Te Tari Taiwhenua
Internal Affairs

New Zealand Government

Guideline:

Virtual Asset Service Providers

Complying with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009

March 2020

Contents

Executive Summary **3**
Disclaimer 3

Overview **4**
Capture Point under the Act 4
Ordinary Course of Business 5
Territorial Scope 5

ML/TF Risks of the VASP sector **6**
VASP Sector Inherent Risk 6
Key Vulnerabilities and High-Risk Factors 6
VASP-specific risk factors 7

Your AML/CFT Supervisor **9**
Who is my Supervisor? 9
What can I expect from my AML/CFT Supervisor? 10
The Department's regulatory approach 10
Monitoring and enforcement 11
Investigations of ML/TF 11

Compliance Obligations **12**
Compliance Officer 12
Risk Assessment 12
Assessing your ML/TF Risks 13
New or developing technologies, or products, that might favour anonymity 15
AML/CFT Programme 15
Annual Reports, Audits, and Recordkeeping 17
Annual Report 17
Independent AML/CFT Audits 17
Record keeping 18
Wire transfers 18
Reporting Transactions 19
Suspicious Activities and Transactions 19
Prescribed Transactions 20
Other Compliance Obligations 20
Financial Service Providers Register 20

Customer Due Diligence (CDD) Obligations **21**
Who do I conduct CDD on? 21
What a business relationship means and when it starts 22
New customers 22
Occasional customers 23

CDD for other types of customers 23
Trusts 23
Companies 23
Sole Traders, Co-operatives, and Partnerships 23
Clubs and Societies 24
Politically Exposed Persons 24
Identity Verification Code of Practice 24
Ongoing CDD and Account Monitoring 25
Different types of CDD 26
Other CDD requirements 26

Where to get further support 28

Executive Summary

Virtual Asset Service Provider (VASP) is a term that encompasses several different activities and services – an individual business may offer some or all of these. VASPs deal in virtual assets – digital representations of value, which can be digitally traded, or transferred, and can be used for payment or investment purposes. A common example of a virtual asset is a cryptocurrency, such as Bitcoin.

Money laundering (ML) is the method by which people disguise and conceal the proceeds of crime and protect and enjoy assets they have derived from illegal activity. Some people in New Zealand may also be facilitating terrorism financing (TF) using similar techniques to avoid detection by authorities and to protect the identity of those providing and receiving the funds. People with criminal intentions value anonymity and are looking for ways to distance themselves from their activities while still enjoying the proceeds of their crime. Both domestic and international evidence suggests that the use of virtual assets, and the associated services provided by VASPs, is a way for criminals to create a false perception of legitimately acquired wealth.

This guidance has been developed to help the VASP sector understand their compliance obligations under New Zealand's Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) regime and works alongside the recently developed VASP Sector Risk Assessment. The development has been driven by the growth of the VASP sector in both size and sophistication, and the introduction of Financial Action Task Force (FATF) standards relating to VASPs.

As a supervisor of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 ('the Act'), the Department of Internal Affairs (the Department) recognises that achieving compliance with the Act will take time and effort. This guideline helps you to determine whether your business must comply with the Act and, if so, what you must do to ensure you comply with the Act. You must comply with the Act by ensuring you identify, understand, and assess the risks of ML/TF to your business, and manage those risks in your day-to-day business via a dedicated AML/CFT programme. AML/CFT programmes will vary from business to business according to professional judgements about how to best manage specific risks.

Disclaimer

This guideline is provided for information purposes only and cannot be relied on as evidence of complying with the requirements of the AML/CFT Act. It does not constitute legal advice and cannot be relied on as such. If after reading this guideline you do not fully understand your obligations, you should seek suitable professional or legal advice or contact your supervisor, the Department of Internal Affairs, at Amlcft@dia.govt.nz

Overview

Capture Point under the Act

A 'capture point' is where a business offers services that fit under the definitions specified in section 5(1) of the Act. Capture points define which businesses have compliance obligations under the Act – if your business undertakes an activity that fits with these definitions, (a 'captured activity') you are a reporting entity with AML/CFT obligations.

VASPs are considered 'financial institutions' as defined in section 5(1) of the Act. VASPs may offer a diverse range of services, for example 'transferring money or value for, or on behalf of, a customer', 'money or currency changing', or 'investing, administering, or managing funds or money on behalf of other persons'. In many cases, VASPs may offer services fitting more than one capture point.

The below table may assist VASPs in determining potential capture points – this should only be considered as a guideline, and VASPs should consider where the services their business offers fit with the various capture points under the Act.

Type of VASP	Typical activities	Examples of possible capture points
Virtual Asset Exchanges	Issuing virtual assets such as virtual currency/digital tokens to facilitate virtual asset trading Providing a digital online platform facilitating virtual asset trading. Trading may occur between virtual assets or between virtual asset and fiat currency.	• issuing or managing the means of payment • transferring money or value for, or on behalf of, a customer • money or currency changing
Virtual Asset Wallet Providers	Providing storage for virtual assets or fiat currency on behalf of others and facilitating exchanges between virtual assets or fiat currency.	• accepting deposits or other repayable funds from the public • transferring money or value for, or on behalf of, a customer • money or currency changing
Virtual Asset Broking	Arranging transactions involving virtual assets.	• transferring money or value for, or on behalf of, a customer
Initial Coin Offering (ICO) Providers	Issuing and selling virtual assets/digital tokens to the public	• transferring money or value for, or on behalf of, a customer • issuing or manging the means of payment • money or currency changing
Providing investment opportunities in virtual assets	If you are providing investment opportunities in virtual assets (e.g. via a derivatives issuer providing virtual asset options), AML/CFT obligations will apply in the same way as if you were providing investment opportunities in traditional assets or financial products. For more information, see https://www.fma.govt.nz/compliance/amlcft/	

Ordinary Course of Business

When your business is involved in any of the capture points defined in the Act, you must determine whether the business activity is within the "ordinary course of business". If your entity is involved in capture points as part its ordinary course of business, you have obligations to comply with under the Act. Whether an activity is within the ordinary course of business will always be a matter of judgement depending on the nature of the business. Some relevant factors to take into consideration would be whether the activity:

- Is normal or otherwise unremarkable for your business
- Is frequent
- Is regular (meaning predictable, consistent)
- Involves significant amounts of money
- Is a source of income
- Involves significant resources
- Involves a service offered to customers

For further information, please refer to the guidance 'Interpreting Ordinary Course of Business' on the Department's website.

Territorial Scope

For a New Zealand registered VASP, in order to be captured by the Act, one or more of the business's activities must be carried on within New Zealand in the ordinary course of business.

A VASP incorporated or formed in New Zealand which, in the ordinary course of business, carries on their business activities wholly outside New Zealand will not be a "reporting entity" under the Act. A VASP in this category would be subject to AML/CFT requirements in the country where its activities are conducted.

VASPs registered outside of New Zealand may also be considered to be carrying on business in New Zealand, and therefore having AML/CFT obligations in New Zealand, if the entity is actively and directly advertising or soliciting business from persons in New Zealand. These entities should also consider their registration obligations under the Companies Act 1993, and the Financial Service Providers (Registration and Dispute Resolution) Act 2008.

Even though the Act only has jurisdiction in New Zealand, VASPs should consider reporting on suspicious activities and transactions that occur offshore as a matter of best practice.

For further information, please refer to the guidance 'Territorial Scope of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009' on the Department's website.

ML/TF Risks of the VASP sector

This section provides more detail on the risks and 'red flags' to be on the lookout for when you are conducting captured activities for your customers The information in this section is taken from the Department's Financial Institutions Sector Risk Assessment. The risk assessment has been developed from information taken from a range of open source publications and professional judgements of subject matter experts. The Department would expect VASPs to be familiar with the Sector Risk Assessment and make reference to this in their own organisation's risk assessment and AML/CFT programme.

This section has been arranged in the following categories:

- VASP Sector Inherent Risk
- Key Vulnerabilities and High-Risk Factors
- VASP-specific Risks

VASP Sector Inherent Risk

Inherent risk is the assessed ML/TF risk before any controls or mitigation measures have been put in place. Residual risk is the assessed ML/TF risk after any controls or mitigation measures have been put in place.

Overall Inherent Risk: High

Whilst individual VASPs will have their own level of residual risk determined by the ML/TF risk factors that apply to their specific services and activities and the controls they will put in place to mitigate these risks, both domestic and international evidence and guidance points to risks presented by the VASP sector. The easy access and wide geographic spread of VASP services, coupled with their pseudo-anonymous nature and use in every phase of ML/TF and in many different ML/TF typologies, means this sector presents a high inherent risk of ML/TF.

Key Vulnerabilities and High-Risk Factors

As part of the Department's Financial Institutions Sector Risk Assessment, six key vulnerabilities and high-risk factors associated with the VASP sector have been identified.

- New Payment Technology
- Anonymity and Complexity
- Lack of ML/TF Awareness
- International Payments
- High risk customers/jurisdictions
- Politically-exposed persons (PEPs) and High Wealth individuals

These risks are described fully in the Sector Risk Assessment.

The Department expects that these are considered as part of your risk assessment, which is described later in this guideline. These are not the only potential risk factors relevant to your business and should not be the only risks considered in your risk assessment – they are however important overarching themes relevant to the VASP sector.

Note that key vulnerabilities and high-risk factors relevant to your business do not operate in isolation but in combination, resulting in a compounding risk of ML/TF. Accordingly, your context is essential in identifying and determining your business' degree of ML/TF vulnerability and risk.

VASP-specific risk factors

Depending on the characteristics of the virtual assets they deal with, VASPs can face similar risks to other providers of higher-risk products/services, such as the money remittance sector, providers of currency exchange, and payment providers.

The nature of the virtual assets will have a large impact on the overall risk the VASP faces. Whether a virtual asset is centralised or decentralised, and convertible or non-convertible, may change the risk profile significantly. These characteristics and some of their associated risks are discussed below.

Many of the example risks listed below are applicable for some virtual assets but not others – i.e. non-convertible virtual assets do not face risks associated with the conversion to other virtual assets, or back to into fiat currency.

A number of specific risk factors for VASPs are detailed below. This is not to be considered an exhaustive list, and VASPs should consult both supervisor-issued guidance, and relevant domestic and international sources of information to determine the risks applicable to them.

Decentralised virtual asset systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. A *centralised virtual asset system* may mitigate some of these risks, however they should not be considered immune to them.

The size of VASPs can vary, but the technology in most cases will allow for *rapid expansion* – as seen in numerous exchanges following the 'bitcoin boom' of 2017. This could lead to VASPs becoming overwhelmed and unable to complete thorough customer due diligence (CDD) or transaction monitoring.

Off-chain transactions provide another avenue to obscure the movement of funds. *Off-chain transactions* are the transfer of value outside of the blockchain. This can occur through the transfer of virtual assets between personal wallets, physical exchange of paper or hardware wallets, transfer of one cryptocurrency to another within an exchange or through the purchase of cryptocurrency for cash via a peer-to-peer service. In these examples, the transactions stay off-chain until they are transferred or spent outside of the intermediary entity. At this point it will be difficult to determine the true source of funds.

The initial purchase of a virtual asset will usually involve the exchange of fiat currency to virtual asset. The conversion to and from fiat currency is the point where a launderer is most exposed – this is particularly relevant for a VASP that operates as an exchange.

VASPs often utilise *non-face-to-face business relationships*. This is a risk factor for ML/TF as customers may hide their true identity to avoid sanctions or attention from law enforcement.

Virtual Asset 'ATMs' or 'Kiosks' present unique risks because they provide or actively facilitate *virtual asset activities via a physical terminal*. Examples include structuring transactions or failing to collect and retain required customer identification information.

Virtual Assets have a history of being used by criminals and organised-crime. Examples include the 'Silk Road' website accepting virtual asset payments for illegal products, Liberty Reserve, unregistered peer-to-peer exchanges, and malware that extorts payment from victims in cryptocurrency.

Some potential customers may be the *victims of scams involving cryptocurrency*. VASPs should be aware of customers stating they need to send money to unlock a computer (ransomware) or pay tax debt, and of customers who have a limited knowledge of virtual assets.

VASPs should be aware of risks involving customers who conduct transactions with wallets or virtual assets that have been *linked to darknet marketplaces* or other illicit activity. Warning signs could include customer transactions being initiated from IP addresses associated with Tor, customer's wallet details appearing on public forums associated with illegal activity, or a transaction that makes use of mixing and tumbling services.

VASPs should be aware of risks of customers who may be operating as unregistered or Illicit peer-to-peer exchangers. Warning signs could include customers receiving a series of deposits from disparate sources that, together, amount to identical transfers to a known virtual currency exchange platform within a short period of time. Alternatively, the customer's phone number or email address being connected to a known peer-to-peer exchange platform advertising exchange services.

The use of virtual assets to avoid international sanctions is a known risk. As regimes and individuals are cut off from the global financial system, they search for alternatives. This has resulted in some countries and individuals trying to turn to digital currencies to offset the impact of economic sanctions. (Examples of states attempting to avoid sanctions via virtual assets include Venezuela and the 'Petro', North Korea's 'Lazarus' Hacking Group)

Virtual Assets' global reach increases the risks of potential ML/TF. Virtual asset systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers with customers avoiding face-to-face interaction, enhancing anonymity.

Virtual Assets can also be used to facilitate trade-based money laundering (TBML) schemes. Given the features of virtual assets such as having inconsistent value, their transnational nature, and favouring anonymity, they become conducive for TBML.

The risk of TF is also significant – terrorist organisations and their supporters and sympathisers are also constantly looking for ways to raise and transfer funds without detection or tracking by law enforcement, and the level of anonymity that virtual assets can provide is attractive to them. There are documented cases of organisations such as Hamas and al-Qaeda utilising virtual currencies to raise funds from donors and move money internationally.

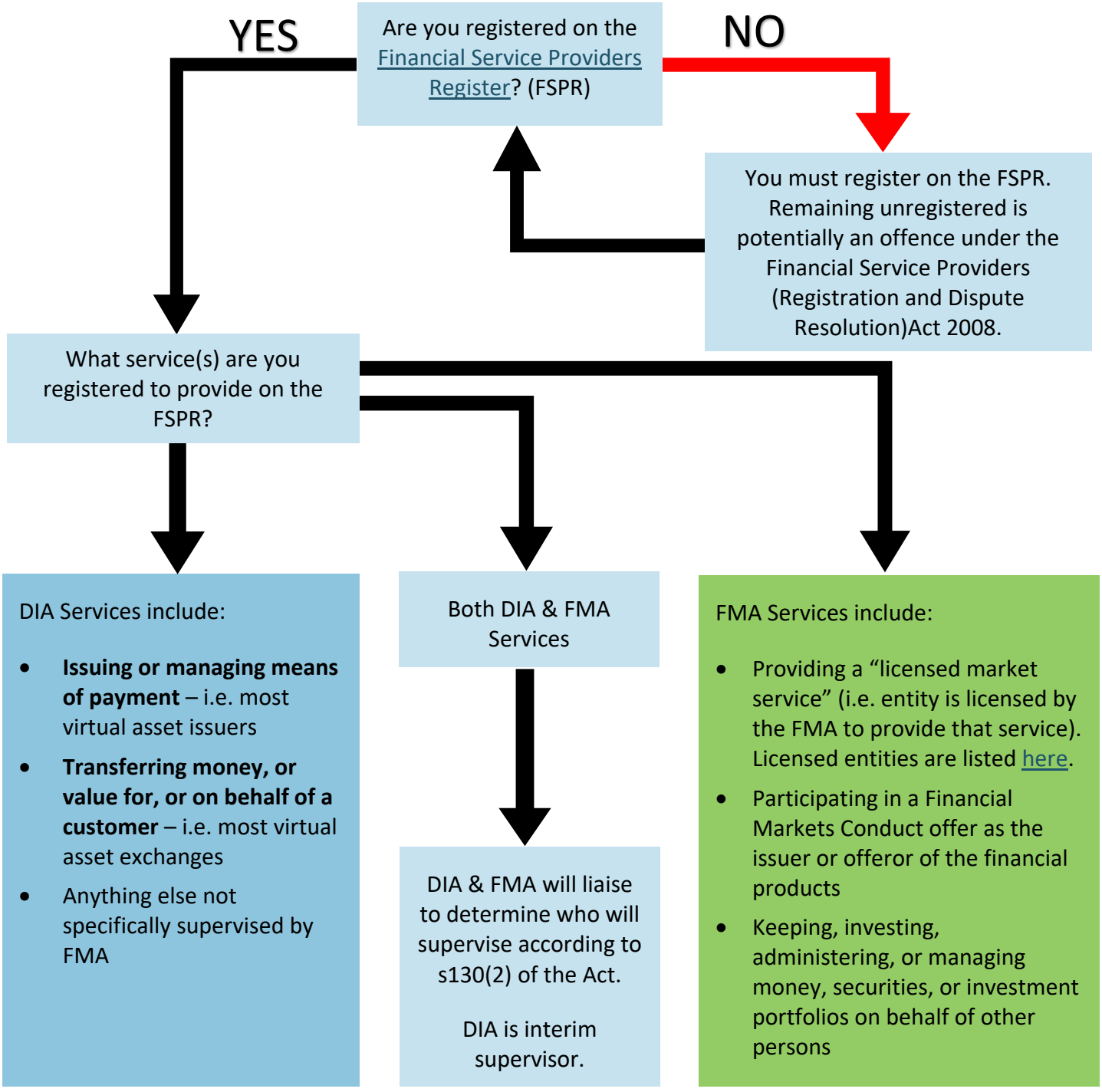
Your AML/CFT Supervisor

Who is my Supervisor?

As a VASP operating in New Zealand, you may be supervised by either the Department as the lead supervisor, or in certain cases the Financial Markets Authority (FMA).

The supervisor is determined based upon the activities you undertake. If you are unsure of who your supervisor is, you should contact the Department in the first instance. The following flowchart and table may assist you in determining their likely supervisor:

Supervisor: Department of Internal Affairs (DIA) or Financial Markets Authority (FMA)?



Type of VASP	Typical activity and likely supervisor
Virtual asset exchanges	If you are issuing your own cryptocurrency, you will be "**issuing or managing the means of payment**" (DIA) If you are facilitating trading, you will be "**transferring money or value for, or on behalf of, a customer**" (DIA) If your activity involves a virtual asset that is a 'financial product' under the Financial Markets Conduct Act 2013 (FMC Act), you will likely be supervised by the FMA. For example, if your virtual asset exchange is facilitating the trading of virtual assets that are financial products.
Virtual Asset Wallets	If the wallet facilitates exchanges it will be "**transferring money or value for, or on behalf of, a customer**" (DIA) If the wallet stores, but does not allow exchange of virtual assets, it will **not** be a reporting entity under AML/CFT Act.
Virtual Asset Broking	If you are arranging transactions, you will be "**transferring money or value for, or on behalf of, a customer**" (DIA)
Initial coin offering (ICO) provider	Depending on the rights attaching to the VA and terms of offer, the provider may be "**issuing or managing the means of payment**" (DIA); and/or "**transferring money or value for, or on behalf of, a customer**" (DIA) If your ICO involves a virtual asset that is a 'financial product' under the Financial Markets Conduct Act 2013 (FMC Act), you will likely be supervised by the FMA. For example, if your ICO offers virtual assets that are financial products.
Providing investment opportunities in virtual assets	If you are providing investment opportunities in virtual assets (e.g. via a derivatives issuer providing virtual asset options), AML/CFT obligations will apply in the same way as if you were providing investment opportunities in traditional assets or financial products. FMA will likely be your supervisor. For more information, see https://www.fma.govt.nz/compliance/amlcft/

What can I expect from my AML/CFT Supervisor?

The Department's regulatory approach

As an AML/CFT supervisor, our role includes monitoring reporting entities for compliance with the Act, providing guidance to reporting entities and investigating and enforcing compliance. This is to ensure the AML/CFT system operates in a robust manner and that criminals seeking to launder money and finance terrorism are detected and deterred.

The Department's regulatory approach for the AML/CFT system is outlined in three publications:

- AML/CFT Regulatory Framework
- Minimising Harm – Maximising Benefit: The Department of Internal Affairs' Approach to Compliance & Enforcement 2012
- AML/CFT Supervisory Framework

We apply a risk-based and responsive regulatory approach that promotes compliance through a mix of strategies, initiatives, and tools. We aim to:

- Make it easy for reporting entities who want to comply
- Help reporting entities who are trying to comply
- Use the full force of the law on reporting entities that refuse to comply

Our preference is to work with you in a responsive and educative manner, although we are fully prepared to escalate our response with enforcement action.

Monitoring and enforcement

The Department uses a variety of regulatory tools to monitor a reporting entity's compliance with AML/CFT obligations. These include desk-based reviews of reporting entities' documents to test technical compliance; on-site inspections to test effectiveness of implementation of AML/CFT programmes; analysis of annual reports; and independent audits.

When the Department identifies reporting entities that are not meeting their obligations under the Act the Department will consider several options. One of these options is a remediation plan with the reporting entity. A remediation plan includes a set of expected outcomes that the reporting entity must complete within a set timeframe. The timeframe includes measurable progress towards meeting the obligations under the Act. In most cases the timeframe and actions are met, and the reporting entity progresses towards meeting the obligations.

In response to more serious or deliberate non-compliance, the Department may decide to issue a formal warning or to accept an enforceable undertaking. Alternatively, the Department may decide to seek an interim, performance, or restraining injunction, or a pecuniary penalty, from the High Court.

In the most serious of cases, acts that are engaged in knowingly or recklessly are criminal offences. There are several further criminal offences; for example, failing to report or keep records relating to suspicious activities, structuring transactions to avoid AML/CFT requirements, and obstructing or misleading a supervisor. Where necessary, the Department will prosecute reporting entities for criminal offences under the Act.

Investigations of ML/TF

In New Zealand it is a criminal offence to knowingly and intentionally engage in, or facilitate any other person to engage in, money laundering or the financing of terrorism. The New Zealand Police are responsible for investigating and prosecuting ML/TF offences, as well as forfeiture proceedings relating to the proceeds of crime. A robust AML/CFT system, in which reporting entities are conducting CDD, keeping customer and transaction records, and reporting suspicious activities, is an important tool in the collective fight against financial and organised crime.

Compliance Obligations

VASPs have the same obligations as other reporting entities under the Act. The initial steps towards AML/CFT compliance involve:

- Appointing a Compliance Officer
- Undertaking a Risk Assessment
- Development of an AML/CFT Programme

Further compliance obligations covered in this section include:

- Submitting Annual Reports
- Independent audits of your AML/CFT Programme
- Record keeping requirements
- Wire transfers

Additional guidance material issued by the supervisors is referenced in the relevant sections. VASPs should also make use of relevant information from both domestic agencies such as the NZ Police Financial Intelligence Unit (FIU) and from international bodies, such as FATF.

Compliance Officer

Appointing a compliance officer is the first step towards compliance. Having a compliance officer is mandated under the Act.

The compliance officer should be an employee of your business who reports to a senior manager or partner of the business. If the VASP is a solo operator, they are expected to act as the compliance officer themselves and take full responsibility for all compliance requirements.

When your compliance officer is appointed, they should contact the Department via the AML Online portal and register their details. It is important that these details are registered and kept up-to-date as this enables the Department to communicate effectively and provide important information and updates.

Risk Assessment

All reporting entities must undertake a risk assessment, and it must be recorded in writing. The specific requirements for a risk assessment are set out in section 58 of the Act, which includes the requirement that you have regard to guidance produced by the AML/CFT supervisors when developing your risk assessment. The following are examples of guidance that have been produced by the Department and should be considered by VASPs in developing their risk assessment.

Risk Assessment Guideline

Financial Institutions Sector Risk Assessment

AML/CFT Risk Assessment and Programme: Prompts and Notes for DIA reporting entities

In addition to considering guidance produced by the Department, the risk assessment is required by section 58 of the Act to have regard to the following:

- The nature size and complexity of your business
- The products and services you offer
- The way you deliver your products and services
- The types of customers you deal with
- The countries you deal with
- The institutions you deal with.

These categories are specifically examined within the Department's Sector Risk Assessment for VASPs, and further information can be obtained from the other NZ supervisors, as well as international sources. A good example of this is the FIU's National Risk Assessment (NRA).

Assessing your ML/TF Risks

An example of some of the questions you might ask yourself when assessing the risks associated to your business:

Category: *The countries you deal with*

- *What are those countries?*
- *What are the risks associated with those countries? For example, is a country a tax haven, subject to international sanctions, that has problems with corruption, drug trafficking or terrorism?*
  - Yes? Then there is a vulnerability and suggests you may have identified an area where your business is at high risk. You will need to carefully consider how risks associated with those countries impact on your business and can be addressed in your AML/CFT programme.
  - No? If you only ever deal with persons or activities within New Zealand, ML/TF risks associated with other countries may not be as relevant to your business.

As supervisors, the Department are looking for a written risk assessment that:

- Shows an understanding of how your business might be vulnerable to ML/TF in the course of business and identifies the higher risk areas
- Assesses the likelihood of those risks happening
- Records the above and explains how you arrived at your conclusions.

A good place to start is working through each of the sections in the Risk Assessment Guideline – using the questions as prompts, then noting whether you consider the risk to your business to be low, medium, or high. Consulting the Sector Risk Assessment will help provide examples of general ML/TF risks, and risks specific to the VASP sector that you should consider.

The Act requires that you consider both your specific business context and the wider risks applicable to your business, and the services you offer, when you conduct your risk assessment. It is important that you take a broad view of the risks that may affect you. You need to state BOTH whether your ML/TF risk is low, medium, or high in each particular area AND how you reached this conclusion. You need to provide justifications and evidence for your ratings, and your supervisor may ask for this information.

Continuing from the above example of the countries you deal with, it is prudent to use verifiable data from your company to differentiate between the different countries you deal with to support the analysis of your related ML/TF risk.

Category: *The countries you deal with*

- *What are those countries?*
  - "For 85% of our business, we deal solely with New Zealand based clients, whom we have obtained and verified this information on. In these circumstances, we consider there is a low risk in the country we are dealing with. However, for 15% of our business we deal with clients based in other countries. Here we consider our ML/TF risk to be higher."

You could follow this with a more detailed look at the other countries you deal with, what the risks of these countries are, who the clients are, and assess what effects these factors have on the associated ML/TF risks.

Two important points to remember when conducting your risk assessment:

- The ML/TF risks associated with the different issues that you must consider as part of your risk assessment are interrelated. For example, the risks associated with the countries you deal with will likely overlap with the ways you deliver your products and services.

- Where you have several higher risk indicators all occurring at the same time, the overall level of risk rises exponentially. As an extreme example, a client from a high-risk country where your engagement is via a website, or through an intermediary, and a complex legal structure (such as a trust) is involved – this constitutes a level of ML/TF risk that is extreme. This should be addressed in your AML/CFT programme and mitigations put in place.

You must regularly review and update your risk assessment when there is any material change to the business, its service offerings, or its client base, or where deficiencies in the effectiveness of the risk assessment are identified. As methods and techniques (known as "typologies") of ML/TF adapt and change, the nature of the risks posed to a business may change also. This is particularly relevant for VASPs, who operate in an environment that is fast-paced and susceptible to change, particularly in the area of new or developing technology.

You should think about updating your business's risk assessment are when:

- The FIU publish a new National Risk Assessment for ML/TF or other report about ML/TF issues that highlights the potential for vulnerabilities in your business activities.
- The Department updates its Sector Risk Assessment.
- You become aware of an increased ML/ TF risk to your business due to a change in the nature of the services you offer or demand for your services.

- International ML or TF-related events trigger you to reconsider your risk assessment.

As part of the periodic reviews, your records should show evidence of the updates that you have made to address any identified deficiencies in its effectiveness. Ways to do this could be to keep a record of version history or retaining historical documents or other evidence that demonstrate your reviews and updates.

New or developing technologies, or products, that might favour anonymity

VASPs are especially exposed to new or developing technologies, or products, that might favour anonymity, which are addressed in section 30 of the Act. The Department treats all VASPs as dealing in new or developing technologies that might favour anonymity. The Department acknowledges that different virtual assets have different characteristics that may affect their level of anonymity, and that not all virtual assets may necessarily favour anonymity. However, the Department expects that you consider and apply section 30 of the Act for all virtual assets you offer, and that this is recorded as part of your risk assessment.

As a supervisor, the Department expects to see reference to this section of the Act throughout the risk assessment and AML/CFT programme, acknowledging the risks associated with virtual assets and the steps that will be taken in order to mitigate the risks posed by virtual assets.

Prompts when considering new or developing technologies, or products, that might favour anonymity

Some ideas for questions you may wish to consider as part of your assessment of section 30 risks are:

- How is the virtual asset normally obtained? Is it easy for customers to obtain it anonymously?
- Can transactions be traced reliably?
    - Is the ledger public or private?
    - Could/does your business trace transactions?
    - Does the trace lead to a pseudonymous address or to a natural person?
- Is the virtual asset specifically designed to provide a higher level of anonymity? (examples of virtual assets specifically designed for high anonymity include Monero or Zcash)
- Is the virtual asset run on a centralised or decentralised ledger?
    - How might this affect the ability for customers to be identified or for transactions to be controlled?

Note this is not an exhaustive list, and the characteristics of the virtual asset you are dealing with will determine what risk factors you should consider.

After identifying the risks associated with the virtual assets you deal with and recording them in your risk assessment, addressing any additional measures you may need to take to mitigate these risks should be recorded in your AML/CFT programme.

AML/CFT Programme

Once your risk assessment is completed, you must develop an AML/CFT programme that includes internal procedures, policies, and controls to detect and manage the risk of ML/TF to your business. Your AML/CFT programme must be based upon your risk assessment and show a clear link between the risks you have identified in your risk assessment, and your policies, procedures, and controls designed to address those risks.

The Act also requires that your AML/CFT programme includes policies, procedures, and controls for:

- Vetting staff
- Training staff
- Customer Due Diligence (CDD)
- Keeping written findings of unusual transactions, or other activity that is likely to be related to ML/TF
- Suspicious activity reports (SARs)
- Prescribed transaction reports (PTRs)
- Record keeping
- Products and transactions that favour anonymity
- Managing and mitigating dynamic risk – for example monitoring your customers for changes in risk profile
- Monitoring compliance with the AML/CFT programme

A simple way to think about policies, procedures, and controls is:

- Policy is ***what*** you are going to do.
- Procedure is ***how*** you will do it.
- Controls are a ***check*** to make sure you are following your policies and procedures.

An example of a policy, procedure and control may be:

Prescribed Transaction Reports (PTRs)	
Policy	We are obligated by the Act to submit prescribed transaction reports (PTRs). Accordingly, the business has determined that PTRs are required for any transactions we undertake that meet the following thresholds: • Are large cash transactions NZ$10,000.00 or more, or; • Are international wire transfers of NZ$1,000.00 or more The report needs to be submitted to the FIU within 10 working days via the GoAML portal.
Procedure	Our customer management system is calibrated to generate an alert reminding staff when they are processing a transaction that meets the PTR policy threshold. The staff member responsible for submitting the PTR is (*title/identifier*). This staff member holds a GoAML login, and will submit the PTR via this portal, no later than 10 working days from the time of the transaction. Once the PTR is submitted, a record of submission from GoAML will be attached to the transaction file by the staff member.
Control	Our compliance officer (*title/identifier*) undertakes a monthly testing sample of eligible transactions and confirms whether the associated PTR has been submitted in GoAML. They do this by taking the records of all transactions in our customer management system that meet the thresholds for a PTR within the month and testing a random sample of these. The random sample transactions will be examined in the customer management system for the attached record of submission from GoAML, and the compliance officer will query GoAML directly to confirm the PTR was submitted.

Like your risk assessment, you must regularly review your AML/CFT programme to ensure it remains up-to date and to identify and remedy any deficiencies. Your records should show evidence of updates that address any identified deficiencies in its effectiveness.

The Act requires that you have regard to guidance produced by the supervisor when developing your AML/CFT programme. The following guidelines may assist VASPs in developing their AML/CFT programme.

AML/CFT Programme Guideline

AML/CFT Risk Assessment and Programme: Prompts and Notes for DIA reporting entities

Note that the guidance is generic in nature. It does not provide prescriptive instructions on how businesses can ensure they are compliant with the Act. This is because each business has unique circumstances that determine their exposure to ML/TF risks, which they need to understand and factor into their unique AML/CFT programme. Businesses will need to apply their own judgement, and where there are questions about compliance, they can either ask the Department for general information, or seek independent advice.

The most important part of your AML/CFT programme is that it is effectively implemented. Having a really good AML/CFT programme on paper is not enough. Your programme needs to work in practice. When we ask you need to be able to show us that your programme is working - that you have been checking how it is working, making any necessary improvements, and recording your checking process and any resulting changes.

Annual Reports, Audits, and Recordkeeping

Annual Report

Reporting entities are required to submit an annual report through AML Online. This report covers the 12-month period from 1 July – 30 June, and may be submitted any time from 1 July, but by no later than 31 August following the reporting period (or other date as advised by your supervisor).

The scope and coverage of your annual report is limited to the AML/CFT activities captured by the Act, for example you only need to provide details on revenue associated with products or services that are covered by the Act during the reporting period. VASPs should use the set of annual report questions for financial institutions.

Annual Report User Guide

Independent AML/CFT Audits

Every two years, you must have an independent audit of your risk assessment and AML/CFT programme. An independent audit provides assurance that your policies, procedures, and controls remain up-to-date, that any deficiencies in your programme's effectiveness are identified, and that any necessary changes have been made and recorded.

The Act requires that the person undertaking your audit is independent and suitably qualified.

Independence means that the person conducting your audit cannot benefit from the results of the audit in anyway. Someone who has been involved in the establishment of your AML/CFT programme (such as completing the risk assessment and/or writing the AML/CFT programme) is not independent and cannot conduct your audit.

The person who conducts your audit is not required to be a Chartered Accountant or otherwise formally qualified, but they do need to demonstrate how they are appropriately qualified to conduct the audit. Being appropriately qualified means that they have knowledge of the AML/CFT system (Act, Regulations, Codes of Practice etc) and an understanding of your business context, and how the AML/CFT regime applies to it.

A copy of the independent audit must be provided to the supervisor on request. The supervisor can instruct a reporting entity to have a new independent audit undertaken at any time.

Further guidance on audits is available here:

Audit Guideline

Record keeping

All reporting entities, including VASPs, must keep adequate records as outlined in sections 49 to 55 of the Act. Records must be in written form in English or be readily accessible and readily convertible into written form in English.

Your records for must be kept for at least five years. Your supervisor or the Commissioner of Police may ask reporting entities to keep records for longer periods in some circumstances. After five years, the records can be destroyed unless there is a lawful reason why they should be retained – for example, the need to comply with another enactment or to enable you to carry on your business.

Wire transfers

Wire transfers are an especially important captured activity for VASPs.

In New Zealand, the definition of wire transfer is set out in section 5 of the Act. For VASPs this definition covers:

- Transactions from fiat currency to virtual assets, and
- Transactions from virtual assets to fiat currency,
- But does not include virtual asset to virtual asset transactions.

VASPs must be particularly aware of their wire transfer obligations as described in sections 27 and 28 of the Act, as well as the associated PTR obligations. These obligations apply to any transaction that is over NZD$1,000.

VASPs should, in addition, be aware of the FATF recommendations in relation to wire transfers, which include virtual asset to virtual asset transactions. VASPs should be aware that other international jurisdictions they deal with (and other VASPs based in those jurisdictions) may require this, and consequently, it would be considered ‘best practice’ for VASPs to include virtual asset to virtual asset transactions in their wire transfer procedures.

Domestic and international wire transfers

Your wire transfer obligations differ depending on whether the transaction is domestic or international – the criteria for a domestic wire transfer are set out in section 27(7) of the Act – any wire transfer not meeting these criteria is considered an international wire transfer.

Wire transfer identity requirements

Section 27(1)(b) of the Act requires VASPs to hold "the originator's account number or other identifying information that may be prescribed and allows the transaction to be traced back to the originator". To meet this requirement, VASPs dealing in cryptocurrency may, for example, choose to record the public key associated with the originator's wallet.

Other wire transfer requirements

Other requirements in section 27 include holding the originator's full name and other identification information. Section 28 requires you to verify this information according to the level of risk involved – this allows for differing levels of verification for transfers with differing levels of risk. An example of this may be differing levels of verification for your customers that are based domestically compared to your customers that are based internationally. The rationale behind your risk classification for each class of transaction, and the processes to verify the corresponding information you have gathered should be thoroughly recorded in your AML/CFT programme.

Wire Transfer Factsheet

FATF Guidance

Reporting Transactions

Suspicious Activities and Transactions

Section 40 of the Act covers Suspicious Activity Reports (SARs). Note that the term SAR is used in line with the definition in section 5(1) of the Act, which includes both suspicious transaction reports (STRs) and SARs.

Reporting entities are required to report suspicious activities when they have formed a suspicion based on reasonable grounds that a transaction is linked to one of the following:

- Money laundering
- Terrorism financing
- Misuse of drugs
- Proceeds of crime
- Any serious offence under the Crimes Act 1961 (punishable by 5 years or more imprisonment)

A suspicious activity will often be one which is inconsistent with a client's known activities and profile, or with the normal business expected for that type of client.

In order to help detect suspicious activity, VASPs must ensure their staff are appropriately trained, and have awareness of red flags, ML/TF typologies, and what may constitute unusual activity. VASPs should consult both domestic and international guidance to help determine indicators of suspicious activity relevant to their business. Particularly useful sources include the FIU reporting guidelines, and NRA, as well as the Department's Sector Risk Assessment, and guidance issued by FATF.

You are required to report suspicious activity through the GoAML web reporting tool provided by the FIU. The FIU has issued guidance on how to submit reports using their GoAML web-based reporting tool. You must use the specific reporting format provided by the FIU.

The Act requires that you report suspicious activity to the FIU as soon as practicable, but no later than three working days after you have formed your suspicion. It is not a defence that you did not actually consider an activity to be suspicious, if in the circumstances a reasonable person would have been suspicious. This means that you need to objectively assess each transaction to make sure no suspicions arise.

If you submit a SAR relating to a customer, you **must not** disclose this information to your customer. This is sensitive information and should only be disclosed to other parties on a need to know basis, which is likely to be very few people.

Prescribed Transactions

You are required to report prescribed transactions in Prescribed Transaction Reports (PTRs). PTRs add further transparency to the financial system by making the methods of ML/TF more difficult to hide and improve the detection and disruption of organised crime.

A prescribed transaction is an international funds transfer of NZ$1,000 or more conducted through a reporting entity or a domestic physical cash transaction of a value equal to or above NZ$10,000.

Both the ordering institution (sender) and beneficiary institution (receiver) are required to file a PTR in respect of an international wire transfer. Unless a VASP is certain that their transaction is domestic in nature as per section 27(7) of the Act, VASPs should consider reporting all wire transfers in line with the international funds transfer PTR obligation.

Other Compliance Obligations

Financial Service Providers Register

In the New Zealand context, registration of Financial Services Providers is required via the Financial Service Providers Register (FSPR).

All VASPs should consider their obligation to register on the FSPR – offering services that come under the Financial Services Providers (Registration and Dispute Resolution) Act 2008 without registering may constitute an offence under that Act.

The FMA has produced guidance for cryptocurrencies which includes information on where VASPs may need to register on the FSPR.

Customer Due Diligence (CDD) Obligations

You need to know your customers.

Before conducting any captured activities, you need to conduct a Customer Due Diligence (CDD) process. The CDD process you follow is determined by the level of risk posed by your customers.

CDD is not optional and must be done for all your customers. If you are not able to complete CDD, you must not undertake a captured activity or transaction for that customer. Transacting a captured activity without performing CDD breaks the law.

This section provides information about:

- Who do I conduct CDD on?
- What a business relationship means and when it starts
- New customers
- Occasional customers
- CDD for other types of customers
- Politically Exposed Persons (PEPs)
- Identity Verification Code of Practice (IVCOP)
- Ongoing CDD and Account Monitoring
- Different types of CDD
- Other CDD requirements

The requirements described in this section are contained in Part 2, subpart 1 of the Act (sections 9-39).

Who do I conduct CDD on?

You must conduct CDD on:

- Your customer
- Any “beneficial owner” of a customer
- Any person acting on behalf of a customer

Who you must conduct CDD on	Comment
Your customer	• Is the person who you enter into the business relationship (or series of related transactions) with • Customers who are individuals (as opposed to trusts or companies for example) may be treated as the beneficial owner if you believe on reasonable grounds that the person is not acting on behalf of anyone else

Any "beneficial owner" of a customer	• Someone who owns more than 25 percent of a company that is your customer • Someone who has effective control of a company that is your customer • The person/s on whose behalf a transaction is conducted The Beneficial Ownership Guideline provides further information relevant to determining beneficial ownership.
Any person acting on behalf of a customer	There are instances where a person is acting on behalf of a customer but is not necessarily a beneficial owner of that customer. For example: • A person exercising a power of attorney for your customer • A legal guardian acting on behalf of a minor who is your customer • An employee who has the authority to act on behalf of a company that is your customer The Acting on Behalf of Factsheet provides further information relevant to determining where persons are acting on behalf of another customer.

What a business relationship means and when it starts

A business relationship is defined in section 5(1) of the Act as *"a business, professional, or commercial relationship between a reporting entity and a customer that has an element of duration or that is expected by the reporting entity at the time when contact is established, to have an element of duration*".

This captures situations where a reporting entity has, or expects to have, a relationship with a customer involving more than one interaction. An example of a VASP starting a new business relationship is when a new customer signs-up to the VASP in order to receive a service. In this example, CDD must be conducted at the beginning of the relationship, as well as when appropriate should there be material changes throughout the relationship.

You need to use your best judgement to determine when a new business relationship with a customer starts. Your business relationship is likely to begin after initial inquiries about the services they need have been made, but before you have commenced any work for them.

New customers

You may not have to conduct CDD on every new customer. You need to establish at the outset of the business relationship whether your new customer is going to require you to conduct any activity captured by the Act. Any customer who requests a captured activity needs to have CDD performed on them in line with the level of risk they represent and in accordance with the requirements in the Act.

You are not required to conduct CDD until your customer requests a captured activity. If may be that your customer does not initially request captured activities and you accordingly have not performed CDD. As soon as the customer requests a captured activity, you must perform CDD before you carry out any captured activities.

Occasional customers

As described in section 14(1)(b) of the Act, you are required to conduct CDD on 'occasional customers'. An 'occasional customer' is someone who seeks to conduct either and 'occasional activity' or 'occasional transaction' through you.

'Occasional activity' and 'occasional transaction' are both defined in the Act. The term "occasional" does not necessarily mean 'single' – it also includes circumstances in which multiple transactions are so intermittent or infrequent that no business relationship is established.

Reporting entities should be aware of customers whose occasional activities increase in frequency to the point at which a business relationship has commenced – a good test of this is whether you reasonably expect that the customer is likely to return for future transactions.

CDD for other types of customers

Factsheets for the identification and verification requirements for customers who may have ownership structures that have unclear obligations for CDD are available under the sub-headings below.

These fact sheets should be read in conjunction with the Beneficial Ownership Guideline.

Trusts

The Act treats trusts as being capable of being customers in their own right, despite a trust not ordinarily having a legal personality. Trusts may have complex CDD requirements depending on their structure and may require different levels of identification for trustees and beneficiaries.

Trusts as a Customer Factsheet

Companies

In New Zealand, both New Zealand based companies, and overseas companies that carry on business in New Zealand are required to be registered on the New Zealand Companies Register. Companies can have complex ownership structures, as well as multiple beneficial owners and persons acting on behalf of the company.

Companies CDD Factsheet

Sole Traders, Co-operatives, and Partnerships

Businesses vary greatly in size and complexity – for example they range from sole traders and some partnerships with simple and transparent structures, whereas others, such as some co-operatives and limited partnerships, are likely to be more complex and may involve both general and limited partners.

Sole Traders and Partnerships Factsheet

Co-operatives Factsheet

Clubs and Societies

The type of entity that the club or society is determines the CDD that is undertaken. A club or society may be one of a variety of types of entity – for example, a trust.

Clubs and Societies Factsheet

Politically Exposed Persons

You are required to identify whether your customers are Politically Exposed Persons (PEPs).

Section 26 of the Act requires you to take steps to identify whether a customer is a PEP as soon as possible after establishing a business relationship or conducting an occasional transaction or activity.

You must conduct enhanced CDD in accordance with section 26 of the Act if you establish a business relationship with a customer or beneficial owner who is a PEP, or if a PEP seeks to conduct an occasional transaction or activity through the reporting entity.

A PEP is defined in section 5(1) of the Act. In summary, a PEP is a person, or an immediate family member or someone who has close business ties to that person, who holds or has held (in the preceding 12 months) a prominent public function in a foreign country.

This may be because they are or were a head of state, senior politician, or an official with a public profile, such as a Supreme Court Judge, or a highly ranked military official. It could also be because they had authority and influence in a state enterprise in any country. PEPs can be exposed to bribery or corruption or their respected status may be misused (knowingly, or unknowingly) to legitimise otherwise suspect transactions.

If you determine that your customer or a beneficial owner is a PEP, your AML/CFT programme must have a process by which your staff will require senior management approval to continue the business relationship. Also, as per obligations under section 26 of the Act, you must obtain information about the source of wealth or funds and verify that information.

If you have already undertaken an occasional transaction or performed a captured activity for someone and you then realise that the person is a PEP, you must conduct enhanced CDD as soon as you realise they are a PEP, and as soon as you can.

The Enhanced Customer Due Diligence Guideline has more information about how to manage compliance where customers are identified as PEPs.

Enhanced Customer Due Diligence Guideline

Identity Verification Code of Practice

The Identity Verification Code of Practice (IVCOP) provides a suggested best practice for all reporting entities conducting name and date of birth identity verification on your customers (that are natural persons) that you have assessed to be low to medium risk.

For VASPs, many customers will not be assessed as low to medium risk, due to the inherent risks of the sector, and the associated obligations to consider risk arising from new or developing technologies or products that may favour anonymity (under s30 of the Act). IVCOP is only applicable to low to medium risk customers and therefore may not be suitable for most VASP customers.

As a supervisor, the Department notes that compliance with the code is not mandatory, but that entities should notify their supervisor if they do not intend to comply with the code. Where the code is not complied with, the Department would expect VASPs to find alternate but equally effective means for identifying their customers – this should be thoroughly documented as part of your AML/CFT programme.

Identity Verification Code of Practice

Ongoing CDD and Account Monitoring

When you are in a business relationship with a customer, you are required to conduct ongoing CDD and account monitoring (under section 31 of the Act).

You are required to keep up-to-date customer account and transaction activity information and to regularly review this information. This ensures that the nature and purpose of your business relationship and the resulting activities or transactions are consistent with your knowledge of the customer and the customer's risk profile. This regular review will also assist with identifying any grounds for reporting a suspicious activity.

You must develop a process for ongoing CDD and account monitoring for your customers according to the level of risk each customer presents.

For higher-risk customers you need to have more frequent and thorough account monitoring than customers deemed to be low or medium risk. The account monitoring you conduct will assist you to identify any activity or transaction behaviour that is not consistent with the expected activity of the customer, their risk profile and the CDD you have previously conducted.

Different types of CDD

There are broadly three types of CDD. You will need to use the right type, which will depend on:

- the unique factors of each business relationship
- the characteristics of the customer(s)
- the nature of the activities and transactions you are facilitating
- the potential for ML/TF risk.

The three types of Customer Due Diligence are:

Simplified CDD

A narrower form of CDD, for use with specific customers or customer types that are considered to be low risk for ML/TF. These customers are specified in section 18(2) of the AML/CFT Act.

VASPs are unlikely to use simplified CDD due to the high risk nature of their operating context.

Standard CDD

The default information that you must collect and verify from all customers.

In the VASP context, this will generally form the basic information to be gathered and verified, prior to obtaining further enhanced CDD information.

Enhanced CDD

A more comprehensive form of CDD, for use when there are factors creating a higher level of ML/TF risk or as otherwise specified in the AML/CFT Act.

There are several forms of enhanced CDD, detailed in sections 22-30 of the Act.

Sections 27-28 (wire transfers) and 30 (new technologies favouring anonymity) are particularly relevant for VASPs.

Your supervisor considers virtual assets to be a new or developing technology, that might favour anonymity. As such, all transactions involving virtual assets will require enhanced CDD in accordance with section 30 of the Act.

You must use your own risk assessment and AML/CFT programme to establish the level of ML/TF risk for each customer. This will help you to determine which kind of CDD to conduct before establishing the business relationship or conducting an occasional transaction or activity.

VASPs will almost always be dealing with a form of enhanced CDD, so should be aware of the different forms of enhanced CDD prescribed in sections 22-30 of the Act.

The Enhanced Customer Due Diligence Guideline is a key resource for VASPs wishing to understand their enhanced CDD obligations.

Other CDD requirements

Regardless of the level of CDD you are conducing on your customer, you must seek information about the nature and purpose of the proposed business relationship or occasional transaction or activity. This means you need to have a good understanding of your client's circumstances and intentions and who else has an interest in their activities. You need to understand who else benefits.

If you are conducting standard CDD you also must obtain sufficient information to allow you to determine whether you should conduct enhanced CDD. Enhanced CDD comes in several different types as described in sections 22-30 of the Act. Enhanced CDD often requires you to ascertain the sources of your customer's wealth and/or funds. With this information you can make an assessment about whether your client's requests are typical, legitimate, or suspicious.

Where to get further support

VASPs can access compliance support from a range of sources:

- Your AML/CFT programme and compliance officer
- The Department as the supervisor
- Independent professional advice
- Open source information from relevant international bodies concerned with AML/CFT

Your AML/CFT programme and compliance officer

Where employees in your business have compliance questions, their first port of call should be your AML/CFT programme. Your programme documentation should be able to provide answers to basic questions that are likely to arise in your specific business context. As questions arise, it is likely that the AML/ CFT programme will need to be updated to include provisions for resolving unanticipated issues and frequently asked questions.

Specific questions should be answered by your compliance officer. Where this approach does not resolve the question at hand, it is important to consider what would be the appropriate next step – seeking support from the relevant professional body, from your supervisor, or from an independent lawyer or other suitable professional.

Support from your supervisor

We aim to provide proactive support to reporting entities. In addition to the resources linked to in this document, the Department's website provides a wide range of information about how to comply with the Act for reporting entities. You can also directly contact the Department at Amlcft@dia.govt.nz.

When to seek independent advice

There will be occasions where VASPs need to seek independent advice to ensure they remain compliant with the Act. When you have specific compliance questions about unique circumstances you may need to seek independent legal advice or advice from an otherwise suitable professional. Supervisors are there to support you, but they cannot provide legal advice to reporting entities.

Open source information from relevant international bodies

There is a wide range of information available in open-source format from international bodies. VASPs may wish to consult the guidance issued by FATF, as well as other overseas supervisors such as AUSTRAC. VASPs should be aware that this information is prepared for other jurisdictions and may not be directly applicable to New Zealand.