Te Tari Taiwhenua
Internal Affairs

New Zealand Government

Guideline:

Accountants

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

March 2018

Contents

Executive summary

It is likely that money laundering is currently going on undetected in New Zealand. Money laundering is the method by which people disguise and conceal the proceeds of crime and protect and enjoy their assets. Some people in New Zealand may also be financing the activities of terrorists and known terrorist organisations. Financers of terrorism use similar techniques to money launderers 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 using gatekeepers, such as accountants, is a way for criminals to create a false perception of legitimately acquired wealth. The recent changes to the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act or the Act) included accountants in the AML/CFT system.[1]

The AML/CFT Act is activities-based. Professionals offering accounting services who undertake activities captured by the AML/CFT Act will need to undertake an assessment of their money laundering and terrorist financing (ML/TF) risk and develop a programme to ensure they comply with the requirements in the Act. This includes accountants, bookkeepers and tax agents – hereafter referred to collectively as "accountants". The flow chart in the "'At a glance'" section of this guideline can help you determine if you are captured by the AML/CFT Act.

This guideline helps you to determine whether your business must comply with the AML/CFT Act and, if so, what you must do to ensure you comply with the Act. You must comply with the AML/CFT 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.

You need to know your customers. Before conducting captured activities, you need to conduct customer due diligence (CDD) according to the level of risk posed by your customers. CDD is not optional. When you are not able to complete CDD, you must not undertake a captured activity or transaction for that customer. To do so would be a breach of the AML/CFT Act.

The Department of Internal Affairs (DIA) is the supervisor charged with monitoring your compliance with the AML/CFT Act. We recognise that adjusting to the new AML/CFT system will take time and effort. This guideline, and other existing guidelines, can help you develop awareness of the risks posed by ML/TF and provide prompts on what to think about when developing programmes to manage these risks. We are available to respond to queries, and we are working with accountants' professional bodies to ensure you are well supported to meet your obligations under the AML/CFT Act.

Disclaimer

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 and cannot be relied on as such. After reading this guideline, if you do not fully understand your obligations, you should seek legal advice or contact your AML/CFT supervisor. DIA can be contacted at amlphase2@dia.govt.nz.

Glossary

Accountants	The use of the term "accountants" in this guideline refers to Chartered Accountants, accountants, bookkeepers, tax agents and anyone else who is providing professional accounting services.
Accounting practice	Defined in section 5(1) of the AML/CFT Act as "an accountant in public practice on his or her own account in sole practice; or, in relation to two or more accountants in public practice, and practising in partnership, the partnership; or an incorporated accounting practice". This definition includes businesses referring to themselves as "bookkeepers" and "tax agents" if they are undertaking activities captured by the Act.
AML/CFT Act	Anti-Money Laundering and Countering Financing of Terrorism Act 2009
Captured activities	Activities that are specified under the definition of "designated non-financial business or profession" in the AML/CFT Act
CDD	Customer due diligence
Compliance officer	An individual (usually an employee) appointed to administer and maintain the AML/CFT compliance programme
Customers/Clients	While the term "clients" is more commonly used, the term "customers" is used throughout the AML/CFT Act. In this guideline the terms "customers" and "clients" are used interchangeably.
DBG	Designated business group
DIA	Department of Internal Affairs
DNFBP	Designated non-financial business or profession
FATF	Financial Action Task Force
FIU	New Zealand Police Financial Intelligence Unit
Financing terrorism offence	As defined in section 8(1) of the Terrorism Suppression Act 2002
goAML	FIU reporting portal
ML/TF	Money laundering or terrorist financing
Money laundering offence	As defined in section 243 of the Crimes Act 1961
PEP	Politically exposed person
PTR	Prescribed transaction report
Reporting entities	Casinos; designated non-financial businesses or professions; financial institutions; high-value dealers; and the New Zealand Racing Board
SAR	Suspicious activity report
SPR	Suspicious property report
STR	Suspicious transaction report
Supervisors	Supervisors have responsibility for monitoring compliance with the AML/CFT Act. DIA is the supervisor for reporting entities in the accounting profession among other sectors. The Reserve Bank of New Zealand and the Financial Markets Authority supervise other sectors.
TCSP	Trust and company service provider. A person (other than a law firm, a conveyancing practitioner, an incorporated conveyancing firm, an accounting practice, or a real estate agent) who carries out any of the activities described in the definition of DNFBP (see section 5(1) of the AML/CFT Act).

Introduction

This guideline is for accounting practices that have compliance obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act or the Act) from 1 October 2018.[2] Those that do are "reporting entities" for the purposes of the Act. The Department of Internal Affairs (DIA) is the supervisor for accounting practices.[3] This guideline uses the term "accountants" to refer to accounting practices – please see the Glossary for definitions.

The terms "accountant" or "accounting practice" are not protected in New Zealand. Nor is there a requirement for individuals or businesses providing accounting services to be members of a professional body. Tax agents and bookkeepers may be captured by the Act, even if they do not refer to themselves as accountants. The determining factor will be whether, in the ordinary course of business, one or more of a number of specific activities are conducted. These activities are described in Section 5(1) of the Act in the definition of "designated non-financial business or profession" (DNFBP) and are referred to in this guide as "captured activities".

If you do not consider your business to be an "accounting practice", but you are conducting activities captured by the definition of DNFBP, you will still be a reporting entity under the AML/CFT Act under the definition of trust and company service provider (TCSP). If you are a TCSP your business will need to comply with the Act from 1 July 2018 rather than 1 October 2018. In either case, this guideline provides you with the information you need to ensure you can comply in the required timeframe, and from this point in the document you should consider any reference to "accountant" to include TCSP also (please see the Glossary for the definition of this term).

Accountants will have obligations under the AML/CFT Act when they conduct certain activities (referred to throughout this guidance as "captured activities").

As your supervisor, DIA expects accountants to:

1. Know your ML/TF risks
2. Know your AML/CFT supervisor
3. Know how to apply the AML/CFT Act to your business
4. Know your compliance requirements
5. Know your customer
6. Know the red flags of ML/TF
7. Know where to get support.

This guideline will help reporting entities in the accounting profession to meet each of the expectations identified above and is structured in that order. The AML/CFT Act requires that reporting entities have regard to any guidance produced by the AML/CFT supervisor and the Commissioner of Police when developing their risk assessment and AML/CFT programme.[4]

This guideline does not provide a "how to" guide or additional prescription to complement the AML/CFT Act. A one-size-fits-all approach will not work well for most reporting entities. Instead, this guideline will help accountants increase their awareness of money laundering and terrorist financing (ML/TF) risks, and provide prompts for how to manage your compliance.

Where the terms "must" or "required" are used, this means that the information is referring directly to an obligation that is specified in legislation. Where we have used the term "should" we are making a recommendation which is your choice to accept or not. While the term "customers" is used throughout the AML/CFT Act, the term "clients" is more commonly used in the accounting profession. The terms "customers" and "clients" are used interchangeably in this guideline.

This guideline may be updated periodically to make minor changes as new information and feedback is assessed. As such, we recommend that instead of printing this guideline in hard copy, you should bookmark the webpage and refer to it online to ensure you have the most up-to-date information to hand.

Over time new case law may become available, new regulations may be made, or existing regulations may be amended and this guideline will be updated. The DIA website provides a reference page to find the relevant regulations.[5] DIA will inform reporting entities of any new regulations or updates to existing guidance. The AML/CFT supervisors have already produced a wide range of guidance, much of which accountants are likely to find useful. The guidelines are all available on the DIA website and are referred to throughout this guideline where relevant.[6] Other guidelines may be produced in the future as needed.

We can be contacted at amlphase2@dia.govt.nz if you have further questions.

At a glance

How to know if you are captured by the AML/CFT Act

The following flow chart provides a quick way to check if you are captured under the AML/CFT Act.

Am I captured by the AML/CFT Act as a DNFBP?

Are you a law firm, a conveyancing practitioner, an incorporated conveyancing firm, an accounting practice, a real estate agent, or a trust and company service provider?

YES

Do you do any of the following activities in the ordinary course of business?

Act as a formation agent of legal persons or legal arrangements

OR

Act as, or arrange for a person to act as, a nominee director, nominee shareholder or trustee in relation to legal persons or legal arrangements

OR

Manage client funds (other than sums paid for professional services), accounts, securities or other assets

OR

Provide real estate agent work to effect a transaction

OR

Provide a registered office or a business address, a correspondence address, or an administrative address for a company or partnership, or for any legal person or legal arrangement (unless that service is provided solely as an ancillary service to the provision of other services that are not captured by the definition of a DNFBP)

OR

Engage in or give instructions on behalf of a customer to another person for:

- Any conveyancing to effect a transaction (see section 5(1) for more detail)
- A transaction within the meaning of section 4(1) of the Real Estate Agents Act 2008
- A transfer of beneficial interest in land or other real property
- A transaction on behalf of any person for buying or selling or transferring of a business or legal person and any other legal arrangement; or
- A transaction on behalf of a customer in relation to creating, operating, and managing a legal person, and any other legal arrangement

NO

You are not captured

NB: If in the future you are asked to conduct any activity described above, you will need to determine if you are captured by the Act

YES

You are captured and must comply with the AML/CFT Act

NO

There is an exemption which excludes your business from compliance requirements

What you need to do to comply

Step 1: Establish a compliance programme

Appoint a compliance officer – Section 56
Reporting entities must appoint a compliance officer who will have responsibility for administering and maintaining the AML/CFT programme. An employee should be appointed to this role who reports to a senior manager. In the case of a sole practitioner, we would expect the sole practitioner to be the compliance officer. If that is not possible, an external person must be appointed as a compliance officer.

Conduct a risk assessment – Section 58
Reporting entities are required to undertake an assessment of the risks posed to their business by money laundering and financing of terrorism crimes. The risk assessment should be in writing and have regard to the applicable guidance material, which is available on the DIA website.

Develop an AML/CFT programme – Section 57
The AML/CFT programme must be based on the risk assessment described above and be in writing. It should include procedures, policies and controls for ensuring all compliance obligations are adequately and effectively met and must have regard to the applicable guidance material.

Step 2: Maintain your compliance programme

Conduct customer due diligence (CDD) – Part 2, Subpart 1
Reporting entities must conduct CDD when conducting an occasional transaction or activity or when establishing a business relationship with a client who is requesting assistance with a captured activity, or when an existing client makes this kind of request (if the reporting entity doesn't hold all the information required already). There are three levels of CDD depending on the circumstances.

Keep records – Sections 49–55
Reporting entities must keep records of transactions, suspicious activities, the documents verifying the identities of customers and other parties or beneficiaries, and any other related records that may be of interest to the supervisor. Records must be kept at least five years.

Ongoing customer due diligence and ongoing account monitoring – Section 31
Reporting entities are required to undertake ongoing CDD and ongoing account monitoring. This is to ensure that you have ongoing confidence that the business relationship and the transactions within the relationship are consistent with the customer's business and risk profile, and you can spot any suspicious activity early.

Review your compliance programme – Section 59
The supervisor expects reporting entities to conduct a regular review of their compliance programme. This is to ensure that any business changes or new risks in the operating environment are referenced in the programme and it remains fit-for-purpose.

Step 3: Report and audit

Submit an annual report – Section 60
Reporting entities must submit an annual report. This report must be in the prescribed form and be submitted to the supervisor at the time set by the supervisor. The report must take into account the results and implications of the audit and any information prescribed in the regulations.

Audit your risk assessment and compliance programme every two years – Section 59(2)
At least every two years a reporting entity must review its risk assessment and compliance programme and have it audited by an independent person who is suitably qualified to conduct the audit. Supervisors may also require an audit to be undertaken on request at shorter notice.

Report to the FIU

Report to the Financial Intelligence Unit – Part 2 subparts 2 and 2A
When reporting entities identify suspicious activity, they must report it to the FIU. They should also submit prescribed transaction reports to the FIU as necessary. No one will be required to submit any privileged communication (as defined in the Act) in either report category.

1. Do you know your ML TF risks?

Undetected financial crime reduces the integrity of national and international financial systems, distorts the economy and diminishes opportunities for legitimate economic activities. The Government loses tax revenue, while people are rewarded for criminal behaviour. New Zealand is at risk of being targeted by international criminal networks to inject the proceeds of crime into the international financial system. Money laundering and financing of terrorism are not solely international crimes. Domestic criminals use a variety of methods to conceal the proceeds of their criminal activities from authorities in New Zealand.

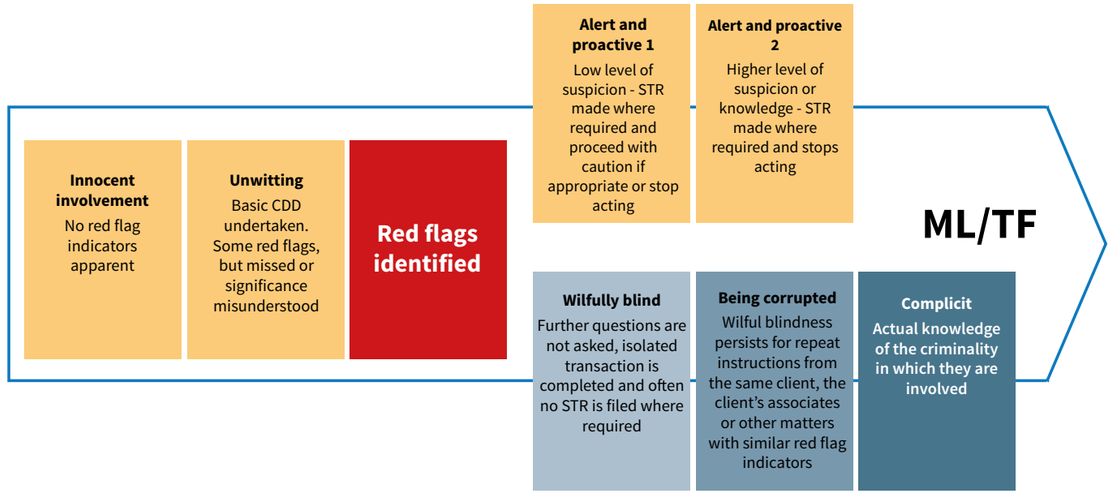
The Financial Action Task Force (FATF) is an inter-governmental body that sets standards for combating ML/TF and other related threats to the integrity of the international financial system. New Zealand has included accountants in the AML/CFT system in response to recommendations made by the FATF in its country review of New Zealand in 2009.[7]

Using accounting professionals is attractive to some criminals because these professionals are required for the completion of certain kinds of transactions and because their specialist skills can be misused to assist the laundering of criminal proceeds or funding terrorism. Accountants can add respectability and a veneer of legitimacy to transactions.

When gatekeeper professionals, such as accountants and trust and company service providers, lack ML/TF awareness, they are more at risk of inadvertently helping criminals. For example, it is important to understand that even small transactions can be indicative of ML/TF. Offenders have been known to conduct a series of continuous, seemingly immaterial, transactions which, when added up, can conceal and disguise a significant amount of criminal proceeds. It is not enough to simply understand the ML/TF risks inherent in accounting practices.

We encourage accountants and other professionals to develop an understanding of the ML/TF risks in the wider sectors and industries that they have business dealings with as well. Given these risks, and the FATF recommendations, the Government has chosen to engage gatekeeper professions in the collective efforts to deter and detect these crimes. The more eyes and ears attuned to the indicators (or red flags) of these crime types, the more likely people will struggle to benefit financially from criminal activities. By expanding the AML/CFT system to include the gatekeeper professions, the Government intends that gatekeepers will be better able to protect themselves from customers who launder money and finance terrorism. FATF has provided the following diagram to describe the two potential trajectories of legal professionals' involvement in ML/TF.[8] These two trajectories can be applied to any of the gatekeeper professions.

The AML/CFT system has been designed to help businesses achieve the level of compliance required to assist authorities to deter and detect criminal customers. Compliance also has a value for business risk management. Professionals closely guard their reputations. It is in their interest to avoid relationships with customers who will cause them disrepute in the community or censure by their professional bodies or government authorities. Businesses that fail to comply and are misused by criminals risk negative media coverage both in New Zealand and internationally. This also diminishes New Zealand's international reputation as a safe place to do business.



2. Do you know what to expect from your AML/CFT supervisor?

This section explains the regulatory approach you can expect from DIA.

The role of supervisors

DIA is the supervisor for accountants, the other DNFBPs, and a range of financial institutions, such as money remitters, that are reporting entities under the AML/CFT Act. The Reserve Bank of New Zealand and the Financial Markets Authority both act as supervisors for other reporting entities. 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 that the AML/CFT system operates in a robust manner and that criminals seeking to launder money and finance terrorism are detected and deterred.

Our regulatory approach

We outline our regulatory approach for the AML/CFT system in two publications: the *AML/CFT Supervisory Framework*[9] and *Minimising Harm – Maximising Benefit*.[10] 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

We focus our efforts carefully and deliberately. We use our insight, knowledge and understanding to identify risks and determine interventions to most effectively ensure compliance. While we are fully prepared to escalate our response with enforcement action, we are equally prepared to work with reporting entities in a responsive and educative manner. We are a member of the National Co-ordination Committee, and we work with the other supervisors and the FIU, as well as with other government agencies, industry bodies and reporting entities to apply a consistent approach to the AML/CFT system.

Monitoring and enforcement

We use 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 compliance programmes; analysis of annual reports; and independent audits.

When we identify reporting entities that are not meeting their obligations under the AML/CFT Act we consider a number of 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 AML/CFT 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, we may decide to issue a formal warning or to accept an enforceable undertaking. Alternatively, we may decide to seek an interim, performance or restraining injunction, or a pecuniary penalty, from the High Court.

In the most serious of cases, civil liability acts that are engaged in knowingly or recklessly are criminal offences. There are a number of 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, DIA 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[11] or the financing of terrorism[12]. The 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.

Territorial scope of the AML/CFT Act

The supervisors have issued guidance outlining their interpretation of the territorial scope of the AML/CFT Act.[13] Even though the AML/CFT Act only has jurisdiction in New Zealand, we strongly encourage reporting entities to report on suspicious activities and transactions that they are party to that occur offshore. For more information about reporting suspicious activity, please see "Suspicious activity reports" in section 4.

3. Do you know how to apply the AML/CFT Act to your business?

The AML/CFT Act is activities-based. This section provides more detail about captured activities and why they are included in the Act. In addition, accountants need to develop a thorough understanding of:

- Exclusions to and exemptions from the AML/CFT Act
- What conducting captured activities "in the ordinary course of business" means
- What obligations are related to the captured activities
- How to determine whether advice to a customer is captured in an activity
- The nature of each of the activities that are captured by the AML/CFT Act

This section elaborates on the captured activities that accountants may perform. The AML/CFT Act imposes obligations only for these captured activities.[14] The obligations of the AML/CFT Act do not apply to any other activities that an accountant carries out in the ordinary course of business.

Exclusions to and exemptions from the AML/CFT Act

There are a number of ways in which entities, transactions or activities can be exempt from the Act's requirements. For instance, the AML/CFT (Definitions) Regulations 2011[15] provide a number of specific exclusions to the definition of "reporting entity", and the AML/CFT (Exemptions) Regulations 2011[16] provide a range of exemptions for specific classes of transactions and services. There are also Ministerial exemptions, which can exempt (from any or all of the provisions of the Act) either specific reporting entities, or classes of reporting entities, as well as transactions or classes of transactions.[17] The AML/CFT (Class Exemptions) Notice 2014[18] provides further detail about class exemptions.

The Ministry of Justice handles Ministerial exemption applications and provides advice to the appropriate Minister who makes the final decisions. Exemptions may be granted by the Minister subject to sections 157 to 159 of the AML/CFT Act.[19] Please review these sections if you are considering making an application.

Interpreting "ordinary course of business"

Activities must be done in the ordinary course of business to be captured by the Act. The AML/CFT supervisors have issued guidance on how to interpret "ordinary course of business".[20] Whether an activity is in your "ordinary course of business" will always be a matter of judgement depending on the nature of your 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

It is likely that the activity is in the ordinary course of your business if one or more of these factors apply.

If you are conducting a captured activity in your personal capacity (as opposed to in your professional capacity) you are not captured by the AML/CFT Act. An example of this would be if you are a trustee for a registered charitable trust in your local community in your personal capacity.

If, after considering the AML/CFT Act and this guideline, you are still unsure as to whether you are a reporting entity, you should seek independent professional advice or contact us at amlphase2@dia.govt.nz.

What obligations are related to the captured activities?

The AML/CFT Act requires you to know who your customers are (as well as who any beneficial owners of your customer are, and any person acting on behalf of your customer) by conducting customer due diligence (CDD) to the level required before you conduct a captured activity or establish a business relationship.

How to determine whether advice provided to your customer is captured

There will be circumstances where you give advice in relation to a captured activity (without necessarily then carrying out the activity). Generally, advice alone, in the absence of any actual captured activity on the accountant's part, will not be captured by the definition of "designated non-financial business or profession".

It may be that in practice you expect to provide a mixture of advice and captured activities for a client over a period of time. In those circumstances, you would need to conduct CDD to the required level *prior* to establishing a business relationship with the client (and prior to providing any advice).

If you regularly provide advice to a client about captured activities, such as providing advice about payments they should make (eg, for tax or payroll), but you never directly control the flow of their funds yourself, you should consider whether there is an apparent ML/TF risk. If you think there is a risk you need to mitigate you should do so in line with your professional obligations.

You also need to be aware of your obligations to report suspicious activities, which can include requests or enquiries about particular services you offer from potential or current clients (regardless of whether you ultimately provide those services).

Activities captured by the AML/CFT Act

This section outlines the activities which are captured by the AML/CFT Act and provides some examples of what these activities may look like for accountants. The examples are illustrative and not exhaustive. As we learn from our experiences regulating the accounting profession we will be able to provide more information about supervisor expectations in certain scenarios.

When in doubt about whether you undertake any of the activities described below, please look to the explanations. If you are still unclear, contact DIA at amlphase2@dia.govt.nz or seek advice.

Activity: Acting as a formation agent for legal persons or legal arrangements

In the definition of "designated non-financial business or profession" an accounting practice which, in the ordinary course of business, acts as a formation agent of legal persons or legal arrangements, is captured by the AML/CFT Act as a reporting entity.

The term "legal arrangement" is defined in the AML/CFT Act as meaning a trust, a partnership, a charitable entity (within the meaning of section 4(1) of the Charities Act 2005), and any other prescribed arrangements that involves a risk of ML/TF.[21]

This activity refers to forming a legal person (such as a company) or legal arrangement on behalf of a client; for example, registering a company on the Companies Office website. The activity does not include instances where you simply provide advice about formation of a legal person that is acted on by either your client themselves or a third party. In the case of forming a trust, if your client asks a lawyer to do that for them the captured activity would be undertaken by the lawyer and they would have to apply their AML/CFT compliance programme to that activity.

If you were to engage a lawyer to form a trust on behalf of your client, then both you and the lawyer would be conducting a captured activity (ie, the activity of forming a company) and would both need to apply your AML/CFT compliance programmes' policies, procedures and controls, including the appropriate level of CDD. Please see further on in this section for discussion about captured activities that involve engaging in, or giving instructions on behalf of a client to another person.

Examples of this kind of activity in practice

- You register a company with the Companies Office on behalf of a client.
- You form an incorporated society on behalf of a client.

ML/TF risks associated with this activity

When an accountant is engaged to register a company or partnership, the actual ownership of the company or partnership being formed may be concealed or obscured; for example, where shell companies, multiple layers of ownership, or other complex legal structures are used. Setting up a trust can also be a way to create a perception of distance between assets and their beneficial owners. International evidence shows that criminals use charitable organisations (such as incorporated societies and charitable trusts) to launder their money or to finance terrorism.

Activity: Acting as, or arranging someone to act as a nominee director, nominee shareholder or trustee

In the definition of "designated non-financial business or profession" an accounting practice which, in the ordinary course of business, acts as, or arranges for a person to act as, a nominee director or nominee shareholder or trustee in relation to legal persons or legal arrangements, is captured by the AML/CFT Act as a reporting entity.

If you are acting as a nominee director, nominee shareholder or a trustee in your personal capacity (as opposed to in your professional capacity) the AML/CFT Act does not apply. An example would be if you were volunteering your time to act as a trustee on a community trust board that funds sports events in your local area.

Examples of this kind of activity in practice

- You act as a nominee director of a company.
- You act as a trustee for a trust.
- You arrange for a person to act as a nominee shareholder for a company.

ML/TF risks associated with this activity

If an accountant is acting as a nominee director, nominee shareholder or a trustee for a company or other legal arrangement (such as a trust or charity), this may provide a false impression of legitimacy for the activities undertaken by the company or legal arrangement. This facade provides criminals with the opportunity to use their companies or other legal arrangements for laundering money or other crime without being detected. The possibility of detection is made less likely because they can do this while maintaining the impression of oversight by reputable New Zealand-based directors.

Accountants who act or arrange for someone to act as a nominee director, nominee shareholder, or trustee need to establish the reason why this arrangement is required. We expect that accountants establish that there is a legitimate economic purpose of the company or other legal arrangement and to know who its beneficial owners are.

Activity: Providing an office or address for a company or legal arrangement

In the definition of "designated non-financial business or profession" an accounting practice which, in the ordinary course of business, provides a registered office or a business address, a correspondence address, or an administrative address for a company, or a partnership, or for any other legal persons or arrangement, is captured by the AML/CFT Act as a reporting entity. The only exception to this is where the office or address is provided solely as an ancillary service to the provision of other services that are not otherwise captured by the definition of "designated non-financial business or profession" in the AML/CFT Act.

Example of this kind of activity in practice

- You allow a sole trader to use your business address as its registered office address but you do not provide them with any other services.

ML/TF risks associated with this activity

For a person who is intent on laundering money or committing other crime, the use of an address that is not their physical location is attractive. It allows them to keep anonymity and distance from the transactions and activities they are undertaking, and if it is the address of an accountant, it adds a perception of legitimacy to their activities. It also makes it more difficult for law enforcement to track them down in person.

Activity: Managing client funds, accounts, securities, or other assets

In the definition of "designated non-financial business or profession" an accounting practice which, in the ordinary course of business, manages client funds (other than sums paid as fees for professional services), accounts, securities, or other assets, is captured by the AML/CFT Act as a reporting entity.

Managing payments to or from your clients' accounts is captured; and, with the exception of payments for professional fees, any instance where you receive or hold client funds and control the payment of those funds will also be captured. The key determining factor is whether you have control over the flow of funds – if you do have control, your activity is captured. Taking a payroll situation, for example, if you are loading payments that are then actioned by your client, you are not controlling the funds, your client is. However, if you are authorising wage and salary payments from your client's account directly into their staff's personal accounts, then this is a captured activity.

Examples of this kind of activity in practice

- You have the authority to make payments on behalf of your client's business directly from their bank accounts.
- You make investments on behalf of a client in securities and/or other assets using funds from their bank accounts which you have the authority to transfer.
- You manage the sale and/or purchase of trust assets for your customer using funds from their bank accounts which you have the authority to transfer.
- You disburse the funds generated from a company's insolvency liquidation to a creditor in line with the relevant administration requirements.
- You exercise the enduring power of attorney which you hold for a client who has lost mental capacity by making payments from their personal account to meet their financial obligations, such as medical bills.
- You operate a trust account to receive tax refunds from Inland Revenue on behalf of your clients and you repay those funds to your clients.

ML/TF risks associated with this activity

Some people will try to avoid accessing banking services typically used in transactions to obscure the trail of funds changing hands as a means to hide their criminal activities. One way to obscure this trail or to add an appearance of legitimacy is to use the trust accounts or other professional services of accountants.

Activity: Engaging in, or giving instructions on behalf of a customer to another person, for a range of specified services (as below)

In the definition of "designated non-financial business or profession" an accounting practice which, in the ordinary course of business, does any of the activities listed in the box below (in italics) is captured by the AML/CFT Act as a reporting entity.

The activities specified in the following box apply to situations where accountants either engage in the activities themselves, or give instructions on behalf of a client to another person for those activities. This means that if you are instructing a third party to undertake activities on behalf of your client, you are captured by the AML/CFT Act – as is the third party you instruct if they fall within the definition of either "designated non-financial business or profession" or "financial institution".[22]

Engaging in or giving instructions on behalf of a customer to another person for—

a. *any conveyancing (within the meaning of section 6 of the Lawyers and Conveyancers Act 2006[23]) to effect a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008[24]), namely,—*
   - *the sale, the purchase, or any other disposal or acquisition of a freehold estate or interest in land:*
   - *the grant, sale, or purchase or any other disposal or acquisition of a leasehold estate or interest in land (other than a tenancy to which the Residential Tenancies Act 1986 applies[25]):*
   - *the grant, sale, or purchase or any other disposal or acquisition of a licence that is registrable under the Land Transfer Act 1952:*[26]
   - *the grant, sale, or purchase or any other disposal or acquisition of an occupation right agreement within the meaning of section 5 of the Retirement Villages Act 2003:*[27]

Note: Only lawyers and conveyancers are able to engage in conveyancing work but an accountant might give conveyancing instructions to a lawyer or conve*yancer.*

b. *a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008); or*
c. *the transfer of a beneficial interest in land or other real property; or*
d. *a transaction on behalf of any person in relation to the buying, transferring, or selling of a business or legal person (for example, a company) and any other legal arrangement; or*
e. *a transaction on behalf of a customer in relation to creating, operating, and managing a legal person (for example, a company) and any other legal arrangement"*

You should read both (D) and (E) to mean undertaking any one of the activities mentioned, not a combination of all activities at once. "Transaction" is defined in section 6 of the AML/CFT Act and means any deposit, withdrawal, exchange or transfer of funds whether (i) in cash; (ii) by cheque, payment order or other instrument; or (iii) by electronic or other non-physical means. There are some inclusions and exclusions specified in the definition.

Examples of these kinds of activities in practice

- You instruct a conveyancer to effect the sale of a house owned by your client.
- You purchase farm land as a trustee (together with the other trustees) for your client's family trust.
- You give instructions to a nominee overseas to purchase a company for your client in that country with funds provided by the client.
- You instruct a trust and company service provider to transfer funds provided by your client to the bank accounts of a newly formed company of which your client is the sole shareholder.

ML/TF risks associated with this activity

The key risk with all the activities described in the previous box is the anonymity and appearance of legitimacy that may be gained by the customer through the accountant engaging in the activities, or giving instructions to another person on their behalf for those activities. The person being instructed by the accountant may be unlikely to have any face-to-face contact with the actual client. If the client has criminal intentions, there would be a protective layer of other people between the client and the transaction they are instructing.

Auditing, and other assurance activities, are not captured by the AML/CFT Act

In general, financial auditing and other assurance services are not captured by the AML/CFT Act, so you will not be required to apply your compliance programme to clients who are only requesting these kinds of services. You may be requested to provide AML/CFT auditing services to businesses which, by virtue of their being either a financial institution or a DNFBP, are required to comply with the AML/CFT Act. Similarly, this activity is not captured by the AML/CFT Act and you will not have to apply your compliance programme to it.

If, however, in the course of your (financial or AML/CFT) auditing or other assurance procedures you have reasonable grounds to suspect that an activity is relevant to the potential investigation or prosecution of any person for a money laundering or other offence, you should consider your obligations to report that activity to the FIU.[28]

4. Do you know your compliance obligations?

Any accounting practice, either existing or established after the introduction of the AML/CFT Act, that conducts captured activities, will be a reporting entity and will have to comply with the Act. You will not be excused from compliance on the basis that to comply would breach any contract or agreement.[29]

Compliance requirements

This section provides guidance on:

- The risk-based approach that reporting entities need to take when developing their AML/CFT programme
- The range of policies, procedures and controls reporting entities must include in their AML/CFT programme to comply with the AML/CFT Act
- Things to consider if you wish to establish a designated business group to share some aspects of your AML/CFT programme and its implementation

Section 5 provides more detail about compliance requirements for CDD. Information on where to access other support to comply is noted in section 7.

Risk-based compliance

The AML/CFT regulatory system in New Zealand is "risk-based". This means your business must assess the risk it is exposed to from money launderers and terrorist financers. You must then apply suitable policies, procedures and controls to effectively manage the risks you have identified for your business. Compliance resources can then be targeted primarily at high-risk areas, which should reduce the overall compliance cost for your business.

You are the best judge of the risks your business is exposed to and how you can most effectively mitigate those risks in line with the requirements of the AML/CFT Act. As your supervisor, DIA expects you to genuinely and accurately assess the ML/TF risks to your business and then apply a suitable and proportionate AML/CFT programme.

AML/CFT programme – policies, procedures and controls

AML/CFT compliance cannot be achieved with a "set and forget" approach. The AML/CFT programme needs to be fully implemented within the business. It should be a living and adaptable programme. Your specific compliance obligations under the AML/CFT Act are summarised below.

Appoint a compliance officer

You must appoint an AML/CFT compliance officer to administer and maintain your compliance programme.[30] The compliance officer should be an employee of the business who reports to a senior manager or partner of the business. If practising on their own account, an accounting professional would be expected to act as the compliance officer themselves and take full responsibility for all compliance requirements unless there is a reason why they cannot. In that case they should appoint a third party to take on this duty.[31]

When you have appointed your compliance officer, or if your compliance officer or other contact information changes, it is important that you advise us at amlphase2@dia.govt.nz. This enables us to communicate effectively with you and provide you with important information and updates.

Conduct a risk assessment

All reporting entities must undertake a risk assessment, and it must be in writing. The specific requirements for a risk assessment are set out in section 58 of the AML/CFT Act.[32] The supervisors have provided guidance on how to conduct a risk assessment.[33] The AML/CFT Act requires that you have regard to guidance produced by the AML/CFT supervisors when developing your risk assessment.[34]

DIA has published its own assessment of the ML/TF risks in the sectors it is responsible for supervising, including in the accounting, bookkeeping and tax agency professions.[35] DIA has also developed a "Prompts and Notes" guideline (*AML/CFT Risk Assessment and Programme: Prompts and Notes for DIA Reporting Entities*), which outlines the factors to be considered in a risk assessment along with some prompts for things to think about when completing a risk assessment and developing your AML/CFT programme.[36] It provides prompts to help businesses undertake their risk assessment in a way that reflects both the size of their business and their level of risk.

In addition, the Financial Markets Authority has published a step-by-step guide for drafting a risk assessment.[37] Together, these resources will help businesses to conduct a realistic assessment of their ML/TF risks, so that their AML/CFT programme is proportionate to the risks assessed.

Risk assessments are required to be regularly reviewed and updated where 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. It is important for accountants, particularly compliance officers in accounting practices, to keep up-to-date with relevant changes in typologies. The Quarterly Typology Reports published by the FIU are an excellent source of typology information.[38]

Good times to think about updating your business's risk assessment are when:

- The FIU publish a National Risk Assessment for ML/TF or a Quarterly Typology Report about ML/TF issues that highlights the potential for vulnerabilities in your business activities
- DIA updates its Sector Risk Assessment
- You have become aware of an increased ML/TF risk to your business due to a change in the nature of or demand in your services
- International ML or TF-related events trigger you to reconsider your risk assessment

Set up an AML/CFT programme

Once a risk assessment has been conducted, all reporting entities must develop an AML/CFT programme that includes internal procedures, policies and controls to detect and manage the risk of ML/TF.[39] The AML/CFT Act requires that you have regard to guidance produced by the supervisor when developing your AML/CFT programme.[40] The supervisors' guidance on developing an AML/CFT programme is available on the DIA website.[41]

The supervisors' guidance is generic in nature. It does not provide prescriptive instructions on how businesses can ensure they are compliant with the AML/CFT 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 supervisor for general information, or seek independent advice.

Customer due diligence (CDD)

Section 5 in this guideline is dedicated to explaining your CDD obligations.[42]

Record keeping

You must keep adequate records as outlined in sections 49 to 55 of the AML/CFT Act. This will enable you to operate your AML/CFT programme effectively and enable it to be audited by an independent auditor and reviewed by the supervisor on request. Records must either be kept in written form in English or be readily accessible and readily convertible into written form in English.

You must keep your records for at least five years. The supervisor or the FIU may ask you to keep records for longer in some circumstances. After five years, the records must be destroyed unless there is a lawful reason why they should be retained, such as the need to comply with another enactment or to enable you to carry on your business.

You must keep the following records.

Record Type	Retention period
Transaction records sufficient to enable the transactions to be fully reconstructed at any time[43]	5 years from the completion of the transaction
Any reports of suspicious activities[44]	5 years after the report is made
Identity and verification evidence (as reasonably necessary to enable the nature of the evidence to be readily identified at any time)[45]	5 years from the end of the business relationship or the completion of the occasional transaction or activity
Risk assessments, AML/CFT programmes and audits	5 years after the date on which they cease to be used on a regular basis
Information relevant to the establishment of a business relationship and any other records that explain the nature and purpose of a business relationship and the activities relating to that business relationship[46]	5 years from the end of the business relationship

You are also strongly advised to keep any detailed records of your assessment of whether a suspicious activity report (SAR) is required, including any determinations of whether information you hold is legally privileged.

Ongoing customer due diligence and account monitoring

When you have established a business relationship, you must conduct ongoing CDD and undertake account monitoring.[47] For more information about what this means in practice, please see "Ongoing CDD and account monitoring" in section 5.

Review your AML/CFT programme

You must regularly review your risk assessment and AML/CFT programme to ensure it remains up-to-date and to identify and remedy any deficiencies.[48] Your records should show evidence of updates that address any identified deficiencies in its effectiveness. Ways to do this would be to keep a record of version history or retain evidence demonstrating reviews and updates.

Annual reporting to your supervisor

Like all reporting entities, you are required to submit an annual report each year covering the period July to June.[49] The date for submission is advised by the supervisor each year, and you will usually have two months to submit. This means the first annual report will likely be due at the end of August 2019. Given the Act applies to accounting practices from 1 October 2018, your first annual report will be for the nine month period 1 October 2018 to 30 June 2019. A new set of annual report questions has been designed for lawyers, conveyancers, accountants and real estate agents and is provided for by Regulations, and a user guide for the new annual report for DNFPBs has been published by DIA.[50] All reporting entities are also expected to respond to any requests for subsequent information from the supervisor in a timely manner.

Independent audits of your risk assessment and AML/CFT programme

Every two years, you are required to have an independent audit of your risk assessment and AML/CFT programme.[51] An independent audit aims to ensure that documents remain up-to-date, that any deficiencies in programme effectiveness are identified, and that any necessary changes are made. For guidance, please see the *Guideline for Audits of Risk Assessments and AML/CFT Programmes*, which is available on the DIA website.[52]

The AML/CFT Act requires you to appoint someone who is independent and suitably qualified to conduct the audit.[53] The audit cannot be undertaken by someone from within the business unless a sufficient degree of independence can be demonstrated. For instance, a very large firm with a dedicated audit function would likely be able to show a sufficient degree of independence. Someone who has been involved in the establishment of the compliance programme (such as completing the risk assessment and/or writing the AML/CFT programme) cannot conduct the audit. The auditor does not need to be a chartered accountant or qualified to undertake financial audits.[54] To be suitably qualified we expect that your auditor would have a working knowledge of the AML/CFT Act and its complexities.

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.

You may be asked to conduct an independent audit as a professional service to a client who is a financial institution or a DNFBP. Auditing and assurance services are not captured under the AML/CFT Act, so you do not have to apply your compliance programme to independent audits that assist a client to meet their own AML/CFT compliance requirements.

Reporting to the FIU

As a key part of your AML/CFT obligations, in specific circumstances you need to report certain information to the FIU. Each reporting entity will have visibility over different parts of any one chain of events leading to an activity or transaction or following on from an activity or transaction. Each report will provide the FIU with information, complementing other types of reports providing further information. It may be that the report you provide will be the one crucial piece that brings enough of the puzzle together to lead the FIU to take appropriate action against a criminal.

When you need to report

From 1 October 2018, you will be required to submit suspicious activity reports (SARs; previously known as "suspicious transaction reports"[55]) and prescribed transaction reports. From that date you will no longer be required to submit suspicious transaction reports under the Financial Transactions Reporting Act 1996.

Suspicious activity reports (SARs)

Section 39A of the AML/CFT Act defines a "suspicious activity" and section 40 of the Act requires you to report suspicious activity to the FIU as soon as practicable, but no later than three working days after forming its suspicion. This has been held to mean that a reporting entity must report a suspicious activity within three days of the point at which the reporting entity becomes aware of facts that would objectively justify a suspicion (or by reasonable diligence would have become aware of them).[56] It is not a defence that a reporting entity did not actually consider an activity to be suspicious, in circumstances where it objectively should have.

Prescribed transaction reports (PTRs)

A prescribed transaction is an international wire 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.[57] The requirement to submit PTRs came into force on 1 November 2017. Please refer to "Wire transfers" in section 5 for more detail on wire transfers (including international wire transfers).

Only an ordering institution and a beneficiary institution are required to file a PTR in respect of an international wire transfer.

An "ordering institution" is defined as "any person who has been instructed by a payer to electronically transfer funds controlled by the payer to a payee via a "beneficiary institution". The ordering institution will be the first reporting entity to transfer the funds that are the subject of the international wire transfer to another jurisdiction – for instance, an accountant that holds client funds in a trust account or has authority to move funds from a client's own bank account, and transfers those funds (including via the formal banking system) to an overseas beneficiary bank.

A reporting entity that simply passes on an instruction to transfer funds, without actually transacting, will not be required to file a PTR. A "beneficiary institution" (in relation to a wire transfer from an ordering institution) is defined as "any person who receives those funds and then makes those funds available to a person (the payee) by crediting it to an account held by the payee or paying it to the payee". The beneficiary institution will be the last reporting entity in the chain that receives the funds before making them available to its customer (the beneficiary of the transaction).

Usually a bank will be a beneficiary institution; however, in some cases the beneficiary institution may be a different reporting entity, such as an accounting practice, depending on where the funds (intended for the customer) end up.

PTRs are intended to add further transparency to the financial system by making the range of methods of ML/TF even more difficult to hide. PTRs will also improve the detection and disruption of organised crime.

Suspicious property reports

You also need to be aware of your obligations to submit "suspicious property reports" (SPRs) under the Terrorism Suppression Act 2002. If you are in control of property that you suspect (on reasonable grounds) is property that is owned or controlled, directly or indirectly by a "designated terrorist entity" (or property derived or generated from that type of property), you must report that suspicion in accordance with sections 43 and 44 of the Terrorism Suppression Act. You must submit the SPR as soon as practicable after forming your suspicion. Designated terrorist entities are identified on a publicly available list that is updated by the New Zealand Police.[58] If you find a match on a list other than New Zealand's terrorist designation list, you must submit an SAR (as opposed to an SPR) to the FIU.

How to report

The FIU has issued guidance on how to submit reports using their goAML web-based reporting tool.[59] You must use the specific reporting format provided by the FIU. If you have reported on your customer, you must not disclose this information to your customer or to any person that is not entitled to receive this information.[60] If, after making a report, you are unsure if you need to end your existing relationship with your customer, you may wish to consider your professional obligations and any code of ethics that you have signed up to, consult your professional body, or seek independent advice. For further discussion on ending or declining business relationships, please see "What to do if you cannot complete CDD" in section 5.

What to do if you hold legally professionally privileged information

There may be occasions where you hold customer information that is protected by legal professional privilege (which the AML/CFT Act refers to as a "privileged communication"). For example, while acting as a tax agent for your customer you may receive tax-related legal advice as an agent for your customer.

The Act does not require any person (lawyer or otherwise) to disclose any information that the person believes, on reasonable grounds, is a privileged communication.[61]

A "privileged communication" is defined in section 42 of the AML/CFT Act as:[62]

- A confidential communication between a lawyer and another lawyer or a lawyer and his or her client made for the purpose of obtaining or giving legal advice or assistance; or
- A communication that is subject to the general law governing legal professional privilege or is specified in sections 53–57 of the Evidence Act 2006[63]

The AML/CFT Act requires all reporting entities to report suspicious activities by filing SARs with the FIU. If it is possible for you to file an SAR without disclosing a privileged communication, you must do so. It is accepted that in some cases this will not be possible. A privileged communication may lose the protection of privilege if prepared for a dishonest purpose or to enable or aid the commission of an offence – in which case, it can be included in an SAR.

Establishing a Designated Business Group

In certain circumstances, accountants may be able to form a designated business group (DBG) with other entities (whether or not those entities are other law firms or accountants or even reporting entities). The term "designated business group" is defined in full in the AML/CFT Act and regulations.[64] In summary, it means a group of two or more persons who have elected (in writing) to form a group to enable some obligations under the AML/CFT Act to be met on a shared basis while the election is in force.

A member of a DBG can rely on another member to carry out certain obligations on their behalf, including CDD (in certain situations[65]). Members can also rely on specified parts of another member's AML/CFT programme, and another member's risk assessment (if relevant), as well as reporting to the FIU. Members may share information and rely on each other but they still retain responsibility for their own compliance. Any decision to apply to become a DBG should include a thorough consideration of the risks and implications for all members.

The supervisor will consider all applications for DBGs. If you are not sure whether or not your proposed DBG meets the criteria in the definition in section 5(1) of the Act, you are welcome to contact DIA to discuss. We would prefer if reporting entities test their proposals with us rather than assume they could not apply. If you are interested in applying to form a DBG, we recommend you familiarise yourself with the two available guidelines to assist reporting entities to create DBGs, one on Scope and one on Formation, before you submit an application.[66] The application form is included in the Formation guideline.

5. Do you know your customer?

This section provides information about:

- What a business relationship means and when it starts
- Who to conduct CDD on
- What the different levels of CDD are, and scenario-based examples of each level
- How to use the Identity Verification Code of Practice
- When you can rely on others for CDD
- When to conduct CDD
- What to think about when participating in international transactions
- What to do if you cannot complete CDD

The requirements described in this section are contained in Part 2, subpart 1 of the AML/CFT Act.[67] The supervisors have prepared a range of fact sheets that are likely to assist accountants with undertaking CDD. The fact sheets are available on the DIA website.[68]

When a business relationship 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 or the carrying out of multiple transactions.[69]

You will need to use your judgement to determine when a business relationship with a customer starts. This is likely to be after initial inquiries have been made, but before any work has commenced.

Who to conduct CDD on

You must conduct CDD on:

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

New customers

You may not have to conduct CDD on every new customer. You need to establish at the outset whether they are going to require you to conduct any activity captured by the AML/CFT Act. If they are, you will need to conduct CDD in line with the level of risk you anticipate and in accordance with the requirements in the Act. See below for the levels of CDD and further explanation of the compliance requirements. If your customer does not require you to conduct a captured activity initially, but over time you are instructed to carry out captured activities, you must ensure you have completed the necessary CDD before you carry out those captured activities.

Existing customers

The term "existing customer" is defined in the Act as a person who was in a business relationship with a reporting entity immediately before the Act began applying to the reporting entity.[70] You must conduct CDD on existing customers if there has been a material change in the nature or purpose of the business relationship with that customer, and/or you have insufficient information about that customer.[71] When considering what information would be sufficient, you will need to assess the level of risk involved, and whether you hold the necessary identity information, verified to the appropriate level. You should not conduct any captured activity until these requirements are met.

Occasional customers

"Occasional activity" and "occasional transaction" are both defined in the Act.[72] 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.

The other people you must conduct CDD on

You must also complete CDD on:	For example:
Any beneficial owner[73] of a customer	Someone who owns more than 25 percent of a company that is your customer[74]
Any person acting on behalf of a customer	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 DIA website provides a range of fact sheets to help you. They cover the following topics[75]:

- Acting on behalf of others
- Clubs and societies
- Companies
- Co-operatives
- Sole traders and Partnerships
- Trusts

The supervisors have also provided specific guidance on beneficial ownership.[76] Customers that are individuals may be treated as the beneficial owner so long as you believe on reasonable grounds that the person is not acting on behalf of anyone else.[77]

The AML/CFT Act treats trusts as being capable of being customers in their own right, despite a trust not ordinarily having a legal personality. The supervisors have provided a factsheet to help reporting entities who engage with trusts as customers.[78]

Different levels of CDD requirements

There are three levels of CDD. You will need to be sure you use the right level, 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, and the potential for ML/TF risk. The three levels are:

- ***Standard CDD*** – for most common situations
- ***Simplified 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[79]
- ***Enhanced CDD*** – for use when there are factors creating a higher level of ML/TF risk or are otherwise specified in the AML/CFT Act

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

Other CDD requirements

Regardless of the level of CDD you are conducing on your client, you must seek information about the nature and purpose of the proposed business relationship or occasional transaction or activity.[80] 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; ie, 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.[81] Enhanced CDD generally requires you to ascertain the sources of your customer's wealth and/or funds (for more information see the "Enhanced CDD" section further on in this section). With this information you can make an assessment about whether your client's requests are typical, legitimate or suspicious.

Scenario-based examples

This section includes a series of scenario-based examples to demonstrate the process of compliance based on a range of fictional circumstances. Most of the examples focus on the captured activity "managing client funds", which many accountants do in their day-to-day work. You should assume for the purposes of these examples that all other relevant legal obligations have been met.

Standard CDD

Accountants must conduct standard CDD[82] if:

- They establish a business relationship with a new customer
- A customer seeks to conduct an occasional transaction or activity through the accounting practice, or
- In relation to an existing customer, and according to the level of risk involved, there has been a material change in the business relationship and there is insufficient information held about the customer (for example, they are a customer that you have dealt with prior to the Act taking effect who is now seeking assistance with captured activities and you are informed there are new investors (beneficial owners) that you do not have any CDD information about)

Identity requirements

When standard CDD applies, the following identity information must be gathered about a customer, the beneficial owner(s), and a person acting on behalf of a customer:[83]

- Full name
- Date of birth
- If the person is not the customer, the person's relationship to the customer
- Address or registered office
- Company identifier or registration number

You must also obtain information about the nature and purpose of the proposed business relationship with the customer, and sufficient information to determine whether enhanced CDD needs to be conducted on the customer.[84]

Verification requirements

Accountants are required to take reasonable steps to ensure that the information gathered is correct.[85] According to the level of risk involved, you need to take reasonable steps to verify the identity of any beneficial owners, and to verify the identity and authority of any person who is seeking to act on behalf of your customer. The supervisors have published a *Beneficial Ownership Guideline* to help you.[86] Verification must be undertaken before the business relationship is established or before the occasional transaction or activity is conducted. There is an exception to this which is described in "When to conduct CDD" later in this section.[87]

The Amended Identity Verification Code of Practice allows chartered accountants (among other identified groups) to act as "trusted referees" to verify identity information. It is important to note that chartered accountants can only do this where they are not themselves party to the activity or transaction with the customer for whom the CDD is being conducted.

Example in practice (low risk): Managing payroll for a small brewery

Customer:	Ms Genevieve Mills, owner of Mills Brewing Limited
Captured activity:	Managing client funds – making payroll payments to staff
Level of CDD required:	Standard CDD
Steps to complete standard CDD	**How this applies to the example**
1. Obtain identity information for all relevant persons	Ms Mills shows you her current passport. You check the Companies Office records online and you see that Ms Mills is listed as the sole director and shareholder of your customer (Mills Brewing), and the company address and business number match those that have been provided by Ms Mills. There are no indicators that enhanced CDD is required.
2. Obtain information about the nature and purpose of the proposed business relationship	Ms Mills explains that with the business growing, it is the right time to obtain professional accounting services for making payroll payments directly to staff.
3. Make a determination of the level of ML/TF risk involved	Based on the information that Ms Mills has provided you and your review of Companies Office records, you establish there are no other people with a beneficial interest in Mills Brewing Limited. You also assess the level of ML/TF risk associated with Mills Brewing Limited as low.
4. According to that level of risk, verify the identity of relevant persons, including natural persons, using the Amended Identity Verification Code of Practice	You view and take a clear copy of Ms Mills' passport. You record the date on which you sighted the passport and made the copy. You print a copy of the Mills Brewing Limited records from the Companies Office website and record the date on which you did.
5. If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions.	You on-board Mills Brewing Limited as a customer and set up systems to support the payroll operation.

If there were any number of changes to the range of facts in the fictional scenario above, the level of CDD required may have been different. For example, if there had been a range of beneficial owners, then you would have had to do CDD on all of them, and the level of CDD would depend on their characteristics and associated levels of ML/TF risk. Or, if the business was receiving investment funds from offshore, then you would have had to consider whether the originating countries have sufficient AML/CFT systems in place and whether they were countries known for ML/TF risks, such as known tax havens.

Example in practice (medium risk): Managing a small farm business's accounts payment

Customer:	Mr Randall Marsh and Mrs Stacy Evans – dairy farm owners
Captured activity:	Managing client funds – making payments from a customer's accounts
Level of CDD required:	Standard CDD
Steps to complete standard CDD	**How this applies to the example**
1. Obtain identity information for all relevant persons	Mr Marsh and Mrs Evans do not have passports so they provide you with their driver licences and birth certificates. Mr Marsh and Mrs Evans explain they have inherited their land from Mrs Evans' parents and there are no investors in their dairy farm business. At this stage, you note there are no indicators that enhanced CDD is required.
2. Obtain information about the nature and purpose of the proposed business relationship	Mr Marsh and Mrs Evans are looking for your assistance to ensure they make the right payments at the right time to keep their dairy farm business operating well.
3. Make a determination of the level of ML/TF risk involved	You note that Mr Marsh and Mrs Evans host occasional hunting and tramping events on their farm and some of the participants are tourists from the United States and Canada who give a gift for the hospitality; these are often large sums in cash. You determine the ML/TF risk is medium.
4. According to that level of risk, verify the identity of relevant persons, including natural persons using the Amended Identity Verification Code of Practice	You take copies of Mr Marsh's and Mrs Evans' driver licences and birth certificates and you use the Companies Register to confirm they are the sole owners of the farm and gain reliable information about the farm's address and business registration number.
5. If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions.	You set up systems to support the business account and payment management services for Mr Marsh and Mrs Evans' dairy farm business.

If there were any number of changes to the range of facts in the fictional scenario above, the level of CDD required may have been different. For example, if it was unclear to you how Mr Marsh and Mrs Evans came to own the dairy farm, you may have had to ask further questions about the source of their wealth. Or, if the occasional hunting and tramping events were a specific business enterprise that was attracting investors, you would have had to identify all people with beneficial ownership.

Simplified CDD

You may complete simplified CDD if your customer is one of those listed in the AML/CFT Act. The list includes a range of organisations such as:

- Government departments
- Local authorities
- The New Zealand Police
- State owned enterprises
- Crown entities
- Registered banks
- Licensed insurers
- Publicly listed companies

For the full list, please see section 18(2) of the AML/CFT Act.[88]

Identity requirements

When simplified CDD applies, you need to record the full name of the entity in question and a brief explanation of how it falls within section 18(2) of the AML/CFT Act.

The following information needs to be gathered about the identity of a person acting on behalf of one of the entities listed in section 18(2) (for instance, an employee of one of those organisations):

- Full name
- Date of birth
- The person's relationship to the customer

You also need to obtain information about the nature and purpose of the proposed business relationship between you and the customer.[89]

Verification requirements

You must verify the identity of a person acting on behalf of a customer, and verify that person's authority to act so that you are satisfied you know who the person acting is and that they have the authority to act. Reasonable steps must be taken according to the level of risk involved. This verification must be undertaken before the business relationship is established (or before the occasional transaction or activity is conducted), or before the person acts on behalf of the customer.

Example in practice (low risk): Provision of tax services for a licensed insurance company

Customer:	A small-scale life insurance provider, Pura Vida Insurance Limited
Captured activity:	Manage client funds – making tax payments to Inland Revenue directly from the customer's business accounts
Level of CDD required:	Simplified CDD
Steps to complete simplified CDD	**How this applies to the example**
1. Identify whether your customer meets the criteria for simplified CDD	Your customer is a licensed insurer which is a category listed in section 18(2) of the Act; so, you check the Financial Service Providers Register online and identify and record that Pura Vida Insurance Limited meets the criteria for simplified CDD.
2. Obtain information about the nature and purpose of the proposed business relationship	The Chief Executive, Mrs Elena Ortiz, explains the tax accounting and payment services she would like your accounting practice to undertake for the business. Her explanation demonstrates an intention for an ongoing business relationship.
3. Identify all relevant persons that need to be identified	Because Pura Vida Insurance Limited meets the criteria for simplified CDD, you only need to obtain information about the identity of the person acting on its behalf, Mrs Ortiz. Mrs Ortiz shows you her New Zealand passport, her employee identification card and a business card that states her to be Chief Executive.
4. Make a determination of the level of ML/TF risk involved	You determine that the risk is low, so you continue with applying simplified CDD.
5. According to that level of risk, verify the identity of relevant persons, including natural persons using the Amended Identity Verification Code of Practice	You take a copy of Mrs Ortiz's passport. You record the date on which you sighted the passport and made the copy. You also take a copy of Mrs Ortiz's Employment ID card and one of her business cards. You also check the Pura Vida Insurance website and record your belief that the chief executive you met with is the same person whose profile and photo is posted and that she has the authority to act on behalf of the customer – Pura Vida Insurance Limited.
6. If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions	You set up the necessary arrangements to provide accounting services to Pura Vida Life Insurance Limited.

If there were any number of changes to the range of facts in the fictional scenario above, the level of CDD required may have been different. For example, if Pura Vida Insurance Limited was an overseas based company that was opening a subsidiary in New Zealand and you were being asked to provide accounting services that are captured activities to the subsidiary, you would need to consider the ownership arrangements of the parent company and whether the country where the parent company resides has sufficient AML regulations in place and whether it is a country known for ML/TF risks.

Enhanced CDD

You must conduct enhanced CDD in specific circumstances:

- If you are establishing a business relationship with, or looking to conduct an occasional transaction or activity for, a customer that is:
  - A trust or another vehicle for holding personal assets; or
  - A non-New Zealand resident who is from a country that has insufficient AML/CFT systems and measures in place[90]; or
  - A company with nominee shareholders or shares in bearer form
- If a customer seeks your assistance to conduct a complex, or unusually large transaction or an unusual pattern of transactions that have no apparent or visible economic or lawful purpose[91]
- When you consider that the level of ML/TF risk involved means that enhanced CDD would be required
- When you have had cause to submit an SAR to the FIU

When conducting enhanced CDD, in the above circumstances, you must obtain information about your customer's source of wealth or source of funds.[92] You must record this information and take reasonable steps, according to the level of risk involved, to verify this information using other reliable and independent sources.[93] Where you identify that the origin of your customer's funds or wealth has come from their beneficial owner(s), it may be necessary, according to the level of risk involved, for you to extend your level of verification to include the source of wealth or source of funds of these persons. You will not need to obtain and verify source of wealth or source of funds for every beneficial owner if they have nothing to do with your customer's source of wealth or source of funds.

You must **also** conduct enhanced CDD in the following circumstances, which have specific prescribed identity and verification requirements:

- When you determine that your customer is a politically exposed person[94]; or
- If you are an ordering institution, an intermediary institution, or a beneficiary institution in relation to a wire transfer[95]; or
- If you are undertaking an activity that involves the use of new and developing technologies that may favour anonymity[96]

The supervisors have published guidance for all reporting entities on enhanced CDD.[97] The following examples have been tailored to suit accountants. Again, you should assume for the purposes of these examples that all other relevant legal obligations have been met.

Example in practice (low risk): Account management for a charitable trust

Customer:	A church that operates as a charitable trust
Captured activity:	Acting as a trustee – you are asked to act as a trustee
Level of CDD required:	Enhanced CDD
Steps to complete enhanced CDD	**How this applies to the example**
1. Identify which criteria your customer meets to decide the level of CDD you must do	You must complete enhanced CDD because your customer is a trust.
2. Obtain information about the nature and purpose of the proposed business relationship	The religious leader requests you to act as a trustee for the charitable trust.
3. Determine the initial level of ML/TF risk	While recognising that donations from the congregation represent a cash-based income, you determine that the risk is low given your knowledge that this church has been operating for a very long time and is well-regarded in the community.
4. Identify all relevant persons that need to be identified and gather information about the source of wealth/source of funds	You ask the religious leader for proof of their identity. You identify that they are listed on the Charities Register as one of the trustees, along with five other people. You ask to see the trust deed, copy this document and record the full name of the trust, its address and a description of the objects of the trust. You ask to see account documentation from their bank showing incoming donations and other income and outgoings for a period of time that you specify. In this case, you select the previous three months.
5. Verify the information gathered, including using the Amended Identity Verification Code of Practice for the identity of individuals[98] (as risk is not deemed to be high)	You take a copy of the religious leader's passport and record the date that you viewed the original. You advise them that you need to verify the identity of the other five trustees. You arrange to attend an upcoming meeting to meet them in person and take photos of their passports. You record the date and save copies of the photos. You review the bank statements provided as proof of source of funds/wealth. They are from a New Zealand-registered bank, which you determine to be a reliable and independent source. The accounts demonstrate prudent spending of income in line with the trust deed. You decide that no third-party verification of source of funds/wealth is required.
6. If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions	You set up the necessary arrangements to act as a trustee for the church.

If there were any number of changes to the range of facts in the fictional scenario above, the level of CDD required may have been different. For example, if the charitable trust had a cash-based income stream and was sending funds to undisclosed offshore locations, you would need to consider the risks associated with terrorism financing, as this is an established typology for terrorism financing activity globally, as well as considering any ML risks with each destination country and the level of AML/CFT regulation in those countries.

Example in practice (medium risk): Voluntary liquidation of a solvent company

Customer:	Nail salon business in liquidation
Captured activity:	Managing client funds – return of funds to beneficial owners
Level of CDD required:	Enhanced CDD
Steps to complete enhanced CDD	**How this applies to the example**
1. Obtain information about the nature and purpose of the proposed business relationship	You meet the director, Mr Poole. He explains to you that the nail salon business has not been as profitable as estimated. He is looking to liquidate as a means to recoup funds that can be redirected to more profitable enterprises. He assures you the company is solvent.
2. Determine the initial level of ML/TF risk	You determine the level of risk is medium based on your knowledge of ML/TF typologies; specifically, proceeds of crime may have been mixed with legitimate revenues, and customers of the business pay cash and are anonymous.
3. Identify which criteria your customer meets to decide the level of CDD you must do	You decide to undertake enhanced CDD because you recognise that nail salons feature in money laundering cases and typologies internationally and carry a risk due to their cash-based nature and potential for links to organised crime.
4. Identify all relevant persons that need to be identified and gather information about the source of wealth/source of funds	Mr Poole explains the ownership arrangements of the nail salon business. There are four individual investors with equal shares. You request the financial records for the past few years that demonstrate the volume and frequency of funds invested in the business by each investor. You request identity information for each investor. You request from Mr Poole copies of the contracts with each investor to show you the terms and conditions of each investment – including the provisions related to company liquidation. You then request information from each investor about the source of the funds that they have invested in the nail salon. They each come back to you with statements from their own accounting practices to show that the sources of funds are either profits from other investments or income gained from their ownership of specific businesses. The statements are each certified by those accounting practices.
5. Verify the information gathered, including using the Amended Identity Verification Code of Practice for the identity of individuals[99] (as risk is not deemed to be high)	You use the Companies Register to confirm that Mr Poole is the director of the nail salon business and you see that the investors' names match the list of shareholders on the Companies Register. The Companies Register also provides you with reliable information about the business number, the physical address of each salon, and the physical address of the head office where Mr Poole manages the salons. At your request, Mr Poole provides you with copies of each investor's passport and his own passport all of which have been certified by a suitable professional. You keep these as a record. You do internet searches on Mr Poole and all of the named investors to see if there is any information that would raise the ML/TF risk – such as whether any are politically exposed persons or are known associates of criminals. You find no such information. Instead you find information which confirms that the investors are involved in a range of legitimate business activities in the Auckland region such as property development, and other commercial investments in hospitality and retail businesses.
6. If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions	You set up the necessary arrangements to liquidate the nail salon business

In this fictional example, the liquidator looks through the corporate entity to understand the beneficial ownership of the payments. If there were any changes to the range of facts in the fictional scenario above, the level of CDD required may have been different. For example, if the company had become insolvent, there would be a lower risk of ML/TF. In that case, there is less risk of abuse of the corporate structure for the personal gain of the beneficial owners.

Example in practice (high risk): Accounting services for a tech start-up company

Customer:	Mr Michele Soto, who is launching a start-up company
Captured activity:	Forming a company and providing a registered address – you are asked to form a company for a customer to develop a smartphone application, and you are asked to provide a registered address for that company
Level of CDD required:	Enhanced CDD
Steps to complete enhanced CDD	**How this applies to the example**
1. Identify which criteria your customer meets to decide the level of CDD you must do	Mr Soto's proposed business would be part funded by an investor, his uncle, who lives in a country that is associated with corruption, so you decide to conduct enhanced CDD.
2. Obtain information about the nature and purpose of the proposed business relationship	Mr Soto explains that the purpose of his start-up business is to generate income from the smartphone application. Users will make subscription payments via an online platform for using the application. Mr Soto explains that he would like your advice on how best to set up this company and your assistance to form it. He explains that he also requires you to offer a registered address for the company as he frequently moves homes. Mr Soto explains that 50% of the seed funding is coming from his parents, with a further 50% from his uncle who lives overseas.
3. Determine the initial level of ML/TF risk	You ask Mr Soto about his uncle. He states that his uncle has various investments in new and developing technology businesses and has offered to top up the seed funding. Mr Soto's reference to using the online payment platform raises your perception of risk as these platforms can enable anonymous payments. You decide that the level of ML/TF risk is such that enhanced CDD is required.
4. Identify all relevant persons that need to be identified and gather information about the source of wealth/source of funds	You ask Mr Soto to provide you with identity information about himself (including proof of his address), his parents and his uncle and information about the sources of his seed funding.

5. Verify the information gathered using a higher level of vigour than provided for by the Amended Identity Verification Code of Practice for the identity of individuals[100] (as risk is deemed to be high)	Mr Soto provides his original passport and you view and take a clear copy. You record the date you sighted the passport and made the copy. Mr Soto also provides you with bank statements that show his home address and show lump sum payments from two sources: his parents and his uncle. You can see from the bank statement that the uncle's contribution originated by wire transfer from the overseas country. However, this does not fully enable you to identify the actual source of the funds. Mr Soto's parents live locally and bring their driver licenses, birth certificates and a recent sale and purchase agreement that shows they have a profit from a property sale – some of which has been given to their son for the seed money. You also ask to see Mr Soto's birth certificate to confirm the relationship and ask whether the funds provided are a gift or a loan. Mr Soto's parents advise that they are a gift, in lieu of future inheritance, and that appropriate paperwork has been filed via their lawyer with the IRD to confirm this. They have this paperwork with them. You make copies of all these documents. You ask to see further documents relating to the source of the uncle's funds and verifiable evidence of his identity. You are provided with a copy of a five-year term deposit bank statement held at a bank in the overseas country, which has been certified by one of the bank's in-house lawyers. This shows that the term deposit concluded shortly before the date on which Mr Soto received funds in New Zealand. There are certified copies of accompanying bank records showing the instruction to send the balance by wire transfer to Mr Soto in New Zealand. You are also provided with a copy of the uncle's New Zealand passport, which has been certified by a suitable professional in the overseas country. So that you can confirm that this person is genuinely Mr Soto's uncle, you also request a certified copy of his New Zealand birth certificate. You receive this, compare it against his parents' birth certificates to ensure there is a relationship, and file it.
6. If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions	You decide that this customer and activity is not suspicious and does not require an SAR to be filed. You then set up the necessary arrangements to form the company for Mr Soto and you record the business number the company is issued.

If there were any number of changes to the range of facts in the fictional scenario above, the level of CDD required may have been different. For example, if you had been unable to identify the source of funds for the seed money and/or if the online payment platform proposed to be used by the smartphone application was known for anonymity, you may have established the risk to be so high as to not be able to be mitigated and you would have considered how to end your engagement with Mr Soto.

Identifying if a customer is a politically exposed person

As soon as possible after establishing a business relationship, or conducting an occasional transaction or activity, accountants are required to take reasonable steps to identify whether their customer (or any beneficial owner) is a politically exposed person (PEP).[101] The Act requires reporting entities to conduct enhanced CDD if they 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.[102]

A PEP is defined in section 5(1) of the Act.[103] 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, you will require senior management approval to continue the business relationship.[104] Also, you must obtain information about the source of wealth or funds and verify that information.[105] If you have undertaken an occasional transaction or activity for someone who you didn't realise is a PEP, as soon as you can after the transaction you also need to obtain and verify information about their source of wealth or funds.

The *Enhanced Customer Due Diligence Guideline* has more information about how to manage compliance where customers are identified as PEPs.[106]

Wire transfers

The supervisors have published guidance on compliance matters when participating in wire transfers.[107]

A "wire transfer" is a transaction carried out on behalf of a person through a reporting entity by electronic means with a view to making an amount of money available to a beneficiary at another reporting entity (the person on whose behalf the transaction is conducted and the beneficiary can be the same person).

An "international wire transfer" is a wire transfer where at least one of the ordering, intermediary or beneficiary institutions is in New Zealand, and at least one is outside New Zealand.

Section 27 of the Act places specific obligations on "ordering institutions" and "beneficiary institutions" when the wire transfer is equal to or above NZ$1,000. It is possible that an accountant could be either an ordering or a beneficiary institution, in which case they must complete identity and verification requirements in line with the AML/CFT Act.[108]

New or developing technologies, or products that might favour anonymity

People with criminal intentions value anonymity and will continually look for new ways to preserve it while conducting their activities. Section 30 of the AML/CFT Act[109] requires that if a customer is seeking assistance for an activity that involves new or developing technologies, or products that might favour anonymity, you must:

- Complete standard CDD identity and verification requirements; and
- Take any additional measures needed to mitigate the risk of the new or developing technology or product being used to commit ML/TF. Depending on the technology and the product, and the ways in which they might favour anonymity, you will need to determine what additional measures are required[110]

Both steps must be done before you enter a business relationship or conduct an occasional transaction or activity for your customer.

How to use the Amended Identity Verification Code of Practice

Identity verification needs to be done by collecting and sighting documents, data, or information provided from a reliable and independent source. You are required to keep records of this information. The Amended Identity Verification Code of Practice provides suggested best practice for anyone conducting name and date of birth identity verification on customers (that are natural persons) who have been assessed to be low to medium risk.[111] The Amended Identity Verification Code of Practice should be read in tandem with the Explanatory Note.[112]

When you can rely on others for CDD

In some specific circumstances, reporting entities can rely on others to conduct CDD if the other party is either:

- A member of the same DBG[113]
- Another reporting entity in New Zealand or a person in another country that has sufficient AML/CFT systems and measures in place and who is regulated for AML/CFT purposes[114]
- An agent[115]; or
- An approved entity[116]

Relying on a member of your Designated Business Group

A member of a DBG (Member A) can rely on another member of that same DBG (Member B) to conduct CDD if the information is given before Member A has established a business relationship or conducts an occasional transaction or activity for the customer. Any verification information must be able to be given to Member A by Member B as soon as practicable but within five working days of the request. In this scenario, Member A (not Member B) is responsible for ensuring that it is complying with the AML/CFT requirements.

Relying on another reporting entity or a suitably regulated person overseas

A reporting entity can rely on another person for CDD so long as the person:

- Is either a reporting entity in New Zealand or is a person resident in a country which is regulated for AML/CFT purposes[117]; and
- Has a business relationship with the customer concerned; and
- Has conducted CDD to at least the standard required by the AML/CFT Act and:
  - Has provided the reporting entity the relevant identity information before it has established a business relationship or conducted an occasional transaction or activity; and
  - Can provide relevant verification information on request of the reporting entity as soon as practicable but within five working days; and
- Consents to conducting the CDD and providing all relevant CDD information to the reporting entity

In this scenario, and as above, the reporting entity requesting the CDD remains responsible for ensuring the CDD is conducted in accordance with the AML/CFT Act.

Relying on an agent

A reporting entity may authorise a person to be its agent and rely on that agent to conduct CDD and obtain any information required for CDD records. "Agent" is not defined in the Act; instead, the ordinary principles of agency law will apply.

Relying on an approved entity

Section 33 of the Act enables a business to rely on an "approved entity". There are not as yet any prescribed approved entities.

When to conduct CDD

You must conduct CDD (ie, obtain the required identity information and verify that information) on your customer *before* a business relationship with the customer is entered into, or an occasional transaction or activity is conducted.

The only exception to this timeframe, which would allow verification to be completed after the business relationship has been established, will be where all the following criteria apply:

- It is essential not to interrupt normal business practice; and
- ML/TF risks are effectively managed through appropriate risk management procedures; and
- Identity verification is completed as soon as practicable once the business relationship has been established[118]

Fast-paced scenarios may be common for some accountants; however, instances of delaying the verification of customer identity information should be rare. The reasons for delaying verification should be fact-based, justifiable and recorded.

Ongoing CDD and account monitoring

Under section 31 of the AML/CFT Act, when you are in a business relationship with a customer, you are required to conduct ongoing CDD and account monitoring. This means that you are required to regularly review any information about their account activity and transactions *you hold* about your customer to ensure it remains current. The purpose of this is to ensure that the nature and purpose of the business relationship and any activities or transactions relating to that business relationship are consistent with your knowledge of the customer and the customer's risk profile. This regular review will also help you to identify any grounds for reporting a suspicious activity.

Reporting entities are required to develop a process for ongoing CDD and account monitoring for their customers according to the level of risk each customer presents. You should think about the level of CDD that was previously undertaken, and consider the level of risk involved with that customer or their activities and transactions. This means higher-risk customers need to have more frequent and thorough account monitoring than customers deemed to be low or medium risk. The account monitoring conducted should 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.

Compliance obligations when conducting international transactions

An area of general business practice that requires specific mention in your AML/CFT programme is your method of ensuring compliance when you are engaged by other professionals on behalf of their customers, when conducting or participating in international transactions with multiple parties, or when you are otherwise engaging with parties in other countries. This is likely to be different for each firm.

Accountants are often engaged by other professionals, such as lawyers, to conduct accounting work that is required by *the other professional's* customer. In these instances it may be difficult to figure out who is *your* customer – the lawyer or their customer? Your answer to this question will be based on the particular circumstances.

Often, the lawyer's customer will be your customer, with the lawyer being a person acting on their behalf in their engagement with you. Alternatively, the lawyer's customer could be a party to an activity or transaction that is being conducted by you for your customer, the lawyer. In practice, this means that you will often need to conduct CDD on both the lawyer and their customer, unless you already hold sufficient CDD information on them and there has been no material change in your business relationship with them. You will then need to consider the level of CDD required depending on the particular circumstances.

In some cases, a lawyer or other professional instructing you on behalf of their customer will themselves be a reporting entity (or equivalent in an overseas jurisdiction). For example, the law firm in New Zealand instructing you on behalf of their customer is captured as a reporting entity under the Act. This means that they must do their own CDD on their customer at the time their business relationship started. When you are subsequently engaged by this law firm to conduct captured activities for their customer, you can choose to rely on the CDD that they have conducted on their customer so long as the criteria set out in section 33(2) are met (including obtaining permission and relevant identity and verification information from the law firm). **If you rely on a third party to conduct CDD, you remain responsible for ensuring that the required CDD is conducted in accordance with the AML/CFT Act.**

Conducting CDD in a multi-party international transaction

The above requirements apply whether you are being engaged by another professional in New Zealand or from another country. DIA recognises that this may be challenging when dealing with professionals who operate in countries where a high standard of AML/CFT regulation is not the norm. Also, there may be instances where there are multiple beneficiaries in multiple countries on whom you require CDD information to allow you to proceed. In such instances you have two options:

1. consider whether it will be possible to obtain the identity and verification information you need via other professionals involved, remembering you remain accountable for completing CDD in accordance with the AML/CFT Act; or
2. conclude your engagement without conducting activities that are captured by the AML/CFT Act. For more information about concluding engagements when CDD cannot be conducted, please see further on in this section.

Dealing with other countries

The supervisors have published the *Countries Assessment Guideline* to help you determine whether a country you are dealing with has effective AML/CFT systems and measures.[119]

There is no definitive list of countries that are deemed not to have sufficient AML/CFT systems and measures, so reporting entities should consider a range of factors when determining the level of risk associated with engaging in a transaction with a country.

For example, is the country:

- Subject to international sanctions, embargos or other measures?
- Identified by the FATF as lacking adequate AML/CFT systems and measures?[120]
- Recognised as having supporters of terrorism, or financing terrorism?
- Considered to have problems with corruption (eg, does it have a low ranking on the Transparency International Corruption Perceptions Index[121])?
- Known as a tax haven[122]?
- Associated with production and/or transnational shipment of illicit drugs?

You must develop an understanding of the ML/TF risks associated with any countries that you deal with.[123]

What to do if you cannot complete CDD

If you are not able to complete CDD for a customer, you must neither carry out an occasional transaction or activity for them nor establish a business relationship with them.[124] If you already have a business relationship with the customer, and that business relationship relates solely to captured activities, this must be terminated (you are free to continue providing non-captured services to the customer). This applies to all circumstances where a customer fails or refuses to provide information, data or documents that you have requested, including in relation to enhanced CDD. This also applies if the information, data or documents that the customer provides are inadequate.

If you are declining to enter into a business relationship or refusing an occasional transaction or activity, you are required to consider whether you need to file an SAR with the FIU.

6. Do you know the red flags?

This section draws on available international information about the vulnerabilities of the accounting profession to misuse for ML/TF purposes by their customers. This information should assist your general AML/CFT awareness and your consideration of the risks your business may face from ML/TF activity.

Red flags identified by the Financial Action Task Force

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 to set global standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

The FATF provides a range of information and advice for the industries and professions that are affected by money laundering and terrorism financing. The FATF published *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorism Financing: High Level Principles and Procedures for Accountants*[125] in 2008 and *Money Laundering Using Trust and Company Service Providers*[126] in 2010. These documents aim to support the development of a common understanding of what a risk-based approach involves; outline the high level principles in applying this approach, and suggest some best practice in designing and implementing a risk-based approach.

The document *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorism Financing: High Level Principles and Procedures for Accountants* highlights the activities conducted by the accounting profession that are vulnerable to potential misuse by those who wish to launder the proceeds of crime or fund terrorist activities. These vulnerable activities can be summarised as follows:

- Management of client money, securities and other assets
- Management of bank, savings or securities accounts
- Creation, operation or management of legal persons or arrangements, and buying and selling of business entities
- Organisation of contributions for the creation, operation and management of companies
- Buying and selling of real estate

These activities correspond closely with the captured activities in the AML/CFT Act that are outlined in section 3 of this guideline. Section 3 also identifies the ML/TF risks with each of the captured activities.

This section provides more detail on the "red flags" to be on the lookout for when you are conducting these activities for your customers. The red flags described below have been taken from a range of open source publications (which are noted in the References section) and professional judgements of subject matter experts. They can be categorised in the following manner:

- Customer risk
- Product, service or delivery method risk
- Country/Geographic risk
- Other risk factors

Customer risk

There are a range of risks that relate to the nature of your customer that you should consider. When thinking about the risks posed by your customers, have regard to whether:

- The business relationship is conducted in a unusual circumstances
- The customer is a resident in a geographical area that is considered to be high risk (see also the "Country/Geographic risk" section below)
- The customer is a legal person or arrangement that is a vehicle for holding personal assets
- The customer is a company that has nominee shareholders or shares in bearer form
- The customer is a business that is cash-intensive
- The corporate structure of the customer is unusual or excessively complex given the nature of the company's business
- You do not have a face-to-face introduction to your customer
- There is a subsequent lack of contact, where contact would be expected normally
- Beneficial ownership of the customer is unclear
- There are inexplicable changes in the ownership of your customer
- The position of intermediaries is unclear
- The activities of the company are unclear
- The legal structure of the customer is frequently altered, including name changes and transfers of ownership, and location of headquarters
- The people who manage the customer appear to be acting according to the instructions of unknown or inappropriate persons

- The reason for the customer using your firm is unclear given the firm's size, location or specialisation
- The customer is reluctant to provide all the relevant information, or you have a reasonable doubt that the information provided is correct or sufficient
- The customer is a politically exposed person, a relative or close associate of a politically exposed person, a head of an international organisation, or a high net worth individual
- The customer works in an industry or occupation that has a high risk of ML/TF

Product, service or delivery method risk

Particular products or services or transaction delivery methods can be vulnerable to misuse by those wishing to launder money or finance terrorism. When considering the risks associated with a product or service or transaction delivery method, have regard to whether:

- The product involves private banking
- The product, service or transaction delivery channel might favour anonymity
- The situation prevents face-to-face business relationships or transactions without certain safeguards, such as electronic signatures
- Payments will be received from unknown or un-associated third parties
- New products and new business practices are involved, including new delivery mechanisms and the use of new or developing technologies for both new or pre-existing products
- The service involves the provision of nominee directors, nominee shareholders, or shadow directors, or the formation of companies in third countries
- The service is open to misuse of pooled client (or trust) accounts or provides safe custody of customer money or assets
- The service requested is for introductions to other financial institutions, where this is not otherwise necessary or ordinary
- The service requested is for advice on setting up legal arrangements that may be used to obscure ownership or real economic purpose (including setting up trusts, companies, or change of name/corporate seat or other complex group structures)

Country/Geographic risk

Moving money from country to country is a key typology for obscuring the criminal origins of funds and/or the true intended destination for funds. There are particular countries that represent higher ML/TF risks and these will change over time in the dynamic AML/CFT environment. When considering the risks associated with dealing with customers or transactions that relate to other countries or geographic regions, have regard to whether the countries are:

- Identified by credible sources as not having effective systems to counter money laundering and terrorist financing
- Identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering, and the production and supply of illicit drugs
- Subject to sanctions, embargos or similar measures issued by, for example, the United Nations or the European Union
- Identified by credible sources to have provided funding or support for terrorism

There are a wide variety of credible sources and it is up to your judgement what information you access and how you perceive the credibility of that information. Generally, sources with expertise in AML/CFT are deemed to be credible, such as the FATF, the Asia/Pacific Group (the FATF-style regional body New Zealand is a member of), and other international organisations such as the United Nations, International Monetary Fund, and the Financial Intelligence Units of countries with strong AML/CFT systems in place.

Other risk factors

These are some factors to consider that can either increase or decrease your perception of risk:

- Involvement of financial institutions or other DNFBPs
- Unexplained urgency of assistance required
- Sophistication of the customer, including the complexity of the control environment (ie, the overall attitude, awareness and actions of directors and management regarding the internal control system and its importance to the entity)
- Sophistication of transaction/scheme
- Country location of accountant
- Working environment/structure of the accountant (eg, sole practitioner or large firm)
- Role or oversight of another regulator
- The regularity or duration of a business relationship (long-standing relationships involving frequent customer contact throughout the relationship present less risk)
- The purpose of the business relationship and the need for an accountant to provide services
- The reputation of customers in the local community
- Whether private companies are transparent and well known in the public domain
- The familiarity of the accountant with a country, including knowledge of local laws and regulations as well as the structure and extent of regulatory oversight

These factors may indicate a higher ML/TF risk:

- Customer instructions or access to funds is out of sync with their business or personal profile
- Your customer conducts individual or classes of transactions that are outside their business profile and are unexpected activities in terms of what you know about your customer
- Your customer's employee numbers or structure is out of keeping with the size and nature of the business (eg, the turnover of a company is unreasonably high considering the number of employees and assets used)
- Sudden activity from a previously dormant customer
- Your customer starts or develops an enterprise with an unexpected profile or early results (ie, unexpected profits)
- Indicators that your customer does not wish to obtain the necessary government approvals or licences
- Your customer offers to pay extraordinary fees for services that would not ordinarily warrant such a premium
- Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment

The nature of the business activities of your customer may be a risk factor. You should seek to understand whether:

- Your customer is an entity with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured
- There are any politically exposed persons engaged in or with your customer
- Your customer invests in real estate at higher or lower prices than expected by the market
- Your customer conducts unusual financial transactions with unknown source(s)
- Your customer has multijurisdictional operations that do not have adequate centralised corporate oversight
- Your customer is incorporated in countries that permit bearer shares

If you have a customer who engages in trade or the provision of goods and services, you should be on the lookout for whether there are instances where there is:

- Over- and/or under-invoicing of goods/services
- Multiple invoicing of the same goods/services
- Falsely described goods/services, such as over- or under-shipments
- Multiple trading of goods/services

There are some red flags you should be looking for when engaging with other professionals in your sector. For example, you may need to be wary of instances where:

- Accounts and/or facilities are opened and/or operated by company formation agents
- Gatekeepers (eg, lawyers, other accountants) appear to have full control
- Known or suspected corrupt professionals are offering services to criminal entities
- Accounts are operated by someone other than the account holder

How to keep up-to-date with changing methods of ML/TF

People with criminal intentions will seek to stay ahead of authorities and the professionals whose services they wish to misuse. Over time new methods of ML/TF will develop and emerge. The FIU and DIA actively maintain a watch for these new methods and communicate them via the FIU's Quarterly Typology Reports[127] and DIA's newsletters.[128] Reporting entities, their compliance officers in particular, are encouraged to look at these resources as well as media reports and information from the FATF and other jurisdictions to keep up-to-date with developments in ML/TF methods.

7. Do you know where to get support?

- Reporting entities can access compliance support from a range of sources:
- Your AML/CFT programme and compliance officer
- DIA as the supervisor
- Your professional body if you have membership with one
- 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. The 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 recognise that this is a new compliance system to adjust to, and so we aim to provide proactive support to reporting entities. Examples of the support we provide range from general information and awareness promotion, all the way to specific support where a reporting entity is experiencing difficulty but has a genuine intention to comply. The DIA website provides a wide range of information about how to comply with the AML/CFT Act for reporting entities.[129]

The AML/CFT Act allows supervisors to create codes of practice. A code of practice is a statement of practice that helps reporting entities to comply with the AML/CFT Act. So far, one code of practice has been developed: the Identity Verification Code of Practice.[130] This was developed in 2011 and amended in 2013. It should be read in tandem with the Explanatory Note.[131] There are no current plans to develop more codes of practice, but the supervisors are open to feedback from reporting entities on whether more would be helpful.

Support from your professional bodies

Accountants are encouraged to keep abreast of the information and education on offer from the professional bodies they have a membership with. The following professional bodies offer support to accountants:

- Chartered Accountants Australia and New Zealand raises awareness via articles and by hosting webinars on AML/CFT topics.
- The Accountants and Tax Agents Institute of New Zealand ensures that AML/CFT topics are well covered in conferences to inform their members.
- The New Zealand Bookkeepers Association Incorporated ensures that AML/CFT topics are covered via membership meetings, conferences, newsletters and social media to keep its members well informed.

When to seek independent advice

There will be occasions where accountants need to seek independent advice to ensure they remain compliant with the AML/CFT Act. Supervisors cannot provide legal advice to reporting entities. When you have specific compliance questions about unique circumstances that the supervisor or your professional body cannot reasonably answer, you may need to seek independent legal advice or advice from an otherwise suitable professional.

Other publicly available information

The Phase 2 Sector Risk Assessment (Phase 2 SRA) is important reading for accountants. This resource gives reporting entities the background understanding of the ways ML/TF poses risk to accountants. The Prompts and Notes guideline outlines the factors to be considered in a risk assessment along with some prompts and questions to think about when completing a risk assessment and developing your AML/CFT programme. The Phase 2 SRA and the Prompts and Notes guideline are available on the DIA website.[132] The FATF has a range of information on its website, both specific to accounting and other gatekeeper professions[133] and to the New Zealand context.[134]

Support that may emerge in the future

As the AML/CFT system becomes established practice among accountants it is likely that relevant training establishments will begin to incorporate AML/CFT into curricula. Professional bodies will be a good source of information when new educational supports are in development. Supervisors are responsible for updating and creating new guidance in line with sector needs. You will be advised when new guides are made available.

Appendix A:Case studies

The case studies come from open source publications – references are provided in the endnotes. The purpose of including these case studies is to raise awareness of how accountants have knowingly, or unknowingly, been involved with ML/TF.

Case study 1: Accountant received funds on behalf of criminal[135]

A methamphetamine manufacturer and dealer in the Waikato region used an accountant to receive cash from his drug dealing and convert it into various purchases of farm land over a number of years. He used two of his farm employees to collect and take cash from drug sales to the accountant's office. The accountant had 12 accounts held at different banks in which he would bank the cash. The accounts were held for his accounting practice, a gift shop he and his wife owned, his personal accounts and a company account he was nominee director and shareholder of on behalf of the methamphetamine manufacturer.

The accountant went to different branches across the Waikato region and banked the cash into the various accounts. Some excuses he gave about the source of the cash were "it was cash takings from a client who owned a bar" or "it was his cash takings from a stall he operated at a market". The deposited cash would then be electronically transferred to his accounting practice to be held on behalf of the methamphetamine manufacturer. With his accumulated wealth, the methamphetamine manufacturer purchased farm land in the name of his family trust. The trustee of his trust was a corporate trustee company that the accountant was the director and shareholder of. This trust arrangement enabled the methamphetamine manufacturer to hide the fact he owned the farm land. It was estimated that, over ten years, he had accumulated NZ$4.8 million from his drug offending. He was sentenced to 12 years prison and his farm land (valued at approximately NZ$5million) was forfeited to the Crown. Whilst it was clear the accountant had engaged in money laundering, he was used as a witness against the methamphetamine manufacturer in exchange for immunity from prosecution.

Case study 2: Using an accountant as an intermediary in the legal structure of a business[136]

In Operation Ark, the New Zealand Police investigated a case where drug offenders had engaged an accountant to set up a complex structure of legal entities, including a trust. This case demonstrates many of the principal ways trusts are used to launder proceeds – in particular, layering entities to hide the beneficial control of companies controlling assets; use of a professional service provider to access complex structures and act as an intermediary; and use of a trust to hide criminal involvement in transactions.

The drug offender used the trust to buy shares in a fitness magazine business and a company with the proceeds of drug offending. Vehicles owned by the drug offender were then registered in the name of the company, ostensibly distancing the offender from ownership of the vehicles. The offender also used his accountant as an intermediary and additional layer in the legal structure of his finances. Ultimately, as was the case in his layering of entities to hide ownership of the magazine and vehicles, the offender used the accountant and the trust to hide his own beneficial ownership of property. For example, the offender's house was put in the name of a company whose nominee shareholder was the accountant's trust company. The accountant's trust company was in turn holding the shares on behalf of the offender's trust.

Case study 3: Accountant facilitated a round-robin tax evasion scheme[137]

"Round robin" tax evasion schemes essentially aim to make funds movements appear as payments to other parties while, in reality, the funds ultimately return to the original beneficiary. In this case enquiries identified that the principal promoter and operator of a tax evasion scheme was a senior partner of an accounting firm based in Vanuatu. Analysis of Australian Transaction Reports and Analysis Centre (AUSTRAC) information uncovered the round robin tax evasion scheme, which involved the transfer of funds between Australia-based individuals and bank accounts of companies in other countries to evade tax in Australia.

The method used to facilitate tax evasion was:

1. Suspects in Australia transferred funds from their companies' accounts to the bank accounts of companies in New Zealand. The New Zealand companies and the bank accounts were controlled by the Vanuatu-based accountant, who was a signatory to the bank accounts.
2. The payments were falsely described in the suspects' companies' records as expenses in the form of "management and consultancy fees". False invoices were created for the fictitious expenses. No evidence was available to show that any consulting work had been carried out. The invoice amounts matched the amounts paid to the bank accounts in New Zealand.
3. The false expense payments were claimed as deductible expenses in the tax returns of the Australian companies, fraudulently reducing the companies' taxable income and the amount of tax they were assessed as liable to pay.
4. The accountant then transferred the funds under the guise of international "loans" through a series of round robin international transactions, through accounts held in the name of companies owned and operated by the accountant.
5. The accountant transferred the funds into the personal bank accounts of the suspects in Australia. The funds were transferred via an overseas company controlled by the accountant, separate to the companies in New Zealand that received the funds originally.
6. In order to disguise the funds as loans, false documents were created purporting to be international loan agreements with a foreign lender. Loans are not assessable income and are tax-free.
7. The funds, disguised as international loans, were not disclosed in the suspects' personal tax returns. The suspects were thus assessed as liable for less tax than they should have been, thereby avoiding income tax obligations.
8. Effectively, the "loans" paid to the suspects were funds from their respective companies but were disguised by the scheme, allowing them to evade approximately AU$750,000 in company and personal tax.

Both suspects in Australia were ultimately convicted of tax evasion and fraud offences and sentenced to three years imprisonment. The suspects also became liable to pay penalties and interest to the Australian Taxation Office of more than AU$1 million and AU$900,000 respectively. The accountant was convicted of conspiring to defraud the Commonwealth and was sentenced to 8 years and 11 months imprisonment.

Case Study 4: Assets forfeited from dishonest accountant in New Zealand[138]

In March 2014, assets valued at an estimated NZ$1.4 million were forfeited from an accountant who used funds stolen from the trust accounts of his clients to fund a lavish lifestyle. For years the Hamilton-based accountant siphoned off funds and used them to build a mansion complete with hydro-slide and to fund purchases such as vehicles, company shares, boats, and a holiday home in Fiji. His actions were concealed by a complex set of entities that were used to hide his fraud, often under the guise of legitimate transactions. The accountant was caught when Inland Revenue noted discrepancies between his assets and his declared income. He has been sentenced to more than five years imprisonment and his status as a chartered accountant has been suspended by the Institute of Chartered Accountants.

Case Study 5: Using shell businesses as a front for drug supply network[139]

In 2013 the High Court restrained around NZ$1.8 million worth of assets related to a drug supply network connected to a roading contractor.
The Crown alleges that the principal offender and a number of associates were involved in a national drug supply network that used the roading contractor's roading and forestry businesses as a front to facilitate offending. The businesses provided ideal fronts for drug distribution and/or manufacture, providing the principal offender with a reason for local and domestic travel required for drug related transactions.

The offenders also appear to have used these companies to commingle the proceeds of the offending. Such businesses provide an opportunity to explain the illicit earnings from drug supply.
The principal offender ensured that his businesses maintained good records of apparent earnings by using professional accountants. In addition to facilitation of predicate offending, the nationally dispersed business interests also would have provided an opportunity to select professional service providers which may have allowed the offenders to select professionals who would be unable to detect illicit activity. These types of arrangements could also allow criminals to seek remote professional services and/or to change professional service providers so as to prevent professionals gaining a full appreciation of any unusual business activity.

In this case, maintaining professionally facilitated business records and declaring earnings for tax helped the offenders to maintain an air of legitimacy.

Using such businesses as fronts for criminal activity may also make law enforcement investigation to establish illicit earnings more complex. However, despite the extensive and well documented earnings, corresponding legitimate business had not been established, giving a strong indication that the illegitimate earnings from drug supply were commingled with whatever legitimate earnings the businesses made. It was concluded that in this case, the offenders' accountants were unwittingly involved in commingling the proceeds of the drug supply business with the legitimate business activity earnings.

Case study 6: Transnational drug dealing[140]

Operation Major involved Asian organised crime using New Zealand-registered companies to act as a cover for the facilitation of drug smuggling into New Zealand. Multiple companies and bank accounts were established for the sole purpose of being able to import legitimate goods that concealed illicit drugs within them (crystal methamphetamine and precursor chemicals). The companies purported to be in the business of international trading and supply of materials relating to polymer technologies. In May 2006, a New Zealand Customs drug seizure found 95kg of crystal methamphetamine concealed in the bottom of 95 paint tins. A few days later a second drug seizure found 150kg of pseudo ephedrine tablets in amongst a shipment of bags of block plaster. Both drug seizures had a combined potential total street value of NZ$135 million. This was the largest and most significant illicit synthetic drug seizure in New Zealand's history. The shell companies involved were registered by accountants and the individuals involved in the drug importations.

References

Consultative Committee of Accountancy Bodies (CCAB), (Published in draft in August 2017, final version expected in mid-2018), *Anti-Money Laundering Guidance for the Accountancy Sector*, CCAB, United Kingdom. https://www.ccab.org.uk/documents/TTCCABGuidance2017regsAugdraftforpublication.pdf

Courts of New Zealand, (28 September 2017), *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Limited [2017] NZHC 2363*. https://forms.justice.govt.nz/search/Documents/pdf/jdo/15/alfresco/service/api/node/content/workspace/SpacesStore/916f5146-d0bb-4c1f-9fda-979cd3d122f0/916f5146-d0bb-4c1f-9fda-979cd3d122f0.pdf

Department of Internal Affairs, Reserve Bank of New Zealand, Financial Markets Authority, (July 2011), *Supervisory Framework*, DIA, RBNZ & FMA, Wellington. https://www.dia.govt.nz/Pubforms.nsf/URL/Supervisory-Framework-FINAL-updated-28-July-2011.pdf/$file/Supervisory-Framework-FINAL-updated-28-July-2011.pdf

Financial Intelligence Unit, (May 2014), *Quarterly Typology Report Third Quarter (Q3) 2013/2014*, FIU, Wellington. http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q3-2013-2014.pdf

Financial Intelligence Unit, (July 2014), *Quarterly Typology Report Fourth Quarter (Q4) 2013/2014*, FIU, Wellington. http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q4-2013-2014.pdf

Financial Intelligence Unit, (October 2014), *Quarterly Typology Report First Quarter (Q1) 2014/2015*, FIU, Wellington. http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q1-2014-15.pdf

Financial Intelligence Unit, (January 2015), *Quarterly Typology Report Second Quarter (Q2) 2014/2015*, FIU, Wellington. http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q2-2014-2015.pdf

Financial Action Task Force, (16 October 2009), *Mutual Evaluation Report: New Zealand,* FATF, Paris. http://www.fatf-gafi.org/countries/n-r/newzealand/documents/mutualevaluationofnewzealand.html

Financial Action Task Force, (17 June 2008), *Guidance on the Risk-Based Approach to Combatting Money Laundering and Terrorism Financing: High Level Principles and Procedures for Accountants,* FATF, Paris. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfguidanceontherisk-basedapproachforaccountants.html

Institute of Singapore Chartered Accountants, (November 2014), *Anti-Money Laundering and Countering the Financing of Terrorism – Requirements and Guidelines for Professional Accountants in Singapore*, Singapore. https://isca.org.sg/ethics/anti-money-laundering-and-countering-the-financing-of-terrorism/

Endnotes

1. The recent changes were made by the AML/CFT Amendment Act 2017 (http://bit.ly/2Cy5p8Q).
2. "Accounting practice" is defined in section 5(1) of the AML/CFT Act: http://bit.ly/2xHGfmy
3. Section 130(1)(c), AML/CFT Act (http://bit.ly/2A2AKj7). There are two other supervisors for other reporting entities: the Reserve Bank of New Zealand and the Financial Markets Authority. References to "the supervisors" in this document refer to all three agencies collectively.
4. Sections 58(2)(g) http://bit.ly/2ly11Dz and 57(2) http://bit.ly/2h2nN59 of the AML/CFT Act.
5. AML/CFT Act and Regulations: http://bit.ly/2hpGU5V
6. Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
7. *Mutual Evaluation of New Zealand*: http://bit.ly/2EBoTyn
8. Financial Action Task Force, (June 2013), *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, FATF, Paris, p. 35. Please note, where it refers to STR in the diagram, it means "suspicious transaction report". We now refer to these as "suspicious activity reports" (SARs).
9. *AML/CFT Supervisory Framework*: https://bit.ly/2J2FyKL
10. *Minimising Harm – Maximising Benefit*: http://bit.ly/2z669Sy
11. Section 243, Crimes Act 1961: http://bit.ly/2zYeqXU
12. Section 8(1) and (2A), Terrorism Suppression Act 2002: http://bit.ly/2lZbZlE
13. *Territorial Scope of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009*: http://bit.ly/2nf664p
14. For the full text of the activities please see section 5(1) of the AML/CFT Act under the definition of "designated non-financial business or profession": http://bit.ly/2xHGfmy
15. AML/CFT (Definitions) Regulations 2011: http://bit.ly/2hrFYy3
16. AML/CFT (Exemptions) Regulations 2011: http://bit.ly/2lAImH6
17. AML/CFT Ministerial exemptions: http://bit.ly/2xCmQU6
18. AML/CFT (Class Exemptions) Notice 2014: http://bit.ly/2zly18h
19. Sections 157–159 AML/CFT Act: http://bit.ly/2aFZRjN
20. *Interpreting "Ordinary Course of Business" Guideline:* http://bit.ly/2Bh3CEI
21. As at 29 March 2018, no arrangements have been prescribed. Section 5(1), AML/CFT Act: http://bit.ly/2xHGfmy
22. Both these terms are defined in section 5(1), AML/CFT Act: http://bit.ly/2xHGfmy
23. Section 6, Lawyers and Conveyancers Act 2006: http://bit.ly/2ztIqyK
24. Section 4(1), Real Estate Agents Act 2008: http://bit.ly/2h79rQS
25. Residential Tenancies Act 1986: http://bit.ly/2iYKoQl
26. Land Transfer Act 1952: http://bit.ly/2iq9a8c
27. Section 5, Retirement Villages Act 2003: http://bit.ly/2lJhJQv
28. Section 43, AML/CFT Act: http://bit.ly/2og1BEW
29. Section 9, AML/CFT Act: http://bit.ly/2iR0JH3
30. Section 56, AML/CFT Act: http://bit.ly/2znn4Dd
31. This will only be possible where the business has no employees. The supervisor expects that if the person who is acting as a compliance officer is not part of the business, there should be a justifiable reason. The reporting entity should be able to demonstrate to the supervisor that the person selected has an appropriate level of access to business information and systems to perform their duties and the authority to advise the senior management of the business about AML/CFT matters.
32. Section 58, AML/CFT Act: http://bit.ly/2ly11Dz
33. Risk Assessment Guideline: http://bit.ly/2sdlv83
34. Section 58(2)(g), AML/CFT Act: http://bit.ly/2ly11Dz
35. Sector and National Risk Assessments: http://bit.ly/2ik1tAu
36. AML/CFT Risk Assessment and Programme: Prompts and Notes for DIA Reporting Entities: http://bit.ly/2EBUMXy
37. Guide for Small Financial Adviser Businesses: http://bit.ly/2z18hNI
38. FIU assessments and reports: http://bit.ly/2xGSiAx
39. Sections 56 and 57, AML/CFT Act: http://bit.ly/2znn4Dd and http://bit.ly/2h2nN59
40. Section 57(2), AML/CFT Act: http://bit.ly/2h2nN59
41. AML/CFT Programme Guideline: http://bit.ly/2iS5I7k
42. The CDD requirements are noted in Part 2, subpart 1, AML/CFT Act: http://bit.ly/2A5PJtA
43. Section 49, AML/CFT Act: http://bit.ly/2zEQkFA
44. Section 49A, AML/CFT Act: http://bit.ly/2iFJ1lM
45. Section 50, AML/CFT Act: http://bit.ly/2zdxog9
46. Section 51, AML/CFT Act: http://bit.ly/2znMDn8
47. Section 31, AML/CFT Act: http://bit.ly/2z1eCIX
48. Section 59, AML/CFT Act: http://bit.ly/2xJWm2P
49. Section 60, AML/CFT Act: http://bit.ly/2gQqiUa

50. *User Guide: Annual AML/CFT Report by Designated Non-Financial Businesses and Professions*: available at Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
51. Sections 59–59A, AML/CFT Act: http://bit.ly/2xJWm2P
52. *Guideline for Audits of Risk Assessments and AML/CFT Programmes*: http://bit.ly/2AfTf7m
53. It is up to you to decide if someone is suitably qualified to conduct an audit of your AML/CFT programme. You should be able to explain to the supervisor your rationale for this decision on request.
54. Section 59B, AML/CFT Act: http://bit.ly/2muArvE
55. The AML/CFT Amendment Act 2017 changed "suspicious transaction reports" to "suspicious activity reports".
56. *DIA v Ping An Finance (Group) New Zealand Limited* (2017) NZHC 2363, at paragraphs 64-67.
57. Section 5(1), AML/CFT Act (http://bit.ly/2xHGfmy); Regulation 5A, AML/CFT (Definitions) Regulations (http://bit.ly/2hbI5p6). Also see the FIU's Prescribed Transactions Reporting web page: http://bit.ly/2zkB9RJ
58. Designated terrorist entities: http://bit.ly/258MtKq
59. goAML – Financial Intelligence Unit reporting tool: http://bit.ly/2ygOri3
60. Section 46, AML/CFT Act: http://bit.ly/2xCrpxz
61. Section 40(4), AML/CFT Act: http://bit.ly/2CB4DYH
62. Section 42, AML/CFT Act: http://bit.ly/2yj0ECT
63. Sections 53–57 of the Evidence Act 2006: http://bit.ly/2Ah1n7T
64. Section 5(1) of the AML/CFT Act: http://bit.ly/2xHGfmy
65. Section 32, AML/CFT Act: http://bit.ly/2hjDuF3
66. Designated Business Group Guidelines: http://bit.ly/2y4KpFa
67. Part 2, subpart 1, AML/CFT Act: http://bit.ly/2A5PJtA
68. Customer Due Diligence Fact Sheets: http://bit.ly/2Bxp2Pc
69. *DIA v Ping An*, paragraph 44.
70. Section 5(1), AML/CFT Act: http://bit.ly/2xHGfmy. For accountants, "existing customer" refers to any person who was in a business relationship with you immediately before 1 October 2018.
71. Section 11(4), AML/CFT Act https://bit.ly/2gRumUg. The term "material change" has been defined in the Enhanced Customer Due Diligence Guideline (available here: http://bit.ly/2GrKaHV) as "an event, activity or situation that you identify during interactions with your customer (or via ongoing customer due diligence and account monitoring) that could change their level of ML/TF risk".
72. Section 5(1), AML/CFT Act: http://bit.ly/2xHGfmy
73. The term "beneficial owner" is defined in section 5(1), AML/CFT Act: http://bit.ly/2xHGfmy
74. More than 25% is the prescribed threshold for the definition of a beneficial owner. Regulation 5, AML/CFT (Definitions) Regulations: http://bit.ly/2yDVy49
75. Customer Due Diligence Fact Sheets: http://bit.ly/2Bxp2Pc
76. *Beneficial Ownership Guideline*: http://bit.ly/2Bxp2Pc
77. Section 11(2), AML/CFT Act: http://bit.ly/2gRumUg
78. *Clarification of the position the AML/CFT supervisors are taking with respect of the AML/CFT Act interpretation of a trust as a customer*: http://bit.ly/2Bxp2Pc
79. Section 18(2), AML/CFT Act: http://bit.ly/2gS5b3V
80. Sections 17, 21 and 25, AML/CFT Act: http://bit.ly/2m1YSjC
81. Section 17, AML/CFT Act: http://bit.ly/2m1YSjC
82. Section 14, AML/CFT Act: http://bit.ly/2z2zU99
83. Section 15, AML/CFT Act: http://bit.ly/2zDSNQt
84. Section 17, AML/CFT Act: http://bit.ly/2m1YSjC
85. Section 16, AML/CFT Act: http://bit.ly/2HAmByd
86. *Beneficial Ownership Guideline*: http://bit.ly/2Bxp2Pc
87. Section 16(3), AML/CFT Act: http://bit.ly/2HAmByd
88. Section 18(2), AML/CFT Act: http://bit.ly/2gS5b3V
89. Section 21, AML/CFT Act: http://bit.ly/2zDTeu5
90. See "Compliance obligations when conducting international transactions" in section 4 for more discussion of how to assess whether a country is considered high risk.
91. Toogood J confirmed in paragraph 34 of *DIA v Ping An* that a transaction that is either complex or unusually large will trigger the enhanced CDD requirements.
92. Section 23(1)(a) of the AML/CFT Act: http://bit.ly/2iFkDBE
93. Section 24(1)(b) of the AML/CFT Act: http://bit.ly/2zXSvDA
94. Section 26 of the AML/CFT Act: http://bit.ly/2BKjPWO
95. Sections 27–28 of the AML/CFT Act: http://bit.ly/2onXXbh
96. Section 30 of the AML/CFT Act: http://bit.ly/2CcOpcE
97. *Enhanced Customer Due Diligence Guideline*: http://bit.ly/2GrKaHV
98. *Amended Identity Verification Code of Practice* 2013: http://bit.ly/2k13AxJ
99. *Amended Identity Verification Code of Practice 2013*: http://bit.ly/2k13AxJ
100. *Amended Identity Verification Code of Practice 2013*: http://bit.ly/2k13AxJ
101. Section 26(1), AML/CFT Act: http://bit.ly/2BKjPWO
102. Section 22(2), AML/CFT Act: http://bit.ly/2zYaTbY
103. See definition of "politically exposed person" in section 5(1), AML/CFT Act: http://bit.ly/2xHGfmy
104. Section 26(2)(a), AML/CFT Act: http://bit.ly/2A8liTh
105. Section 26(2)(b), AML/CFT Act: http://bit.ly/2A8liTh
106. Enhanced Customer Due Diligence Guideline: http://bit.ly/2GrKaHV
107. Wire Transfers: http://bit.ly/2ERdQBp
108. Sections 27–28, AML/CFT Act: http://bit.ly/2hRYKyV
109. Section 30, AML/CFT Act: http://bit.ly/2gWmRLD
110. Section 22(5), AML/CFT Act: http://bit.ly/2zYaTbY
111. *Amended Identity Verification Code of Practice 2013*: http://bit.ly/2k13AxJ
112. *Identity Verification Code of Practice – Explanatory Note*: http://bit.ly/2k13AxJ
113. Section 32(1), AML/CFT Act: http://bit.ly/2hjDuF3
114. Section 33(1), AML/CFT Act (http://bit.ly/2nQNm8F), and see the supervisors' *Countries Assessment Guideline* (http://bit.ly/2Fc2upe) or the Basel Index (https://index.baselgovernance.org/ranking), which ranks countries by AML/CFT risk.
115. Section 34, AML/CFT Act: http://bit.ly/2HDbWTl
116. Please note that the option of relying on an approved entity provided by section 33(3A) in the AML/CFT Act has not yet been made operational and is not available for use by reporting entities.
117. Please note that neither law firms, conveyancing practices, nor accounting practices in Australia are specifically regulated for AML/CFT purposes.
118. Section 16(3), AML/CFT Act: http://bit.ly/2iTi1Da
119. *Countries Assessment Guideline*: http://bit.ly/2Fc2upe
120. High-risk and other monitored jurisdictions: http://bit.ly/1lTBG24
121. The Transparency International Corruption Perceptions Index for 2016 is available at: http://bit.ly/2j3Y63K The Basel Index, which ranks countries by AML/CFT risk, may also be useful: http://bit.ly/2djRNDR
122. The Council of the European Union has developed a list of non-cooperative jurisdictions for tax purposes: http://bit.ly/2Flrv4A
123. Section 58, AML/CFT Act: http://bit.ly/2ly11Dz
124. Section 37, AML/CFT Act: http://bit.ly/2hydAdM
125. *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorism Financing: High Level Principles and Procedures for Accountants*: http://bit.ly/29OakqM
126. *Money Laundering Using Trust and Company Service Providers*: http://bit.ly/2FJRwHU
127. FIU assessments and reports: http://bit.ly/2xGSiAx
128. AML/CFT news: http://bit.ly/2z7lAd4
129. *Anti-money laundering and countering financing of terrorism*: http://bit.ly/2zbaCoS
130. *Amended Identity Verification Code of Practice 2013*: http://bit.ly/2k13AxJ
131. *Identity Verification Code of Practice – Explanatory Note*: http://bit.ly/2k13AxJ
132. *Phase 2 AML/CFT Sector Risk Assessment* (http://bit.ly/2o155u8) and *AML/CFT Risk Assessment and Programme: Prompts and Notes for DIA Reporting Entities* (http://bit.ly/2EBUMXy).
133. FATF – All publications: http://bit.ly/2Ff66He
134. FATF evaluations of New Zealand: http://bit.ly/2nY08F1
135. Financial Intelligence Unit, (May 2014), *Quarterly Typology Report Third Quarter (Q3) 2013/2014,* FIU, Wellington http://bit.ly/2zijNkM
136. Financial Intelligence Unit, (October 2014), *Quarterly Typology Report First Quarter (Q1) 2014/2015,* FIU, Wellington http://bit.ly/2A2XKC6
137. Financial Intelligence Unit, (May 2014), *Quarterly Typology Report Third Quarter (Q3) 2013/2014,* FIU, Wellington http://bit.ly/2zijNkM
138. Financial Intelligence Unit, (May 2014), *Quarterly Typology Report Third Quarter (Q3) 2013/2014,* FIU, Wellington http://bit.ly/2zijNkM
139. Financial Intelligence Unit, (July 2014), *Quarterly Typology Report Fourth Quarter (Q4) 2013/2014*, FIU, Wellington (The text in the case study uses some updated information.) http://bit.ly/2hZZogQ
140. Financial Intelligence Unit, (January 2015), *Quarterly Typology Report Second Quarter (Q2) 2014/2015,* FIU, Wellington http://bit.ly/2BfP21c