Getting back to basics

PwC Risk and Compliance Benchmarking Survey / July2013

Achieving simplicity

pwc

Contents

2013 PwC Risk and Compliance Benchmarking Survey

Contents

Foreword

Results and market insights

Key findings

The industry is aiming for simplicity

Smaller teams: having to do more with less

> ***Simple can be harder than complex.*** It requires a lot of thought to achieve it, but it's worth it because you end up doing the things you are meant to do, better.

The 2013 results

This is the sixth year that we have surveyed Australia's leading fund managers and superannuation funds about their compliance practices, their views on the industry, and the regulator's area of focus. We listened to feedback from last year's participants and for the first time have broadened the scope of this paper to look at compliance in the 'bigger' picture – that is, how organisations are integrating compliance with governance and risk management.

The past 12 months has seen the final chapters of regulatory change written in response to the events of the Global Financial Crisis (GFC). Major deadlines (1 July, 2013) for Future of Financial Advice, Simple Superannuation and Australian Prudential Regulatory Authority (APRA) Standards have come and gone, with most of our participants implementing a solution that achieves a baseline of compliance that can be built upon for further change.

As organisations now move out of the 'project management phase' into 'business as usual', Risk and Compliance functions are starting to evaluate and determine how these new solutions are to be integrated into the existing risk and compliance frameworks. In particular, compliance monitoring and supervision activities and the consequential impact on resources. Many of you have indicated that over the last 12 months you have reviewed how Risk and Compliance functions operate in the organisation. The message we hear is consistent and compelling – the industry is aiming for simplicity.

Not surprisingly, our participants expressed the same challenges - project fatigue and concerns around the ever-growing complexities of managing regulatory, industry and internal obligations while still demonstrating value to the business. This has been heightened by the fact that most of our participants are doing this with smaller teams.

Reflecting on our previous Compliance Benchmarking Surveys, market events and regulatory change it is evident that achieving a state of simplicity is not that simple. Risk and Compliance functions need to take the opportunity to step back and really challenge the way in which things are done, how information is being used and who is ultimately responsible for decisions.

A prime example of this 'comfort behind complexity' is how organisations have evolved their incident and breach management arrangements. As outlined within this survey, many organisations have an operating model that consists of multiple review and approval layers across multiple functions of the business (i.e. compliance, risk, legal…) resulting in extended timeframes - in some cases taking up to six months to come to a conclusion. Where there is complexity, often accountability is absent.

"I would personally like to thank this year's participants and those that have continued to support this initiative over the past six years. We hope you find this year's Risk and Compliance Benchmarking meaningful and insightful and look forward to discussions with you and your teams."

Nicole Salimbeni

Partner
Risk Consulting

The highlights

2013 Benchmarking

This year we had 42 of Australia's leading fund managers and superannuation funds take part in the Risk and Compliance Benchmarking Survey.

The focus areas of Risk and Compliance functions have not changed over the past 12 months. However, it is evident that increased regulation, business complexities and continual strain on budgets is causing Risk and Compliance functions to think about how things can be simplified and how to achieve more, with less.

To help with this challenge we have included within this paper some specific activities Risk and Compliance functions can consider to help simplify the way in which they operate.

12

breaches reported to ASIC with 483 non reportable

X4

average number of Compliance Committee members and times per year they met

22 Incidents

average number in 2013, up from 19 in 2012


19%
of organisations identified a new conflict of interest
Survey participants:
x42
Fund Managers and Superannuation Funds
10
Days
the time for 95% of complaints to be closed, 48 resulting in paid compensation
$1 Donated
to the PwC Foundation by the AskU App for every survey question answered
2033
number of complaints received by six participants

Risk-based compliance monitoring

Key findings

Risk Compliance checklists may become obsolete

The higher the risk, the higher the level of monitoring

"Risk management should be the responsibility of everyone in an organisation and not just staff who have specific risk management duties ." [1]

A risk-based approach

This year, we saw more organisations move towards a risk-based approach to compliance monitoring. This was notable with the larger organisations and we anticipate a trend in the industry over the coming years. A targeted, risk-based compliance plan monitoring program focuses the nature, timing and extent of monitoring procedures to higher-risk areas of a particular business.

In the organisations where we have seen participants take a step towards the risk-based approach, we are already seeing the benefits – that is, being clever with limited resources and targeting effort to where it is most needed. Simple. One organisation will lower their testing samples in the lower-risk areas of the compliance plan and increased sample sizes in higher-risk areas in order to focus more on the significant risks to the business. Frequency of testing is also aligned to the riskiness of the particular compliance obligation – with more frequent monitoring where there are known areas of weakness (eg- a trend in unit pricing errors would see the Compliance team perform more detailed compliance monitoring over these particular obligations) or where the Compliance team is aware that there is significant change.

We see two key drivers of this move to more responsive compliance monitoring. Firstly organisations within the managed funds industry are continuing to mature their risk and compliance capability –hence, the concepts supporting a risk based approach are well known. Secondly, as Risk and Compliance teams are doing more work, with less staff than in prior years (as our survey results indicate) this is simply a smarter way to monitor compliance. We could very well see that monthly or weekly checklists against every compliance plan obligation become a thing of the past.

[1] Risk Management Systems and Responsible Entities, ASIC March 2013

Rules of simplicity

1. Challenge the monitoring responsibilities of the business verses those of the Risk and Compliance Function. Reduce the amount of testing duplication.
2. Explore the ability to use real time business data to reduce business disruption and identify early warning signs.
3. Connect the dots of all monitoring activities and other critical processes (i.e. complaints and breaches) to maintain relevance of the monitoring program.

Benefits

- A more effective use of resources
- Productivity gains as compliance monitoring is aligned to the risk management framework

Implications

- External auditors will need to alter their approach to gain comfort that the organisation has complied with its obligations during the period (i.e. by focussing on the high risk areas how does the organisation ensure that they are complying with the lower risk obligations?)
- Risk and Compliance teams need to ensure that in monitoring "problem areas" they don't become part of the remediation

"Every business takes risks to operate and grow, and needs to manage those risks to do so. Risk management is not about eliminating risk. It is about controlling risks to increase the likelihood of meeting business objectives."

ASIC Consultation Paper 204.
Released March 2013.

Attributes
of an effective Risk and Compliance Function

Key findings

The average time taken to fill a vacany in Risk and Compliance teams

38% of respondents used short term contractors to resource the regulatory change agenda

The demand for professional, highly credible and savvy leaders is on the rise

Increased scrutiny

In the last 12 months we have seen the Risk and Compliance profession come into the firing line of the media, regulators and business management. The increased scrutiny has brought into question the capabilities of Risk and Compliance functions to drive and embed a firm wide culture of acceptable risk management and compliance.

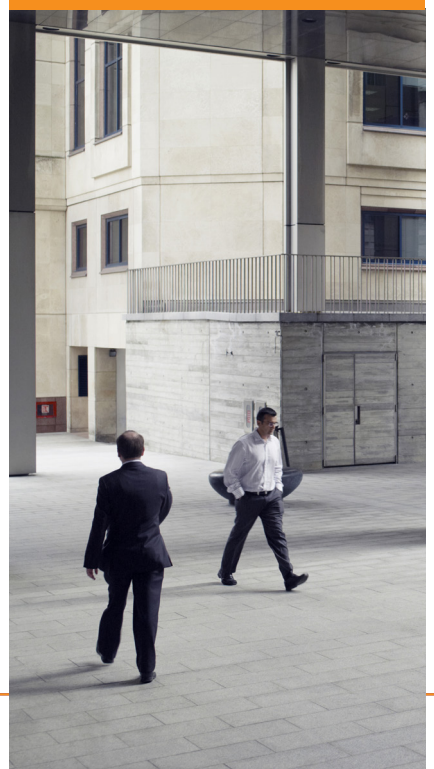
Most notably, the Australian Securities and Investments Commission (ASIC) have directly raised their concerns through recent enforceable undertakings over the size and capability of Risk and Compliance functions. However, these concerns are not new. Over the past five years, many of the concerns raised by ASIC relating to monitoring and supervision, conflict of interest and breach management all have an underlying theme linking back to the role and capability of the Risk and Compliance function within the organisation.

Although it is common to see the statement 'compliance is everyone's responsibility', not everyone is required to be an expert. Therefore, it is the role of the Risk and Compliance function to tirelessly enforce and embed the meaning of this statement throughout the organisation – from frontline staff to the Board of Directors. Organisations are now raising the bar in what they are seeking from their Risk and Compliance leaders. The demand for individuals that are professionally qualified, highly credible and commercially savvy are what is driving the ongoing battle for talent.

Considering these current events and a future that only foresees further scrutiny, Risk and Compliance functions need to look internally and ask whether they are adequately equipped to manage the demands of the business now and in the future.

Rules of simplicity

1. Refresh and define roles and responsibilities of the Risk and Compliance function, the business, management and the board.
2. Set expectations with the business as to the role of the Risk and Compliance function.
3. Consider resource requirements based on current risk and strategic drivers.



From project to business as usual

Over the past five years the Australian financial services sector has seen an exorbitant amount of regulatory change which has led to Risk and Compliance teams expanding their scope of work to deal with these sizable projects.

Given many of these projects are now coming to an end there will be a need to re-assign or restructure Risk and Compliance teams to ensure these new 'business as usual' activities (mainly the new monitoring and reporting requirements) are resourced effectively to meet the expectations of the regulators, Boards, clients and shareholders.

This will likely present a number of challenges for Risk and Compliance teams to provide opportunity for their people without adopting inefficient practices or taking on business responsibilities in the pursuit of demonstrating value.

Most of our survey participants are starting work to respond to this challenge and to address how they can strengthen or redefine their operating model, engage with the business and maximise their value.

What's next...

There will always be a need for high performing risk and compliance individuals, and the attributes that define this today are likely to be different to what is needed in the future. In particular, with the implementation of APRA's Prudential standards for superannuation funds, we have already seen some movement of risk and compliance professionals to this segment. The level of business change, and the speed in which this occurs is often the leading factor for businesses to re-evaluate how their Risk and Compliance functions operate and are resourced.

How would Risk and Compliance like the business to perceive them?

- As an enforcer – distinctly separate to the business...3%
- Primarily providing assurance and advice/input for business initiatives as required...49%
- Proactive involvement as a trusted business partner/adviser... 48%

Simply speaking

Breach and incident management

Key findings

Confusion is caused by widespread disconnect between policy and authors

Well defined criteria achieves greater consistency when applied by employees

Demystifying the definitions

Incident, exception, error, occurrence, issue, event, violation, contravention, and breach were the variety of terms dispersed within the vernacular and policies of our respondents. When considering that in some cases, more than half of such terms were used in a single document, it should be no surprise to hear that employees are finding it tough to fully grasp what each of these words mean, and the when they should be used!

Much of this confusion could be attributed to the widespread disconnect between policy authors and the people ultimately charged with interpreting and implementing them.

Nearly all our respondents indicated that incidents are owned and managed by the business unit from where they originated. However, the policies or procedures which govern this process are more often than not, written and owned by the Risk, Compliance or Legal function. Therefore, while the relevant legislations and standards have been interpreted and documented by compliance professionals, convoluted explanations, poor communication or inadequate training about key terms and process milestones heightens the likelihood of poorly managed or inconsistently adopted response protocols.

Less is probably more in this case. We found that organisations with well defined criteria are achieving greater consistency in employee understanding.

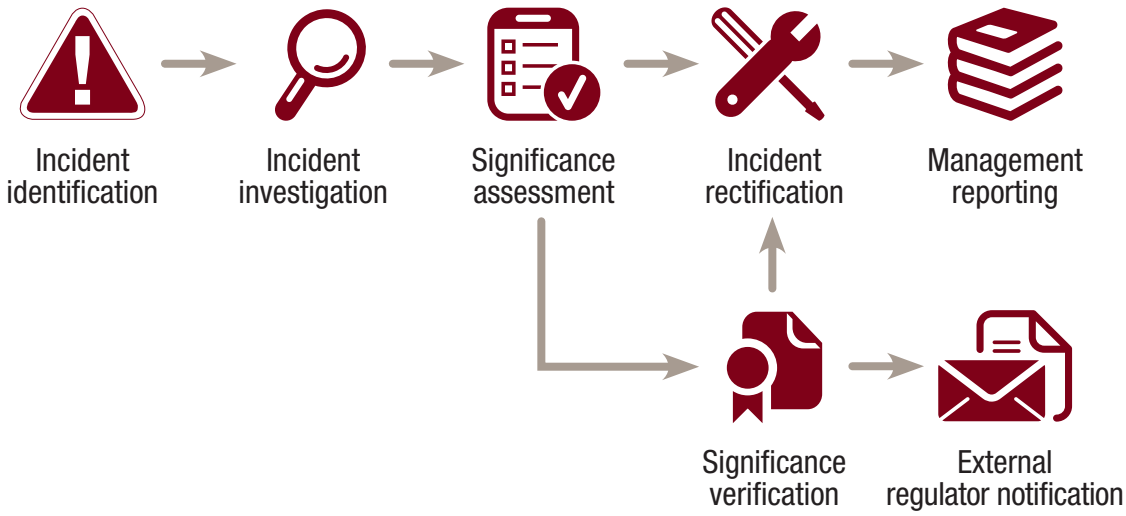
Have you performed a health check lately?

Some questions we have been asking during our compliance plan audits are:

- What actions are you taking on top of publishing your incident management policy on the intranet to make sure your business consistently understand its requirements?
- What refresher training is provided to your staff in addition to their initial risk management induction training?
- Do you perform spot checks on your employees to assess whether they understand what they are required to do in the event of an incident?
- What are the regular reviews you have undertaken internally to assess whether your incident management framework meets internal policy requirements and regulatory requirements?

Incident response should be efficient, effective and timely. A typical incident management workflow process is illustrated below:

Incident response – efficient, effective and timely



While it is interesting to consider which of the above components are prevalent within your own organisation, a matter which has become topical during the time of our survey is the time taken from incident identification to when it is reported as a significant breach to the regulators. In some examples, it has taken more than 18 months from identification to regulator notification which begs the question;

Do you know what part of your organisation is holding up this process?

Trigger and aim

Timeliness is very much front of mind for corporate regulators. Both APRA and ASIC require organisations to report any 'significant' or likely breach, within 10 business days of first becoming aware it. The trigger point for when the 10 business day timeframe starts is widely contentious in the industry. On one hand, ASIC has issued guidance within its 'Regulatory Guide 78 – Breach reporting by AFS licensees' stating that licence holders should not wait for all avenues of investigation to be completed, nor approvals from the Board of Directors

Some responses we received

"It is difficult to react immediately and move resources from BAU activities to investigate incidents.

Its best to consult.

Challenges in analysing the extent of the incident due to complex data mapping issues and at times, the need to extract them from legacy systems.

Delays in obtaining responses or approvals from another team or team member."

Rules of simplicity

1. Flatten the decision making process and empower the person ultimately responsible for making decisions on significance.
2. Create awareness within the business on time critical requirements for accessing data and generating reports. Where complete data is not readily available, engage people within the business to establish reasonable assumptions.
3. Consider an early warning process with the regulator. While not a formal significant breach report, it provides the regulator with notification of the issue and establishes reasonable activities and timeframes in which a decision can be made.

or internal/external legal advisers prior to notification. Interestingly however, most participants' Incident and Breach Management Policies reference the requirement to obtain either Legal, the Directors, Head of Risk Management, Head of Compliance, or the Compliance Committee's approval before commencing the 10 business day countdown.

Organisations should consider whether the consultation process they adopt is in line with regulators expectations of a timely breach investigation and notification.

Who has the overall view of your organisations' incidents

The general consensus across the industry is that the business owns their incidents and the Risk and Compliance functions aid in ensuring that incidents are managed in accordance with internal policy and procedure requirements. This is generally the case for operational incidents. But some incidents within an organisation are more complex than operational errors, these include:

- Physical security issues
- Conflicts of interest
- Incidents identified from complaints
- Policy non-compliance
- Work health and safety cases
- Information Technology/data security incidents
- Near misses

From our experience, these different types of incidents are managed and reported in silos and there are a limited number of organisations which consider the interconnected relationships between incident types. For example, data security is generally overseen and managed by the organisation's IT function, but such incidents may have privacy and financial impacts that may need to be assessed by others (i.e. Legal.).

All superannuation

Key findings

Greater expectation of the Risk and Compliance function by boards and stakeholders

Synergy between their Governanace, Compliance and Risk Management functions

Risk as the enabler

Post-GFC, risk and compliance have evolved from afterthoughts into integral components of business strategy. This has coincided with a greater expectation of the Risk function from Boards and stakeholders alike.

The role of the Risk function with respect to the Board and the compliance function is one that continues to evolve. As regulators visit RSE Licensees with new powers over 2013 and 2014, they will seek to observe what value risk adds to business processes.

The commencement of SPS 220 means what was previously considered "best practice" for many funds is now enforceable. In February 2013, APRA's Chairman expressed the regulator's desire to raise the industry standard of risk management, charging Boards to drive the cultural change necessary in order to bring this about.

Data integrity

The role that data plays in customer relationship management, risk and compliance is seldom appreciated. It is too late to take action when a security breach occurs or major strategic decision necessitates a change in administration platforms. Responsibility for risks associated with data and cyber rests ultimately with the Board.

Technological development; increased sophistication of cyber attacks; and heightened customer service expectations are three of the main drivers of change in technology solutions. The intangible nature of data often results in it being an underappreciated asset and therefore the commensurate risk of compromise is underestimated.

Related to data integrity is the increased expectation around data security. In May 2013, APRA released 'CPG 234 – Management of Security Risk in Information and Information Technology'. The interrelationship between security risk and IT risk within the broader sphere of operational risk is spelled out within this guide.

Rules of simplicity

1. Establish common ground across the governance, risk management and compliance functions. That is, applying a common vocabulary, approach and ideally technology infrastructure.
2. Identify and reduce duplication of effort between existing (siloed) frameworks.
3. Go to the business as a united front demonstrating how all elements are driving towards a single set agenda.

Governance

Dr. John Laker's (Chairman, APRA) speech to industry in February 2013 emphasised the centrality of governance to risk management performance across all regulated industries. This coincided with the commencement of 'SPS 220 – Risk Management' on 1 July 2013, which includes minimum expectations of Boards. Risk Appetite Statements have been integral to demonstrating Board involvement in risk governance and risk management in other regulated industries to date.

It is clear that APRA is becoming more prescriptive on the role of Boards in holding executives and officers accountable for risk management. APRA will seek to observe RSE Licensees developing governance frameworks and competencies that are reminiscent of banking and general insurance industries over time.

In addition to the fit and proper requirements under 'SPS 520 – Fit and Proper', SPS 220 refers to the relationship between board committees and senior management with respect to the risk management framework. This standard does not yet require separate board audit and risk committees, which is a requirement from 1 January 2014 for all industries other than Superannuation under 'CPS 220 – Risk Management'.

"Funds have yet to tap into the synergies between their Governance, Compliance and Risk Management functions."

PwC makes complex simple.

www.pwc.com.au

Sydney

Nicole Salimbeni

Partner, Risk Consulting
Phone: +61 2 8266 1729
Email: nicole.salimbeni@au.pwc.com

Edwina Star

Director, Risk Consulting
Phone: +61 2 8266 4940
Email: edwina.star@au.pwc.com

Caroline Haremza

Senior Manager, Risk Consulting
Phone: +61 2 8266 0386
Email: caroline.haremza@au.pwc.com

Gemma Pridgeon

Senior Manager, Risk Consulting
Phone: +61 2 8266 1454
Email: gemma.pridgeon@au.pwc.com

Ben Santamaria

Manager, Risk Consulting
Phone: +61 2 8266 2486
Email: ben.santamaria@au.pwc.com

Melbourne

George Sagonas

Partner, Assurance
Phone: +61 3 8603 2160
Email: george.sagonas@au.pwc.com

Rachael Phelan

Partner, Risk Consulting
Phone: +61 3 8603 0155
Email: rachael.phelan@au.pwc.com

Richard Gossage

Principal, Risk Consulting
Phone: +61 3 8603 5360
Email: richard.gossage@au.pwc.com

Simple can be harder than complex.