FMA

FINANCIAL MARKETS AUTHORITY

TE MANA TATAI HOKOHOKO - NEW ZEALAND

Getting the best outcome from your AML/CFT Audit

Getting the best outcome from your AML/CFT Audit

The *Anti-Money Laundering and Countering Financing of Terrorism Act 2009* (AML/CFT Act) and its Regulations place obligations on New Zealand's Reporting Entities (REs) to detect and deter money laundering and terrorism financing (ML/TF).

The AML/CFT Act requires REs to audit their risk assessment and AML/CFT programme every two years or when asked by their supervisor. Please refer to section 59 of the AML/CFT Act and the 'Guideline for audits of risk assessments and AML/CFT programmes' available on our website for more information.

The table and information that follows has been formulated from questions we have received from the REs we supervise. This information is intended to help our REs, especially small financial adviser businesses, get value from their AML/CFT Audit. Adopting all (or any) of these items in discussions with auditors is optional, but we believe that by considering these suggestions, REs are more likely to achieve the best possible results from their audit.

Does your audit report include?	Explanation
Audit title	The title should include the words 'Independent AML/CFT Audit' of 'Entity Name', FSP No. etc. Or if it covers multiple entities, all entity details.
Period	The report should tell you the period which the audit covers e.g. July 2013 – June 2014.
Auditor details	Your auditor's name, address etc.
Overview of the entity	This demonstrates that the auditor knows and understands the RE business. It should include the activities of the RE that bring it into scope of the AML/CFT Act (i.e. why is this entity a RE?). A description of the business, products, and its management structure is also useful for readers of the report.
Overview of the AML/CFT programme history	This overview can include when the AML/CFT programme was first finalised (i.e. formally approved) and implemented. It can include any changes (when and what) to versions subsequent to implementation date.
Experience and qualifications	A simple overview of how the auditor is suitably qualified to conduct your audit. This might comment on their AML/CFT experience and knowledge, auditing qualifications (and how they stay current), and/or industry knowledge. You should expect that your auditor: • has the required expertise of the AML/CFT Act and its Regulations • understands your industry • has audit experience. Where we are unfamiliar with your auditor, we may ask you to explain to us why you believe your auditor is appropriately qualified to conduct the audit. Your regular accountant or lawyer may not be suitably qualified so you should check this prior to engaging them. We have rejected audit reports received because we were not provided with the necessary evidence to satisfy us that the auditor was appropriately qualified.

Does your audit report include?	Explanation
Independence	The report should confirm the auditor's independence and explain any other services they may have provided in addition to the audit. Some points to consider are detailed below. 1. Does your auditor have a financial interest in your business? 2. Will their interests be harmed by the results of an audit or do they have conflicting interests? An example of where we may have concerns about conflicting interests (and thus independence) is where two REs decide to audit each other's AML/CFT programmes. 3. Is there perceived independence from your business? Whether or not the auditor is really independent doesn't matter when there is no perceived independence. It is essential that the auditor not only acts independently, but appears independent too. 4. Will we conclude that your auditor's objectivity is beyond question? An example of where we may have concerns about objectivity is where an auditor has provided AML/CFT consulting services to the RE prior to the audit (beyond a readiness type check). We have rejected audit reports received because we were not provided with the necessary evidence to satisfy us that the auditor was appropriately independent.
Scope and type of audit i.e. limited or reasonable assurance	This includes what will and will not be covered during the audit, including what you have agreed the auditor will review. This should be explained so any reader of the report can clearly understand it. It may also be useful if the auditor explains the number of samples tested (if this is the basis of their conclusion in a particular area). As an RE, your auditor may offer you a limited versus reasonable assurance audit. These terms come from financial audit terminology and can be quite confusing when all you really want to know is what you're doing wrong and how to fix it. Basically, a reasonable assurance audit is giving you and the FMA greater comfort that you are meeting your minimum requirements. It does so by going into more depth (typically greater testing) during the audit than would a limited assurance audit. The type of audit selected is up to you, as both would meet minimum requirements. For your first audit you may wish to have a more in depth audit to assure yourself that you are meeting the minimal requirements. For your next audit, you may wish to have a reduced scope if, for example, there hasn't been a lot of change to your RE since your more in depth audit. As with all AML/CFT considerations, it would be wise to take a risk-based approach.
Criteria	This includes the minimum requirements you, as the RE, will be audited against. This ensures you receive the right level of assurance that you are meeting your regulatory obligations.
Managements' responsibilities	This includes the responsibilities that rest with management. This is especially helpful for larger REs where it is important to provide feedback to management as a result of the audit.
Auditors' responsibilities	This includes the responsibilities that rest with the auditor.

<table>
<tr><th>Does your audit report include?</th><th>Explanation</th></tr>
<tr><td>The auditor’s approach or summary of work performed</td><td>It is useful if the auditor provides a description of the methods used to determine the adequacy and effectiveness of your AML/CFT programme. For example:
checking the risk assessment and programme against prescribed requirements
assessing the adequacy of the AML/CFT programme
testing effectiveness in key areas.
Your auditor should:
set out the law (what the auditor is checking against)
explain what they examined (how the auditor agreed your AML/CFT programme against the law)
document findings (areas of compliance and non-compliance).
All primary areas of your AML/CFT programme must be examined and reported on. It should be clear to you in which areas you are:
compliant
non-compliant.
Your auditor should not attempt to gloss over significant areas of non-compliance by telling you that you are partially compliant in particular areas, where clearly the more correct conclusion is non-compliance. If your report states that you are partially compliant in a particular area, the exceptions identified should be minor and few.</td></tr>
<tr><td>Reference material</td><td>Reference materials should include any standards, codes of practice or guidance notes the auditor referred to during the audit. This assists you with reference information or further help when completing any remedial actions after the audit.</td></tr>
<tr><td>An executive overview/ summary</td><td>This section should include:
key findings and the methodology the auditor used to rate their findings and any risks they identified
an overview of the time frame they expect will be required to address any gaps found.</td></tr>
<tr><td>Audit opinion or conclusion</td><td>This section should include the elements detailed below.
Whether or not the auditor considers you as the RE to be compliant with the AML/CFT Act, and if they have identified any breaches and any remedial actions required to address any weaknesses. Depending on the type of RE you are, you may have an obligation to report these breaches to the FMA and outline how you are addressing the breach.
The auditors’ recommended course of action to rectify non-compliance issues. This may include recommendations on the highest priorities for rectifying non-compliance.
You should know that auditors can only provide an opinion based on what they have seen or what has been disclosed to them. They can never tell you that you are absolutely compliant. We do not expect the auditor to state this and nor should you.</td></tr>
</table>

Does your audit report include?	Explanation
Signature	The date and signature of the auditor should be included.
Appendix - Audit findings	If the audit is more in depth, it will usually provide a table of matters reviewed, observations and any remedial actions required (possible solutions to your issues). This will help you keep on track to address these issues. This will often be a starting point for the planning of future assurance checks or your next audit.
Management comment	You can request that you are provided with an opportunity to respond directly in the report to any issues (particularly material ones) identified. These comments should include an explanation of the actions you intend to take to address the issues and a time frame for resolution. Management comments demonstrate buy-in and acceptance of the issue to the FMA (remember it's not the auditor's issue, it's your issue). If you disagree with the issue, you should also be provided with an opportunity in the report to explain why.

Other things to consider about your audit

Cost consideration	The likely cost of the audit is a factor in deciding on an auditor, but this should not be the only factor or the most important. This is your money you are spending, so make sure you get value by obtaining a quality audit that is going to be meaningful and informative, providing you with the level of assurance that is required. Your AML/CFT programme should be designed to operate to prevent activities that could facilitate ML/TF. Engaging a capable auditor who can identify compliance issues in your programme is critical. If issues are not identified and addressed early in the regime, the cost to remediate may be significantly higher. For example, if your customers have not had appropriate customer due diligence (CDD), we may require you to go back and address all customers on-boarded since 1 July 2013.
More on cost	You are engaging a professional person or organisation to understand your business and AML/CFT programme, review your documentation and policies, perform testing, interview staff and write a report. This takes time and effort and with that comes cost. We encourage you to take time to understand what actions your auditor is carrying out, so you have a greater appreciation for the associated costs and benefits. For very small, non-complex entities, you may reasonably expect a smaller cost, but the basic activities the auditor must perform should not change. It is reasonable that your auditor takes a risk-based approach and concentrates the greater part of their efforts in certain areas (such as CDD and transaction monitoring). However they are examining broad compliance with the AML/CFT Act so are likely (and expected) to at least touch on most areas of your AML/CFT programme.
Audits – don't be afraid	We understand that many of our REs are unfamiliar with audits and auditors and may have some apprehension. Auditors are not trying to catch you out or trip you up. They are professional people providing you with a service primarily designed to improve your compliance with the AML/CFT Act. They know your industry and your business so we encourage you to consider this audit as an opportunity to improve.

You're going to have issues	Your auditor will almost certainly identify issues with your risk assessment and/or AML/CFT programme. Given the AML/CFT regime only came into full effect on 30 June 2013, it would be surprising if you didn't have any issues while your programme is being bedded down. The audit is an opportunity for you to have those issues identified and subsequently corrected. We also encourage you to engage early with us when significant issues are identified, to discuss the matter and to review the actions that you propose to take. In cases where issues are appropriately addressed, we would be unlikely to engage further on these issues.
Types of issues	There may be a number of terms your auditor uses to explain issues and their severity. These should be clear to you (and us) so that you can prioritise remediation efforts. • Typically any areas of non-compliance with the AML/CFT Act should be addressed to a point where you are then compliant. Auditors can use terms such as 'breach' and 'material/significant' to describe these types of issues. In these instances the expectation is that you take immediate corrective action to remediate the issue. When the auditor provides you a recommendation to address these types of issues, you should not mistake the requirement to take corrective action as optional – the recommended solution proposed by the auditor might be optional but the need to fix the issue is not. • Your auditor may find areas where you can make process improvements. Auditors can use terms such as 'process improvement' and 'value add' to describe these types of issues. For example, there may be alternative, more efficient ways of achieving compliance to processes you have adopted. For these types of issues the need to address them is optional.
Help your auditor	Before the audit begins, you should have an agreed engagement letter with your auditor. This should clearly set out the expectations. Your auditor will need access to staff, records etc. You should not hamper the auditor in their work as this may result in delays and additional costs. Your auditor may ask for copies of some of your documentation before they start on-site, or while they attempt to cost the audit or work out a timescale. This is perfectly normal. As an RE you are unique and so is your documentation. The audit and by extension cost, timescale etc. will need to be adapted to your unique situation.
Tone of the report	This is a formal process. Findings and conclusions should be factual and devoid of emotion.
Findings and results should be clear	The report should be simple and easy to read, with findings (particularly material issues) clearly documented. There should be no attempt to 'bury bad news' in the report. Significant issues should be given prominence.
Tell your auditor	REs often know before their auditor begins the audit where they have concerns or are likely to have issues. By explaining this to your auditor up front, your auditor can adapt the audit accordingly. Many auditors have significant experience in addressing areas where remediation is required. Don't be afraid to ask them for help and recommendations. You should consider working towards building an ongoing relationship with your AML/CFT auditor, based on mutual trust and respect over a period of time. This will come with having honest conversations with your auditor.

Don't ignore your issues	If your auditor identifies issues of non-compliance (i.e. those that require corrective action rather than simply best practice recommendations), we expect that you will take reasonable and timely steps to address them. If we select your entity for a monitoring visit in the future, your audit report will be requested and we will likely start with any issues identified. If there are long outstanding material issues, we will consider a more forceful response. Ignoring small 'best practice' type issues may not affect your compliance with the AML/CFT Act now, but in our experience, small issues can become more significant at a later date and make remediation much more difficult. The Annual AML/CFT Report that you recently completed asked if you have made the changes identified as being necessary in your most recent independent audit. These responses will be considered along with the audit report if we perform a monitoring visit to your RE. Finally, your auditor will provide recommendations but they can't require you to do something. Remediation is your responsibility.
Build relationships and compliance history with the FMA	If we receive an audit report we believe has been completed to a good standard, it will influence our monitoring behaviour. For example, we take a risk-based approach to our inspection programme and a good audit (with good outcomes) will likely reduce the need for us to have a direct engagement with your RE.
Exemptions	You cannot be given an exemption from having to have an AML/CFT audit performed. If you are a RE you must have an audit performed (just as you must complete an Annual AML/CFT Report).

The content the FMA expects to see in your AML/CFT Audit and good practice suggestions for our REs

Minimum Requirement	Good practice: consider having your auditor comment on these areas
1. Risk Assessment • Whether the Risk Assessment complies with all obligations in section 58(3) of the AML/CFT Act. • Nature and extent of the risk assessment and its application.	• The design, clarity and positioning of your risk assessment. • Is there a clear overview of your business – type, nature, size, complexity? • Have you completed an appropriate summary of your key ML/TF risks and risk areas? • How well you have applied the National and Sector Risk Assessments. • A review of the methodology you used to rate the risks. • How you described your approach to keeping your risk assessment current. • Other considerations, such as your employee risk. • How effectively your risk assessment communicates key and emerging risks to staff.
2. AML/CFT Programme • Whether the AML/CFT Programme complies with all of the obligations in section 57 of the AML/CFT Act. • Whether the policies, procedures and controls are based on the risk assessment. • Whether the policies, procedures and controls are adequate. • Whether the policies, procedures and controls have operated effectively throughout the period.	• Design, clarity, positioning of your AML/CFT programme. • How effectively the risk assessment drives and influences your AML/CFT programme. • A review of the processes you applied for CDD including if electronic verification is being used. • How ongoing account monitoring is achieved. • The triggers identified as high risk for transaction monitoring. • The suspicious transaction reporting (STR) filed and registration with goAML. • Record keeping practices. • How you as the RE will stay current with AML/CFT information, guidance notes, emerging risks etc. • Staff training material. • Staff understanding of the policies. • Support and training for your AML/CFT compliance officer. • Governance and culture of your organisation in regard to ML/TF risk. • Any assurance testing and reporting being completed internally. • Triggers for review and updating your AML/CFT programme. • Any key gaps in your control environment. • How well you have described your oversight of third parties and any assurance activity you have developed in this area. • Your process for on-boarding new customers who are Politically Exposed Persons (PEPs) or entering into new banking relationships. • Review of reporting to senior managers.

Glossary

AML/CFT Act	Anti-Money Laundering and Countering Financing of Terrorism Act 2009
CDD	Customer due diligence
Code of Practice	Identity Verification Code of Practice
FMA	Financial Markets Authority
ML/TF	Money laundering/terrorist financing
PEP	Politically Exposed Person
RE	Reporting Entity
STR	Suspicious transaction reporting

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

WELLINGTON OFFICE
Level 2
1 Grey Street
PO Box 1179
Wellington 6140

www.fma.govt.nz
October 2014

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND