2015 Risk and Compliance Benchmarking Survey / July 2015

The emergence of new threats

pwc.com.au

Contents

Introduction

Welcome to our Risk and Compliance Benchmarking Survey for 2015 – PwC's eighth annual survey of Australia's leading Asset Managers and Superannuation funds which aims to give Risk and Compliance function leaders a view of how their peers structure and staff their organisations and the biggest risk factors they face.

Each year we evolve the survey based on feedback from participants and incorporate hot topics while keeping a core set of questions for comparison purposes. This year we have again integrated insights from recent global PwC surveys to provide an international perspective.

We received 40 responses to our 2015 survey from Risk and Compliance executives – roughly the same total as in 2014. Survey responses received were evenly split between Asset Managers and Superannuation funds, with funds under management ranging from under $1 billion to over $50 billion.

Our survey results were consistent in detailing what Risk and Compliance functions believe will impact them the most going forward.

Operationalising policies and procedures that have been introduced to address increasing regulation is seen as a top threat to business growth. With the continual wave of new regulation being imposed on the Asset Management and Superannuation industries, implementing an appropriate governance structure is fundamental in adequately managing operational risk.

Reputational risk was another concern to respondents. The monitoring and timely resolution of complaints and breach reporting is important, especially with the dependence on third-party relationships.

A business threat gaining prominence is privacy and cybersecurity. The survey results show that there is a range of maturities when it comes to managing privacy and cybersecurity risk. In addition the survey results suggest there is a disconnect between this level of concern and the allocation of internal resources and investment to address these risks.

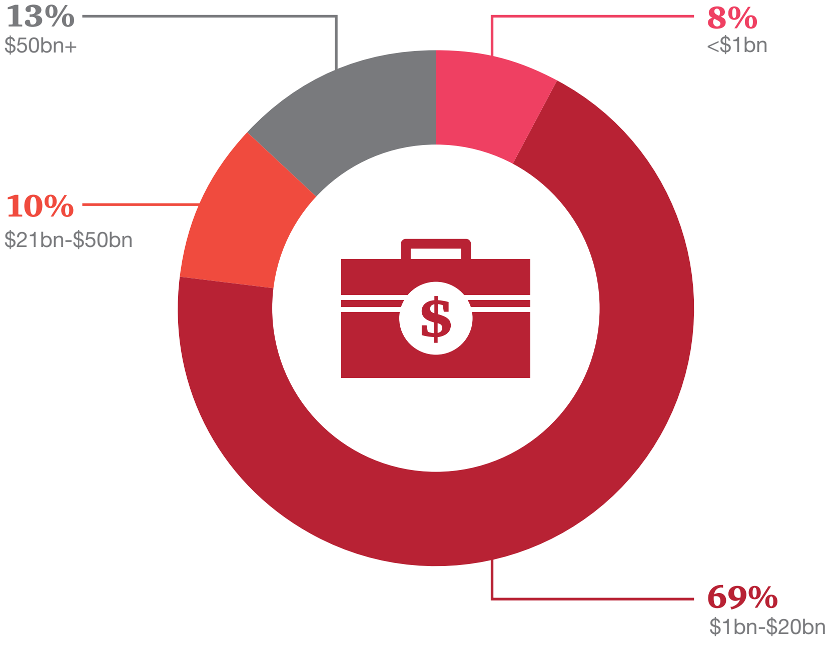
Developing a culture that embeds risk and compliance into the day to day tasks of those outside the Risk and Compliance function will help organisations turn these risks into opportunities.

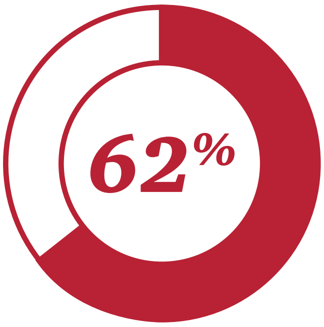
We hope you find the information in the 2015 PwC Risk and Compliance Benchmarking Survey insightful and valuable.

George Sagonas
Partner, Assurance

Highlights

Respondents' funds under management





Have yet to perform a privacy and cybersecurity risk assessment and gap analysis, with 16% not planning to do so soon.

Top 3 risk categories organisations are most concerned of

Operational risk **54%**

Reputational risk **46%**

Cybersecurity & privacy **44%**

Of the total **1,300 breaches** identified over half were the result of a control failure by external service providers

No respondent recorded a reportable privacy breach to the Privacy Commissioner during the fiscal year.

Similar to last year, 95 per cent of respondents suggested they operate, to varying degrees, a Three Lines of Defence model.

95%

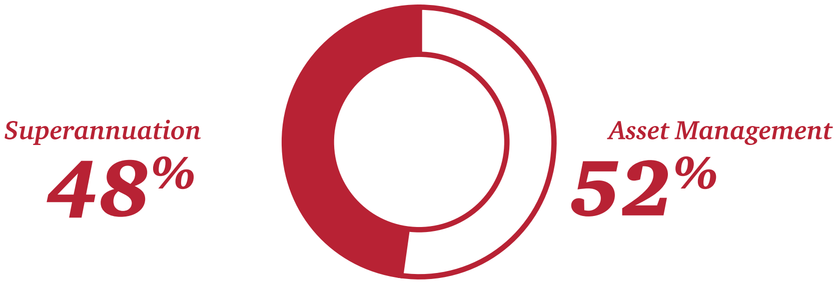
Out of those respondents, only 15 per cent felt that the lines of defence are highly defined and clearly demarked with a strong understanding of roles and responsibilities.

15%

56 per cent of respondents stated that there is a fair degree of overlap and duplication in their organisations which indicates the way organisations have implemented the three Lines of Defence Model will continue to evolve.

56%

Respondents by sector type

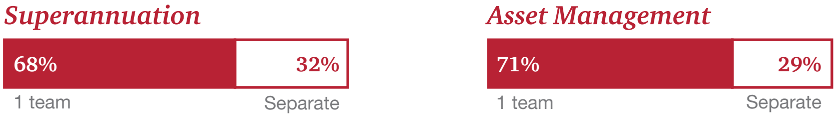


Superannuation

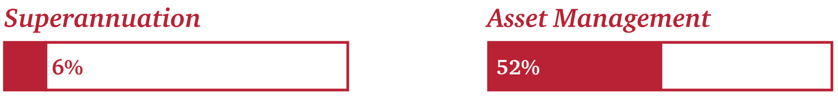
***42%** of Superannuation respondents upskilled or recruited for new skills as a result of regulatory change agenda compared to **19%** of Asset Management respondents.*

Asset Management

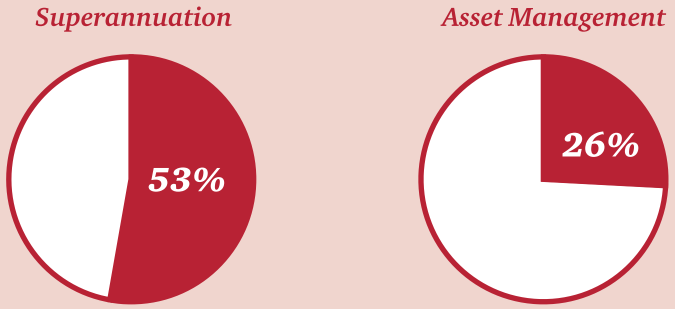
Risk & Compliance team structure



% respondents who have a Chief Information Security Officer



Percentage of respondents that rely moderately to heavily on vendors for privacy and cybersecurity risk mitigation



Cybersecurity threat within Asset Management and Superannuation

Threat profile

Nature of the Asset Management and Superannuation industry makes it an attractive target for Cyber criminals, eg large balances, members infrequently accessing accounts or checking balances.

Number of participants in the value/supply chain increases complexity, risks and scope for Cyber attack, eg employers, gateways, administrators, financial planners, mail house and technology providers.

Increased automation and integration in the industry is changing the threat profile, eg SuperStream.

Our observations

We have seen an increase in cyber crime across the industry, eg identity theft and targeted phishing attacks ('spear phishing').

Cybersecurity in the Superannuation sector is typically less mature than other financial services organisations, reflected in lower investment in cybersecurity relative to others.

We are seeing an increasing prevalence of Asset Management and Superannuation organisations exploring cyber insurance to mitigate risk, there is a need to check coverage and exclusions.

Regulator engagement

Keeping up with regulatory changes

The pace of changing regulation has not slowed and over half of those surveyed included keeping up with regulatory change expectations in their top three risk challenges.

Those surveyed identified APRA Prudential Standards and Reporting, monitoring of overseas outsourced service providers, Privacy Act and Superstream as the top regulatory changes taking up the greatest amount of their time.

This pace of regulatory change is consistent with the global outlook. In the *2015 PwC State of Compliance survey* 78 per cent of CEOs around the world view increasing regulation as the top threat to business growth, but only 35 per cent engaged with the Chief Compliance Officer to proactively manage the regulatory risks that could derail their strategy.

This environment provides both threats and opportunities to compliance teams.

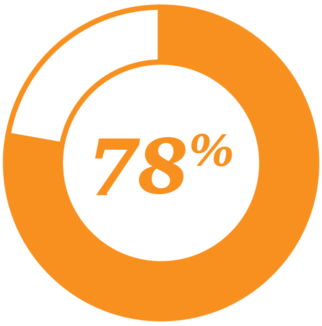
Organisations are continuing to use a proactive approach when engaging with regulators in an attempt to build compliance into the strategic objectives that derive incremental value to the wider organisation.

The frequency of regulator visits and conduct reviews were up year on year, with two thirds of respondents having a visit in the current period compared to just over half in our 2014 survey.

Through the survey, the majority of respondents included the following as methods for embedding regulatory change into their organisations:

- training
- communications on policy changes
- reviews and updates of existing risk and compliance framework.

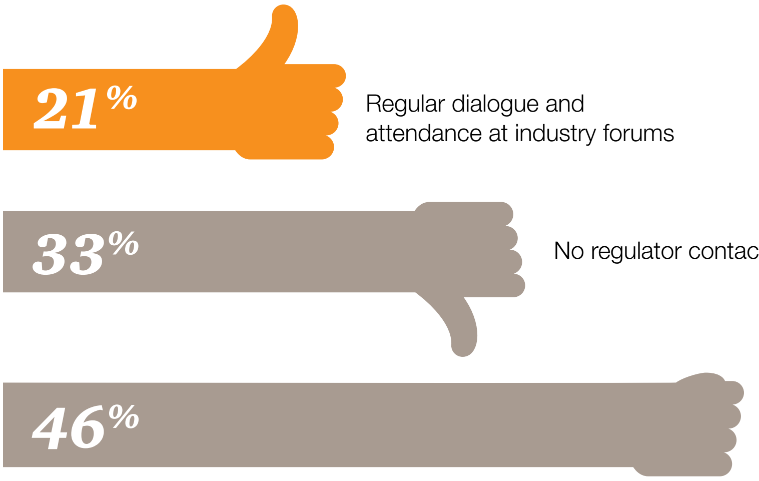
As a further assessment, half of organisations perform post implementation reviews over the regulatory changes implemented.



In the 2015 PwC State of Compliance survey 78 per cent of CEOs around the world view increasing regulation as the top threat to business growth

Locally, over half of respondents rated their relationship with the regulators as positive, stating they had open and regular dialogue and often attended industry forums.

How would you describe your relationship with regulators?



58%

of organisations identified more than one breach, an increase from 38% in last year's survey.

Complaints and breach reporting

Complaints

Monitoring and resolving complaints and breach reporting effectively is important in managing reputational risk. The volume of complaints was more or less in line with last year. The nature of these complaints year on year are depicted below.

All complaints were closed within the stipulated required timeframe and only 3 per cent of the total complaints received escalated to breaches.

Breach reporting

The majority of breaches related to non-compliance with laws and regulation, suggesting that organisations are struggling to keep up with the pace of regulatory change.

Of the total 1,300 breaches identified over half were the result of a control failure by external service providers, highlighting the importance in organisations performing effective monitoring of those third parties they outsource to.

Reporting privacy and cybersecurity breaches

Despite the increase in breach reporting relating to non-compliance with applicable laws and regulation, no respondent recorded a reportable privacy breach to the Privacy Commissioner during the fiscal year.

The criteria for establishing whether there has been a reportable breach is different to determining whether there is a reportable privacy or cybersecurity incident. Organisations should carefully assess these requirements to ensure that all reporting obligations have been met.

In addition, 62 per cent of respondents indicated that they have yet to conduct a privacy and cybersecurity risk assessment and gap analysis in line with the expectations held by the regulators. The engagement of the Privacy Commissioner in relation to privacy and cybersecurity breaches may change by the end of the year 2015.

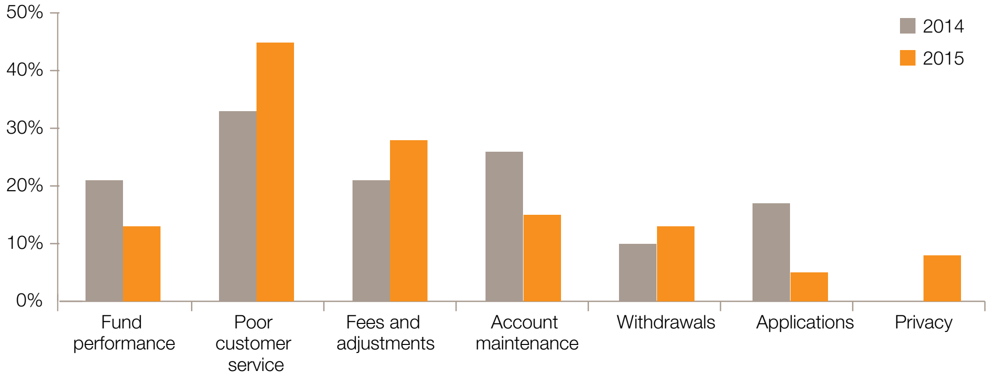
Potential mandatory data breach notification – Privacy Commissioner

The Office of Australian Information Commissioner (OAIC) has recently announced its intention to introduce mandatory data breach reporting obligation by the end of 2015.

Should the bill be passed, organisations will have a statutory obligation to notify the Privacy Commissioner and affected individuals in the event of a data breach. The extent of the reporting is not known, but the implementation would most likely translate to increased engagement with the regulator.

Pending the introduction of the mandatory breach reporting obligation, the Privacy Commissioner has issued a guide to outline reasonable steps that organisations can adopt when responding to data breaches.[1]

Nature of complaints



[1] http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

Managing privacy and cybersecurity incidents

The survey further demonstrates that over half of the respondents (56 per cent) do not have a written cyber or privacy incident management and response plan. A further 24 per cent of these respondents are not planning to construct one soon.

Of the respondents who have an incident management plan, half of them do not regularly test their incident management plans.

Having a robust privacy and cybersecurity incident management or response plan is essential to mitigate the severity of an incident as it occurs. In the event of an incident, the lack of a planned response may result in grave financial and reputational damage.

With the ever rising costs of privacy and cybersecurity incidents, organisations should no longer see having an incident management/response plan as an option, but as a necessary control to mitigate potential risks.

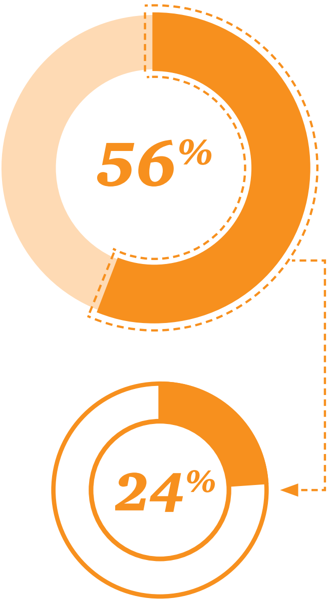
141%

Increases in the number of financial firms reporting losses of $10 million to $19.9 million resulting from cybersecurity incidents.[2]

24%

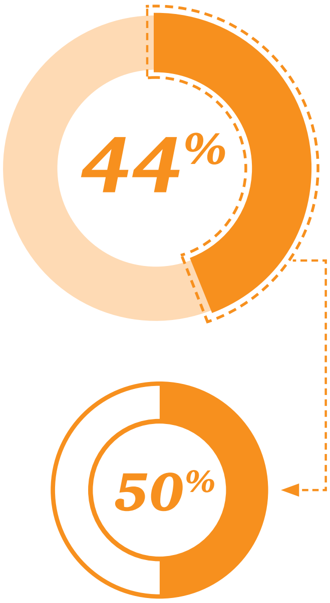
The costs of security incidents jumped 24%, with big losses leading the way [2]

Respondents who indicated that they ***do not have a written cyber or privacy incident management and response plan***



Respondents who are not planning to construct one soon

Respondents who indicated that they have an incident management plan



A further half of these respondents regularly test their incident management plans

[2] 2015 PwC Global State of Information Security Survey

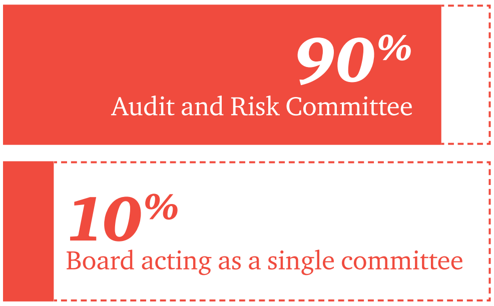
Governing risk and compliance

72%
Risk and Compliance respondents wear multiple hats.

Governance

With the continual wave of regulations being imposed on the Asset Management and Superannuation industries, implementing an appropriate governance structure is fundamental in adequately managing operational risk.

How do you handle Risk Governance?



Through the survey, the majority of respondents included the following as the Committee's responsibilities for governing risk:

- review of enterprise risk
- overseeing risk dashboard reporting
- establishment of risk appetite
- review of strategic plan and risk mitigation strategies
- review of the organisation's cybersecurity plan and approval of risk policies.

Governance is also largely driven by the chief risk officer with 92 per cent of the respondents having a chief risk officer or equivalent who has been officially designated with responsibility for overseeing the organisation's risk management program.

Risk and compliance roles

The constant regulatory change impacting the industry over the past five years has resulted in an insatiable demand for experienced risk and compliance personnel across the industry. Risk and Compliance are required to support the business in change projects, whilst managing their day to day compliance processes.

One of the themes coming out of our prior year's survey was that Risk and Compliance roles are not dedicated roles, with respondents indicating that 45 per cent of individuals with the most responsibility for Risk and Compliance wear multiple hats. The need for those officers to manage multiple responsibilities has increased to 72 per cent in the current year, which calls into question whether these individuals are able to dedicate the appropriate time and attention to their Risk and Compliance role. We do note this is largely driven by the size of the organisation.

Within organisations, there has been a move to the centralisation of Risk and Compliance functions as supported by 87 per cent of respondents to the survey.

In our prior year's survey, 37 per cent of respondents reported they have separate Risk and Compliance teams. This has decreased in the current year to 26 per cent which suggests a greater connectivity and commonality between the two functions.

Monitoring of outsourced service providers

1
Performance against SLAs
2
Self attestation or third party certificate from ESP
Follow up incidents, breaches & complaints
Regular meetings with ESP
3
Site visits

49%

It is interesting to note that only 49 per cent of respondents have inter-organisational service level agreements in place considering the large level of regulator focus in this regard.

External service providers

New standards for established Responsible Entities (REs) and Custodians of managed investment schemes came into effect on 2 January 2015. As such, outsourcing to service providers is front of mind with almost all respondents outsourcing their custody, administration and asset management. Other material outsourcing arrangements include unit registry, data storage and IT support.

There was a mix of responses in terms of who within the organisation monitors the outsourced service providers between business unit heads, compliance, fund accounting and investment operations. The majority of respondents monitor third party service providers most effectively by way of self-attestations or third party certifications from the external service provider; site visits and regular meetings; as well as follow up of incidents, breaches and complaints. 23 per cent of respondents also included upfront due diligence as one of the ways of monitoring their external service providers.

23%

Organisations perform upfront due diligence on their external service providers.

Where Service Level Agreement requirements are breached, the majority of respondents issue formal correspondence with the external service providers with a small percentage stating that fees are reduced as a result of the breach. In some cases no action is taken by the organisation where an SLA requirement is breached. 10 per cent of SLA breaches resulted in a reduction in fees paid to the outsourced service provider.

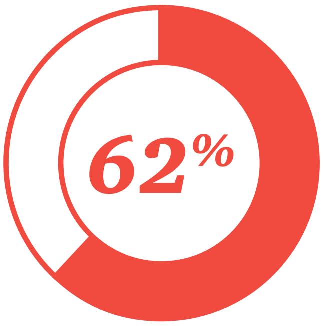
Managing third parties privacy and cybersecurity obligations continues to remain a challenge for many organisations.

Management information systems

One of the key insights that has emerged from our 2015 annual global CEO survey, *State of Compliance 2015: Moving beyond the baseline*, is that to meet the rising demand of compliance with shrinking resources, compliance teams must find new ways to increase operational efficiency and effectiveness through technology and innovating staff models.

Whilst human intervention is required to ensure a control is performed, assess whether it is adequate or if it meets regulatory requirements, it appears that organisations are increasingly relying on risk management systems to be the cornerstone of their risk function.

62 per cent of respondents indicated that they use a professionally developed compliance program designed to facilitate and manage risk within their organisation. These programs are used to initiate the completion of a control, provide



Percentage of organisations use a professionally developed compliance program to facilitate and manage risk.

compliance related reporting, and help an organisation manage and track the remediation of breaches and incidents. However we did note that maintaining the technology and data infrastructure to support risk decision-making was called out by a third of respondents as one of their organisation's three biggest risk management challenges.

Superannuation

In the recent ASFA/PwC CEO Superannuation Survey[3], we noted how CEOs' opinions have shifted over the last few years, in particular the shift in the last 12 months of the industry's perceived levels of compliance with the regulatory framework. Superannuation funds see themselves as more compliant than in prior years but are still embedding behaviours and processes into operations.

With the introduction of SPS 220 *Risk Management* there is a heightened focus on risk management and more engagement at the board level with directors having to sign the risk management declaration (RMD). Additional work has been performed by Risk and Compliance teams in the current and prior year to prepare the board for signing the RMD. Respondents included increased training; increased reporting relating to attestation of various stakeholders; additional reporting and sign-offs by management provided to the board as additional requirements. This attestation process will need to be shortened in the coming year as Superannuation funds are required to report within three months after year end.

Three lines of defence

The Three Lines of Defence Model is widely recognised as the optimum model to monitor and manage risk in an organisation. The way organisations interpret and implement this model varies across the industry and depends amongst other things on an organisation's risk appetite and the availability of resources.

Similar to last year, 95 per cent of respondents suggested they operate, to varying degrees, a Three Lines of Defence model.

Out of those respondents, only 15 per cent felt that the lines of defence are highly defined and clearly demarked with a strong understanding of roles and responsibilities. 56 per cent of respondents stated that there is a fair degree of overlap and duplication in their organisations, which indicates there is a way to go on the maturity of the Three Lines of Defence Model.

15% of respondents noted that the lines of defence are highly defined and clearly demarked.

15%

Reporting lines are important in determining the actual and perceived level of independence of line 2 compliance. 57 per cent of respondents in line 2 roles stated that they report directly to a governing body within an organisation e.g. audit and risk committee, whilst the remaining respondents indicated they reported directly into the CFO or CEO.

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

Privacy and cybersecurity

Growing importance

The marketplace that Asset Management and Superannuation organisations operate within demands the collection of personal information (PI) of consumers to conduct business. At the same time, these organisations are expanding their operations on a local and global basis, and engaging vendors and other third-party service providers beyond Australian borders.

With a deluge of constantly changing privacy-related requirements, the challenge of protecting the PI of consumers has grown exponentially in recent years.

In the past 12 months, we have seen a spike in high profile privacy and cybersecurity incidents which attracted tremendous public attention.

Despite the rise in privacy and cybersecurity incidents and heightened concerns, this year's survey shows that there is a mismatch between the level of concern and the allocation of internal resources to address privacy and cybersecurity risks. Key insights of the survey include the following:

- lack of ownership of privacy and cybersecurity responsibilities
- lack of the board's oversight in privacy and cybersecurity risks
- reluctance in investing in a privacy and cybersecurity budget.

42.8m
Total number of cybersecurity incidents in FY14 – an increase of 48%.[4]

8%
Rise in cybersecurity incidents in the financial sector in FY14 in comparison with FY13.[4]

61%
CEOs view cybersecurity as a potential threat amongst others, an increase from 48% in 2014.[5]

Investing in Digital Trust

In the 2015 PwC Global CEO Survey, 72 per cent of respondents believed that investment in digital technologies creates high to very high value in Digital Trust, including cybersecurity.

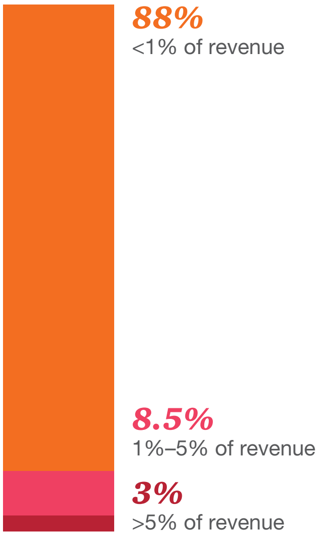
Despite the belief in high value returns, our survey results indicate that 88 per cent of respondents have set their privacy and cybersecurity budget for FY15 as less than 1% of their revenue.

This is consistent with the global trend amongst financial services firms. The 2015 *Global State of Information Security Survey* showed that security spending amongst financial services institutions has not kept in pace with the rise in security incidents and costs, as security spending for financial firms has stalled at less than 4 per cent of the total IT budget for the past seven years.

In addition, the survey indicates that 62 per cent of the respondents have not increased their budget for privacy and cybersecurity for FY16.

With the budget allocation constituting only a small percentage of organisational revenue stream, the lack of interest in increasing the privacy and cybersecurity budget further increases the risks of not having the appropriate controls and remediation plan in place to manage privacy and cybersecurity risks.

Privacy and cybersecurity budget as a percentage of revenue



[4] 2015 PwC Global State of Information Security Survey

[5] 2015 PwC Global CEO Survey

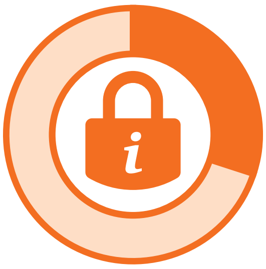
Having the right person to do the right job

Based on the survey results, we have observed varying approaches to the ownership of privacy and cybersecurity within the industry organisations:

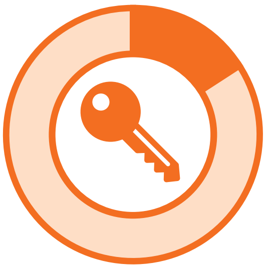
- only 30 per cent of the respondents have a full time Chief Information Security officer
- the number almost halved to 16 per cent for a full time Chief Privacy Officer
- 89 per cent of respondents indicated that those with the most responsibilities for privacy and cybersecurity compliance matters wear multiple hats.

Juggling multiple responsibilities, in combination with the lack of human resources available to focus on privacy and cybersecurity issues, could result in a lack of oversight over the way data is being managed. Responsible personnel would face increased pressure to tackle heightened concern in this sphere. For some organisations, it could also result in these areas being sidelined in light of immediate operational matters.

The disconnect between resource allocation and strategic importance may be due to the fact that these areas are relatively new, therefore organisations do not know where, or how to start tackling these issues.



30% Percentage of the respondents who have a full time Chief Information Security Officer (CISO).



16% Percentage of the respondents who have a full time Chief Privacy Officer (CPO).

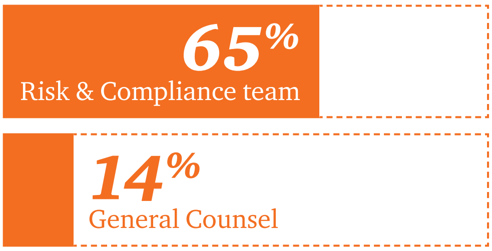
89% Percentage of those with the most privacy and cybersecurity responsibilities who wear multiple hats.

Viewing privacy and cybersecurity as a business issue

With the accelerating development in privacy and cybersecurity, the survey indicated that organisations still view privacy and cybersecurity as a legal, compliance or technology issue, rather than a business issue.

65 per cent of the respondents indicated that the primary handler of privacy within their organisations are their Risk and Compliance team; another 14 per cent by General Counsel.

Who is the primary handler of privacy within the organisation?



Our view is that privacy and cybersecurity is neither solely a legal, compliance nor technology issue – it's a business issue. Therefore, organisations should adopt a holistic view when approaching privacy and cybersecurity. Whilst the Risk and Compliance team, General Counsel or Chief Information Officer may bear the primary responsibility of managing privacy and cybersecurity risks, it is important that they work hand-in-hand with other personnel to tackle privacy and cybersecurity from a whole-of-business standpoint.

Another related area where organisations need to adopt a holistic view is around data governance and data security. Organisations with well-defined frameworks are able to identify and secure 'critical' data, ensuring that they comply with privacy and other regulations.

Privacy and cybersecurity in the Boardroom

The avalanche of data incidents over the past year has resulted in a lot of discussion about Board involvement in privacy and cybersecurity across the financial sector. Yet, the organisations surveyed clearly have not elevated privacy and cybersecurity issues to a Board level discussion.

The lack of review inevitably leads to inadequate Board's oversight in this sphere.

According to the survey, only ***5%*** *of respondents rated their Board's privacy and cybersecurity risk oversight as strong*

Corresponding ***95%*** *rated the oversight as weak or sufficient but needing improvement*

Only 8%
of respondents review cybersecurity or privacy at every board meeting

Culture

44%

Do not have risk and compliance staff aligned to business units.

Compliance is organisation wide

Culture drives the way organisations are perceived. It is important to define a clear culture that considers risk and is understood by those across the organisation and not just in the Risk and Compliance function, irrespective of the size or complexity of the organisation.

Three quarters of those surveyed identified creating a culture that supports organisation-wide risk communication and assessment in their top three risk management challenges and over a quarter noted clearly defining the organisation's risk tolerance as also difficult.

To mitigate these risk management issues organisations need to understand their compliance obligations, who within the business is responsible for those obligations and how they are monitored and reported internally.

This begins with compliance owners understanding their part in helping the organisations achieve its business strategies and collaborating with business owners.

Breaking down the compliance walls

Compliance officers can help the organisation to identify compliance issues that may impact the corporate strategy early and build solutions up front, rather than waiting for an issue to emerge and playing catch up. This way compliance requirements can be added into business process as opposed to an add on after the fact.

One respondent said: *"A mature risk culture is present when personnel at all levels routinely anticipate risks and report issues of concern, look out for each other and the firm, and respond to evolving opportunities and threats in line with corporate risk goals".*

Encouragingly 55 per cent of those surveyed stated that the majority of breaches were identified by the business itself, suggesting that the business owners (line one of the Three Lines of Defence) understand the scope of their own responsibilities and self-regulating themselves.

Contacts

Melbourne

George Sagonas

Partner, Assurance

+61 3 8603 2160
george.sagonas@au.pwc.com

Peter Malan

Partner, Risk Assurance

+61 3 8603 0642
peter.malan@au.pwc.com

Grace Guinto

Director, Risk Assurance

+61 3 8603 1344
grace.guinto@au.pwc.com

Adrian Gut

Director, Assurance

+61 3 8603 6417
adrian.gut@au.pwc.com

Sydney

Craig Cummins

Partner, Assurance

+61 2 8266 7937
craig.cummins@au.pwc.com

Nicole Salimbeni

Partner, Risk Consulting

+61 2 8266 1729
nicole.salimbeni@au.pwc.com

Deanna Chesler

Director, Assurance

+61 2 8266 0003
deanna.chesler@au.pwc.com

Peter Quigley

Director, Risk Assurance

+61 2 8266 3917
peter.j.quigley@au.pwc.com

pwc.com.au

PwC Australia helps organisations and individuals create the value they're looking for. We're a member firm of network of firms in 157 countries with more than 184,000 people who are committed to delivering quality in assurance, advisory, tax & legal, and private clients services.

127029765