ASIC
Australian Securities & Investments Commission

REPORT 528

Responsible entities' compliance with obligations: Findings from 2016 proactive surveillance program

June 2017

About this report

This report sets out the findings from the proactive risk-based surveillance program we carried out in 2016, which covered responsible entities' compliance with their obligations.

In light of our findings, we have required some responsible entities to take specific actions. We have also made various recommendations on how entities can improve their compliance and meet their obligations.

About ASIC regulatory documents

In administering legislation ASIC issues the following types of regulatory documents.

Consultation papers: seek feedback from stakeholders on matters ASIC is considering, such as proposed relief or proposed regulatory guidance.

Regulatory guides: give guidance to regulated entities by:

- explaining when and how ASIC will exercise specific powers under legislation (primarily the Corporations Act)
- explaining how ASIC interprets the law
- describing the principles underlying ASIC's approach
- giving practical guidance (e.g. describing the steps of a process such as applying for a licence or giving practical examples of how regulated entities may decide to meet their obligations).

Information sheets: provide concise guidance on a specific process or compliance issue or an overview of detailed guidance.

Reports: describe ASIC compliance or relief activity or the results of a research project.

Disclaimer

This report does not constitute legal advice. We encourage you to seek your own professional advice to find out how the Corporations Act and other applicable laws apply to you, as it is your responsibility to determine your obligations.

Examples in this report are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

Contents

Executive summary

Responsible entities' obligations

1 As the holder of an Australian financial services (AFS) licence, a responsible entity must comply with a number of general obligations under s912A of the *Corporations Act 2001* (Corporations Act). These obligations include doing all things necessary to:

(a) ensure that the financial services covered by the AFS licence are provided efficiently, honestly and fairly; and

(b) comply with the conditions of the AFS licence and financial services laws, including requirements for disclosure and dispute resolution.

2 Responsible entities are also subject to a range of obligations under the Corporations Act that are specific to the operation of registered managed investment schemes (schemes). These obligations include duties to:

(a) act in the best interest of the members of the scheme;

(b) comply with the compliance plan of the scheme;

(c) ensure scheme property is clearly identified and held separately from the property of the responsible entity and the property of any other scheme; and

(d) hold that property on trust.

3 These important obligations seek to ensure that responsible entities are competent and provide financial services that are in the best interests of investors in their schemes. The obligations also ensure that if something goes wrong, investors have protections under the law.

4 Gatekeepers such as responsible entities play a crucial role in the overall health of the financial system. Their conduct influences the level of trust and confidence that investors can have in the financial system.

Our surveillance program

5 We use a number of different regulatory tools, including surveillance, to ensure responsible entities are continuing to meet their obligations. For a number of years we have undertaken an annual, risk-based surveillance program of responsible entities. We have adopted a risk-based and increasingly data-driven approach to our surveillance activities, with a focus on areas that pose the greatest risk to investors.

6 We have identified, and subsequently resolved, a range of issues through this surveillance program. In previous years we have dealt with such issues as:

(a) non-compliance with key AFS licence conditions, including the net tangible assets (NTA) requirement, the base level financial requirements, the professional indemnity (PI) insurance requirement and the external dispute resolution (EDR) scheme membership requirement;

(b) compliance measures that are outdated or inappropriate for the nature, scale and complexity of the licensee's business;

Note: We use the expression 'measures' to refer to the policies, processes, procedures, arrangements, frameworks or control systems of AFS licensees.

(c) poor dispute resolution measures;

(d) poor breach identification and reporting measures;

(e) inadequate measures to manage related party transactions; and

(f) defective or misleading disclosure.

7 As a result of our surveillance program, we have required entities to rectify the breaches identified and amend and update compliance frameworks and risk management systems. We have also required entities to withdraw disclosure documents or issue revised or supplementary disclosure. We have sometimes needed to impose additional licence conditions. We actively follow up with responsible entities to ensure the necessary changes are made in a timely manner.

Focus of the 2016 surveillance program

8 In *ASIC's Corporate Plan 2015–16 to 2018–19: Focus 2015–16*, we indicated that we would incorporate culture and incentives more explicitly into our risk-based surveillance and use the findings to better understand how culture and incentives are driving conduct among gatekeepers. We also confirmed that we would discuss the findings with those we regulate where we saw problems.

9 In *ASIC's Corporate Plan 2016–17 to 2019–20: Focus 2016–17*, we introduced our view of 'what good looks like' for the sectors we regulate. For the funds management sector, we have identified that responsible entities should:

(a) treat fund members and investors fairly;

(b) deliver financial product and services that are transparent, fit-for-purpose, and aligned with consumer needs and preferences;

(c) strike the right balance between innovation and risk to meet fund objectives; and

(d) ensure that investors are fully compensated when losses result from poor conduct.

Key findings

10 In general, we found that the responsible entities in the surveillance program demonstrated a commitment to complying with their obligations under the law. These responsible entities generally have established measures for compliance, risk and governance, and disclosure, supported by ongoing reviews to address their obligations.

11 However, our findings also indicate a number of areas where the responsible entities fall short of our expectations and our view of what good looks like in the funds management sector.

12 Three responsible entities continue to be the subject of high-intensity broad-based surveillance at the time of writing this report. We have required 20 of the remaining 25 responsible entities to address specific concerns we identified through the surveillance program. The concerns we raised include the adequacy of the responsible entities' measures for:

(a) PI insurance;

(b) managing conflicts of interest;

(c) breach reporting;

(d) custody;

(e) dispute resolution;

(f) risk management systems;

(g) compliance;

(h) cyber resilience;

(i) values and behaviours;

(j) rewards and incentives; and

(k) whistleblowing.

13 Where we identified non-compliance or deficiencies in the compliance measures of responsible entities, we required those entities to rectify these and provide us with details of the actions taken. As noted at paragraph 12, three of the 28 responsible entities remain the subject of surveillance.

14 Table 1 summarises our findings and our response. We also identify some general recommendations that responsible entities should take on board in considering their compliance measures. The detailed findings are contained in Section B.

Table 1: Summary of findings, actions taken and recommendations

Area	Key findings	Actions taken	Recommendations
PI insurance	While all responsible entities had PI insurance in place, two entities had less than the minimum level of cover required. We also identified a general lack of awareness of the requirements, set out in Regulatory Guide 126 *Compensation and insurance arrangements for AFS licensees* (RG 126), for the PI insurance policies retained by responsible entities. It is important that this is improved if investors are to be properly compensated for losses resulting from poor conduct.	We required both the responsible entities that had less than the minimum level of cover to take immediate steps to address the breach. We raised concerns with eight responsible entities about issues to do with PI insurance requirements. These responsible entities confirmed their compliance with the minimum requirements.	Responsible entities should review their PI insurance policies to ensure they understand the levels of coverage and that the level of cover is adequate for the nature, size and complexity of their businesses. Entities should also take into account the minimum requirements under the conditions of their AFS licence and RG 126. We expect responsible entities to proactively address any deficiencies in their PI insurance policies.
Conflicts of interest	We found that, for most of the responsible entities, management of conflicts of interest formed an integral part of board responsibilities. However, six of the responsible entities indicated that conflicts of interest is not a standard agenda item at board meetings. Conflicts management is key to delivering financial products and services that are aligned with consumer needs and preferences.	We required four responsible entities to review and amend their conflicts management measures as a result of failures of their existing measures or inadequate details in their conflicts registers. As a result, all four entities have amended their conflicts management measures.	Responsible entities should review our guidance in Regulatory Guide 181 *Licensing: Managing conflicts of interest* (RG 181) and, where necessary, strengthen their conflicts management measures to ensure they are adequate, implemented and maintained.
Breach reporting	We found that 19 of the responsible entities identified compliance breaches or control failure incidents. Six identified 10 or more breaches and incidents. In general, responsible entities reviewed their documented standalone measures for their breach reporting obligations annually. In a small number of cases we were unable to determine when, if at all, breach reporting measures were reviewed.	We requested additional information from three responsible entities about breaches identified by them in the 12 months before our surveillance. We required one responsible entity to review and enhance its breach reporting measures.	Responsible entities should regularly review their breach reporting measures to ensure they remain effective to identify, manage and, where necessary, report breaches.

Area	Key findings	Actions taken	Recommendations
Custody	While the majority of the responsible entities relied on the services of an external custodian, only around half of the entities had established standalone documented measures for monitoring these arrangements. We found that board oversight of the ongoing review of documented measures for the custody of scheme assets was generally lacking. Responsibility for the review rested with compliance committees or compliance personnel. We identified a small number of responsible entities that had not formally reviewed their custody measures in the 12 months before our surveillance, raising concerns about compliance with the changes to custody standards that came into effect in February 2015.	One responsible entity has updated the agreement it has with its third-party custodian to ensure it complies with current requirements. Others have confirmed that their measures meet current requirements.	Responsible entities should review their custody measures to ensure they meet the requirements of Regulatory Guide 133 *Managed investments and custodial or depository service providers: Holding assets* (RG 133) and, where necessary, update their measures.
Dispute resolution	We found that it is common for dispute resolution, including assessment of and decisions on disputes, to rest with a single staff member—usually a director, head of compliance or complaints officer. Only three of the responsible entities explicitly identified the board as having a role in either reviewing all complaints or reviewing escalated matters. To ensure investors are treated fairly, it is essential that dispute resolution measures are robust and have appropriate oversight from the board.	We required two responsible entities to review their dispute resolution measures and confirm to us that the high number of disputes received, as well as disputes escalated to external dispute resolution (EDR) schemes, were not as a result of systemic weaknesses. These entities have since reviewed their measures and verified there are no systemic weaknesses.	To ensure accountability, top management of a responsible entity should be provided with reports about disputes that include information on the actions taken and decisions made on the disputes: see Appendix 1 of Regulatory Guide 165 *Licensing: Internal and external dispute resolution* (RG 165). Responsible entities should review their internal dispute resolution (IDR) measures to ensure that they meet the requirements outlined in RG 165.

Area	Key findings	Actions taken	Recommendations
Risk management systems	Most responsible entities had in place risk management systems that had been reviewed in the 12 months before our surveillance. We found two responsible entities that did not have risk management systems in place. The top three risks identified by responsible entities were operational risk, closely followed by market and regulatory risks. Other risks identified included governance, capital, personnel and liquidity risks.	We required two responsible entities to create and implement risk management systems, and another two responsible entities to update their risk management systems.	As AFS licensees, responsible entities must have adequate risk management systems in place. Responsible entities should review and, if necessary, amend their risk management systems to take into account our guidance in Regulatory Guide 259 *Risk management systems of responsible entities* (RG 259).
Compliance measures	Most responsible entities had reviewed their compliance measures to ensure that they addressed the risks identified through their risk management systems. We found all responsible entities had at least one person with responsibility for their compliance function. The larger responsible entities dedicated, on average, three compliance personnel to compliance functions. We also observed that, in some instances, the compliance resource within an entity is not a dedicated role. Reporting lines for personnel who are responsible for the compliance function within the entity vary significantly, depending on the size of the operation of the responsible entity. Most commonly, personnel who are in charge of the compliance function have a direct reporting line to the board. However, we also found other direct reporting lines for compliance personnel. We had a number of concerns about the quality of compliance plans. For instance, where no documented standalone measures are maintained, some compliance plans do not contain sufficient details on the legal concepts and requirements, the tasks that must be carried out, the person responsible, how the obligations can be met and how the tasks are to be monitored. We were also concerned by plans that require one person to monitor a number of, if not all, the measures, or plans where the persons nominated have other significant and possibly conflicting duties.	Two responsible entities lodged updated compliance plans in response to specific concerns we raised. We are continuing our surveillance of two other responsible entities because we are concerned about the quality of their compliance plans. Five other responsible entities have lodged replacement compliance plans with ASIC since the commencement of our surveillance program.	Responsible entities should actively monitor and amend their compliance measures to ensure they remain adequate and have been implemented. We recommend that responsible entities continually monitor and regularly review their compliance measures, including the adequacy of resources applied to the compliance function, and amend them as necessary.

Area	Key findings	Actions taken	Recommendations
Cyber resilience	We found that the responsible entities recognised the growing threat of malicious cyber activity and had put in place a wide range of measures to address cyber risks. Nine of the responsible entities and three service providers to the responsible entities were subject to malicious cyber activity in the 12 months before our surveillance. A significantly high proportion of the agreements that responsible entities have in place with external service providers do not explicitly address cyber risks.	We required seven responsible entities to address the adequacy of their existing cyber resilience measures as part of their overall risk management obligation. As a result, six responsible entities have initiated reviews of their cyber resilience measures. Our continuing surveillance includes one responsible entity because of our concerns about their cyber resilience measures.	Responsible entities should review and, where applicable, strengthen their existing cyber resilience measures against the US National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework): see Report 429 *Cyber resilience: Health check* (REP 429) for more information. We consider that the NIST Cybersecurity Framework has particular relevance as a standard to manage cyber resilience and as a global benchmark for financial services providers.
Values and behaviour	We found that the majority of the responsible entities had documented standalone measures addressing this area in various forms, and that the majority had reviewed their measures in the 12 months before our surveillance. Less than half of the measures on values and behaviour were approved by the responsible entities' board. Responsibility for approval was delegated to the chief executive officer, director or board committees in all other instances.	We did not take any action in this area. We will, however, continue to monitor these issues to help us develop our understanding of industry practice and, if appropriate, respond to poor conduct in this area.	Boards should influence the culture within the responsible entity by: • setting the tone from the top, to ensure that desired values and behaviours are given appropriate prominence; • putting in place governance structures to ensure this tone is implemented in an effective way throughout the entity; • monitoring the management team's alignment with the entity's values and behaviours; and • making sure the management team are held accountable where there is a misalignment.

Area	Key findings	Actions taken	Recommendations
Rewards and incentives	We found that the majority of the responsible entities had formal measures in place to review conduct of directors and employees. However, less than half of the responsible entities had documented measures to address rewards and incentives within the entity. The majority of the responsible entities also review employment arrangements to identify incentives that may result in directors or employees behaving in a way that does not comply with the entity's obligations under their AFS licence.	In response to concerns we raised, one responsible entity included provisions for assessment of directors in its compliance measures and another revised its measures to require annual declarations about the conduct of their responsible managers.	Remuneration, rewards and incentive structures should be aligned to the values of the responsible entity, to motivate and reinforce the culture of the entity and the conduct expected of its staff. Responsible entities should review and integrate incentive governance as part of their overall risk management systems and compliance measures to ensure the structure of rewards and incentives does not promote unnecessarily risky behaviours.
Whistleblowing	We found that under half of the responsible entities had measures addressing employees' right to report an employer's misconduct, and less than one third had established and maintained specific whistleblowing measures. Where responsible entities maintained whistleblowing measures, they had generally been approved or reviewed in the 12 months before our surveillance. We also noted that board involvement in and oversight of the ongoing review of whistleblowing measures was not high. We found that the board was involved in the review for just over half of the responsible entities that had whistleblowing measures.	As a result of the concerns we raised, one responsible entity updated its whistleblowing measures and introduced proactive measures that ensure the whistleblowing measures contain accurate information and clearly assign roles and responsibilities. We have required another entity to introduce documented whistleblowing measures.	Responsible entities should implement appropriate whistleblowing measures to ensure they meet their legal obligations and support an open and transparent culture within the entity. Responsible entities should also set up training for all staff and periodically check on the effectiveness of their measures.

Area	Key findings	Actions taken	Recommendations
Product approval and review	We found that under half of the responsible entities had specific measures for product design, approval and review. The majority of the measures were approved or reviewed in the 12 months before our surveillance. Most notably, we found that board involvement in reviewing measures for product design, approval and review was very low, with only three responsible entities' boards being involved in the review of these measures. It is important that products are approved and reviewed, to ensure responsible entities strike a balance between innovation and risk to meet fund objectives.	We have noted the lack of consumer-focused measures for the introduction of new financial products and the review of existing ones. However, we did not take any action in this area in light of Treasury's proposals paper, *Design and distribution obligations and product intervention power*, published in December 2016.	Responsible entities should have a consumer-focused culture. As part of their duty to act in the best interests of their investors, they should consider whether their financial products meet and continue to meet the needs of their investors. Responsible entities should assess their product approval and review measures to ensure they include this consideration.

A Our surveillance program

Key points

This section contains the background to our surveillance program. Specifically, it details the program's areas of focus and the methodology we used to select the responsible entities for surveillance.

About our surveillance

15 Our surveillance program included 28 responsible entities, which we selected using a profiling methodology that identified those entities that exhibited a potentially higher risk of non-compliance in our areas of focus.

16 In total, the 28 responsible entities:

(a) manage over $49 billion in scheme property across 336 schemes;

Note: As at 30 January 2017, ASIC records show there are 3,634 registered managed investment schemes (excluding those schemes being wound up or deregistered), which means our sample represents approximately 9% of all schemes.

(b) $6 billion in total assets across 41 unregistered managed investment schemes; and

(c) over $41 billion in assets under managed discretionary account services.

17 We issued the responsible entities with a notice requesting information using ASIC's power under s912E of the Corporations Act (s912E notice). After reviewing this information, we selected four of the responsible entities for high-intensity broad-based surveillance. These four responsible entities were responsible for 17 registered schemes with just under $1.28 billion in scheme property.

18 Our surveillance focused on a range of issues, including:

(a) use of fund assets (e.g. mandate compliance, fees, related party transactions, custody measures;

(b) disclosure (e.g. misleading disclosure, failure to comply with continuous disclosure obligations, approval and oversight of disclosure);

(c) the adequacy of and compliance with governance, risk and compliance measures, focusing on:

(i) recruitment and training;

(ii) rewards and incentive structures and promotions;

(iii) whistleblowing;

(iv) management of conflicts of interest;

(v) dispute resolution;

(vi) the extent to which a consumer-focused culture is supported through robust product approval and review measures; and

(vii) supervision of outsourced activities;

(d) cyber resilience; and

(e) AFS licence conditions (i.e. financial resource requirements, PI insurance requirements, monitoring and supervision of representatives).

19 This report sets out the findings of our 2016 surveillance program, noting that further work is continuing on a number of the responsible entities.

Methodology of our surveillance program

20 Our methodology involved:

(a) considering and applying metrics to publicly reported returns data of schemes;

(b) applying filters to all schemes and all responsible entities using the data available to ASIC, including publicly available information on schemes and responsible entities; and

(c) analysing information, obtained from the responsible entities under a s912E notice, on the areas of their compliance with AFS licence conditions, their governance, their risk management, scheme information, and their disclosure.

21 The information we sought from the responsible entities was aimed at:

(a) obtaining further details about how the responsible entities met their obligations in the areas identified in paragraph 18, and whether those measures were adequate, to help us identify four responsible entities for detailed surveillance; and

(b) providing information about how a subset of our population is addressing issues of concern to ASIC.

B ASIC's findings

Key points

This sections sets out the key findings from our surveillance program, any actions we took as a result of these findings and our recommendations for responsible entities. It covers the following areas:

- PI insurance (paragraphs 22–28);
- conflicts of interest (paragraphs 29–35);
- breach reporting (paragraphs 36–41);
- custody (paragraphs 42–47);
- dispute resolution (paragraphs 48–52);
- risk management systems (paragraphs 53–59
- compliance measures (paragraphs 60–70)
- cyber resilience (paragraphs 71–80
- values and behaviours (paragraphs 82–85);
- rewards and incentives (paragraphs 86–92);
- whistleblowing (paragraphs 93–98); and
- product approval and review (paragraphs 100–105).

PI insurance

22 All AFS licensees providing financial services to retail clients must have arrangements in place to compensate clients, which generally means holding adequate PI insurance. Our minimum requirements for PI insurance are set out in RG 126 and in the responsible entity's AFS licence conditions.

23 More specifically, AFS licensees that are authorised to operate a scheme must maintain an insurance policy for professional indemnity and fraud by officers that covers claims amounting, in aggregate, to whichever is the lesser of:

(a) $5 million; or

(b) the sum of the value of all property of all schemes for which it is the responsible entity.

Our findings

24 We found that all responsible entities had PI insurance in place, but two responsible entities had less than the minimum level of cover required.

25 We also identified a general lack of awareness of the RG 126 requirements for the PI insurance retained by responsible entities. In particular, we were concerned by some responsible entities' responses about:

(a) defence costs—some entities were unsure whether defence costs were included in the minimum limit of indemnity or over and above the required minimum limit of indemnity;

(b) policy reinstatement—some PI insurance policies did not include at least one automatic reinstatement; and

(c) fraud and dishonesty cover—some PI insurance policies did not provide fraud and dishonesty cover, as required under RG 126.

Actions taken

26 We required both the responsible entities that had less that the minimum level of cover to take immediate steps to address the breach. As a result, these breaches were rectified.

27 We raised concerns with eight responsible entities about issues to do with PI insurance requirements. These responsible entities confirmed their compliance with the requirements under RG 126.

Recommendations

28 Responsible entities should review their PI insurance policies to ensure they understand the levels of coverage and that the level of cover is adequate for the nature, size and complexity of their businesses. Entities should also take into account the minimum requirements under the conditions of their AFS licence and RG 126. We expect responsible entities to proactively address any deficiencies in their PI insurance policies.

Conflicts of interest

29 Adequate conflicts management measures help minimise the potential adverse impact of conflicts of interest on consumers. Conflicts management measures help promote consumer protection and maintain market integrity. This is based on our experience that conflicts of interest that are not properly managed or eliminated are a key indicator of regulatory issues for responsible entities.

Our findings

30 We found that two responsible entities did not have any measures to address obligations and issues relating to conflicts of interest. One responsible

entity's measures for managing conflicts of interest, contained in the scheme's compliance plans, were inadequate.

31 We also found that it was most common for the board to be responsible for measures relating to conflicts of interest. Other roles or committees responsible for conflicts of interest measures included conflicts and risk committees, the head of compliance, the head of legal, and executive directors.

32 Just under half (13) of the responsible entities identified conflicts of interest in the 12 months before our surveillance, and a small number recorded a significantly higher number of conflicts. Three recorded 10 or more conflicts, three recorded between six and nine conflicts, and seven recorded five or less conflicts.

33 We found that, for most of the responsible entities, management of conflicts of interest forms an integral part of board responsibilities. However, six of the responsible entities indicated that conflicts of interest was not a standard agenda item at board meetings.

Actions taken

34 We required four responsible entities to review and amend their conflicts management measures as a result of failures of their existing measures or inadequate details in their conflicts registers. As a result, all four responsible entities have amended their conflicts management measures.

Recommendations

35 Responsible entities should review our guidance in RG 181 and, where necessary, strengthen their conflicts management measures to ensure they are adequate, implemented and maintained.

Breach reporting

36 Breach reporting is an area we regularly identify as being problematic. Over time we have identified problems with the breach reporting measures of a number of responsible entities.

Our findings

37 We found that 19 of the responsible entities identified compliance breaches or control failure incidents in the 12 months before our surveillance. Six identified 10 or more breaches and incidents.

38 We also found that 21 of the responsible entities maintain measures addressing their breach reporting obligations, and 17 keep these as documented standalone measures on breach reporting. As is the case with complaints management, some responsible entities identified that their breach reporting measures are contained in scheme compliance plans.

39 Most (20) responsible entities reviewed their standalone measures for breach reporting obligations in the 12 months before our surveillance; however, one reviewed these measure in the last two years. Some responsible entities did not explicitly identify a review date, and therefore we were unable to determine when measures were reviewed, if at all.

Actions taken

40 We requested additional information from three responsible entities about breaches identified by them in the 12 months before our surveillance. We required one responsible entity to review and enhance its breach reporting measures.

Recommendations

41 Responsible entities should regularly review their breach reporting measures to ensure they remain effective to identify, manage and, where necessary, report breaches.

Custody

42 Custodians play an integral role in the investment industry and, increasingly, responsible entities are relying on the services of custodians to hold and safeguard the assets of investors, including the ongoing management of information. Given the important role that custodians have, it is crucial that responsible entities have adequate measures to monitor and review the activities of these asset holders.

Our findings

43 We found that 23 of the responsible entities relied on the services of custodians to hold scheme property on trust. However, only around half (16) of the entities had established documented standalone measures for monitoring the services outsourced to custodians, while others relied on the measures for ongoing monitoring of custody arrangements in the schemes' compliance plans and in documented agreements between the responsible entities and custodians.

44 We also found that, of the 16 responsible entities that have documented standalone measures relating to custody, 15 of them had reviewed these measures in the 12 months before our surveillance. However, board oversight of the ongoing review of documented measures for the custody of scheme assets was generally lacking. Responsibility for review rested with schemes' compliance committees or responsible entities' compliance personnel.

45 Four responsible entities had not reviewed the custody measures in their compliance plans in the 12 months before our surveillance. Two of these responsible entities last reviewed these measures over four years ago. While the numbers are not high, we are concerned that responsible entities may not be compliant with the changes to custody standards that came into effect in February 2015.

Actions taken

46 One responsible entity has updated the agreement it has with its third-party custodian to ensure it complies with current requirements. Others have confirmed that their measures meet current requirements.

Recommendations

47 Responsible entities should review their custody measures to ensure they meet the requirements of RG 133 and, where necessary, update their measures.

Dispute resolution

Our findings

48 On average, each responsible entity received two complaints in the 12 months before our surveillance. We found that only a very small number of complaints were escalated through to EDR schemes. Where complaints are escalated, however, compliance with EDR scheme rulings appears to be high.

49 Most (22) of the responsible entities maintain documented standalone measures for dispute resolution, while the other six relied on dispute resolution measures that were contained in the compliance plans for the schemes they operate. We found 19 of the documented standalone measures were last reviewed in the 12 months before our surveillance, two were last reviewed two years ago and one was last reviewed three years ago. Only three of the six responsible entities who relied on dispute resolution measures in compliance plans had reviewed these measures in the 12 months before our surveillance.

50 We found that it is common for dispute resolution, including assessment of and decisions on disputes, to rest with a single staff member—usually a director, head of compliance or complaints officer. A committee or more than one staff member was responsible for dispute resolution in 10 responsible entities. Only three explicitly identified the board as having a role in either reviewing all disputes or reviewing escalated matters.

Actions taken

51 We required two responsible entities to review their dispute resolution measures and confirm to us that the high number of disputes received, as well as disputes escalated to EDR schemes, were not as a result of systemic weaknesses. These entities have since reviewed their measures and verified there are no systemic weaknesses.

Recommendations

52 To ensure accountability, top management of a responsible entity should be provided with reports about disputes that include information on the actions taken and decisions made on the disputes: see Appendix 1 of RG 165. Responsible entities should review their IDR measures to ensure that they meet the requirements outlined in RG 165.

Risk management systems

53 As AFS licensees, responsible entities are legally obliged to have adequate risk management systems. These systems are fundamental to mitigating exposure to relevant risks and informing business decision making. Under s912A(1)(h) of the Corporations Act, responsible entities have an ongoing obligation to maintain adequate risk management systems.

54 The international standard for risk management defines risk as the 'effect of uncertainty on objectives' and risk management as 'coordinated activities to direct and control an organization with regard to risk': see International Standard ISO 31000:2009 *Risk management: Principles and guidelines.* Adequate risk management systems identify, analyse and treat the material risks faced by the responsible entity and the schemes it operates in a comprehensive and systematic way. Sound corporate governance and management oversight are an essential part of any effective risk management systems.

Our findings

55 The top three risks identified by responsible entities were operational risk, closely followed by market risk and regulatory risk. Other risks identified included governance, capital, personnel and liquidity risks.

56 Most (22) of the responsible entities had reviewed their risk management systems in the 12 months before our surveillance. Four responsible entities reviewed their risk management systems two years ago. Two did not have risk management systems.

57 We found that the risk management systems of the four responsible entities that did not review their system annually did not meet the requirements of international standards governing risk management.

Actions taken

58 We required two responsible entities to create and implement risk management systems, and another two responsible entities to update their risk management systems.

Recommendations

59 As AFS licensees, responsible entities must have adequate risk management systems in place. Responsible entities should review and, if necessary, amend their risk management systems to take into account our guidance in RG 259.

Compliance measures

60 As AFS licensees, responsible entities must establish and maintain compliance measures that ensure, as far as is reasonably practicable, that they comply with obligations as a licensee. Responsible entities also have duties under the Corporations Act to ensure the compliance plan of a registered scheme sets out adequate measures to ensure compliance with the Corporations Act and the constitution of the scheme, and that these measures are followed. Compliance plans and measures should not be seen as static.

61 We sought to understand the level of board involvement in the approval and review of responsible entities' documented measures for scheme operation, disclosure, compliance and risk management. Where responsible entities have documented standalone measures, we found that board oversight in the areas of related party transactions and conflicts of interest were highest; 20 boards were involved in approving and reviewing these measures.

62 Around half (15) of the responsible entities' boards approve and review measures for risk management, complaints management, outsourcing and information technology. We found that boards were least involved in the approval and review of measures for scheme operations, such as product design and calculation of payments and returns. Another area that may potentially benefit from an increase in board oversight is disclosure issued

about schemes. We noted that responsibility for the approval and review of measures for areas with least board oversight are often delegated to heads of departments or board committees.

Our findings

63 Nearly all (25) of the responsible entities review their compliance measures to ensure that they address the risks identified through their risk management systems. We found that the majority of reviews were undertaken at most 18 months before our surveillance.

64 Consistent with our finding on risk management systems, we also found that the same four responsible entities, whose risk management systems do not meet international standards, do not have compliance measures that meet international standards governing effective compliance.

65 We found that all responsible entities had at least one person within their compliance functions; the larger responsible entities dedicated, on average, three compliance personnel to compliance functions. We also observed that in some instances, the compliance function within an entity is not a dedicated role.

66 The reporting lines for personnel who are responsible for the compliance function within the entity vary significantly, depending on the size of the operation of the responsible entity. Most commonly, personnel who are in charge of the compliance function have a direct reporting line to the board. However, we also found compliance personnel with direct reporting lines to the chief operating officer, chief financial officer, general counsel, compliance committee, executive directors, and chief actuary and risk officer. In one instance, the personnel responsible for compliance did not have a reporting line to the board or management.

67 We had a number of concerns about the quality of compliance plans. In some cases the inadequacies were general in nature, and in other cases the issues related to specific compliance measures not being included in the plan or being inadequately set out in the plan. For instance, where no documented standalone measures are maintained, some compliance plans do not contain sufficient details on the legal concepts and requirements, the tasks that must be carried out, the person responsible, how the obligations can be met, and how the tasks are to be monitored. We are also concerned by plans that require one person to monitor a number of, if not all, the measures, or where the persons nominated have other significant and possibly conflicting duties.

Actions taken

68 Two responsible entities lodged updated compliance plans in response to specific concerns we raised. We are continuing our surveillance of two other responsible entities because we are concerned about the quality of their compliance plans.

69 Five other responsible entities have lodged replacement compliance plans with ASIC since the commencement of our surveillance program.

Recommendations

70 Responsible entities should actively monitor and amend their compliance measures to ensure they remain adequate and have been implemented. We recommend that responsible entities continually monitor and regularly review their compliance measures, including the adequacy of resources applied to the compliance function, and amend them as necessary.

Cyber resilience

71 Cyber resilience is now widely regarded as one of the most significant concerns for the financial services industry and the economy at large. We have previously emphasised that the cyber resilience of our regulated population is a key focus. Cyber resilience is of particular importance given the role financial services providers play in our economy.

Our findings

Cyber resilience landscape

72 While it appears that responsible entities are recognising cyber risks and are taking steps to manage these risks, we noted that the degree of sophistication and robustness in cyber risk management practices varies significantly.

73 Approximately half of the responsible entities described their cyber risk management as 'risk-informed' against the NIST Cybersecurity Framework implementation tiers. We found that these cyber risk management measures were approved by management, but that there was no entity-wide approach to managing cyber risks and responding to cyber threats.

74 The larger responsible entities described their cyber risk management as either 'repeatable' or 'adaptive'. These were characterised by a formal and rigorous entity-wide approach to managing cyber risks. Accordingly, these responsible entities are, or should be, able to respond more effectively to changing cyber threats and technology landscapes.

75 In general, we found that the responsible entities recognised the growing threat of malicious cyber activity. We also found a wide range of standards, frameworks and approaches being used to address cyber risks. The extent to which responsible entities have adopted recognised frameworks and standards for addressing cyber resilience varies significantly, with some meeting only certain aspects of the US-developed NIST Cybersecurity Framework.

Malicious cyber activity

76 We found that nine of the responsible entities were subject to malicious cyber activity in the 12 months before our surveillance. Two responsible entities did not know whether they had been subject to any malicious cyber activity.

77 All but three of the responsible entities addressed cyber risk as part of the entity's overall risk management framework.

78 We also found that a significantly high proportion of the agreements that responsible entities have in place with external service providers did not explicitly address cyber risks. Only 11 responsible entities had such clauses in their agreements. This is particularly concerning, given responsible entities' reliance on external service providers in areas of investment management, compliance, information technology, fund administration and custodian functions. The service providers of three responsible entities were subject to malicious cyber activity in the 12 months before our surveillance, but four responsible entities did not know if their service providers have been subject to any malicious cyber activity.

Actions taken

79 We required seven responsible entities to address the adequacy of their existing cyber resilience measures as part of their overall risk management obligation. As a result, six responsible entities have initiated reviews of their cyber resilience measures. Our continuing surveillance includes one responsible entity because we are concerned about their cyber resilience measures.

Recommendations

80 Responsible entities should review and, where applicable, strengthen their existing cyber resilience measures against the NIST Cybersecurity Framework, particularly in light of the number of responsible entities within our sample that have experienced malicious cyber activity: see REP 429 for more information. We consider that the NIST Cybersecurity Framework has particular relevance as a standard to manage cyber resilience and as a global benchmark for financial services providers.

Values and behaviours

81 It is important for the board and senior management of responsible entities to promote a culture where everyone has ownership and responsibility for doing the right thing and ensuring good outcomes for consumers.

Our findings

82 We sought to identify the manner in which responsible entities determine and embed the values and behaviours they expect of their people, to reinforce the culture of the entity.

83 We found that 17 of the responsible entities had standalone measures addressing this area in various forms—such as employee handbooks, codes of conduct and employment manuals—while others detailed their expectations in individual employment contracts and human resources statements. We also found that 13 of these were reviewed in the 12 months before our surveillance, but only 10 of the documented measures were approved by the responsible entities' board. Responsibility for approval was delegated to the chief executive officer, director or board committees in all other instances.

84 While it is encouraging to see that responsible entities have measures in place that express their values and expected behaviours, we are concerned that in a number of entities' boards have delegated the responsibility for approval of these to other parties within the entity.

Recommendations

85 Boards should influence the culture within the responsible entity by:

(a) setting the tone from the top, to ensure that desired values and behaviours are given appropriate prominence;

(b) putting in place governance structures to ensure this tone is implemented in an effective way throughout the entity;

(c) monitoring the management team's alignment with the entity's values and behaviours; and

(d) making sure the management team are held accountable where there is a misalignment.

Rewards and incentives

86 Remuneration, incentives, performance management and promotions can act as motivators and reinforce behaviours. Research generally supports the principle that where employees have an interest in the companies they work

for, this can lead to greater engagement and improved business performance. However, when combined with the wrong culture, incentives can lead to great harm to companies and consumers.

Our findings

87 We found that 24 of the responsible entities have formal processes in place to review conduct of directors and employees. Most (20) responsible entities review employment arrangements to identify incentives that may result in directors or employees behaving in a way that does not comply with the entity's obligations under their AFS licence.

88 We also found that responsible entities that do not review employment remuneration measures as part of their risk management systems also do not assess employment arrangements against their compliance measures.

89 Just under half (11) of the responsible entities had specific documented measures to address rewards and incentives within the entity. The majority of these measures were approved and reviewed by the board. Additionally, 12 responsible entities had in place specific measures to address employee breaches and appropriate disciplinary action. Board involvement in reviewing disciplinary measures is higher compared to involvement in reviewing rewards and incentives measures.

90 We found the processes adopted by responsible entities for approving employment arrangements vary significantly, depending on the size and complexity of the entity. Larger responsible entities adopted a panel process, such as a remuneration committee, whereas smaller responsible entities often relied on the approval of a single person (e.g. a chief executive officer or senior executive).

Actions taken

91 In response to concerns we raised, one responsible entity included provisions for assessment of directors in its compliance measures and another revised its measures to require annual declarations about the conduct of their responsible managers.

Recommendations

92 Remuneration, rewards and incentive structures should be aligned to the values of the responsible entity, to motivate and reinforce the culture of the entity and the conduct expected of its staff. Responsible entities should review and integrate incentive governance as part of their overall risk management systems and compliance measures to ensure the structure of rewards and incentives does not promote unnecessarily risky behaviours.

Whistleblowing

93 We have been highlighting the importance of culture in promoting trust and confidence in the market. We sought to understand the extent to which responsible entities have in place measures that encourage and protect an employee's rights to express concerns about the activities of the responsible entities.

94 Company officers and other persons have legal obligations under the Corporations Act if a whistleblower discloses information to them. Unless they handle the disclosure correctly, they may inadvertently breach the Corporations Act if they tell an unauthorised third party (including other officers of the company). Any unauthorised disclosure may trigger significant civil and criminal consequences.

Our findings

95 Just over half (15) of the responsible entities had measures addressing employees' rights to report their employer's misconduct, but only nine of these responsible entities have established and maintained documented measures specific to whistleblowing. Only seven of the whistleblowing measures were approved or reviewed in the 12 months before our surveillance.

96 We also found that board involvement in and oversight of the ongoing review of whistleblowing measures was not high. Only eight boards were involved in the review of their responsible entity's documented whistleblowing measures.

Actions taken

97 As a result of the concerns we raised, one responsible entity updated its whistleblowing measures and introduced proactive measures that ensure the whistleblowing measures contain accurate information and clearly assign roles and responsibilities. We have required another entity to introduce formal documented whistleblowing measures.

Recommendations

98 Responsible entities should implement an appropriate whistleblowing measures to ensure they meet their legal obligations and support an open and transparent culture within the entity.

99 Responsible entities should also set up training for all staff and periodically check on the effectiveness of their measures.

100 The Corporations Act does not prescribe any particular procedures. Ideally, any training should focus on the importance of obtaining the whistleblower's consent to pass on the information to necessary third parties so that it can be investigated or its impact assessed. Responsible entities should consider whether the measures recommend that whistleblowers disclose directly to an appropriate person—such as the chairman of the audit committee of the board or some other person, as required by another regulator or overseas regulatory requirement relevant to the company.

Product approval and review

101 We sought to understand the extent to which responsible entities undertake consumer testing before approving products. We consider it important that responsible entities take into account the needs of consumers when designing and targeting their products.

Our findings

102 Just over a third (11) of the responsible entities had documented measures specific to product design, approval and review. The majority of these measures were approved in the 12 months before our surveillance. Most notably, only three boards of responsible entities were involved in the review of these measures.

103 We also found that, in smaller responsible entities, the personnel or group responsible for the approving financial products offered by the entity are often also responsible for reviewing those financial products. However, the measures in larger responsible entities are more resource intensive, often involving the board, due diligence committees, compliance personnel, legal teams and product specialists (head of products).

104 We found that there is a general lack of consumer-focused culture. The majority of the responsible entities did not consider whether their financial products meet and continue to meet the needs of the target investor market as part of their product approval and review measures. We also found that only four of the responsible entities undertake consumer testing before offering their products to the market.

Recommendations

105 Responsible entities should have a consumer-focused culture. As part of their duty to act in the best interests of their investors, they should consider whether their financial products meet and continue to meet the needs of their investors. Responsible entities should assess their product approval and review measures to ensure they include this consideration.

Key terms

Term	Meaning in this document
AFS licence	An Australian financial services licence under s913B of the Corporations Act that authorises a person who carries on a financial services business to provide financial services Note: This is a definition contained in s761A.
AFS licensee	A person who holds an AFS licence under s913B of the Corporations Act Note: This is a definition contained in s761A.
Corporations Act	*Corporations Act 2001*, including regulations made for the purposes of that Act
EDR scheme	An external dispute resolution scheme approved by ASIC under the Corporations Act (see s912A(2)(b) and 1017G(2)(b)) and/or the National Credit Act (see s11(1)(a)) in accordance with our requirements in Regulatory Guide 139 *Approval and oversight of external complaints resolution schemes* (RG 139)
financial service	Has the meaning given in Div 4 of Pt 7.1 of the Corporations Act
financial services provider	A person who provides a financial service
IDR measures	Internal dispute resolution measures that meet the requirements and approved standards of ASIC under RG 165
measures	The policies, processes, procedures, arrangements, frameworks or control systems of AFS licensees
NIST Cybersecurity Framework	National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
PI insurance	Professional indemnity insurance
REP 429 (for example)	An ASIC report (in this example numbered 429)
retail client	A client as defined in s761G of the Corporations Act and Div 2 of Pt 7.1 of Ch 7 of the Corporations Regulations 2001
responsible entity	The company named in ASIC's record of a scheme's registration as the responsible entity or temporary responsible entity of the scheme
RG 126 (for example)	An ASIC regulatory guide (in this example numbered 126)

Term	Meaning in this document
s912A (for example)	A section of the Corporations Act (in this example numbered 912A), unless otherwise specified
s912E notice	A notice issued by ASIC exercising our powers to request information under s912E of the Corporations Act
scheme	A registered managed investment scheme under Ch 5C of the Corporations Act

Related information

Headnotes

breach reporting, compliance frameworks, compliance measures, compliance plans, conflicts of interest, custody, cyber resilience, dispute resolution, product approval and review, professional indemnity insurance, registered managed investment schemes, responsible entities, rewards and incentives, risk management systems, surveillance, values and behaviours, whistleblowing

Regulatory guides

RG 126 *Compensation and insurance arrangements for AFS licensees*

RG 133 *Managed investments and custodial or depository service providers: Holding assets*

RG 165 *Licensing: Internal and external dispute resolution*

RG 181 *Licensing: Managing conflicts of interest*

RG 259 *Risk management systems of responsible entities*

Legislation

Corporations Act, s912A, 912E

Reports

REP 429 *Cyber resilience: Health check*

Other documents

ASIC's Corporate Plan 2015–16 to 2018–19: Focus 2015–16

ASIC's Corporate Plan 2016–17 to 2019–20: Focus 2016–17

ISO 31000:2009 *Risk management: Principles and guidelines*

Treasury, *Design and distribution obligations and product intervention power*