AML/CFT

Anti-money laundering and countering financing of terrorism

Audit Guideline

for risk assessment and AML/CFT programme

May 2025

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

Reserve Bank of New Zealand
Te Pūtea Matua

Internal Affairs
Te Tari Taiwhenua

Contents

Introduction

1. This guideline is designed to support reporting entities to understand the Anti-Money Laundering and Countering Financing of Terrorism (**AML/CFT**) audit ("**audit**") requirements[1] under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 ("the **Act**") and to undertake an effective and credible audit of their risk assessment and AML/CFT programme.

2. This guideline will also be useful to persons who perform audits of risk assessments and AML/CFT programmes for reporting entities.

3. The Act does not specify how these audits are to be conducted. This guideline provides an overview of matters to consider when arranging such an audit.

4. In this guideline, reporting entities are also referred to as 'you' or 'your'.

5. Reporting entities are advised to plan well in advance to meet their audit deadline. It is your responsibility to engage an independent and appropriately qualified auditor who can conduct your audit and complete it within the required timeframe.

6. A successful audit will help to ensure that your procedures, policies and controls remain up-to-date and that any deficiencies in the adequacy and effectiveness of your AML/CFT programme can be identified and remediated. This can help to protect your business from the risks of money laundering and terrorism financing.

7. This guideline is structured in three parts:
   - Part 1: Your obligations under the Act;
   - Part 2: Getting the most out of your audit – outlining what you need to know before you commence the planning of your audit; and
   - Part 3: Planning and performing your audit – taking you through the audit process including choosing an auditor.

Part 1: Your obligations under the Act

8. Your risk assessment and AML/CFT programme **must** be independently audited by an appropriately qualified and independent person every three years, unless you are notified by your AML/CFT supervisor that a four-year timeframe applies.[2]

9. You must also keep adequate records relating to your independent audit.[3]

[1] Section 59(2), 59A and 59B of the Act.

[2] Sections 59(2) and 59B of the Act, and Regulation 13 of the AML/CFT (Requirements and Compliance) Regulations 2011.

[3] Section 51 of the Act.

10. The supervisors expect your AML/CFT programme to include procedures, policies and controls for undertaking an independent audit and note when your last audit was undertaken. Remediation undertaken as a result of the audit should be explained in a version control table in the relevant document.

11. The key legal obligations relating to the audit requirement are summarised below:

Obligation	Details	Section of the Act
Scope of audit	Your risk assessment and AML/CFT programme must be audited.	59(2)
	The audit of your risk assessment is limited to whether it fulfils the requirements in section 58(3) of the Act. However, this will require consideration of other requirements under section 58.	59B(4)
Frequency	Every three years unless you are notified by your AML/CFT supervisor that a four-year timeframe applies, or at any other time at the request of your supervisor. This requires that you have an audit completed every three years. An audit is not complete unless the final audit report is issued by your auditor. You then have three years from the date of your last audit report, to have your next audit completed and the audit report issued.	Regulation 13 AML/CFT (Requirements and Compliance) Regulations 2011. 59(2)
Record keeping	You must keep records relating to your audit. These records must be kept for a period of at least five years after the date on which they ceased to be used on a regular basis. You must make your records relating to audits available to your supervisor on request.	51(1)(b), 51(2) and 51(3).
Auditor requirements	Your audit must be carried out by an independent person appointed by your reporting entity, who is appropriately qualified to conduct the audit. This includes the requirement that the auditor must not have been involved in the undertaking of your risk assessment or the establishment or implementation or maintenance of your AML/CFT programme. These requirements are explained further in Part 3: 'Choosing Your Auditor'.	59B
Providing a copy to your supervisor	You must provide a copy of any audit report to your supervisor on request.	59B(5)
Annual report	Your annual AML/CFT report includes questions related to your audit result and actions you have taken in response to your findings.	60

High-value dealers	The audit requirements for high-value dealers differ from other reporting entities. High-value dealers are only required to undertake an audit when requested by their supervisor. The scope of their audit should cover compliance with AML/CFT obligations under section 6(4)(d)(ii) of the Act, and any relevant regulations.	59A

Part 2: Getting the most out of your audit

12. This section outlines points that you should carefully consider before planning your audit. They are written to clearly reflect the expectations of the supervisors and what you should take into account before you plan your audit and engage an auditor.

Plan ahead

13. Reporting entities can determine for themselves the best time to have their audits conducted. You are responsible for your own compliance with the audit requirements, so it is advisable to plan ahead. New reporting entities should consider having their audits completed early. Bringing forward your audit will provide you with a number of benefits, which include:
    - audit resources to perform the independent review will be more readily available;
    - early independent assurance around your AML/CFT programme compliance;
    - a properly planned and executed independent audit performed to an appropriate standard may reduce the likelihood that your supervisor will need to visit you for a supervisory visit, as supervision is conducted on a risk-based approach.

Assurance of the audit report

14. The Act does not require a specific level of assurance; however, each reporting entity will need to balance the costs of the audit against the degree of confidence required from the audit.

15. An auditor can perform either a ‘reasonable’ or a ‘limited’ assurance audit. Typically, a reasonable assurance goes into more depth (more testing) during the audit than a limited assurance audit would. The type of audit selected is up to each reporting entity.

16. Auditors can only provide an opinion based on the information they have gained access to and, for this reason, auditors cannot be expected to guarantee that a reporting entity is “absolutely” compliant.

Scope of your audit

17. The audit is a systematic check of a reporting entity's risk assessment and AML/CFT programme and its application. The audit will assess whether your AML/CFT programme is functioning in practice as intended, and whether the procedures, policies and controls are based on the risk assessment and have been adequately designed and operated effectively throughout the given period.

18. The audit of the risk assessment and AML/CFT programme can be treated as one process and documented in the same report. However, both should be adequately considered.

19. While the Act limits the audit of the risk assessment to comply with the obligations in section 58(3) of the Act, it is expected that consideration be given to all obligations under section 58(2) of the Act.

20. The scope of your audit will be different in format and content to other audits that are undertaken for your entity.

Audit outcome, report and recommendations

21. The audit will result in a written report on whether:
    - your risk assessment and AML/CFT programme comply with the minimum requirements of the Act;
    - the AML/CFT programme was adequate and effective throughout a specified period, and
    - changes are required as a result of deficiencies identified in your risk assessment or AML/CFT programme.

22. The audit report may include actions that are required to rectify non-compliance as well as identifying areas for recommended improvement in behaviour and practice. This includes an indication of where there are potential failings and a recommended course of action.

23. Non-compliance or partial compliance identified in the audit report must be addressed. How each reporting entity responds to these issues is their responsibility.

24. While the recommended solution proposed by the auditor may be optional, the need to remediate identified non-compliance is not. Your supervisor expects that you will take appropriate corrective action to remediate any issues identified in the audit report. Your supervisor may also ask questions about what issues have been identified and how remedial actions have been addressed by your organisation.

25. In your annual AML/CFT report to your supervisor, you must state whether the necessary changes have been made to address issues raised in the audit report.

26. While the Act requires an audit outcome in the form of a written report, it does not specify any format. To assist you, the supervisors have included *Appendix 1: Suggested information you can expect to be included in an audit report for guidance.* Particular consideration needs to be given to the content, the thoroughness of the information presented and how the information is structured.

27. You should have the opportunity to correct factual inaccuracies by reviewing a draft report.

28. If the auditor has had difficulties in gathering information, this may result in the auditor giving a qualified opinion.

29. In terms of section 43 of the Act, anyone carrying out your audit who becomes aware of any suspicious activity, may refer the suspicious activity to the New Zealand Police Financial Intelligence Unit.

Part 3: Planning and performing your audit

Choosing your auditor

30. The Act requires the audit to provide an "independent" view and to be carried out by someone "appropriately qualified".

    - **The audit must be conducted by an independent person** – the Act states that your auditor **must** be independent, and not involved in the development of your risk assessment or the establishment, implementation or maintenance of your AML/CFT programme. You should also consider any other potential conflicts of interest that may call into question their independence. The person/s appointed to undertake the audit may be an employee(s) (for instance, an internal audit team), provided they are adequately independent from the AML/CFT area of your business. You should be able to explain to your AML/CFT supervisor how you determined that your auditor is independent.[4]

    - **The auditor must be appropriately qualified** – The Act states that your auditor **must** be appropriately qualified to conduct the audit. This does not necessarily mean that the person must be a chartered accountant or qualified to undertake financial audits. It does mean that the person has to have relevant skills or experience to conduct an AML/CFT audit. You should be able to explain to your AML/CFT supervisor how you determined that your auditor is appropriately qualified.[5] This includes having knowledge of the Act, and its supporting regulations, as well as audit experience or sufficient knowledge of audit processes.

[4] Section 59B(1) and (3) of the Act.

[5] Section 59B(1) and (2) of the Act.

31. You may choose to appoint an external firm to perform the audit provided you are satisfied the auditor is independent, appropriately qualified and no conflict of interest exists with the auditor.

32. The supervisors expect reporting entities to have documented what they have considered when assessing the auditor's independence and relevant experience to perform the audit.

33. Factors to consider when assessing the "independence" of your auditor:
    - Was the auditor involved in the development of your risk assessment? Or the creation, implementation or maintenance of your AML/CFT programme? If they were, they are not considered to be sufficiently independent to perform your audit.
    - Does the auditor have financial interest in your business, or do you have a financial interest in your auditor's business? If yes, would your or their interests be harmed by the results of the audit, or could there be influence over the audit outcome?
    - Does the auditor have any relationship with any shareholder, director, senior management and or employees, e.g. family, friends, ex-colleagues, etc.
    - If reciprocal auditing is intended (where two reporting entities decide to complete each other's audits) how can you demonstrate that each auditor is objective in their assessment and not affected by the nature of the reciprocal process?

34. Things to consider when assessing how "appropriately qualified" your auditor is:
    - What level of knowledge do they have about AML/CFT? Do they understand the Act and its supporting regulations? Do they understand the Code of Practice and guidelines? If they haven't had direct involvement with the development or implementation of your risk assessment and AML/CFT programme, how can they then demonstrate the level of knowledge required in order to effectively audit these documents and their implementation?
    - Do they have audit experience? Ideally your auditor should have experience conducting an audit, if they don't, they should demonstrate how they have sufficient knowledge of audit processes in order to effectively undertake your audit.
    - How much knowledge do they have of your industry, and how can they demonstrate this?

Other matters to consider when planning your audit

35. Hampering the auditor in their work may cause delays and additional costs.

36. Your audit should be based on your unique business situation and the content of your audit report should not be copied by your auditor from other entities' audit reports.

Preparing for your audit

37. The auditor will tell you what they need from you. This is likely to include information to give them a better understanding of your business.

38. You should discuss and agree the scope of your audit and confirm the following in writing with your auditor in an engagement letter:

    - What information is required – when, how and who will provide it to your auditor;
    - Review of information – when will the review commence and when is it expected to be completed, who will be responsible for performing the review;
    - Audit report – who will be responsible to draft it, when will the draft report be provided (e.g. 10 working days after completion of review of information) for review of accuracy and comment by you, what the timeframe will be for you to provide confirmation and or comments (e.g. 10 working days after delivery of draft report), when the final audit report will be issued.

39. Your engagement letter should be signed off by you and your auditor. Your supervisor may ask you to produce this.

40. The auditor may request a written acknowledgment of your responsibility for compliance with the applicable AML/CFT requirements. This establishes that you have provided the auditor with all the relevant information and access agreed to, and that you have disclosed any relevant matters to the auditor (for example, any non-compliance with the Act).

41. The auditor may also ask for:
    - documents relating to the development of your risk assessment and AML/CFT programme;
    - access to staff members and/or senior management;
    - access to files, customer identification records, transactions and or outputs from your systems;
    - disclosures of all known instances of non-compliance; and
    - the results of your own monitoring and reviews of your risk assessment and AML/CFT programme.

42. Information contained in suspicious activity reports must not be disclosed to your auditor.[6]

Reviewing the audit process

43. As this is an important process for a reporting entity, it is recommended that you review how the process has worked for you, as well as evaluating whether your auditor has met your expectations. This may help you in undertaking a better audit next time.

[6] Section 46 of the Act.

44. Questions to help assess your audit process:
    - Did the audit meet the performance criteria as reflected in the engagement letter?
    - Are you in agreement with the auditor on the significant risk areas of your entity?
    - Did the audit provide details on the quality of your entity's AML/CFT reporting (including Suspicious Activity Reports and Prescribed Transaction Reports), including whether your judgments are reasonable?
    - If there was a change in your business from the previous audit, did the auditor adjust the audit accordingly?
    - Was the cost reasonable for the size, complexity and risks of your entity?
    - Were sufficient and appropriate resources dedicated to the audit?

45. Questions to help your assessment of your auditor:
    - Does your engagement letter consider your agreed timeline for delivering the audit report? If the timeline was not met, did the auditor discuss the reasons for this?
    - Did the auditor maintain open dialogue with management and were communications always comprehensive and understandable?
    - Did the auditor ask for feedback on the audit and how did they respond to this feedback?
    - Did the auditor discuss the audit plan and the entity-specific areas of assurance it would address?
    - Does the auditor understand your business, industry and how AML/CFT can impact your business? Do you agree with the auditor on the significant risk areas of your entity?
    - Did the auditor demonstrate a good understanding of the current AML/CFT regime and environment and how these may impact your entity?

Appendix I: Suggested information you can expect to be included in an audit report

The Act does not prescribe the content of an audit report. To assist reporting entities the supervisors have provided the following suggested information that can be expected in an audit report. While supervisors will accept various formats, they do expect a degree of professionalism which covers the information discussed.

1. **Audit title**

   The title should include the words 'Independent AML/CFT Audit' of 'Entity Name', etc. Or if it covers multiple entities, all entity details.

2. **Period**

   The report should include the period which the audit covers e.g. July 2023 – June 2024.

3. **Auditor details**

   Auditor's name, address etc.

4. **Overview of the entity**

   The overview information should demonstrate that the auditor knows and understands the reporting entity's business. It should include the activities of the reporting entity that bring it into scope of the Act. A description of the business, products, and its management structure is also useful for readers of the report.

5. **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.

6. **Experience and qualifications**

   An overview of how the auditor is suitably qualified to conduct your audit.

7. **Independence**

   Information that confirms the auditor's independence and an explanation of any other services the auditor may have provided in addition to the audit.

8. **Scope and type of audit**

This details 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). This might also include whether they have conducted a limited or reasonable assurance audit.

9. **Criteria**

This details the minimum requirements you, as the reporting entity, will be audited against. This will help ensure you receive the right level of assurance that you are meeting your regulatory obligations.

10. **Management's responsibilities**

This details the responsibilities that rest with management. This is especially helpful for larger reporting entities where it is important to provide feedback to management as a result of the audit.

11. **Auditor's responsibilities**

This details the responsibilities that rest with the auditor.

12. **The auditor's approach or summary of work performed**

Your auditor should:

- set out the law (what the auditor is checking against)
- explain what they examined (how the auditor examined your risk assessment and AML/CFT programme against the law)
- document findings (areas of compliance and non-compliance).

All primary areas of your risk assessment and AML/CFT programme must be examined and reported on. It should be clear to you in which areas you are:

- compliant
- non-compliant

It is useful if the auditor provides a description of the methods used to determine the adequacy and effectiveness of your risk assessment and AML/CFT programme. For example:

- checking the risk assessment and AML/CFT programme against prescribed requirements

- assessing the adequacy of your risk assessment and AML/CFT programme
- testing effectiveness in key areas.

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.

13. **Reference material**

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.

14. **An executive overview/summary**

This should include:

- key findings and the methodology the auditor used to rate their findings and any risks they identified, and
- an overview of the timeframe they expect will be required to address any gaps found.

15. **Audit opinion or conclusion**

This should include the elements detailed below:

- whether or not the auditor considers you as the reporting entity to be compliant with the Act, and if they have identified any breaches and any remedial actions required to address any weaknesses.
- the auditor's 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. The supervisors do not expect the auditor to state this and nor should you.

16. **Signature**

The date and signature of the auditor should be included. An audit is only considered to be completed once the report has been signed off and issued.

17. **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.

18. **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.

Appendix II: Audit timeframes under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009

Section 59(2) of the Anti-Money Laundering and Countering Financing of Terrorism (**AML/CFT**) Act 2009 requires you to ensure that your risk assessment and AML/CFT programme are audited by an independent and appropriately qualified auditor.

Regulation 13 of the AML/CFT (Requirements and Compliance) Regulations 2011 requires that an independent audit is conducted every three years, unless you are notified by your AML/CFT supervisor that a four-year timeframe applies, or at any other time at the request of your AML/CFT supervisor.

The audit of your risk assessment and AML/CFT programme is not complete until the date on which the final audit report is issued. This means that you must ensure that your next audit report is issued on or within three years from the date on which your last AML/CFT audit report was issued. The examples below provide further guidance on when your audit reports must be completed.

When do I have to complete my first AML/CFT audit?

You will have three years (or at any other time at the request of your AML/CFT supervisor) from the date you became a reporting entity to have your first audit report completed.

When do I have to complete my second (or subsequent) AML/CFT audit?

Your second (or subsequent) AML/CFT audit report will be due three years from the date of your last AML/CFT audit report. The examples below illustrate how this applies.

Examples

Business completes an AML/CFT audit

ABC Limited became a reporting entity on 31 August 2021. ABC Limited completed its first AML/CFT audit (including the audit report) on 31 August 2024. ABC Limited's next AML/CFT audit report must be issued by 31 August 2027 (i.e. three years from 31 August 2024).

Business completes an early AML/CFT audit QWE Limited became a reporting entity on 30 June 2021. The company completed its first AML/CFT audit (including the audit report) on 30 March 2024, before the due date of 30 June 2024. QWE Limited's next AML/CFT audit report must be issued by 30 March 2027 (i.e. three years from 30 March 2024).
Business completes an additional AML/CFT audit XYZ Limited became a reporting entity on 15 March 2021. The company completed its first AML/CFT audit (including the audit report) on 3 March 2024, before the due date of 15 March 2024. However, as this audit was not completed to a satisfactory standard, its AML/CFT supervisor requested XYZ Limited to complete an additional audit, by 16 April 2024. This additional audit was completed on 15 April 2024. XYZ Limited's next AML/CFT audit report must be issued by 15 April 2027 (i.e. three years from 15 April 2024).
Business completes an overdue AML/CFT audit PQR Limited became a reporting entity on 15 March 2021. The company's first AML/CFT audit was due on 15 March 2024. However, PQR Limited completed its first AML/CFT audit (including the audit report) on 30 October 2024 (i.e. 7 months overdue). PQR Limited's next AML/CFT audit report must be issued by 30 October 2027 (i.e. three years from 30 October 2024). PQR Limited's AML/CFT supervisor may take regulatory action, as appropriate, against PQR Limited to address the above overdue audit.[7]

Version History

December 2012	Original version
October 2019	Fully revised version
May 2025	Revised version to reflect Regulation 13 of the AML/CFT (Requirements and Compliance) Regulations 2011

[7] Note that for departures from the audit timeframes, the reporting entity may expect regulatory action under Part 3 of the Act from its supervisor. Supervisors take a risk-based approach to compliance and will use the enforcement option appropriate to achieve compliance. The response will be proportionate and guided by factors such as a regulated party's history of compliance and degree of openness and preparedness to cooperate. This can include, for example, a warning under section 80 of the Act. The relevant supervisor may also request for an additional audit, which may have the effect of realigning or altering the reporting entity's next audit due date. The obligation is on the reporting entity to ensure that its risk assessment and AML/CFT programme are audited (with audit report issued) before the due date.

Disclaimer: This guideline has been produced by the AML/CFT supervisors under section 132(2)(c) of the Act. It is intended to assist reporting entities to understand their audit obligations under the Act. This guideline cannot be relied on as evidence of complying with the requirements of the Act. It does not constitute legal advice.

After reading this guideline, if you do not fully understand your obligations you should seek legal advice or contact your AML/CFT supervisor.

Where AML/CFT guidance material is referenced, it can be accessed at the following websites:

Department of Internal Affairs	http://bit.ly/2gQ3Iev
Reserve Bank of New Zealand	http://bit.ly/2n6RYdp
Financial Markets Authority	https://bit.ly/3fjcKlD