AML / CFT

Anti-money laundering and countering financing of terrorism

Designated Business Group – Scope Guideline

Updated in December 2017

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND

RESERVE BANK OF NEW ZEALAND

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 designed to help reporting entities understand which obligations may be 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 Act 2009 (the AML/CFT Act) and Regulations. Further information concerning eligibility and the election process, including how to notify the AML/CFT supervisor, is provided in the DBG Formation Guideline.

3. This guideline is provided for information only and cannot be relied on as evidence of complying with the requirements of the AML/CFT Act. It does not constitute legal advice from any of the AML/CFT supervisors and cannot be relied on as such.

4. If, after reading this guideline, an entity does not understand whether it can rely on another member of a DBG to discharge a particular obligation on its behalf, it should seek legal advice or contact its AML/CFT supervisor.

Designated business group (DBG) overview

5. A DBG is defined in section 5(1) of the AML/CFT Act. A DBG is a group of two or more persons where there is a written agreement between the persons that make up the group. Further guidance on DBG eligibility and notification to the AML/CFT supervisors is in the DBG Formation Guideline.

6. 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 AML/CFT Act, provided certain conditions are met.

Responsibility for complying with obligations

7. As mentioned throughout this guideline, liability for compliance with the AML/CFT Act and Regulations remains with the reporting entity and not the member of the DBG being relied upon. It is not possible to devolve all responsibility to the DBG or another member of the DBG.

8. Reporting entities considering forming a DBG should seek legal advice if they are unclear of their obligations under the AML/CFT Act or any associated regulations.

Alternatives to DBGs

9. DBGs are just one way in which the AML/CFT Act allows entities to cooperate. Entities may also consider reliance on other reporting entities or persons in another country (under section 33 of the AML/CFT Act), or reliance on agents (under section 34 of the AML/CFT Act), to conduct customer due diligence (CDD).

Obligations a DBG may share

10. A member of a DBG can rely on another member to carry out some obligations on their behalf as set out in section 32 of the AML/CFT Act. These include:
    - CDD
    - Parts of an AML/CFT programme – such as record keeping, account monitoring and ongoing CDD
    - Submitting annual reports on behalf of another member of the DBG
    - Risk assessments
    - Suspicious activity reporting
    - Prescribed transaction reporting

Customer due diligence

11. Section 32 of the AML/CFT 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. Procedures relate to the process or methods of collection and verification of information on the identity of the customer. For example, member A can rely on member B in a DBG to carry out the CDD procedures on a customer or potential customer. Procedures followed by member B must comply with the AML/CFT Act and meet the minimum standards set by member A.

12. Identity information includes name, date of birth, address, and source of funds where appropriate. It must be given to the member seeking to conduct a transaction with a non-customer (member A) before an account is opened or an occasional transaction or activity[1] takes place. Information obtained to verify identity information may be provided later, but member B must supply the verification information to member A as soon as practicable on request but within five working days of that request.

13. The identity and verification information can be provided to member A in any form so long as it is documented to comply with the record-keeping provisions in section 50 of the AML/CFT Act. Further information on record keeping within a DBG is below.

AML/CFT programme

14. Each reporting entity is required to have an AML/CFT programme under section 56 of the AML/CFT Act. An AML/CFT programme sets out the policies, procedures and controls in a business to detect money laundering and terrorism financing (ML/TF) and manage and mitigate the risk of it occurring. AML/CFT supervisors have developed guidance covering the requirements of an AML/CFT programme. The parts of the AML/CFT programme specified in the AML/CFT Act that may be adopted, shared and used relate to:
    - Record keeping
    - Account monitoring
    - Ongoing CDD

[1] As defined in section 5(1) of the AML/CFT Act.

15. Adopting, sharing and using parts of an AML/CFT programme means that members of a DBG may benefit from the same systems and controls that may be used to manage the obligations for the aspects of an AML/CFT programme identified above. For example, sharing and using record keeping may mean that one electronic and physical storage system is used and operated by one entity on behalf of other members of the DBG. Likewise, account monitoring and ongoing CDD may be managed through a system operated and maintained by a central member of the DBG.

16. Establishment, implementation and maintenance of an AML/CFT programme is the responsibility of each reporting entity whether or not some policies, procedures and controls are adopted, shared and used by each entity in the DBG.[2] Reporting entities need to assess whether it is appropriate for them to share and use the same policies, procedures and controls as another member of a DBG and document the reasoning behind that decision.

17. AML/CFT supervisors may require additional information on policies, procedures and controls in an individual reporting entity within a DBG where a higher risk exists in relation to that member and that risk does not appear to be adequately addressed by shared aspects of a risk assessment or AML/CFT programme. Alternatively, AML/CFT supervisors may require individual reporting entities to develop specific policies, procedures and controls in an AML/CFT programme for their business.

18. Each reporting entity in a DBG will need to determine how they share aspects of their obligations under the AML/CFT Act and how much they share within the scope allowed for by the AML/CFT Act and Regulations.

Annual reporting

19. Section 32 of the AML/CFT Act also allows for some sharing relating to annual reporting. Part Two of the annual report relates to any shared aspects of a risk assessment, an AML/CFT programme and submitting suspicious activity reports (SARs) or prescribed transaction reports (PTRs). These elements may be responded to by one DBG member on behalf of all DBG members. It will still be necessary for reporting entities to report separately on other matters.

Risk assessment

20. The risk assessment is the basis for each reporting entity's AML/CFT programme and central to managing and mitigating the risk of ML/TF in its business. 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 seeking to rely on it. A risk assessment would only be relevant if it adequately addresses the types of products and services, customers, institutions or geographies that are applicable to the DBG member relying on the assessment.

21. A reporting entity may use a risk assessment of another DBG member in whole or in part only. Reporting entities should satisfy themselves whether the level of risk posed in one business is given adequate attention as a result of its inclusion in a wider risk assessment or by applying a risk assessment undertaken by a business

[2] Section 32(1)(b) of the AML/CFT Act.

with varied business interests. For example, if the majority of the business is a product that another member of the DBG also offers to similar types of customers, then a reporting entity must be satisfied that the shared risk assessment places sufficient focus on that particular risk.

22. The obligation to undertake a risk assessment remains with the reporting entity. An AML/CFT supervisor may still require a reporting entity to undertake its own risk assessment that reflects the business of that entity.

23. It may not be appropriate to use a risk assessment of another member of a DBG where:

    - There are variations in products or services offered by one member that would require a different risk rating of products and services in another DBG member business
    - The risk ratings of products and services are altered by a different customer profile
    - Risk ratings are altered by focus on a specific country or countries; or
    - There have been material changes to the business in any entity since a shared risk assessment was developed

Suspicious activity reporting

24. A member of a DBG may make an 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 as designated by the Commissioner of Police. This provision is subject to the privacy and jurisdictional considerations in section 36 of the AML/CFT Act highlighted below.

Prescribed transaction reporting

25. A member of a DBG may make a PTR on behalf of another member of a DBG. In some circumstances, one member may submit PTRs for the entire DBG. PTRs are submitted to the New Zealand Police Financial Intelligence Unit as designated by the Commissioner of Police. This provision is subject to the privacy and jurisdictional considerations in section 36 of the AML/CFT Act.

Other sharing

26. Some other aspects of an AML/CFT programme may also be shared where appropriate.[3] For example:

    - Vetting – Policies and procedures may be different where different levels of vetting information is required. Vetting procedures could be undertaken by another DBG member, so 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 policies, procedures and controls must be in place as part of an AML/CFT programme.

[3] Section 32 of the AML/CFT Act.

However, each reporting entity may include in their policy that training may be undertaken by another member of the DBG.

- Review – A reporting entity must regularly review its risk assessment and AML/CFT programme to ensure they remain current, and ensure that any deficiencies in effectiveness are identified and appropriate changes are made. The obligation to ensure that the risk assessment continues to be current remains with each reporting entity, whether another DBG member's risk assessment is used or not. If one member of the DBG undertakes the risk assessment and it covers an assessment of another member's business, then any review should also include a review of that business as well. The compliance officer and senior management of the reporting entity need to be satisfied that any review appropriately incorporates their business. The same applies for ensuring that the AML/CFT programme – and any policies, procedures or controls outlined within that AML/CFT programme – remain current and any necessary amendments address any concerns raised.
- Audit – A reporting entity must ensure that its risk assessment and AML/CFT programme are independently audited every two years. 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. The compliance officer in each member must be satisfied this is the case.

Code of practice

27. A reporting entity that complies with an obligation by other equally effective means rather than by following a code of practice must 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

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

29. As mentioned 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 programme, review or audit.

Compliance officer

30. The primary requirement is that all reporting entities must have a compliance officer. The requirements for who can be a compliance officer are set out in section 56 of the AML/CFT Act and described further in the AML/CFT Programme Guideline.

31. Importantly, the compliance officer must be an employee of the reporting entity, 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 their reporting entity. The compliance officer is responsible

for ensuring the AML/CFT programme in a reporting entity is implemented and maintained.

Privacy considerations

32. Although suspicious activity reporting can be shared within the DBG, there are certain privacy requirements that must be considered. Members of a DBG should be conscious of the privacy implications when sharing any information between entities.[4] This includes situations where a member of a DBG that is based overseas, or a third-party provider, could be required to submit an SAR or equivalent in that jurisdiction.

33. Section 36 of the AML/CFT Act refers to the privacy considerations for personal information that may be shared in the context of a DBG. The AML/CFT 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 5–11 within the Privacy Act 1993. 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.

34. SARs and PTRs are required to be made to the Commissioner of Police. The New Zealand Police Financial Intelligence Unit will receive and process the reports on behalf of the Commissioner of Police. Information concerning an SAR can be shared with another member of a DBG to the extent necessary for the reporting entity to decide whether to make an SAR.[5]

[4] Sections 33–36 of the AML/CFT Act.
[5] Section 46(2)(e) of the AML/CFT Act.