RG 132 Funds management: Compliance and oversight

This section looks at new guidance on compliance and oversight obligations for investment funds, including some background on ASICs existing compliance guidance and why are proposing to update it, then an outline the new guidance we have proposed in Consultation Paper 296.

Background: Why have we updated RG 132?

The proposed new Regulatory Guide 132 *Funds Management: Compliance and oversight* is a new RG that provides new, updated and consolidated guidance.

The new RG is intended to replace our existing compliance plan guidance, which is currently set out in a variety of places. This includes the existing RG 132, as well as RGs 116-120, which provide commentary on compliance plans for specific types of MIS – agricultural MIS, financial asset MIS, contributory mortgage MIS, pooled mortgage MIS and property MIS.

In the new RG 132, we propose to provide guidance about:

- how an effective and responsive compliance management system can be developed to comply with the broad compliance obligation in s912A of the Corporations Act;
- where an investment fund is required to have a compliance plan, the content of a compliance plan that meets the requirements of the Corporations Act; and
- oversight functions performed by compliance committees, compliance plan auditors, depositaries for CCIVs, and implementation reviews and independent oversight entities for Australian passport funds.

RG 132 has not been updated since 1998. We are taking this opportunity to update and consolidate our guidance in light of our experience with compliance plans since then.

We are attempting to produce guidance that takes into account previous surveillance findings and global standards for compliance.

Previous ASIC surveillance projects have found, for example:

- inappropriate compliance controls due to the use of off the shelf compliance plans or the adoption of controls from the compliance plan for a different type of MIS;
- many compliance controls are too vague so that it is not possible to determine whether the control has actually been complied with;
- problems with the quality and thoroughness of compliance audits, including lack of audit standards, testing of master compliance controls rather than audit testing of controls for each MIS, and limited assessment of whether the compliance plan is adequate in addressing compliance risks; and
- ad hoc, and sometimes poor, standards for compliance committee members.

We have focused on improving our guidance in these areas.

Outline of our proposed new guidance

In refreshing our guidance on compliance and oversight requirements for investment funds, we have taken into account the broad compliance obligation as an AFS licensee, as well as specific compliance and oversight requirements that exist for investment fund operators.

What is the broad compliance obligation?

AFS licensees are subject to the broad compliance obligation under the Corporations Act. That is, an AFS licensee is required to do all things necessary to ensure its financial services are provided efficiently, honestly and fairly under s912A(1)(a) and comply with the financial services laws under s912A(1)(c) and comply with the conditions on its AFS licence under ss912A(1)(b).

These requirements apply to:

- responsible entities of registered MIS;
- licensed operators of unregistered MIS;
- corporate directors of CCIVs (both retail and wholesale CCIVs);
- platform operators;
- MDA providers

RG 104 *Licensing: Meeting the general obligations* contains existing guidance for all AFS licensees and this will continue to apply to the wider set of AFS licensees. Our proposed new guidance in RG 132 builds on the principles in RG 104 but is limited to our expectations for the compliance management systems of the funds management industry.

How do you meet the broad compliance obligation?

We consider that implementing an effective and responsive compliance management system is the way that entities can meet their obligations as AFS licensees.

Our proposed guidance is based on the international standard for compliance management systems (AS ISO 19600:2015). We think it is important that our guidance doesn't conflict with existing standards – and that it is capable of being implemented across vertically integrated businesses.

In our proposed guidance, we have outlined what we consider to be the key features of an effective compliance management system. These include:

- an understanding of the context in which the MIS, CCIV, IDPS or MDA operates – we don't take a 'one-size-fits-all' approach to what is required for a compliance management system. But rather, we acknowledge that what the operator needs to do to comply with its compliance and oversight obligations will vary according to the nature, scale and complexity of its organisation;

- clear articulation of the values, purpose and strategy of the responsible entity, corporate director, wholesale scheme operator, IDPS operator or MDA provider. The compliance management system should reflect the values, purpose and strategy of the organisation – this may involve, for example, fostering an awareness within the organisation of compliance issues, tailoring compliance processes for the organisation rather than generic policies designed merely to satisfy a regulatory requirement, training staff to understand the operator's compliance management system, and adequately resourcing the compliance function;

- identification of compliance obligations, risks and objectives – this means a structured and systematic process that considers the operator's compliance obligations, identifies the risks of non-compliance, and establishes compliance controls designed to meet these risks. It is more than just a "tick the box" exercise. I will talk more in a moment about implementation of compliance controls to respond to these identified compliance obligations, risks and objectives;

- clarity of roles and responsibilities of those people involved in the compliance management system – an important aspect of compliance is the 'three lines of defence' model, which involves:

    - taking responsibility at the operational level for carrying out appropriate compliance controls to ensure compliance with the law, the compliance plan and the constitution;

    - an independent compliance function within the organisation having oversight of compliance throughout the organisation; and

    - independent oversight, including internal and external audit functions providing independent assurance over the compliance framework;

- organisational support for the compliance management system – appropriate organisational support will depend on the nature, scale and complexity of the operator, the fund and its compliance management system;

- appropriate documentation and record keeping – documenting compliance controls and responsibilities and ensuring that that documentation is easily accessible by staff and management should assist in embedding the compliance management system within the organisation, while record keeping will assist in the evaluation of the compliance management system;

- monitoring and reporting of performance against the compliance management system – monitoring and evaluation encompasses all aspects of the compliance management system, including feedback to determine the root causes of non-compliance, assessing whether the responsibilities of employees involved in the compliance management system are appropriate and are being carried out appropriately, whether reporting to senior management and the directors is adequate, whether resources are adequate, whether any additional audits are required, and so on; and

- procedures where non-compliance occurs and for continual improvement of the compliance management system – depending on the nature, scale and complexity of the operator, fund and compliance management system, non-compliance procedures could include things such as rectifying non-compliance and managing the consequences, reviewing the effectiveness of action and identifying the root cause to determine where changes should be made to the compliance management system, timely escalation and reporting to ASIC where necessary.

Compliance plans

In addition to its broad compliance obligation as an AFS licensee, a responsible entity of a registered scheme or a corporate director of a retail CCIV must ensure that the investment fund has a compliance plan and that it complies with the compliance plan.

The compliance plan is an important part of the overall compliance management systems for registered MISs and retail CCIVs.

Establishing adequate compliance controls in the compliance plan

We consider that in order to establish adequate compliance controls in a compliance plan, the investment fund operator should ensure that:

- The compliance controls in the compliance plan are aligned with the investment fund operator's values, objectives and strategy, taking into account the nature, scale and complexity of the particular investment fund and, for a CCIV, each sub-fund of the CCIV. This ensures that compliance is more than just a "box ticking" exercise;
- There should be a clear and demonstrated nexus between the compliance obligations and compliance controls, and the compliance controls should reflect the actual procedures, processes and practices of the investment fund operator and the investment fund – while the content of the compliance plan will depend on the nature, scale and complexity of the operator and the fund, we would expect, as a minimum, the compliance plan to include content about:
    - The scope of the compliance plan;
    - A description of the investment fund operator and its operations and the investment fund and its investment strategy or, for a CCIV, the investment strategy of each sub-fund;
    - The specific compliance obligations that apply to the investment fund operator and the investment fund – we note that a compliance plan may incorporate parts of another plan, however the incorporated plan should be for the same type of investment fund – a model or off-the-shelf plan is less likely to adequately target the risks of the specific investment fund;
    - The identified compliance risks and compliance controls to address these risks, including details about:

        - Who is responsible for performing the compliance control and monitoring that performance – the compliance plan must clearly identify the person responsible for a compliance control or monitoring process so that there is sufficient accountability for actions under the compliance plan, and provide for separate people to have responsibility for carrying out a particular compliance control and the monitoring of that compliance control;

        - The frequency with which the compliance control must be performed – the frequency and quantity of compliance controls, and their monitoring, should be sufficient to effectively manage the compliance risks;

        - How compliance with the compliance control is monitored – the processes for monitoring compliance with the compliance controls should be described with sufficient details and certainty to assess whether they will be or have been complied with;

        - Who is responsible for reporting on whether or not the compliance control has been followed and when and how reporting takes place – any non-compliance should be reported to the compliance committee, the board or ASIC as required;

    - The compliance plan should include information about when it will be reviewed, how it will remain fit for purpose, how the investment fund operator will ensure that necessary changes are identified and that the compliance plan is updated – the compliance plan must be maintained so that it is adequate and up to date at all times;

- The compliance controls should be set out with enough certainty to allow the investment fund operator, ASIC and the auditor of the compliance plan to assess whether the investment fund operator has complied with the compliance plan – this doesn't necessarily mean that a compliance plan should detail each and every step, check, detailed procedure or action, but the compliance controls, and processes to monitor them, should be specific and measurable to identify an output or outcome. The compliance controls should be described in a way that represents more than mere platitudes or broad ambitions of compliance;

- The compliance plan should be written in a clear manner so that it is usable by its target audience – users could include compliance and operational staff, internal audit and review, the compliance committee, senior management, directors, the compliance plan auditor, and ASIC. Each of these end users may have similar or different requirements and needs that should be considered as part of the planning for a compliance management system.

What compliance risks should be addressed in the compliance plan?

In giving guidance about the content of a compliance plan, the approach we have taken in RG 132 recognises that some compliance risks exist at two levels:

- The group level – by this we mean those compliance risks that arise from requirements that apply because the investment fund operator is an AFS licensee, management of staff,

finances and other processes at the investment fund operator level, or, for a CCIV, processes that are common across the various sub-funds of the CCIV; and

- Compliance risks at the registered MIS or sub-fund level which are largely driven by the nature, diversity and structure of assets invested in by the registered MIS or sub-fund and the investment strategy the operator employs.

Our guidance is not intended to be a checklist of compliance controls for investment fund operators. However, we propose to provide some illustrative guidance to assist responsible entities and corporate directors plan and establish their compliance plans.

Group level compliance controls

We propose to include some questions that responsible entities and corporate directors can consider in designing group level compliance controls.

Where group compliance risks exist, compliance controls can apply across the investment funds or sub-funds operated by the investment fund operator. It is not necessary for these compliance controls to be tailored and individualised to each specific registered scheme or sub-fund of a retail CCIV operated by the investment fund operator. However, the compliance controls must be appropriate for the operator, rather than generic controls taken from an off-the-shelf compliance plan.

Our proposed RG 132 identifies some compliance risks that we think commonly sit at the group level. These include:

- Management and oversight
- Training, recruitment and experience
- Accounts and record keeping
- Use of external service providers
- Related party issues
- Cyber resilience and business continuity
- Applications, redemptions and distributions
- Disclosure and reporting
- Distribution channels
- Identifying, recording, rectifying and reporting of breaches
- Complaints handling
- AFS licence conditions

Compliance risks for CCIVs can also be subject to group level compliance controls. These can include, for example, matters relating to establishing new sub-funds, allocation of assets and liabilities to a sub-fund, and the relationship between the depositary and corporate director.

Registered MIS or sub-fund level compliance controls

At the registered MIS or sub-fund level, a compliance plan should address compliance risks and compliance controls that are tailored to the nature, scale and complexity of the investment fund (and sub-fund of a retail CCIV where applicable) and the investment strategy the operator employs. This means that, for different types of registered MIS or sub-funds, there will be different areas of focus in the development and implementation of appropriate compliance controls.

As I mentioned at the start, our existing compliance plan guidance is currently set out in the existing RG 132, as well as RGs 116-120 for agricultural MIS, financial asset MIS, contributory mortgage MIS, pooled mortgage MIS and property MIS. Given our desire to move to more granular asset kinds for registered MIS and CCIVs, having multiple tailored RGs for each asset kind is not feasible. Instead we are proposing to give combined guidance in the new RG 132.

Our new approach picks up aspects of our current guidance in RG 116 to RG 120. We have also brought in material from other guides where appropriate, for example the guidance currently in RG 133 on asset holding and custodial arrangements, or the compliance guidance in our existing cyber resilience information sheet.

As with our guidance on group level compliance risks and controls, our approach is to include some questions that responsible entities and corporate directors can consider in designing registered MIS or sub-fund level compliance controls. We have identified some compliance risks that we think commonly sit at this level, depending on the type of fund and the assets it invests in. These compliance risks include:

- Investment strategy, including sovereign risk, technology dependence, and agricultural and environmental risks
- Fees and costs
- Asset holding and custodial arrangements
- Valuation
- Pricing of interests and shares
- Securities trading
- Leverage
- Credit
- Other business risks

Compliance plan requirements for CCIVs

Compliance plan requirements for CCIVs are based on the existing Corporations Act requirements for registered MIS. That is, the compliance plan must set out adequate measures that the responsible entity or corporate director is to apply in operating the fund to ensure compliance with the Act and the fund's constitution. Although the existing s601HA includes some specific content requirements for registered MIS compliance plans, the CCIV legislation has been drafted to be less prescriptive. However, we would expect corporate directors and responsible entities to take similar approaches in preparing their compliance plans.

Compliance plans for Australian passport funds

Under the Australian Passport Rules, the operator of an Australian passport fund is required to have a compliance framework that ensures ongoing compliance with relevant laws and regulations.

We propose that an Australian passport fund will satisfy this requirement through complying with the relevant Corporations Act requirements. That is, by having a compliance plan, compliance plan audit, and, if required, a compliance committee.

In addition, where the Australian Passport Rules impose obligations beyond those required of registered MIS and retail CCIVs under the Corporations Act, we expect the compliance plan for an Australian passport fund to address those additional requirements. This could be, for example, compliance controls to ensure delegated functions are performed in accordance with the Passport Rules, compliance with portfolio allocation limits or restrictions, or performance fee arrangements.

Oversight

We propose to include in RG 132 a new section setting out guidance about oversight functions. This will cover oversight functions for registered MIS, as well as the new oversight functions introduced as part of the CCIV and ARFP regimes.

Oversight of registered MIS and CCIVs occurs through:

- Compliance committees;
- Compliance plan audits; and
- Depositaries of CCIVs.

Compliance committee

Our proposed guidance about our expectations on aspects of a registered MIS's compliance committee is new. Our surveillance findings have shown us that guidance about what we expect from compliance committees was needed. So we have included our expectations on issues including:

- The functions and duties of the compliance committee, such as monitoring compliance with the compliance plan, reporting breaches to the responsible entity and ASIC, and assessing whether the compliance plan is adequate;

- What should be addressed in the terms of appointment of compliance committee members. This includes the role, objectives and responsibilities of compliance committee members, and their independence;

- Appropriate standards for experience, qualifications and competence of compliance committee members, including ongoing training and education. These standards should cover matters such as relevant tertiary qualifications, experience in undertaking compliance activities and investigations, experience in managing or overseeing the management of assets of the type invested in by the fund, and an understanding of regulatory requirements and how they apply; and

- The performance of functions of the compliance committee, including the holding of regular meetings and appropriate record-keeping.

Compliance plan audit

We propose to include guidance on the conduct and standards of compliance plan audits. This guidance is not intended to replace Auditing and Assurance Standards Board standards, but rather RG 132 refers to the AUASB standards, and merely provides minimal additional ASIC guidance on discrete issues which are particularly problematic for compliance plan audits.

So, for example, where an operator has group level compliance controls or a master compliance plan which apply to more than one registered MIS or sub-fund, we consider that the auditor is still required to assess whether the compliance plan is adequate for each registered MIS or sub-fund. It may be sufficient in some cases to test compliance with common compliance controls across investment funds, rather than individually for each investment fund. However, it would not be sufficient to rely on a sample of the investment fund operator's compliance controls or testing across only some of the investment funds if there are important differences in the types of funds that affect the design or effective operation of a compliance control.

Depositaries of CCIVs

We propose to give guidance about how a depositary can perform its oversight role and meet its obligations. Rather than propose a lot of prescriptive guidance about depositaries when this is a new oversight function in the Australian market, we have provided some high level guidance. Over time, we would expect that our guidance in this area might be fleshed out. But at this stage we didn't want to be too restrictive.

We propose to give guidance on:

- The requirement that the depositary must act on instructions. . For example, the depositary should establish and implement appropriate procedures to verify that the instructions from the corporate director are lawful and comply with the constitution, as well as an escalation procedure where the instructions are not lawful or do not comply with the constitution;

- In performing its oversight duties, we consider a depositary should test and verify the procedures that are the responsibility of the corporate director or its delegate. In our view, this testing and verification can occur after the fact, rather than at each point the corporate

director performs the activity. The depositary should ensure that an appropriate testing, verification and reconciliation procedure is implemented and frequently reviewed; and

- Where the corporate director has outsourced services, it is not sufficient for the depositary to simply rely on a report prepared by the auditor of the service provider. We expect the depositary to obtain sufficient and appropriate evidence on which to base its supervision of the corporate director and the outsourced service provider.

Oversight of Australian passport funds

The oversight requirements under the Australian Passport Rules do not replace the requirements of the Corporations Act. This means that we expect an Australian passport fund to still meet the requirements of the Corporations Act in relation to compliance plans, compliance committees and compliance plan audits. However, we expect that where the obligations overlap, the operator can satisfy both sets of obligations at the same time.

For example, the independent oversight entity required under the Passport Rules is each of the external directors of the Australian passport fund operator or, if there is a compliance committee, the compliance committee. This means that we do not expect the Australian passport fund operator to appoint a separate person or group of people to act as the independent oversight entity separate from the compliance committee.

An Australian passport fund operator must ensure that an implementation review of the operation of the Australian passport fund is conducted annually. This implementation review must be conducted by a registered company auditor, an audit firm or an authorised audit company. We consider that the auditing standard on compliance engagements - ASAE 3100 *Compliance engagements* - is the appropriate standard for an implementation review, similar to our expectations for a compliance plan audit. The requirement for an annual implementation review of an Australian passport fund is in addition to the requirement for a compliance plan audit. However in forming their opinion, the reviewer will need to take into account information available to them from any compliance plan audit they have conducted.

Questions

What is the utility of the depositary having to ensure that the instruction complies with the constitution, given that constitutions are generally very broadly drafted?

That's a Treasury requirement, not an ASIC one. That requirement is a continuation of existing requirements, rather than a new one for the ARFP or CCIV regime.

Do you think compliance committees will be introduced for CCIVs?

That's also a matter for Treasury. But I think Treasury will consider the existing oversight functions that exist.

What interaction does ASIC expect between the requirements in RG 259 and the requirements in RG 132, in relation to group, scheme and sub-fund risks?

They should be consistent with each other. In RG 132 we are trying to reflect areas of focus where we're looking at specific registered MIS or CCIV types, and the focus should be more on compliance outcomes than risk.

RG 259 also includes best practice examples that help you align between risk management and compliance expectations. We would expect you'll be using RG 259 when you're developing your compliance functions and looking at your risks, so it fits in the planning, development. And then RG 132 is more about the outcomes of those risks, and how they flow through to compliance.

What does ASIC consider keeping compliance plans up to date at all times looks like?

Obviously there's a practical element of that, and you can't be updating things constantly. But some of the surveillance results that we saw when we looked at a compliance plan audit, we found that a law or guidance had been updated 6 months previously and no-one had updated the compliance plan, and/or the compliance audit didn't red flag that. So in those sorts of situations, you should be considering that to be out of date. You need to keep up to date with changes to the law or regulations, significant changes to guidance, or changes within the fund.

Can you elaborate on ASIC's interpretation of the difference between a fund 'must do', 'should do', 'could do' and 'ASIC's expectations'?

First of all the RGs are drafted to reflect the legislation. Where the legislation says something must be done, this is reflected in our guidance.

Where we use ‘should do’ or ‘ASIC expects’, it generally reflects what we consider to be the best practice. However, it is not normally something that must be done in the legislation. Often this type of guidance results from surveillance findings or other regulatory data that shows standards should improve.

We generally use ‘could do’ where we recognise that there are different options to choose from. It’s up to the operator to determine whether what is being suggested will work for them and their fund..

When ASIC introduces a new Australian standard for compliance plans, will existing regulatory guides that refer to the existing requirements be updated?

We will generally make that decision when new standards are introduced. Often we will try and include these types of updates as part of general updates and policy reviews.

High level comparing between the CCIV oversight and the responsible entity space. And in the Venn diagram the depositary is part of that oversight. Does that means for the responsible entity or MIS a similar function is all captured within the responsible entity oversight?

Essentially, the depositary has a clear legislative oversight function, and that function is limited to certain things. But the legislative settings for the MIS regime are different. The responsible entity or compliance committee are performing, broadly, an oversight functions, but because of the

difference in the legislative settings, there will be differences that flow through to each of those roles.

Regarding RG 259, is there a plan or a need to extend that beyond the MIS and to CCIVs as well?

We would expect that it will be extended to cover CIVs, and corporate directors. The reason we would do that is that is that otherwise there will be some regulatory arbitrage between two vehicles that are similar in nature. And what the Government is keen to avoid is where one regime looks better than another regime.