AML/CFT

Anti-money laundering and countering financing of terrorism

Designated Business Group – Scope Guideline

September 2025

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

Reserve Bank of New Zealand
Te Pūtea Matua

Te Tari Taiwhenua
Internal Affairs

Guideline to reporting entities to assist the decision on whether to form a designated business group

1. This guideline is to support reporting entities to understand which obligations may be relied on or shared by members of a designated business group (**DBG**).

2. Entities may form a DBG if they are eligible to do so under the Anti-Money Laundering and Countering Financing of Terrorism (**AML/CFT**) Act 2009 (**Act**) and regulations. Further information concerning eligibility and the election process, including how to notify your AML/CFT supervisor, is provided in the *DBG Formation and Change Guideline.*

3. This guideline has been produced by the AML/CFT supervisors under section 132(2) of the Act. This guideline does not constitute legal advice.

4. Section 57(2) of the Act requires you to have regard to this guideline when developing your AML/CFT programme (if you are forming or are part of a DBG). After reading this guideline, if you still do not understand any of your obligations relating to a DBG you should contact your AML/CFT supervisor or seek legal advice.

Designated business group overview

5. A DBG is a group of two or more eligible entities that have elected (in writing) to form a group. An entity that elects to join a DBG may rely on another member of the DBG to carry out some of its obligations under the Act, provided certain conditions are met. Relying on another DBG member and sharing AML/CFT obligations within a DBG enables compliance efficiencies.

Responsibility for complying with obligations

6. When relying on another member of a DBG to carry out AML/CFT obligations, you are still responsible (and liable) for your compliance with the Act and regulations. Liability does not shift to the member of the DBG you are relying on. It is also not possible to devolve all AML/CFT responsibilities to the DBG or to another member of the DBG.

Alternatives to DBGs

7. DBGs are just one way in which the Act allows entities to cooperate. Reporting entities may also consider reliance on other reporting entities or equivalent entities in another country (under section 33 of the Act), or reliance on agents (under section 34 of the Act), to conduct customer due diligence (**CDD**). For further information, refer to the supervisors' *AML/CFT Programme Guideline*.

Obligations a DBG may share

8. A member of a DBG can rely on another member to carry out some obligations on their behalf. These include:

    - CDD
    - Parts of an AML/CFT programme – record keeping, account monitoring and

ongoing CDD
- Submitting annual reports on behalf of another member of the DBG
- Risk assessment
- Suspicious activity reporting
- Prescribed transaction reporting.[1]

Customer due diligence

9. Section 32 of the Act allows a reporting entity to rely on another member of a DBG to conduct CDD procedures on its behalf if certain conditions are met.

10. For example, member A can rely on member B in a DBG to carry out the CDD procedures on a customer or potential customer. This includes any CDD requirements under the Act, including name, date of birth, address or enhanced CDD information such as source of funds or wealth (when required). The conditions for member A to rely on member B are:

    (a) member B must provide all applicable identity information to member A **before** member A establishes a business relationship with the customer or conducts an occasional transaction or activity[2] for the customer.

    (b) member B must provide any verification information[3] **as soon as practicable on request** from member A but **within five working days** of that request.[4]

    (c) if member B is outside New Zealand, member B must conduct the relevant CDD requirements to at least the standard required by the Act.[5]

AML/CFT programme

11. Each reporting entity is required to have an AML/CFT programme under section 56 and 57 of the Act.

12. An AML/CFT programme sets out the written procedures, policies and controls in a business to detect money laundering and terrorism financing (**ML/TF**) and manage and mitigate the risk of it. The parts of an AML/CFT programme that may be adopted, shared, and used between members of a DBG include record keeping, ongoing CDD and account monitoring.[6]

13. Each reporting entity in a DBG must determine which aspects of these obligations under the Act they will share, including the practicalities and benefits of doing so. For example, sharing record keeping may only require one electronic or physical storage system to be used (operated by one entity on behalf of other members of the DBG). Likewise, account monitoring and ongoing CDD may be managed through a system

[1] Section 32 of the Act.

[2] As defined in section 5(1) of the Act.

[3] Verification information means a copy of the records used by the person being relied on to verify the customer's identity – refer Regulation 14 of the AML/CFT (Requirements and Compliance) Regulations 2011

[4] Section 32(1)(a) of the Act

[5] Regulation 13D of the AML/CFT (Requirements and Compliance) Regulations 2011

[6] Section 32(1)(b) of the Act

operated and maintained by a central member of the DBG. As well as being more efficient, this may enable a more effective cross-group approach to account monitoring obligations, including identifying suspicious activities.

14. Note: The requirement to establish, implement and maintain an AML/CFT programme remains the responsibility of each reporting entity, even in relation to those procedures, policies and controls that are shared.[7] Relatedly, you should consider whether it is appropriate for you to share and use the same procedures, policies and controls with another member of a DBG. You should document the reasons for this.

15. Your AML/CFT supervisor may require additional information on the procedures, policies and controls implemented at an individual entity level within a DBG where a higher risk exists. This is to determine if those higher risks are adequately addressed by the shared aspects of a AML/CFT programme. If not, the AML/CFT supervisor could require an individual member to develop specific procedures, policies and controls in an AML/CFT programme.

Annual Reporting

16. An annual AML/CFT report must be submitted by all members of a DBG.[8] However, if you share your risk assessment and AML/CFT programme with another member of a DBG, only one of you needs to respond to Part Two of the annual report (on behalf of all DBG members). The other member(s) can leave this blank. All other parts of the annual report must be completed separately.

Risk assessment

17. Your risk assessment is the basis for your AML/CFT programme and central to managing and mitigating your ML/TF risk.

18. A member of a DBG can use a risk assessment of another member; however, the risk assessment must be relevant to the business of the member that is relying on it. This will only be possible if the risk assessment adequately addresses the types of products and services, customers, institutions, or geographies that are applicable to all DBG members relying on it (to the level required by section 58 of the Act).

19. A reporting entity may use a risk assessment of another DBG member in whole or in part. If you are considering sharing a risk assessment (or parts of a risk assessment), you should satisfy yourself that the risks faced by your business are given the required level of analysis within a wider group risk assessment. For example, if the majority of your business is a product or service that another member of the DBG also offers, but to different types of customers, then you must be satisfied that a shared risk assessment places sufficient focus on your risks.

20. As with other shared obligations, the responsibility to undertake a risk assessment remains with the reporting entity. Your AML/CFT supervisor may, if this is determined

[7] Section 32(2) of the Act.

[8] Unless a member of a DBG is not a reporting entity in New Zealand.

necessary, require you to undertake a separate risk assessment that is specific to your business.

21. Situations where it **may** not be appropriate to use a risk assessment of another member of a DBG are when:

    - There are variations in products or services offered by one member such that there are different risk profiles across the DBG members
    - There are different types of customers, with different risk profiles across the DBG members
    - Risk ratings differ between DBG members due to different country risks; or
    - There are material changes to a DBG member business since any shared risk assessment was developed.

Suspicious activity reporting

22. A member of a DBG may make a suspicious activity report (**SAR**) on behalf of another member of a DBG. In some circumstances, one member may submit SARs for the entire group. SARs are to be made to the New Zealand Police Financial Intelligence Unit (**FIU**) through the goAML reporting tool. This provision is subject to the privacy and jurisdictional considerations in section 36 of the Act (refer paragraphs [31] to [32] below).

Prescribed transaction reporting

23. A member of a DBG may make a prescribed transaction report (**PTR**) on behalf of another member of a DBG. In some circumstances, one member may submit PTRs for the entire DBG. PTRs are also submitted to the FIU through the goAML reporting tool. This provision is also subject to the privacy and jurisdictional considerations in section 36 of the Act.

Other sharing

24. Some other aspects of an AML/CFT programme may also be shared where appropriate.[9] Again, responsibility for each obligation remains with the individual reporting entity. Examples of other aspects of AML/CFT programmes that can be shared are:

    - **Vetting** – While procedures, policies and controls policies for vetting may differ across different members of a DBG, vetting procedures could be undertaken by one DBG member on behalf of another (as long as the standards are met, and appropriate procedures and privacy requirements are followed).
    - **Training** – Training on AML/CFT matters for senior managers, the AML/CFT compliance officer and any other employee engaged in AML/CFT duties is the responsibility of the reporting entity. Adequate and effective procedures, policies and controls must be in place as part of an AML/CFT programme. However, as with vetting, one member of a DBG may undertake training (or parts of its training) procedures for another DBG member.

[9] Section 32 of the Act.

- **Review** – A reporting entity must regularly review its risk assessment and AML/CFT programme to ensure they remain current and that any deficiencies in effectiveness are identified with appropriate changes made. Any review of risk assessment and/or AML/CFT programme to meet this obligation should consider the currency and effectiveness of the documents for each member of the DBG using them (or parts of them).
- **Audit** – A reporting entity must ensure that its risk assessment and AML/CFT programme are independently audited every three years or every four years if notified by their AML/CFT supervisor that the four-year timeframe applies. An audit may also be required at any other time when requested by the AML/CFT supervisor. An audit may be undertaken on a consolidated DBG basis so long as it adequately and effectively addresses the elements relevant to each member of the DBG.

Code of practice

25. A reporting entity that intends to comply with an obligation by other equally effective means rather than by following a code of practice must first notify its AML/CFT supervisor of its intention to do so. If each reporting entity in a DBG intends to opt out of compliance with any code of practice, they may do so via a combined written notification, provided that documentation confirms that each entity agrees to opt out of compliance with the code of practice or part thereof.

Obligations members of a DBG must meet themselves

26. Despite the sharing provisions for members of a DBG, there are obligations within the Act that reporting entities must meet themselves.

27. As noted at paragraphs [15] and [20] above, an AML/CFT supervisor may require a reporting entity to undertake a risk assessment separately to the DBG, and similarly for any AML/CFT procedures, policies and controls, review, or audit.

AML/CFT Compliance Officer

28. A primary requirement of the Act is that all reporting entities must have an AML/CFT compliance officer (**compliance officer**). The requirements for who can be a compliance officer are set out in section 56 of the Act. There is further detail in the supervisors' *AML/CFT Programme Guideline.*

29. Importantly, the compliance officer must be an employee of the reporting entity,[10] unless the reporting entity does not have any employees. In that case another person may be appointed as the compliance officer for that reporting entity. That same person can also act as the compliance officer for another member of the DBG so long as the compliance officer is appropriately trained and reports to the senior management of each reporting entity in the DBG (for which the compliance officer acts). The

[10] Or the designated partner of a partnership that is a reporting entity. The partner so designated must report to another partner designated for the purpose of receiving those reports by the partnership (s56(5) of the Act).

compliance officer is responsible for ensuring the AML/CFT programme in a reporting entity is administered and maintained.

30. Note: Subject to certain conditions, Part 7 of the Schedule of the AML/CFT (Class Exemptions) Notice 2018 allows members of a DBG to share their compliance officer.

Privacy considerations

31. Although suspicious activity reporting can be shared within a DBG in limited circumstances[11], there are certain privacy requirements that must be considered. Members of a DBG should understand the privacy implications when sharing any information between them.[12] This includes situations where a member of a DBG that is based overseas, could be required to submit an SAR or equivalent in that jurisdiction.

32. Section 36 of the Act sets out the privacy considerations for personal information that may be shared in the context of a DBG. The Act provides protection for personal information by requiring all members of a DBG, including overseas entities, to agree in writing to comply with privacy principles 5 – 12 within section 22 of the Privacy Act 2020. Section 36 applies to personal information that is either the information obtained when conducting CDD or information received for the purposes of adopting part of another member's AML/CFT programme. The privacy requirements extend to the record keeping obligations related to that personal information.

Version history

December 2017	Various changes
October 2022	Updated Privacy Act 1993 references to Privacy Act 2020 Updated audit timeframe references from two years to three-four years or on request by an entity's supervisor
September 2025	Updated following amendment to regulations in relation to reliance on another member of a DBG. Further formatting and editorial changes for clarification purposes.

[11] Section 46(2)(e) of the Act.
[12] Section 36 of the Act.