents are still victims of unravelling data lineage, overwhelming complexity of data flows and definitions, and incomplete data inventories that are aligned to compounding processes.

30%

of respondents have incomplete data inventories

Data governance practices are of particular importance when implementing SuperStream reform, with money and information consistently transmitted across the super system between employers, funds, service providers and the ATO. The importance and scale of SuperStream is echoed by the ATO who have labelled it as 'the largest compliance program in Australia since the introduction of GST'.[3]

In the end, if organisations do not fix the fundamentals, they will never be able to effectively clean, identify, integrate, manage, and utilise data effectively.

[2]As laid out by *Prudential Practice Guide: CPG 235 – Managing Data Risk*, September 2013

[3]ASFA/PwC CEO Superannuation Survey, *Superannuation: Successfully managing change,* November 2014

Continued rise of cyber security risk

Cybercrime keeps climbing

As highlighted in the PwC Global State of Information Security Survey 2016, *Turnaround and transformation in cyber security,* year on year, cyber attacks continue to escalate in frequency, severity and impact.

These global trends were also highlighted in our 2015 survey results and again in 2016, where respondents indicated that preparing for cyber attacks continues to be in the top three risks management face.

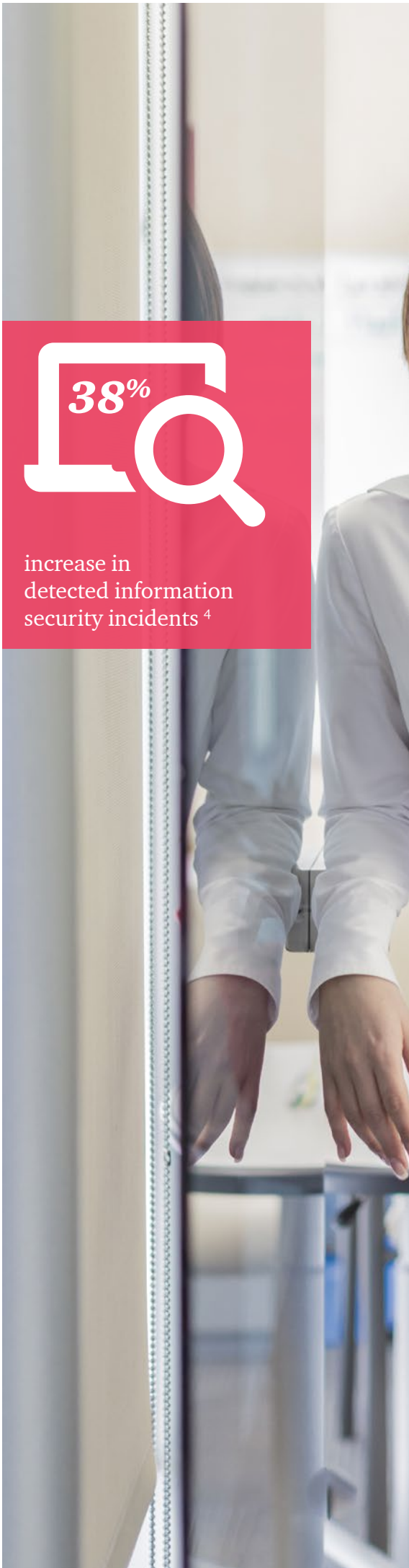
Some of today's most significant business trends – the explosion of data analytics, the digitisation of business functions and a blending of service offerings across industries – have expanded the use of technologies and data, and that is creating more risk than ever before. In addition, many executives see over-regulation as a prime long-term disruptive trend in their industries. Together, these issues illustrate why cyber security risks have become top of mind for leaders in business and government.

Whilst the prior year's survey results suggested there was a disconnect between this level of concern and the allocation of internal resources and investment to address the cyber security risks, the 2016 survey shows improvements in strengthening this connection.

Many executives are declaring cyber as the risk that will define our generation. As a result, businesses are taking an enterprise-wide business-oriented view of this important risk area.[5]

Dennis Chesley, Global Risk Consulting Leader for PwC

49%
of cyber security budgets have increased



[4] *Turnaround and transformation in cyber security: Key findings from the PwC Global State of Information Security Survey 2016*

[5] *Turnaround and transformation in cyber security: Key findings from the PwC Global State of Information Security Survey 2016*

The importance of the tone from the top

The increase in cyber security budgets suggests that the Wealth Management sector is investing in technologies to mitigate the risk of cyber threats. Yet the spotlight on technical advances can dim the focus on the roles, competencies and training of people – an often neglected, yet very effective defence.

There is no one more pivotal in cyber security risk mitigation than the top information security officer, typically the Chief Information Security Officer (CISO) or Chief Security Officer (CSO).

65%
have performed a cyber security and privacy risk assessment and gap analysis

It is a role whose responsibilities and competencies have become increasingly visible and critical. Today's CISO or CSO should be a senior business manager who has expertise not only in cyber security but also risk management, corporate governance and overall business objectives. They should have access to key executives to provide insight into business risks and should be able to competently articulate risk-based cyber security issues to the C-suite and Board.

Put simply, the cyber security leader should have the ability to effect change on par with C-level executives. However, it appears that the respondents are failing to leverage on their designated CISO or CSO to articulate risk-based cyber security issues to the C-suite and Board.

This is further reflected in PwC's 2016 Global Economic Crime Survey which highlighted that engagement of leadership is critical, but less than half of board members request information about their organisation's state of cyber-readiness.[6]

[6] *Adjusting the Lens on Economic Crime, PwC Global Economic Crime Survey 2016*

Supplier risk management

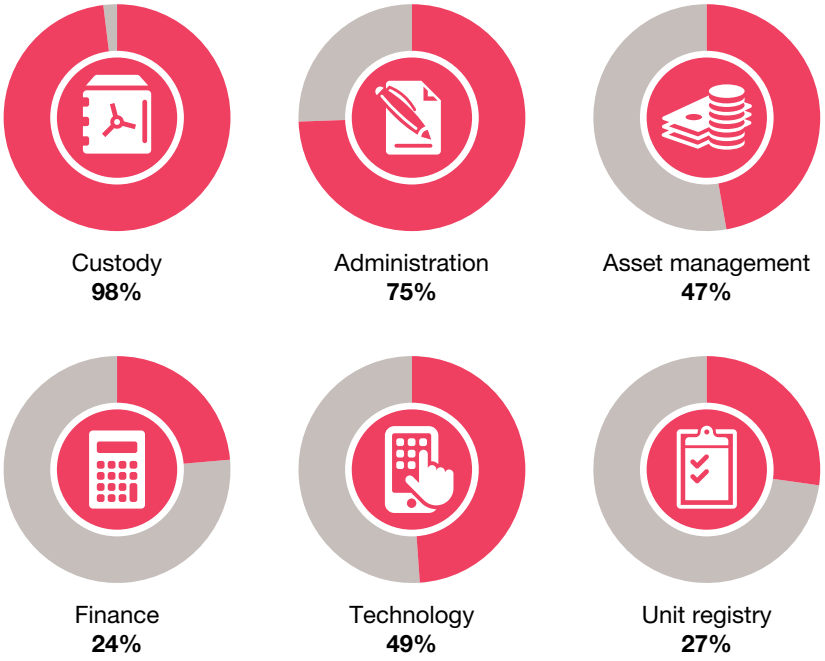
Changing technology impacting how functions are outsourced

With new standards for established Responsible Entities (REs) and Custodians of managed investment schemes coming into effect in January 2015[7], our 2016 survey results continue to show that outsourcing to service providers is still front of mind for respondents. The 2016 results show that custody, administration, information technology and asset management continue to be the key functional areas where material outsourcing arrangements exists.

In addition, the way in which functions are being outsourced is changing through the use of new technologies and increasingly critical data is being sent offshore.

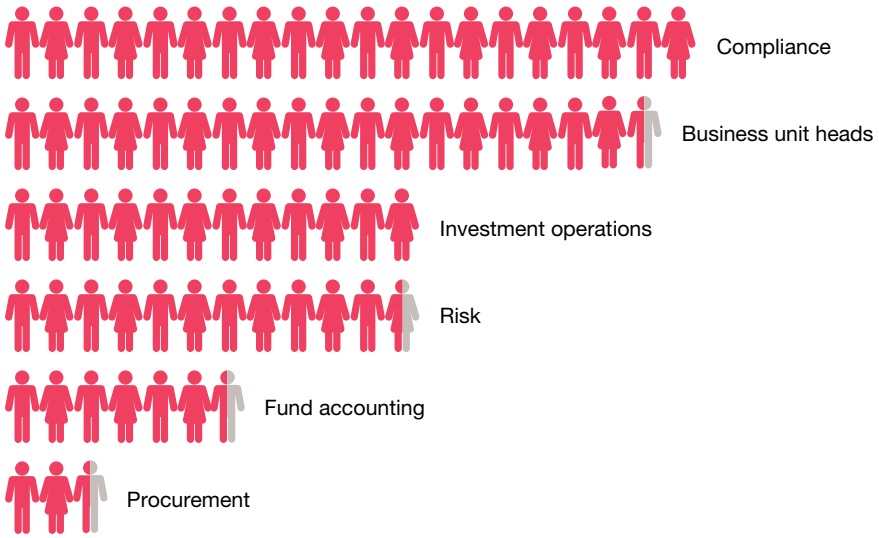
Against this backdrop, the Wealth Management sector must continue to efficiently oversee the third parties. The 2016 results demonstrate that the responsibility for monitoring outsourced providers continues to be led by the Compliance and Business Unit Heads, which indicates that monitoring is currently both centralised and decentralised amongst respondents.

Percentage of respondents that outsource the following functions



[7]ASIC Regulatory Guide 133, *Managed investments and custodial or depository services: Holding Assets*, November 2013

Who conducts monitoring over outsourced providers?



50% of respondents maintain data offshore

Consistent with prior year responses, site visits remain the most effective mechanism to monitor performance and compliance of external service providers. With the changing way in which functions are being outsourced, this approach may become more difficult to facilitate going forward.

Interestingly, self-attestations of third parties was consistently ranked as second even though the regulator has suggested that organisations should be doing more than simply confirming compliance.

Top three most effective ways for monitoring external service providers

A coordinated approach to supplier risk

A coordinated approach will give both customers and regulators comfort. We've highlighted the steps that organisations within the Wealth Management sector can take to achieve this:

- **Map out the risks of dealing with suppliers and outsourcing activities in the Risk Appetite Statement** – then set the level of risk that you are prepared to take with your outsourcing arrangements. Data breaches are increasingly being traced back to third parties, so it is important you know what data your suppliers have access to.
- **Understand, prioritise and categorise your supplier base** – some organisations aren't even clear who their suppliers are. Start by separating those suppliers who provide critical activities and pay special attention to those that handle your data. Make sure you take a risk based approach when prioritising.
- **Get a strong senior management level buy-in** – this is essential to integrate your third party risk plan into your wider Risk Management Framework.
- **Future-proof your procedures** – to deal with changes in both supplier landscape and the regulatory environment. Continuously monitor your supplier's risk levels. A low-risk supplier can be elevated to high-risk if they are given access to more of your data.

Disaster recovery framework has to be enterprise wide

With the increasing reliance of Asset and Wealth Management and Superannuation on third party data centres and service providers, the existence of an enterprise wide disaster recovery framework is critical. The existence of this framework helps businesses to recover or continue operations when there are technology based incidents such as cyber attacks, loss of critical IT infrastructure and applications, including data centres.

Scenario testing is often the most common type of disaster recovery exercise. It enables the facilitators to creatively plan interjections and test weak areas of the plans. Teams should increase the complexity of the scenarios for fully developed disaster recovery frameworks. This is just as important as conducting the exercise altogether. Thus, inclusion of dependencies such as key suppliers, internal teams, and IT is critical to truly understanding the recovery capability of a business.

The Wealth Management sector is not alone in seeking out how to achieve operational transparency over the security, availability, processing integrity and confidentiality in place to manage the handling of their customers' data.

Most in the Wealth Management sector gain assurance from third party control reports specifically in relation to the financial reporting process (referred to as GS007's). With the increased risks associated with data and cyber, there is an increased trend of GS007's expanding or other forms of assurance reporting being requested from suppliers.

76%
of organisations ***test a range of scenarios*** as part of their disaster recovery framework.

The burden of significant change exposes gaps in business as usual

Increasing reportable breaches a sign of the times

Rise in reportable breaches

Our survey shows there has been an uplift in the number of organisations having reportable breaches across the Wealth Management sector compared to last year.

Superannuation continues to report more breaches than Asset and Wealth Management.

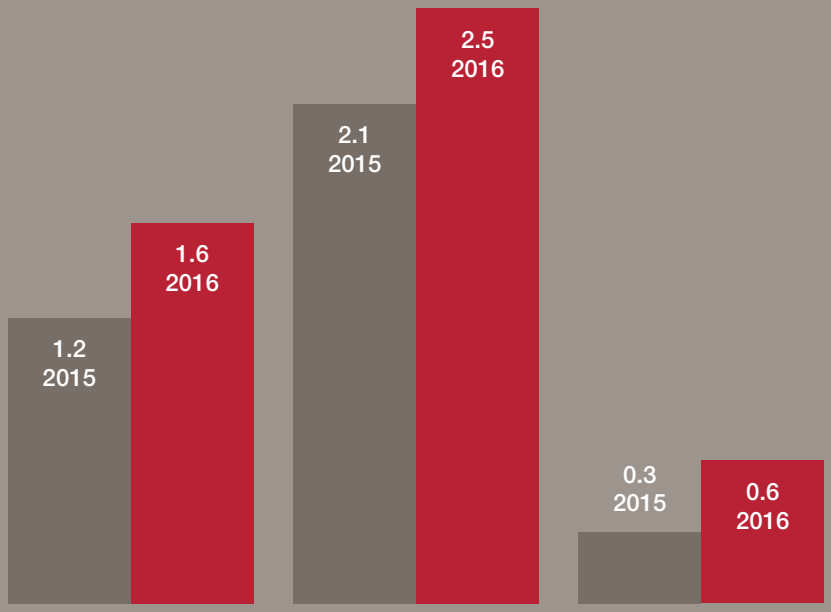
We believe the rise in the number of reportable breaches observed in this year's results is reflective of:

1. The increasing burden being placed on the Wealth Management sector to adjust to the constantly evolving environment they operate in which is competing for resources otherwise spent on business as usual compliance; and
2. A shift in the reporting culture of risk and compliance functions, acknowledging the increasing expectations of regulators relating to breach reporting.

Similar to the results in our prior year survey, the majority of breaches identified by organisations relate to non-compliance with laws and regulation, suggesting management and Boards are trying to keep up with the pace of regulatory change facing the industry whilst managing day to day transactions.

Innovation is increasing the automation of processes and volume of data being generated. This will lead to breaches being more systemic in nature. As a result, the use of data analytics to identify incidents and breaches is expected to increase in the future.

1.6 The average number of reportable breaches per respondent for the year ended 31 March 2016.



56%
of respondents had a reportable breach to either ASIC, APRA, AUSTRAC or the Privacy Commissioner for the year ended 31 March 2016

40%
of respondents had a reportable breach to the year ended 31 March 2015

One area of non-compliance which has been a trend across Superannuation is the failure of the RSE licensee to complete a standard rollover no later than three business days after receiving the request in accordance with SIS r. 6.34A.

Disclosure requirement breaches have also been common and are particularly topical with the upcoming Regulatory Guide 97. The new rules are designed to provide accuracy and consistency in the disclosure of fees and costs in Product Disclosure Statements and periodic statements across Asset and Wealth Management and Superannuation and are effective 1 February 2017.

Furthermore, of the total 2,200 non reportable breaches disclosed by respondents, 40% of these were as a result of a control failure by service providers, compared with 50% in the prior year. We believe the reduction demonstrates the increased focus organisations are placing on monitoring activities over service providers. We have also noted an increase in incidents and breaches being raised by first line teams across the larger organisations, which indicates an increased awareness of breach reporting by the business.

When is a breach a breach?

One of the ongoing debates within the industry centres on the length of time it should take for an organisation to report a breach to the regulator. We have seen some organisations report all breaches, including potential breaches, within the defined time frames outlined by the regulators as they continue to investigate the root cause and significance of the potential breach. Other organisations consider the breach reporting period to have commenced only from the time that the breach is formally assessed as a reportable breach.

Having clear expectations of what constitutes a breach and when it needs to be reported is of particular importance in the Wealth Management sector where outsourcing of key functions is common practice.

Such operating models result in additional layers in the chain of command, which can add interpretation risk and create a potential lag in reporting.

Consistent with last year, the nature of complaints raised by members continue to be around poor customer service, product fees and account maintenance issues.

Regulator engagement

Year on year we have seen an increase in the interactions organisations are having with the regulators, a direct response perhaps to the constantly changing environment they are operating within.

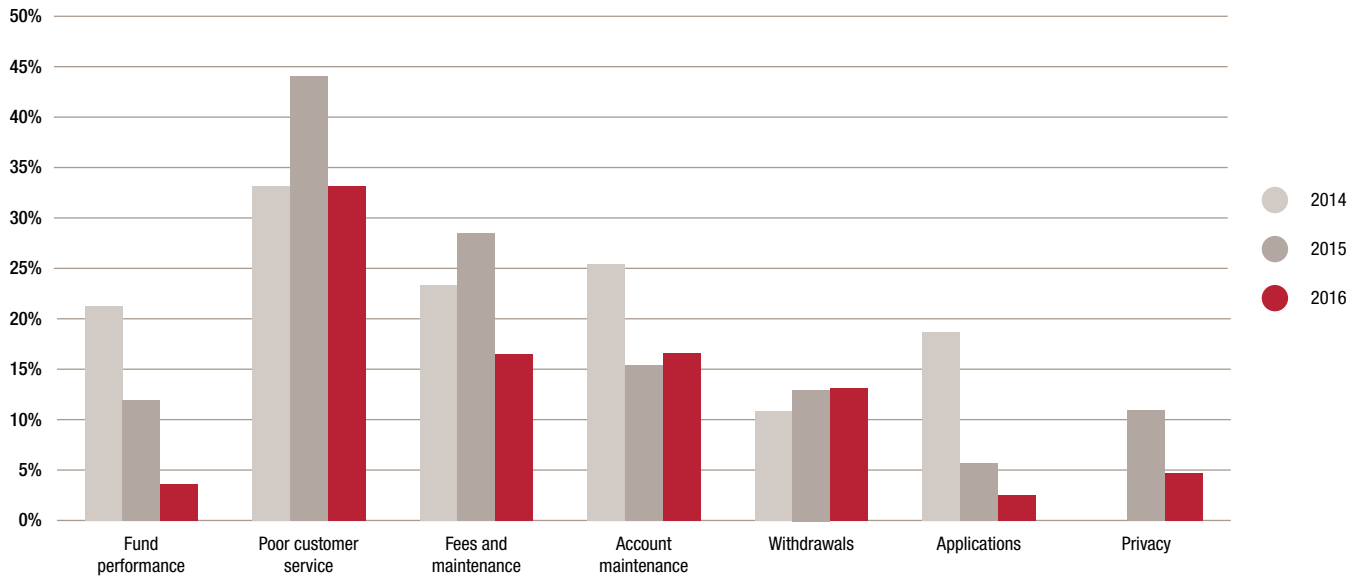
These respondents have indicated more regular interactions with the regulators over the past 12 months and attend industry forums where regulators are present.

57%

of respondents rated their relationships with the regulators as positive

That's an increase of ***21%*** from 2015

Nature of complaints



The role of culture in risk and compliance

The culture dimension

The importance of creating the right culture

Government, Boards, Senior Management and regulators all acknowledge the importance of determining and identifying the right culture to deliver the right outcomes for all stakeholders.

How organisations measure culture is evolving.

Recruiting the right people

People and culture are the first line of defence in managing risk. Developing a culture that is aligned to the strategic objectives of an organisation is key, especially with technological innovation changing the way that the Wealth Management sector is doing business.

Building the right culture starts with recruiting and retaining the right workforce.

90%

of respondents felt that their organisations recruited individuals with the requisite skills to recognise and escalate risks

95% – Asset & wealth management

86% – Superannuation

Organisations are experiencing considerable turnover in risk and compliance roles. Recruiting good personnel that fit into the culture of the organisation is proving challenging.

Fostering the desired culture requires a strong tone from the top, whereby target behaviours and conduct is aligned to the organisation's risk appetite.

Just over half of respondents recognised that risk related objectives and metrics impacted their annual performance review and ratings.

55%

of respondents recognised the link between performance review results and risk related objectives

of respondents have a risk culture that encourages escalation of business risks to senior leadership

67%

of respondents responded that they use a professionally developed risk and compliance program

However there was recognition that further tailoring to the software is required for the system to be completely integrated into their organisation.

Measuring culture

Consequence management is evolving, with a significant number of those surveyed yet to establish clear incentives or consequence management frameworks that are impacted by observed conduct. Those more advanced in the monitoring of behaviour are linking KPI's of observed conduct to remuneration structures.

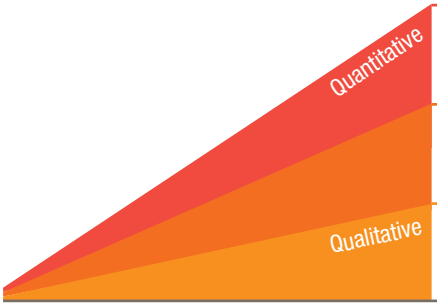
In many organisations culture and conduct are managed in a top-down, passive way through codes of conduct and training. An organisation in the early stages of measuring culture and conduct will tend to deep dive into the data and use data analytics to visualise behaviour. This analytical approach looks at the actual outcomes that have been measured and produce information about what has happened, including things that have gone wrong.

More advanced organisations keep track of leading indicators, such as a misselling of financial products to customers and members. These indicators are generated in real time to monitor conduct and culture.

Participants indicated opportunity for improvement to existing functionality of IT systems used to manage risk within their organisations.

There was a very strong sense of a supportive culture that encourages the escalation of business risks to senior leadership in both Asset and Wealth Management and Superannuation.

Continuum of Culture and Conduct measurement

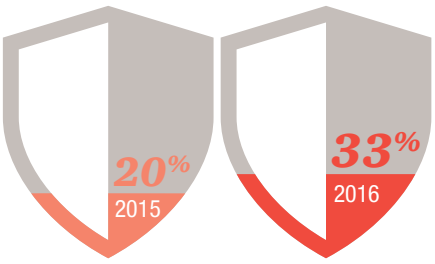


Leading Edge	Analytics in real time	Strong data quality	Triangulation of data sets
Emerging	Data analytics on historical data sets	Data quality improvement initiatives	KPIs to measure and monitor
Basic	Codes of conduct	Guidelines for BAU	Targeted conduct training

Responsibility and accountability

Organisation wide responsibility

The importance of culture as a key driver of conduct within the financial services industry has been highlighted by the regulator[8], with a particular focus on an organisation-wide appreciation of risk management, risk and compliance teams and staff roles and responsibilities across the three lines of defence.



of respondents indicated the three lines of defence model to manage risk within their organisations are highly defined.

This year on year growth suggests Boards and Senior Management are starting to appreciate the value this model can bring to their organisations when managing risk.

Understandably smaller organisations with limited resources at their disposal do struggle to implement a highly defined three lines of defence model, with segregation of roles and responsibilities between risk management and the business harder to achieve.

Management recognise the importance of risk management and the need for focus and expertise to address the continuous regulatory change impacting their organisations.

This is echoed by ASIC who have proposed to provide guidance to responsible entities on their expectations to maintain adequate risk management systems.[9]

65%

of respondents indicated staff responsible for risk and compliance roles within their organisations have a pure stand-alone role and do not double hat responsibilities across risk and compliance.

This is a ***30%*** increase compared to last year.

[8]ASIC Speech, *Tone from the top: Influencing conduct and culture*, 21 June 2016

[9]ASIC Consultation Paper 263, *Risk management systems of responsible entities: Further proposals*, July 2016

Contacts

Melbourne

George Sagonas
Partner
+61 (3) 8603 2160
george.sagonas@pwc.com

Nicole Oborne
Partner
+61 (3) 8603 2914
nicole.oborne@pwc.com

Grace Guinto
Director
+61 (3) 8603 1344
grace.guinto@pwc.com

Owain Norman
Manager
+61 (3) 8603 0458
owain.a.norman@pwc.com

Sydney

Craig Cummins
Partner
+61 (2) 8266 7937
craig.cummins@pwc.com

Carley Bryce
Partner
+61 (2) 8266 2028
carley.bryce@pwc.com

Deanna Chesler
Director
+61 (2) 8266 0003
deanna.chesler@pwc.com

Adelaide

Kim Cheater
Partner
+61 (8) 8218 7407
kim.cheater@pwc.com

Brisbane

Paul Collins
Director
+61 (7) 3257 8558
paul.d.collins@pwc.com

pwc.com.au

127041779