FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

May 2018

Compliance assurance programmes

This information sheet explains the Financial Markets Authority's expectations for a compliance assurance programme (CAP). It will be useful for entities holding or applying for a licence under the Financial Markets Conduct Act 2013, and anyone involved in the creation, implementation and ongoing operation of a CAP.

Overview

Entities licensed under the Financial Markets Conduct Act 2013 (FMC entities) are required to have adequate and effective arrangements for challenging and testing their own compliance functions, framework and controls. This is a minimum standard for licensing, and to meet this obligation FMC entities should consider having a CAP in place.

This information sheet provides guidance about CAPs, including the minimum standards, our expectations, and what we look for when assessing a licence application and during monitoring of an FMC entity. It also includes elements of what we believe good practice looks like for a CAP.

We discuss the application of the minimum standards in the following section.

What is a compliance assurance programme?

A CAP is the programme of independent checks to test whether an entity's processes and controls are effective in ensuring the compliance of the business.

We appreciate the term 'compliance assurance programme' is easily confused with a Compliance Programme, but the two are very different.

A CAP provides the entity's oversight body (for example, the board of directors) with *assurance* that the compliance systems operate effectively and ensure the ongoing compliance of the business. It should challenge and test the design and operation of the entity's processes and controls, the adequacy of governance and management information.

The document that describes the CAP may be part of the entity's wider risk, compliance and governance framework and policies, or it may be a stand-alone document – but the CAP itself is a programme of checks, not a policy, compliance plan or risk register. If the CAP is documented within a policy or framework, its attributes need to be clearly distinguished from other parts of the document.

Effective compliance assurance is an important part of governance arrangements for a licensed firm, but it does not need to be elaborate or complicated. As with core compliance processes, the CAP should be fit for purpose for the entity.

The overriding principle for a CAP is that the programme must be *performed independently* of those responsible for undertaking and directly managing the functions that are tested.

Minimum standards

1. Compliance assurance – you have adequate and effective arrangements to challenge and test the design and operation of your processes and controls, and the adequacy of your governance and management information. This is your compliance assurance programme.

Testing compliance

Compliance testing should challenge the operation of processes and controls, the adequacy of governance, and the information provided to management and the oversight body. Testing can be risk-based, following a clear assessment of risk.

The scope, methodology and results of testing should be documented. The exact nature of testing will vary depending on the company's structure and the relevant risks, but consideration should be given to:

- the nature and size of the business
- how systems and processes are designed
- the types and levels of risk in the business
- how involved the directors/oversight body are in overseeing day-to-day functions.

Larger businesses generally have more formal processes and greater separation between the governing body and staff, so will need more extensive testing to ensure processes and controls are working as intended.

A smaller business where oversight body personnel perform key functions, or manage staff that do, may be able to rely more on direct oversight or business knowledge and less on testing. Testing can then focus on specific areas of risk, instead of comprehensively covering all areas of the business.

Entities should explain the nature and level of testing, why they consider it appropriate for the business, and how findings are reported and followed up on.

Testing should include a review of the design and effectiveness of controls. This helps ensure controls address the risks they are intended to address, and that controls remain effective as the business changes.

Testing should consider:

- the nature of the control and how often it is performed
- adequacy of sampling – size and content of the sample need to be relevant to the process
- the risk rating of the process – higher-risk processes should be subject to more frequent control testing
- dependency on other controls
- exceptions in control effectiveness, and how they are reported and investigated.

For example

Client on-boarding applications and procedures – confirm procedures followed, records kept and exceptions reported.

Actioned by: Internal Audit

Report findings and actions to: Oversight body

Sample size: 5% of applications

Frequency: Quarterly

2. Your compliance assurance programme goes beyond day-to-day controls for key processes, by including more in-depth testing of processes and controls.

The guidance for this standard is covered in the following points.

The testing (and the design of it) is done independently of those involved in day-to-day processes and oversight – for example testing is done by a separate compliance or internal audit function, or by an external organisation.

Independence of testing

There is flexibility in how independence is achieved. For example, testing can be executed by a separate compliance function or by an external organisation.

- Larger businesses are likely to have a separate compliance assurance function that creates the CAP, undertakes compliance testing and reports to the oversight body on progress and findings.
- Smaller businesses may not find it practical to perform compliance assurance entirely independent of the specific function being tested. For example, in very small businesses, compliance testing may include staff peer-reviewing each other's work.

You allocate sufficient, appropriate resources to planning and carrying out the programme, and ensure those involved have the skill and experience to carry out the work.

Resources

FMC entities are required to allocate sufficient resources to planning and executing their CAP. These resources comprise personnel, technology and systems, which should be supported by adequate commitments from the oversight body.

The personnel involved should include those who understand the business of the entity and those who understand the compliance obligations. They need sufficient skill and relevant experience for their responsibilities, and should receive training to ensure their knowledge remains current and in line with legal and regulatory requirements.

Where appropriate to the size of the entity, internal resource can be complemented by external support from independent experts. This can help smaller entities in particular to avoid key person risk, where one person is responsible for multiple tasks that conflict with their other duties.

We expect people involved in testing to be independent and have appropriate authority to ensure findings or deficiencies are reported to the oversight body and any corrective actions are taken.

The technology and systems required to support the CAP will most likely be an extension of the wider compliance systems. However, the development of a specific framework of tools, recording systems, and support from information technology will help create a more robust process.

Outsourcing

Some FMC entities may choose to outsource all or part of their CAP. This may include establishing or reviewing the framework, and the compliance testing. Outsourcing may be appropriate for small businesses that don't have the scale or structure to employ an independent person for the role.

Regardless of which elements, if any, are outsourced, all FMC entities must recognise that outsourcing does not absolve them of their compliance obligations and responsibilities as a licensed entity. FMC entities must ensure they fully understand any documents, policies, procedures or testing plans produced by external parties. FMC entities should appoint personnel who are responsible for implementation and ongoing operation of any documents or plans created by external parties and must be able to explain their meaning and application to the FMA.

- Your compliance assurance programme is approved by your oversight body.
- Your oversight body is kept updated about progress against the compliance assurance programme – you also report significant findings to them and follow up on remedial action needed.

The oversight body and governance

The oversight body is the principal beneficiary of the CAP. The outcome of a well-structured and -implemented CAP is the assurance they gain that the compliance systems operate effectively and ensure the ongoing compliance of the entity.

FMC entities are required to have an oversight body to oversee compliance with their licence obligations, and to consider the adequacy and robustness of the entity's governance arrangements. Members of the oversight body should be senior members of the entity who can provide guidance and perspective in their governance of the CAP.

In smaller entities, the oversight body will often be the board of directors. In larger entities with more diverse operations, the oversight function may be performed by a committee of senior managers and representatives from legal, risk and compliance areas, with the board providing high-level oversight.

Regardless of the composition of the oversight body, its activities are likely to include:

- providing final approval of the CAP itself and reviewing at least annually. We expect the oversight body to provide management with guidance on the CAP, challenge its structure and content, and recommend changes where appropriate
- receiving regular information from management about the CAP's operation, planned and completed testing, and actions proposed to deal with any exceptions or failures
- meeting regularly to discuss management information and any other information (for example, from the third line of defence, regulators or external parties) about the CAP's design and operation.

The minimum standards require the oversight body to be kept updated about progress against the CAP. Our expectation is that FMC entities have processes in place to ensure information is provided to the oversight body regularly and in a timely manner to allow for proper oversight and decision-making.

Discussion of information from management, for example in a meeting of the oversight body, is an opportunity for the oversight body to observe management and question whether the 'tone from the top' relating to compliance is feeding down throughout the entity.

The oversight body should be provided with reports on the operation of the CAP – including any material findings or deficiencies, and any remedial actions. We expect oversight body meetings to be minuted, to provide evidence of discussion on findings, remedial actions and progress on implementation.

FMC entities should determine the most appropriate frequency to provide information to the oversight body. It should be regularly enough to enable the oversight body to understand how the CAP is operating, and to utilise the information in their decision-making processes. Additionally, we expect any external review of the CAP, for example by an auditor or regulator, would be reported to the oversight body.

Elements of good practice

Throughout the licensing process and during ongoing monitoring of FMC entities, we have encountered many examples of good practice in relation to CAPs, including the following:

- Compliance and assurance reporting included as a standing item on the oversight body's agenda, with the oversight body receiving reporting that provides an overview of recent and planned testing.
- The internal assurance function reporting directly to the oversight body or audit committee, which promotes independence and ensures the oversight body is properly informed of material issues within the business.
- Clearly defined roles and responsibilities for overseeing compliance within the entity.
- The skills and experience of the compliance person, function or provider who performs the independent checks are documented.
- Where external compliance consultants develop and maintain the CAP, the entity considers whether the CAP is designed specifically with the business in mind and is not just 'off the shelf'.
- The CAP is reviewed at least annually, and whenever it is impacted by business or regulatory changes.
- There is a register that sets out the obligations the FMC entity needs to comply with, and what controls are in place to achieve compliance.
- Documented details of how agreements with clients and outsource providers are monitored, and how failures are reported and addressed.

Monitoring

What the FMA might look for

FMC entities must meet the FMC Act eligibility criteria for the period of their licence. We monitor the licensed population and, while we may not engage regularly with all licensed entities, we expect entities to review their compliance on an ongoing basis, and strengthen processes and controls where and whenever possible.

The purpose of our monitoring is to determine how FMC entities are complying with their obligations. This feeds into our overall objective of promoting conduct that contributes to the objectives of the FMC Act – fair, efficient, transparent financial markets – as well as confident and informed participation in those markets.

During monitoring engagements, we look for evidence of how governance and compliance operates in practice, and how that compliance is tested and monitored.

The following areas may be examined as part of a monitoring engagement:

- Whether or not the CAP was developed with a risk-based approach that focuses resources on the most significant risks, and how those risks are assessed and prioritised.
- Whether or not the CAP is fit for purpose. For example, a very long or complex document may not be necessary or even practical for a small entity with only a few staff.
- How often the document is updated and whether it has version control and a review date. We may also look at what triggers reviews, for example auditing and regulator engagements.
- Evidence that the CAP is implemented and integrated into the business, functions as designed and is effective.
- How findings and exceptions are reported, and how they are then escalated and remediated.
- Evidence that the oversight body is using reporting from the CAP to challenge management and aid decision-making.
- That roles and qualifications of staff executing each function are clearly defined. For larger entities this may include whether the CAP covers assurance at the three lines of defence.
- That those using the CAP should understand its purpose.
- That the CAP has been approved and the approval is documented.
- Whether compliance documentation includes an obligations register and how this relates to the CAP.
- Whether the CAP is a stand-alone document or integrated into the compliance programme.
- That records of testing include details of how and when it was conducted, and the results.
- What information is provided to the oversight body and how it is used.

AUCKLAND

Level 5, Ernst & Young Building
2 Takutai Square, Britomart
PO Box 106 672, Auckland 1143

Phone: +64 9 300 0400

WELLINGTON

Level 2, 1 Grey Street
PO Box 1179, Wellington 6140

Phone: +64 4 472 9830

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO