pwc.com.au

Has the bar been raised?

Compliance Benchmarking Survey 2012

pwc

Contents

1

Introduction

Compliance and the industry in 2012

We are pleased to share the results of our 2012 Compliance Benchmarking survey with you. This is the fifth year that PwC has surveyed Australia's leading fund managers about their compliance practices, their views on the industry, and the regulator's areas of focus.

This year, as well as considering what effective governance looks like and the role the regulator plays, we have addressed 'hot topics' such as incident and conflict resolution, complaints management, breach and monitoring. We have also looked at the growing role of technology in each of these areas, as well as the impact that developments such as cloud computing may have on the industry. As talent management continues to be a key concern in the PwC Global CEO Survey, we have also discussed what this means for fund managers.

As in 2011, the financial services industry continues to undergo enormous regulatory change. Changes such as FoFA, FATCA and StrongerSuper, are having a strategic and even operational impact on fund managers too. That is, as the reforms affect fund managers' business partners, clients and suppliers, so do they affect the fund managers themselves.

It is therefore not surprising that many respondents continue to feel overwhelmed by the pace and volume of regulatory change. One of the common challenges faced is how to effectively split time and resources between business-as-usual activities and understanding/planning for the new reforms. Planning for the new reforms is not just about compliance – it's also about having a business strategy that takes into account the new requirements and uses them to differentiate products/services.

And it's not just new regulation that our respondents are grappling with. As the fallout from the Trio collapse continues, ASIC is likely to focus its attention on fund managers. This attention may be in the form of more surveillance visits, greater clarity about its expectations regarding compliance plans, more guidance on disclosure requirements, less lenience when things go wrong – or all of the above. Either way, many respondents reported an increase in ASIC activity, particularly in relation to investigation of breaches and the lodgement of compliance plans.

Our survey revealed more than just industry changes and a tougher regulator. It also highlighted very positive developments in most areas of compliance. Be it fewer complaints, better monitoring or (in some cases) increasing involvement of Compliance by the business, we commend those who have made great strides in strengthening their risk and compliance frameworks.

"The funds management industry is finding it increasingly challenging to allocate funds and resources between compliance projects and business enhancements."

Nicole Salimbeni
Partner

Highlights

Key survey findings include:

94%	*rely on 7 or less compliance staff*
70%	*did not identify any actual or potential conflicts*
39%	*have not had any complaints during the year*
77%	*do not monitor social media sites for complaints*
26%	*had at least one reportable breach during the year*
25%	*of reportable breaches generated regulatory follow-up*
80%	*have a centralised Compliance function and of these none employ more than 20 staff*
61%	*of boards/compliance committees receive compliance training*
54%	*review appropriateness of their Responsible Managers annually*
45%	*do not use compliance monitoring software – half of these employ 30 or fewer staff in total and use external service providers extensively*

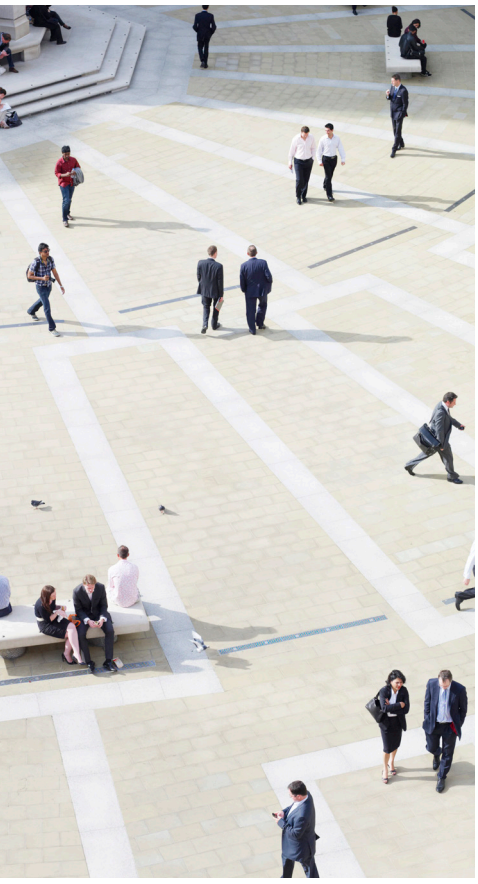
2

Governance

Managing the risks of the unknown unknowns

70%

of respondents have not been reviewed or visited by ASIC during the previous 12 months



Smart business is about identifying which risks you want to take, and making sure you can manage them appropriately. A good governance model helps organisations effectively manage their risks, and gives boards and stakeholders comfort that appropriate mechanisms are in place to oversee and monitor risk across the business. Many different mechanisms and structures exist across the financial services industry; what drives effectiveness is not necessarily the model, but rather the people within it. A deep understanding of the business, the risks involved, and the organisation's appetite to take on risk are critical in fostering sound governance.

Are the gatekeepers watching?

Recent public collapses such as Trio have highlighted the importance of having people with the right skills devoting sufficient time to the management and oversight of the organisation. ASIC itself has noted that "compliance committee oversight is not as effective as it could be because there are no requirements as to the experience, competence or qualifications for compliance committee members" [1].

It is therefore pleasing that most respondents have compliance committee members with experience in risk and compliance, management, finance and asset management – reflecting a broad range of relevant skills. Better practice organisations have clear terms of appointment for committee members, with a 3 - 5 year rotation policy. In addition, they have mechanisms for reviewing the effectiveness of the compliance committee. These mechanisms range from a formal independent review, to self-assessments, to feedback from peers and management. The results of the reviews are used to identify and address any gaps in knowledge or skill sets, and as input into the recruitment of future committee members.

Better practice organisations have also developed formal induction programs for independent committee members. This is to ensure they are appropriately informed of the organisation's broader strategic focus, key initiatives supporting the business strategy, and consequently the regulatory and operational risks that may arise.

1 PJC Inquiry into the collapse of Trio Capital Limited: Submission by the Australian Securities and Investments Commission, p34

61%

provide compliance training to the Compliance Committee or Board

Recent high-profile corporate collapses and subsequent investigations have also led to a shift in the nature of information requested by boards and committees. Historically, management has driven the nature, content and depth of reporting to these governing bodies. However, we have recently witnessed a growing trend of directors/committee members proactively identifying the information they would like to see. As a result, the reports are starting to include additional 'non-compliance' data such as that relating to business operations and financial standing in order to enhance their understanding of the business. This has not necessarily led to an increase in the volume of reporting, but more importantly to more targeted, in-depth reports that are often supplemented by dashboards and trend analyses.

ASIC is watching – albeit from a distance

ASIC has been quoted as saying it has sufficient resources to visit each regulated entity, on average, only once every seven years.[2] Our research is strongly consistent, with 70% of respondents not having been reviewed or visited by ASIC during the previous 12 months. Similarly, two-thirds of respondents advised that they had either no contact or only ad hoc contact with the regulator.

This should not suggest, however, that ASIC is in any way disengaged from the funds management industry. At the Australasian Compliance Institute conference in late 2011, ASIC advised that it would be performing additional reviews on compliance plans in the near future – an intention confirmed by a number of respondents who have received questions from ASIC about new compliance plans lodged in the last 12 months.

Questions raised by the regulator ranged from how organisations assess the effectiveness of the role of the compliance plan in the overall compliance framework, to whether more detailed requirements (e.g. qualitative standards for audits) should be included in the compliance plan itself. ASIC has agreed that guidance about compliance plans could be improved and is considering doing so, although no public timeframe has been announced.

> ***"Compliance committee oversight is not as effective as it could be because there are no requirements as to the experience, competence or qualifications for compliance committee members"[1]***

2 ASIC: The outlook for enforcement 2012-13, Thomson Reuters

3

People and culture

Doing the right thing when no-one is watching

This year respondents are finding it easier to attract the right people into compliance roles although the trend of penalising poor compliance behaviours rather than rewarding effective behaviour continues.

Having the right compliance team for your business

The 2012 PwC Global CEO Survey revealed that organisations are finding it increasingly difficult to attract the right staff for their business, to the extent that over 50% of respondents thought there needed to be changes to how they manage talent in order to succeed. While this may be true for many aspects of the financial services sector, our survey shows that local fund managers are in fact finding it easier than before to recruit compliance staff. In our 2011 survey, more than one-third of respondents found it difficult to fill vacant roles. This year, less than 20% of respondents expressed difficulty, and the average time taken to fill a role has also dropped. One of the main reasons for this is that there are more candidates in the market looking for roles. A recent survey by the Australasian Compliance Institute confirmed that 30% of compliance professionals are looking for a new job.

Although almost 50% of our respondents have retained their compliance staff for three to five years, the above surveys indicate that this may start to change. It is therefore important to invest time in communicating compliance obligations, expectations and the key systems and processes to new and existing staff. The overwhelming majority of you are already doing this by including compliance modules in your induction program and by mandating annual refresher training.

A match made in heaven

While the business no longer tends to see compliance as an obstacle, there are times that compliance officers do not share the views of the business. The strength of the relationship between Compliance and the business is therefore crucial to encouraging continuous engagement. Indeed our survey revealed that most compliance officers (74%) want to be perceived by the business as proactive and trusted business partners. The good news is that, in the majority of cases, the business sought Compliance's advice on complaints, regulatory changes, special projects, business changes and new products.

Specifically for special projects, 42% of respondents consulted Compliance throughout the majority of project stages. A further 26% consulted Compliance at every stage of the project. Although this demonstrates a high level of engagement, there is a risk that the business may lose or stop taking accountability for its projects and initiatives. The best way to address this is by taking a risk-based approach to the selection of project milestones for review and sign-off by Compliance rather than a blanket approach to their involvement.

Another challenge is the tension between funding available for business enhancements versus that required for regulatory change projects. So in an environment that remains characterised by extensive regulatory change, it's important to engage regularly with the business to identify opportunities for change that address both process improvement and mandatory regulatory requirements.

Most of our respondents agree that measuring, assessing and reporting on organisational culture is a key challenge and remains an area of focus for Boards/Committees.

The carrot or the stick?

One way to embed a culture of compliance across the business is to make all staff responsible and accountable for compliance. Our survey revealed that respondents are taking a mixed approach to this.

Almost 90% of respondents confirmed that there are consequences for poor compliance behaviours, a significant increase from last year's results (71%). However, only 16% of respondents confirmed that all staff had compliance objectives in their performance plans, and about 25% revealed that no staff did. This suggests that some organisations are considering compliance objectives on an ad hoc basis (either informally, for compliance staff only or not at all) and are not reinforcing proactive compliant behaviour, which is less effective than building compliance objectives formally into the employee appraisal process.

Compliance objectives that can be built into performance plans include:

- age of open compliance recommendations (made to the business during reviews)
- days outstanding for open incidents/breaches/complaints
- number of recurring breaches/ incidents
- number and cost of complaints referred to FOS
- cost of non-compliance (fines, settlements).

However, adherence to compliance is not just about punishment when things go wrong – it is also important to reward good compliance practices (not just good business practices). About one-third of you do reward good compliance practices, which is a small increase from our 2011 survey. These rewards tend to be a mixture of hard incentives such as monetary bonuses, and soft incentives such as open recognition.

Measuring, assessing and reporting on culture

Most of our respondents agree that measuring, assessing and reporting on organisational culture is a key challenge and remains an area of focus for Boards/Committees.

16%

of all staff had compliance objectives in their performance plans

4

Complaints

What are your customers hearing about you, and telling the world?

Complaint handling continues to improve in traditional mediums however few of our respondents monitor social media for customer feedback.

Getting back to basics

Much has been written about complaints over the last few years, and many organisations now recognise that successful complaint handling can have a positive effect on previously disenfranchised customers. Equally importantly, ASIC has advised that poor internal dispute resolution outcomes are often 'red flags' that suggest deeper problems may exist. Organisations, therefore, have both commercial and regulatory imperatives to pay attention to their complaint handling processes.

For those respondents who recorded complaints during the year, there was an increase on the previous year (up from an average of 32 to an average of 37 per organisation). In contrast, we noticed a drop in the number of respondents who had complaints escalated to the Financial Ombudsman Service (from 19% last year to 17% this year). Interestingly, respondents also recorded a 66% drop in the actual number of complaints referred to FOS. This suggests that internal dispute resolution systems are working more effectively and that fewer clients feel aggrieved enough to escalate their complaints.

The overall increase in complaints recorded is an indication that organisations are better equipping their staff to recognise, record and respond to complaints. Examples of how they are doing this include:

- conducting regular training for client-facing staff
- continuously updating scripts/ guidance for client-facing staff
- revising complaint handling policies and procedures
- updating PDSs and other customer information to address communication gaps
- evolving products and their fee structures based on customer feedback.

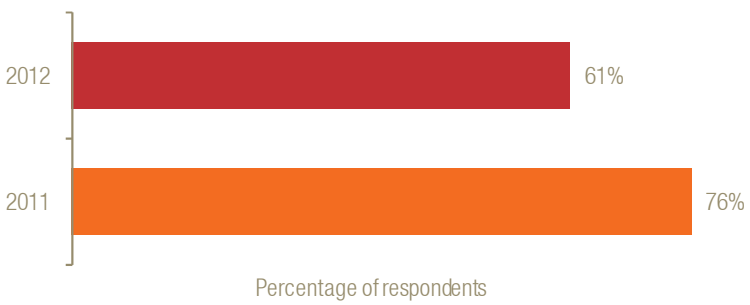
In addition to this, in recent years many organisations have invested heavily in complaint handling and data collection systems. As a result, their focus has turned to generating meaningful data analysis and building this into a continuous product and service feedback loop. This is the key to taking complaint handling beyond compliance and making it an important part of the product development lifecycle.

The role of social media

The increase in complaints is also driven in part by consumers' continued willingness to question products and services that do not meet their expectations. We now know modern consumers expect more, trust the opinions of their peers, are informed, have a wide variety of choices and have a voice that can be heard[3].

A case study cited in the Standards Australia Handbook *The why and how of complaints handling* concludes that unhappy customers tell twice as many people about the poor handling of their complaint as do those who were satisfied with its resolution. In addition, the growing popularity and integration of social media platforms into our daily lives provides a convenient channel to express these frustrations. If they go unheard, these complaints can go viral and can have a significant impact on your organisation's brand and reputation. United Airlines attributed a 10% single-day drop in its market value to a complaint posted on YouTube in the form of a song.

Percentage of respondents who recorded complaints



3 The new digital tipping point: Using digital to drive future banking profitability. PwC Australia, June 2012

A recent survey performed by PwC found that 16% of respondents would blog about a bad customer experience rather than write a letter or make a phone call to formally raise a complaint

On the other hand, some organisations have used these platforms and their customers' willingness to interact on them to generate positive customer engagement, loyalty and advocacy. For example, American Express has created a number of online forums such as OPEN and The Idea Hub that allow small businesses to connect, share ideas and provide feedback.

Our survey reveals that only 23% of you monitor social media sites for complaints, and less than half of those respondents record these formally as complaints and track them to completion. This represents an area of great opportunity for those not monitoring social media (or doing so informally). One way to take the first step in harnessing the power of the world's largest focus group is to start listening to this communication channel. The most popular online platforms and the tools that can help you monitor them are:

Popular online platforms	Tracking and listening tools and sites
Facebook	Google News
LinkedIn	Factiva
Twitter	FeedDemon
Orkut	SocialMention.com
YouTube	Tweetgrid.com
Google Plus	Mediamonitors.com.au

Why did you receive complaints?

The top five causes of customer complaints in 2012 were:

- Fund performance (26%)
- Client dissatisfaction with Customer Service (23%)
- Fees and Adjustments (23%)
- Applications (13%)
- Account maintenance (13%)

These are largely unchanged from last year, although "applications" is now within the top five and "withdrawals" has dropped from fifth to seventh place. This downward movement of withdrawals (from 21% to 6%) most likely reflects a decrease in the number of frozen funds during the survey period.

Both fund performance and dissatisfaction with customer service have fallen from 43% to 26% and 23% respectively.

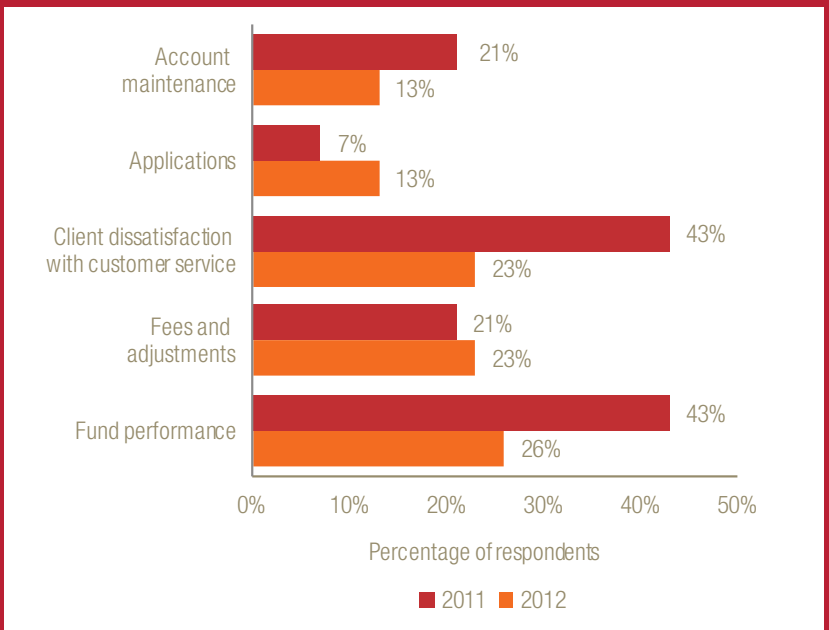
Social media users are more likely to give and receive advice about purchasing products.

72%

of social media users say that after an online search, they communicate with others about a product or service.

Source: American Express Global Customer Service

The top five causes of customer complaints in 2012



5

Technology in compliance

Is it friend or foe?

When used well, technology creates opportunities for greater customer engagement as well as increased internal efficiencies. It also creates a number of potential risks that, when not managed, may outweigh the expected benefits. Our respondents this year indicated that technology is both friend and foe.

Risk and Compliance Software

55% of respondents use compliance monitoring software, with different market segments preferring both customised and off-the-shelf-packages. No single software package was preferred by the majority of respondents, reflecting the large number of software packages available as well as the diverse size and nature of fund managers participating in the survey.

Some of the benefits that those using compliance software have reported include:

- increased efficiency
- more effective control (in relation to monitoring and issue resolution)
- real-time reporting
- stronger audit evidence/trail.

One respondent noted that their newly implemented trade-cycle compliance software provides greater oversight of the trade cycle, helping them to identify potential breaches and issues before they crystallise.

Another benefit of the increased efficiency provided by compliance software would appear to be the opportunity to partly overcome the problem of compliance resourcing levels, as identified as a key constraint by most respondents.

Is your data clouded?

Given that almost 50% of our respondents outsource data storage, it is likely that at least some are affected by "the cloud". In simple terms, cloud computing involves accessing hardware, software, or operating systems via the internet.

55% *use compliance monitoring software*

This emerging technology can offer both organisational efficiencies and cost savings compared to bricks-and-mortar technology.

However this type of technology also creates risks that need to be fully understood and appropriately managed. Depending on where the data is hosted, there may be privacy implications for your clients. Data security expectations and standards may also differ from one jurisdiction to another and this is something to consider and clarify in negotiations with external service providers.

Here are some questions to consider when assessing whether to use your own cloud computing model or when conducting vendor due diligence:

- Will confidential data be hosted on a cloud computing model?
- Is the cloud computing infrastructure offshore?
- Have your clients given you permission for their data to go offshore?
- How do you monitor data integrity, data backups and security in a cloud computing model?
- What governance and compliance frameworks do your external service providers have for this technology?
- Does your own organisation need a new governance or compliance model to accommodate this new technology?
- Will this technology integrate with existing IT solutions, potentially offering further efficiencies/ savings in the future?
- Should you build an internal or private cloud to minimise the risk of security and compliance threats?

For those outsourcing data storage, it is essential to understand the detail of how this arrangement will work. And the same goes for those looking to use cloud computing internally. To do this effectively, organisations will need to consider whether their decision-making processes – including, for example, risk appetite statements – adequately take into account both the benefits and risks of emerging technology such as cloud computing.

A large US-based multinational was able to move from more than 20 data centres (10,000m² of floor space) to three centres (300m² of floor space) using cloud computing

6

Monitoring your business

Is your eye on the ball, internally and beyond?

While

94%

of respondents involved Compliance in the monitoring of External Service Providers, only

40%

involved the Business Unit Heads in the process.

It goes without saying that organisations need appropriate levels of internal and external monitoring. Not only is this good business sense, but ASIC expects it too. This year the accountability for internal monitoring continues to improve with the strengthening of the 3 Lines of Defense Model (3LOD), however the nature and frequency of monitoring does vary for services that have been outsourced to external service providers (ESPs).

Who's minding the store? Getting compliance ownership right

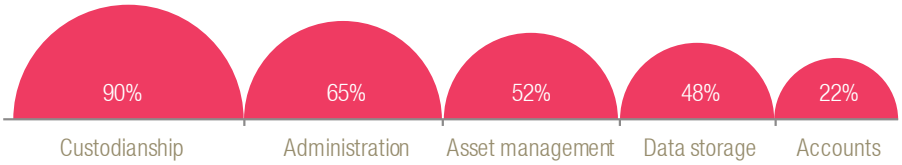
The 3 Lines of Defence (3LOD) model has become prevalent across the financial services industry over the past 5 – 10 years. It means that frontline staff and management are responsible for managing and supervising core processes and controls, while Compliance is responsible for monitoring adherence by the frontline.

Historically, there has been a significant level of reliance on the 2nd line (Compliance) to identify and communicate breakdowns in processes or controls. In recent times, as highlighted in Section 3, we have seen a growth in the level of risk-awareness and ownership by the 1st line (management). This in turn has enabled Compliance to step back and take a more risk-based approach to conducting monitoring over key controls. While this is a very positive trend and helps foster a culture of accountability, it can raise challenges: for example, in cases where compliance monitoring has been scaled back in an area that is less mature; or where there are limited resources; or where the organisation is undergoing a period of significant change. Conversely, some participants have identified instances where a lack of clarity has led to overlap and duplication of efforts across the 3LOD.

Ensuring there is a clear mandate of responsibility and accountability across the 3LOD, – and that the lines of communication remain open and active between each line, – will assist in embedding an effective, transparent approach to risk ownership.

Respondents tend to place most reliance on monitoring performed by Compliance teams, followed by monitoring performed by external auditors, self-assessments (i.e. by the business) and internal audit.

External service providers: outsourced activities



Out of sight but not out of mind?

Outsourcing continues to be an area of high priority for regulators, with one regulator warning that it can lead to core expertise leaving the business, sometimes never to return. These risks need to be carefully weighed up against any potential cost or efficiency savings from using ESPs and a sufficient monitoring plan put in place to mitigate this transfer of control.

In relation to ESPs, 90% of respondents outsource custodianship, with 65% outsourcing administration and 52% outsourcing asset management. Other functions commonly outsourced are data storage (48%) and accounts (42%). Since the collapse of Trio, the role of custodians in particular has been the subject of regulatory scrutiny, with ASIC noting a wide expectations gap between what is legally required of trustees and what investors (and some investment managers) expect of custodians. ASIC has just released a report on custodian services in Australia and will further consult with industry as to whether regulatory changes are required.

In general many respondents use the same types of mechanisms to monitor ESPs as they do to monitor their operations internally however it is the frequency that tends to differ. Where 60% of respondents monitor internal operations on an ongoing basis, only 35% monitor ESPs this frequently. This is interesting given that the regulator expects the same duty of care from the Responsible Entity regardless of whether services are outsourced or not. To address this some respondents apply a risk-based monitoring approach to ESPs similar to that used internally by the 3LOD model. ESPs are risk assessed (e.g. as High, Medium or Low risk) using factors such as:

- average time taken to resolve complaints
- number of repeat breaches and incidents
- quality and frequency of reporting
- performance against SLAs.

Using this assessment, the frequency and type of monitoring performed is tailored accordingly. Better practice organisations tend to involve business unit heads in this monitoring given that they are often more closely involved with the ESPs on a day-to-day basis. This ensures that the monitoring is not simply about adherence with SLAs, but more closely related to the ongoing business needs of the organisation.

Organisations with centralised compliance functions

7

Breaches and conflicts of interest

Do you and ASIC see eye to eye?

Effective management of breaches and conflicts of interest remains an area of crucial importance for the industry and an area of focus for the regulator.

Conflicts of interest (COI) and breaches are an undeniable part of the financial services industry and are most likely to occur or be identified during business or industry change. That is why it is essential for organisations to proactively identify, manage and mitigate actual as well as potential conflicts and breaches on an ongoing basis.

Have you identified all of your conflicts?

Despite recent industry and regulatory change, 70% of respondents did not identify any actual or potential conflicts during the year and 13% assess actual conflicts only. Some organisations consider conflicts on an annual rather than a more frequent periodic or continuous basis. This means that COI triggers throughout the year may be missed or forgotten by the time an annual declaration is made by the business.

To address this, the following changes can be used to prompt a review of the COI register:

- New external services providers (especially related parties)
- New business partners or mergers/acquisitions
- New products or changes to existing products
- New staff or changes to regulation/legislation
- Removal/disintegration of Chinese walls.

Of those conflicts that were identified, 74% were done so by Compliance as part of its monitoring program. But relying on the results of the monitoring program means there may be a delay between actual or potential conflicts arising, and their identification. Accordingly the business may benefit from additional or refresher training on the types of conflicts and triggers they should be aware of and how to record them.

70% ***did not identify any new actual or potential conflicts of interest during the last year***

When things go wrong, what do you do?

Breaches continue to be a key concern for senior management, with respondents confirming that they are routinely discussed at board and compliance committees throughout the industry. This continued scrutiny may have contributed to the downward trend in both reportable and non-reportable breaches since last year. However the trend may also be a factor of the significant time taken by some organisations to assess breach reportability; for example, one organisation routinely took more than 12 months to do so.

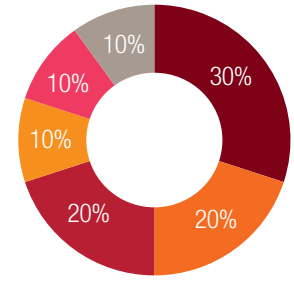
This year only 26% of respondents had a "reportable breach" (one that was considered significant enough to require reporting to ASIC) compared to approximately 33% last year. In addition the average number of breaches per organisation fell from 1.4 to 0.6.

What has not fallen is the time taken to assess the reportable nature of breaches. Organisations are still taking well in excess of the 10 business days permitted. While appropriate stakeholder engagement is essential to assessing reportability and can be time-consuming, consistently late reporting of breaches acts as a red flag for the regulator. ASIC's recent focus is not only on whether breaches are accurately reported and adequately resolved, but what these breaches may indicate about the organisation's broader compliance framework. It also shows that ASIC is taking a more active role in understanding whether a contravention by one organisation is symptomatic of a broader breakdown in the industry. Accordingly over the last three years, the proportion of reportable breaches that have generated regulatory follow-up from ASIC has increased from 4% to 25%.

This 'portfolio view' of breaches looks at whether breaches are systemic in nature, what their root cause is, and whether the compliance framework supports their prompt identification, assessment and resolution. Effective trend analysis is a key tool in forming this holistic view, although unfortunately about one-third of respondents do not conduct this analysis for breaches. When done well, trend analysis can act as an early indication of a wider problem (or a repeat problem in another part of the business) and aid Compliance in addressing the issue before it spreads. Given that 50% of breaches are detected by Compliance (ie not by the business when they occur but through a compliance monitoring program), tools such as this are imperative to managing breaches effectively.

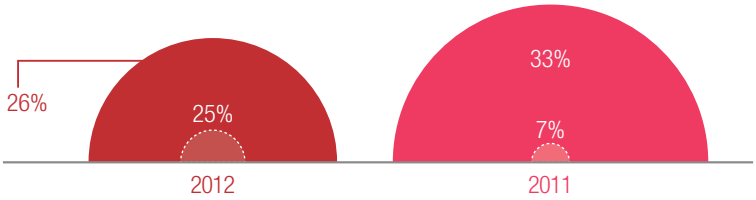
If ASIC does follow up, some respondents may find it difficult to prove that their breaches are not systemic given that one third of you do not conduct trend analysis on breaches.

Nature of reportable breaches



- Non compliance with AFSL
- Inappropriate due diligence
- Mis-disclosure of offer documents
- Inaccurate valuation of scheme assets
- Unit pricing issues
- Non compliance with law

Respondents who have had a reportable breach



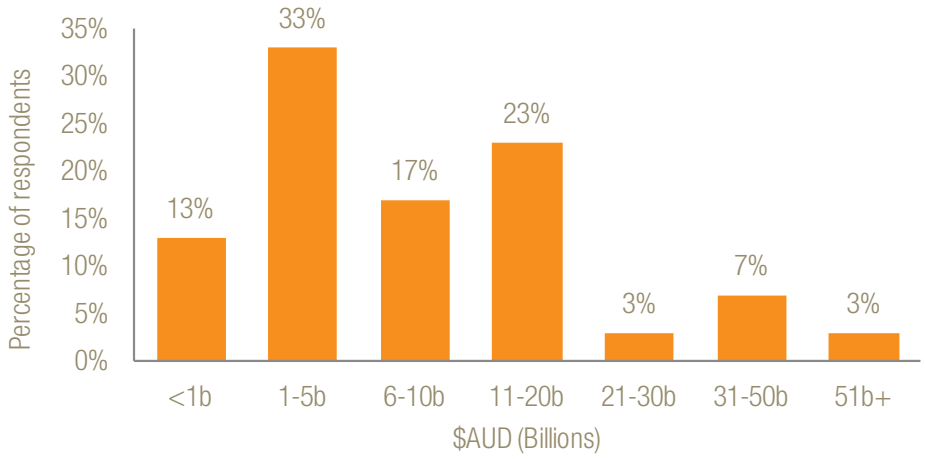
- Respondents who have had a reportable breach
- Respondents who have had a reportable breach and received follow up from ASIC

8

Appendix

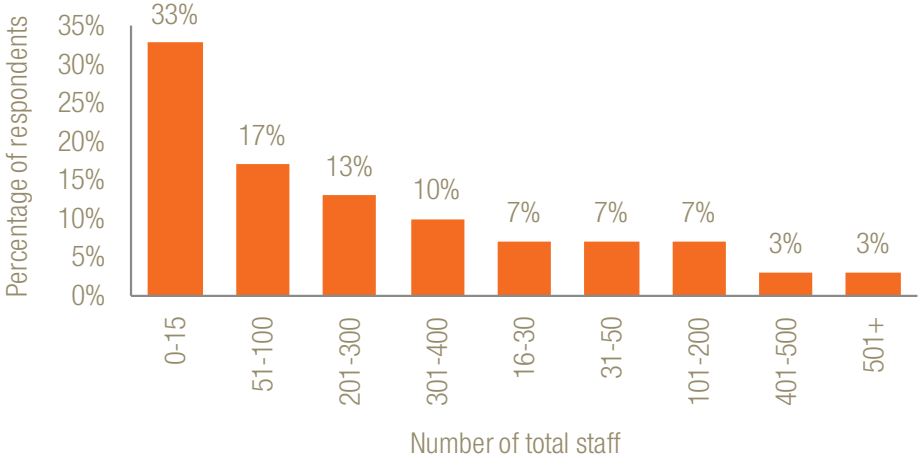
About our respondents
Additional facts and figures

About our respondents



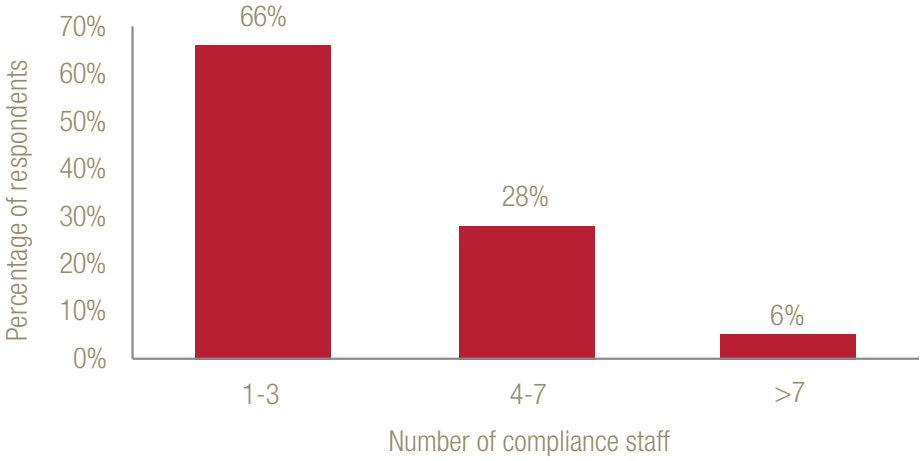
What is the value of Funds Under Management (FUM) for the Responsible Entity?

87% of our respondents had FUM of 20 billion dollars or less and half of those had FUM of 5 billion dollars or less.



How many staff members (full time equivalents) are employed by the Responsible Entity?

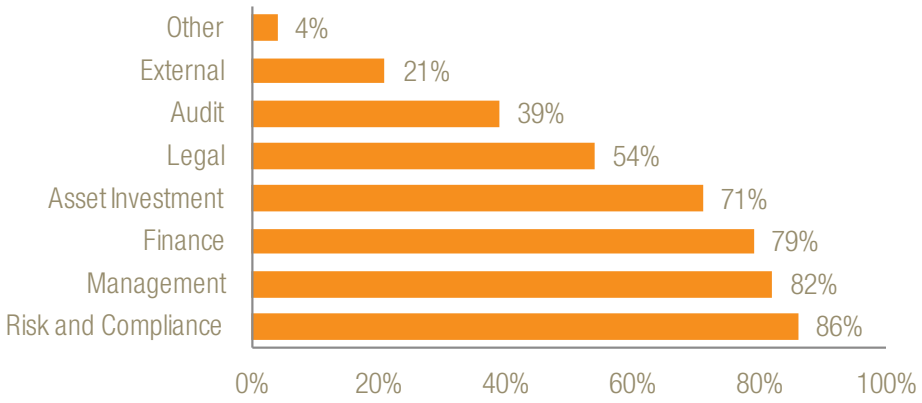
More than half of our respondents employee 300 staff members or less.



How many staff members (full time equivalents) work for Compliance?

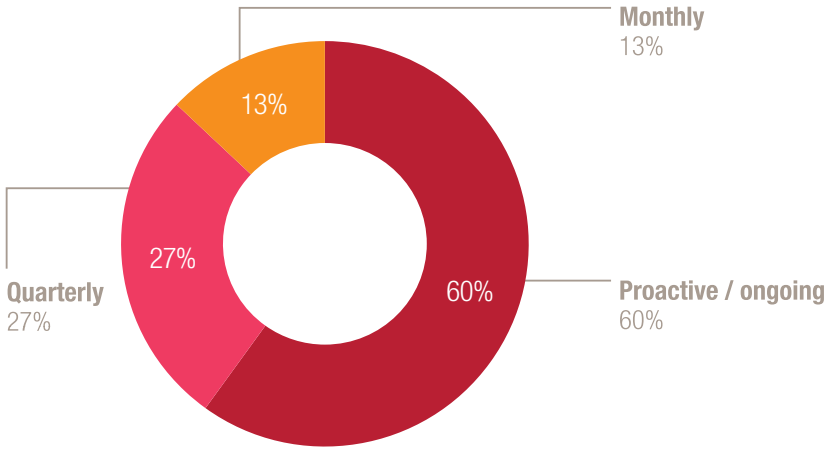
Two thirds of our respondents employee 3 staff members or less in the Compliance function.

Additional facts and figures



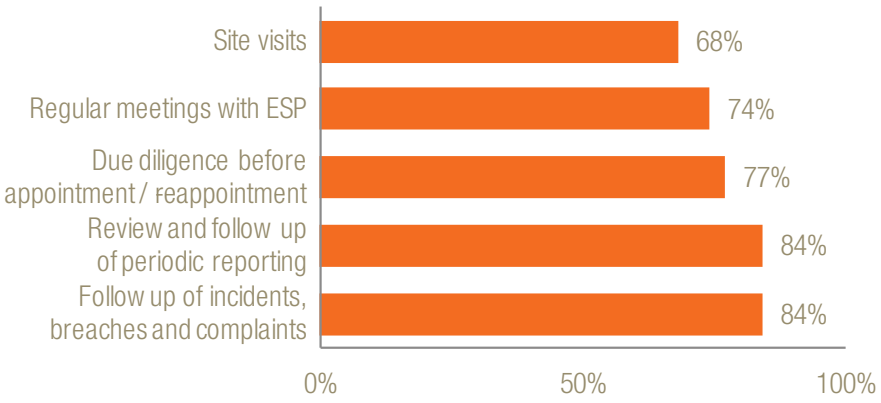
What are the skills and background of the committee / board members?

Our respondents indicate that their committee / board members have a range of skills including risk & compliance, finance, legal and audit.



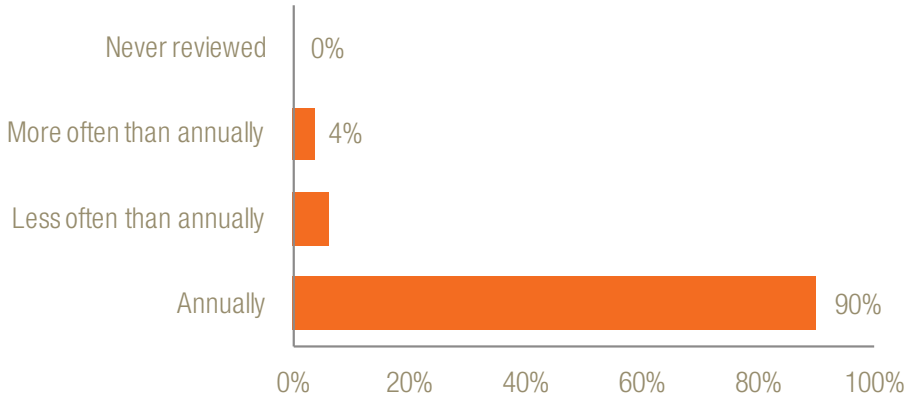
What frequency is the majority of compliance monitoring undertaken?

40% of organisations perform monitoring on a periodic basis, with 27% of organisations monitoring on a quarterly basis and 13% monthly.



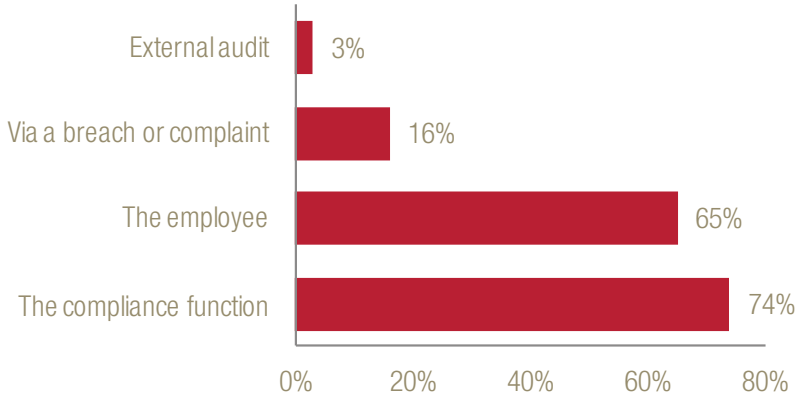
What type of monitoring is conducted for ESPs?

Most respondents conduct their compliance monitoring of ESPs via follow up of incidents, breaches and complaints and through review of periodic reporting.



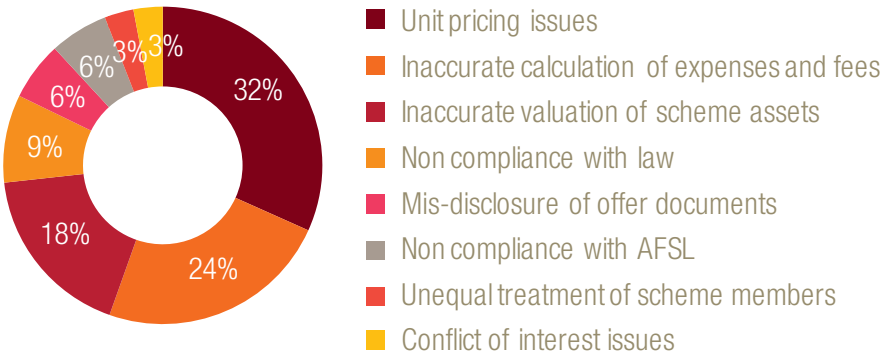
How often is the Compliance Plan reviewed?

Almost all respondents review their compliance plans on an annual basis.



Who identifies conflicts of interest for the organisation?

None of our respondents identified conflicts of interest through internal audit or during a review by the regulator.



What was the nature of non-reportable breaches?

Unit pricing issues continues to be the most common cause of non-reportable breaches.

Contacts

Nicole Salimbeni
Partner

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

Rachael Phelan
Partner

+61 (3) 8603 0155
rachael.phelan@au.pwc.com

George Sagonas
Partner

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

Shari Emin
Senior Manager

+61 (3) 8603 3050
shari.emin@au.pwc.com

pwc.com.au