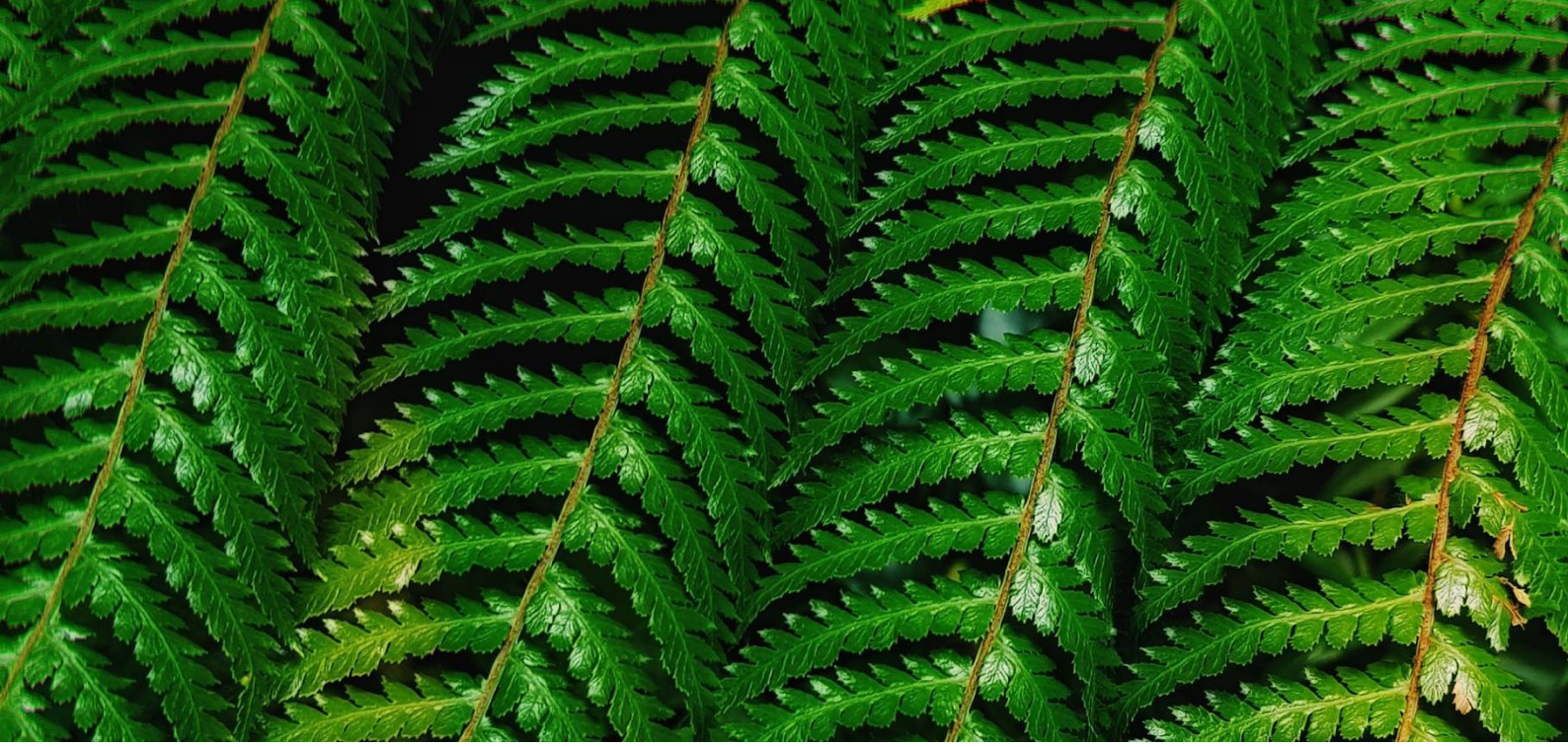

MAY 2025

AML/CFT Guideline: Customer Risk-Rating

This guideline is for FMA AML/CFT Reporting Entities

It gives guidance on customer risk-rating and should be read together with the triple-branded AML/CFT Risk Assessment and AML/CFT Programme guidelines.

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

Document history

This version was issued in May 2025

Contents

Introduction

1. This guideline supports reporting entities[1] to comply with the requirements of the Anti-Money Laundering and Countering Financing of Terrorism (**AML/CFT**) Act 2009 (the **Act**) relating to customer due diligence (**CDD**) for new customers.

- From 1 June 2025, reporting entities are required to risk-rate a new customer on establishment of a business relationship, or when a person seeks to conduct an occasional transaction or activity as part of CDD requirements.[2]

2. In addition, reporting entities must keep a record of the customer's risk rating, review the rating when conducting ongoing customer due diligence and account monitoring, and should update the rating where appropriate.[3]
3. A risk-based approach is central to the effective implementation of the Act. It requires reporting entities to identify, assess and understand the money laundering and terrorism financing (**ML/TF**) risks they face and then implement mitigation measures commensurate with those risks.
4. Knowing who your customer is and verifying information based on the risk involved is a key part of a risk-based approach and assists to protect your business from misuse. Rating customers for their level of ML/TF risk helps reporting entities to allocate resources efficiently, applying additional AML/CFT measures where customers are higher risk and lesser measures where risks are lower.
5. This guideline is based on the requirements of the Act and associated regulations and has been produced by the FMA under section 132(2) of the Act. This guideline does not constitute legal advice.
6. Examples provided in this guideline are suggestions to help you meet your obligations under the Act. They are not exhaustive and are illustrative in nature.
7. Sections 57(2) and 58(2)(g) of the Act require you to have regard to this guideline. It is important that you have read and taken this guideline into account when developing or updating your risk assessment and AML/CFT programme. After reading this guideline, we recommend you contact your AML/CFT supervisor or seek legal advice if you still do not understand any of your obligations.

FMA view:

Many AML/CFT requirements are risk-based,[4] and to comply with the Act you must determine the level of risk posed by the customer, their transactions or activities. The FMA considers that, implicitly, the Act has always contained a requirement to risk-rate customers. The explicit requirement to do so formalises this existing obligation.

A customer's risk rating can be used to inform the extent of the various AML/CFT measures that must be applied to each customer. Importantly, this includes your CDD, ongoing CDD and account monitoring. In turn, the risk rating supports you to comply with your AML/CFT obligations as efficiently and

[1] Within the meaning of section 5(1) of the Act.
[2] Regulation 12AC, AML/CFT (Requirements and Compliance) Regulations 2011 and ss 14 and 22 of the Act.
[3] Regulation 12AC(2) AML/CFT (Requirements and Compliance) Regulations 2011 and s 31 of the Act.
[4] See for example ss 12, 14, 16, 20, 24, 28, 30 and 31 of the Act, which relate to obligations "according to the level of risk" and Reg 11(3) and 11A(3) of the AML/CFT (Requirements and Compliance) Regulations 2011

effectively as possible. For instance, accurate risk ratings inform which of your customers require more regular review and monitoring, and which require less ongoing scrutiny. This allows the most efficient use of your compliance resource and is central to a risk-based approach.

In addition, the requirement to keep a record of the risk rating assists you to comply with your record keeping requirements more broadly. It demonstrates the rationale for the level of CDD, ongoing CDD and account monitoring that you undertake for each customer.

Risk-rating process

8. To risk-rate a customer you should undertake an objective determination of the level of ML/TF risk associated with them based on a risk-rating process or model.
9. There is no one-size-fits-all risk-rating process or model. You have flexibility in the process or model you implement for the risk-rating of your customers.
10. When determining the right process or model, a reporting entity must rely on its AML/CFT programme and its risk assessment. The process and sophistication of any model adopted should be appropriate to the level of risk the reporting entity faces and the nature, size and complexity of its business.
11. The risk-rating process should be guided by the results of the reporting entity's risk assessment conducted under section 58 of the Act. The analysis of the following matters in your risk assessment will be of particular importance:
    a. the types of customers, countries and institutions you deal with;
    b. the products and services you offer;
    c. the methods by which you deliver your products and services; and
    d. the National Risk Assessment 2024 and any applicable sector risk assessment (**SRA**) produced by your supervisor.
12. For most reporting entities, particularly smaller businesses with a small number of customers, and that offer a single or more limited range of products or services, the risk-rating process or model can be straightforward. Based on the existence of higher or lower risk indicators considered at onboarding, an objective determination against a rating scale of **low, medium** and **high risk** can be made.
13. For other reporting entities with a larger customer base and/or a more complex range of products and services, a more sophisticated methodology may be required. This reflects the multiple and more nuanced variables associated with risk across a large or complex business and its products and services. In some circumstances, it may be necessary to adopt a more nuanced rating scale. For example, including additional rating categories of **low-medium** and/or **medium-high** risk, using a numerical score and/or incorporating risk-rating elements specific to transaction monitoring.

FMA view:

FMA considers for most small businesses with a lower number of customers and single or limited range of products/services, a simple manual risk-rating process can be adopted. If the determination made is

objective, based on your risk assessment and as part of the CDD being conducted on the customer, this should meet the risk-rating requirement for onboarding a new customer.

For reporting entities that are larger and/or more complex businesses, FMA considers more sophisticated risk-rating models are required. This may include scorecards or matrix-based tools that assign weightings to various risk factors, numerically or otherwise. Options to do this could involve an automated solution, or using a qualitative assessment made by an employee onboarding the customer, or some combination of the two.

Risk-rating at onboarding

14. The information you obtain when conducting CDD, including information relating to the nature and purpose of a business relationship and that to determine whether the customer should be subject to enhanced CDD, should be a key part of determining the risk rating. Information such as that a customer seeks to conduct a complex, unusually large transaction or unusual pattern of transactions, or is a politically exposed person (**PEP**), is likely to be particularly relevant to the risk rating assessment.

FMA view:

An approach that you may take for a manual onboarding process is:

1. Determine an initial risk rating based on your business's risk assessment and the information you obtain from the customer when commencing the CDD process.
2. Upon completion of all required CDD verification steps, check that your initial risk rating is the correct risk rating of the customer.

Note: Each indicator of higher risk you identify during the risk-rating process should not exist in isolation. They should be viewed in combination. Where there are two or more higher risk indicators together, your level of ML/TF risk compounds. For reporting entities that opt to utilise a numerical process to arrive at a risk rating, care should be taken to ensure that the weighing of risk areas produces a risk score that aligns with the risk reasonably faced by your business. For example, if all your customers are New Zealand resident individuals, this should be down-weighted to ensure that higher risk customers are identified accurately.

Updating risk rating during ongoing CDD and account monitoring

16. Once a risk rating has been determined as part of your CDD at onboarding, this should inform the intensity and frequency of ongoing CDD and account monitoring of that customer. Likewise, the risk rating should inform any controls that may need to be put in place to mitigate ML/TF risks, for example transaction limits or senior management approval for certain levels of transaction or types of activity.

Your risk rating should be reviewed and updated as appropriate during ongoing CDD and account monitoring.[5]

17. In addition, you should note that ML/TF risk is dynamic and can evolve quickly in the event there is a change in a customer's activity or transactions. This could be detected by your account monitoring processes, for example by a particular transaction, rather than as part of any scheduled ongoing CDD review.

18. If this occurs, and in addition to any enhanced CDD or other AML/CFT measures applied, this should also trigger a review and likely increase in the risk rating.

FMA view:

Reporting entities should consider taking the opportunity to align their approach by risk-rating pre-1 June 2025 customers when undertaking ongoing CDD. This would over time contribute to consistency across the customer base and support an integrated and effective risk -based approach.

Record keeping

- Records of a customer's risk rating, including dates of review or update, must be kept.[6] These records must be retained for at least five years after the end of the business relationship (or the completion of the occasional transaction or activity).[7] These records must be kept in a form that is immediately accessible.[8]

19. Recording the reasons for all risk-rating decisions made will assist when you next review the customer's risk rating. This will also assist you to demonstrate you are discharging the risk-based CDD obligations of the Act effectively.

AML/CFT programme

20. Your policies, procedures, and controls for CDD, ongoing CDD and account monitoring, including the risk-rating of new customers, must be documented in your AML/CFT programme.

FMA view:

The FMA considers that there should be controls in place to periodically review the customer risk-rating process or model that you use. This should include reviewing and testing previous risk-rating settings to provide you assurance that your risk-rating process is effective.

As with the risk-rating process itself, the complexity of the assurance process you adopt and the frequency with which you use it, can be dependent on the size, nature and complexity of your business. However,

[5] Refer s 31(4)(c) of the Act and Reg 12AC and Reg 15J of the AML/CFT (Requirements and Compliance) Regulations 2011.
[6] Refer Reg 12AC(2) of the AML/CFT (Requirements and Compliance) Regulations 2011.
[7] Refer s 51(1) of the Act. Also Reg 15N(2) of the AML/CFT (Requirements and Compliance) Regulations 2011.
[8] Refer s 52 of the Act. Also *Department of Internal Affairs v OTT Trading Group Ltd* [2020] NZHC 1663 at [77]-[78].

when deficiencies are identified, there should be amendments made to the process or recalibration of the model.

Further Information

22. For further information relating to assessing ML/TF risk, please refer to the supervisors' Risk Assessment Guideline. As referred to in the Risk Assessment Guideline, reporting entities should likewise refer to the following when developing and implementing a risk-rating process or model:
    a. National Risk Assessment 2024;
    b. Financial Intelligence Unit (**FIU**) guidance material (accessible to reporting entities registered with the FIU's goAML system);
    c. relevant SRAs produced by the AML/CFT supervisors; and
    d. industry-specific risk summaries – for example the Law Firms Money Laundering and Terrorism Financing Risk Summary.
23. When developing and implementing your risk-rating process or model, you should consider guidance provided by the supervisors in the AML/CFT Programme Guideline.
24. The Financial Action Task Force provides useful information on ML/TF risks, likewise the Asia Pacific Group on Money Laundering provides information relevant for this region, including yearly typology reports and up-to-date news on methods and trends.

Appendix: Example Customer Risk-Rating Onboarding Table

This serves as an example only and is designed to assist smaller, less complex businesses.

25. The following table contains some key questions and considerations of risk factors that could be incorporated in a qualitative judgment-based risk-rating process or model for a new customer.
26. You can determine the customer's risk rating by assessing the extent to which factors that increase risk are present (or not). Note that this is an example only, and not an exhaustive list of factors or the sequencing of steps your business should take.
27. A similar table could be designed for risk rating reviews conducted as part of ongoing customer due diligence and account monitoring. At review, particular attention should be paid to observed activity or transaction patterns including if they are consistent with the customer profile or nature and purpose of the business relationship.

Risk Areas:	Risk Determination:
(i) Customer's occupation or business: Does the customer's type of business or occupation indicate a higher ML/TF risk? *[Consider: where is the customer's money or assets likely to come from and whether there is opportunity for proceeds of crime to be moved. This includes the complexity of the activities or transactions the customer will likely conduct, whether this could be on behalf of others, and the level of cash involved. For an individual, consider if they are a regular salary earner or have a less consistent income, for example self-employment, or whether they are a PEP]*	
(ii) Customer's structure - **If the customer is a legal person or legal arrangement, does the CDD information you have obtained indicate that beneficial ownership could be obscured?** *[Consider: the information you have obtained regarding beneficial ownership and legal structure, and whether this could be an attempt to conceal the identity of beneficial owners]*	

(iii) Product or service risk: Does the product or service to be provided to this customer indicate a higher ML/TF risk? *[Consider: the level of risk associated with the product or service, if the customer's use of the product or service appears legitimate and if any anticipated transactions or activity specific to this customer elevate their risk]*	
(iv) New or developing technologies: Is your customer involved in new or developing technologies that may favour anonymity? *[Consider: if so, how does this impact on the activities or transactions to be conducted through your reporting entity]*	
(v) Enhanced CDD if conducted: If enhanced CDD is being conducted, does the information you have initially obtained indicate a higher level of ML/TF risk? *[Consider: whether the information on the customer's source of funds or wealth or other information is plausible, or whether it raises concerns or requires further examination]*	
(vii) Nature and purpose and other information obtained: Does the information you obtained from the customer indicate anything unusual or unique about them for your business that indicates a higher ML/TF risk? *[Consider: whether the customer fits the profile for this proposed type of business relationship and if there is anything out of the ordinary about the information provided to you]*	
Additional factors that may increase the risk further:[9]	
(viii) Method of delivery: Does the way that you will deliver your products and services to this customer increase the risk? *[Consider: the extent to which there is the opportunity for the customer to interact with you remotely, anonymously, and/or through an intermediary or agent]*	
(ix) Country risk: **If the customer or proposed transactions or activities to be conducted have links to another country, does this increase the ML/TF risk?** *[Consider: the nature of the customer's links or proposed activities with the other country, which other country it is, and if it is a high-risk country]*	
(x) ML Typologies and Red Flag Indicators: Does there appear to be the presence of any red flag indicators? *[Consider: the red flag indicators relevant to your sector, product or service]*	
Initial risk rating (prior to completing CDD verification)	**Low / Medium / High**
Is the initial risk rating supported after completion of CDD verification?	Yes / No

[9] Note that an absence of these additional factors should **not** be seen as decreasing the risk.

Onboarding risk rating	**Low / Medium / High**
Notes:	

Disclaimer: This guideline has been produced by the FMA under s132(2)(c) of the Act for reporting entities on the application of risk-rating new customers when conducting customer due diligence. This guideline does not set out all obligations under the Act, its associated regulations or codes of practice. This guideline does not constitute legal advice.

AUCKLAND – Level 5, Ernst & Young Building | 2 Takutai Square, Britomart | PO Box 106 672 | Auckland 1143
WELLINGTON – Level 2 | 1 Grey Street | PO Box 1179 | Wellington 6140

fma.govt.nz